



Configurar e gerenciar

StorageGRID software

NetApp
July 23, 2026

Índice

Configure e gerencie um sistema StorageGRID	1
Administrar StorageGRID	1
Administrar StorageGRID	1
Comece a usar o Grid Manager	1
Controle o acesso ao StorageGRID	28
Use a federação de grid	73
Gerenciar segurança	111
Gerenciar locatários	183
Configurar conexões de cliente	203
Gerenciar redes e conexões	246
Use o AutoSupport	266
Gerenciar nós de armazenamento	281
Gerenciar nós de administração	294
Gerencie objetos com ILM	296
Gerencie objetos com ILM no StorageGRID	296
ILM e ciclo de vida de objetos	297
Crie e atribua níveis de storage no StorageGRID	319
Utilize pools de storage	322
Use Cloud Storage Pools	330
Gerencie perfis de codificação de apagamento no StorageGRID	349
Configure regiões S3 para StorageGRID	353
Criar regra ILM	355
Gerenciar políticas ILM	371
Trabalhe com políticas ILM e regras ILM no StorageGRID	387
Use o Bloqueio de Objeto S3	391
Exemplos de regras e políticas de ILM	399
Reforço do sistema para StorageGRID	421
Saiba mais sobre a proteção do sistema para StorageGRID	421
Diretrizes de reforço para upgrades de software do StorageGRID	421
Diretrizes de reforço para redes StorageGRID	422
Diretrizes de reforço para nós do StorageGRID	423
Diretrizes de reforço para TLS e SSH no StorageGRID	427
Diretrizes de reforço para logs, senhas e mensagens de auditoria no StorageGRID	428
StorageGRID com FabricPool	429
Fluxo de trabalho de configuração para usar StorageGRID com FabricPool	430
Informações necessárias para conectar StorageGRID como uma camada de nuvem FabricPool	431
Use o assistente de instalação do FabricPool	432
Configure StorageGRID manualmente	446
Configure o System Manager do ONTAP para adicionar o StorageGRID como uma camada de nuvem FabricPool	456
Configure as entradas do servidor DNS para StorageGRID com FabricPool	458
Melhores práticas do StorageGRID para FabricPool	459
Remova os dados do FabricPool do StorageGRID	463

Configure e gerencie um sistema StorageGRID

Administrar StorageGRID

Administrar StorageGRID

Utilize estas instruções para configurar e administrar um sistema StorageGRID.

Sobre estas instruções

As principais tarefas para configurar e administrar StorageGRID permitem que você:

- Use o Grid Manager para configurar grupos e usuários
- Crie contas de locatário para permitir que aplicativos cliente S3 armazenem e recuperem objetos
- Configure e gerencie redes StorageGRID
- Configurar AutoSupport
- Gerenciar configurações do nó

Antes de começar

- Você possui um conhecimento geral do sistema StorageGRID.
- Você possui um conhecimento bastante detalhado de shells de comando Linux, rede e configuração e instalação de hardware de servidor.

Comece a usar o Grid Manager

Requisitos do navegador web para StorageGRID

Você precisa usar um navegador web compatível.

Navegador da Web	Versão mínima suportada
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Defina a janela do navegador para uma largura recomendada.

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Faça login no StorageGRID Grid Manager

Você acessa a página de login do Grid Manager inserindo o domínio totalmente qualificado (FQDN) ou o endereço IP de um nó de administração na barra de endereços de um navegador da web compatível.

Cada sistema StorageGRID inclui um nó administrativo primário e qualquer número de nós administrativos não primários. Você pode acessar o Grid Manager em qualquer nó administrativo para gerenciar o sistema StorageGRID. No entanto, alguns procedimentos de manutenção só podem ser realizados a partir do nó administrativo primário.

Conecte-se ao grupo HA

Se os nós de administração estiverem incluídos em um grupo de alta disponibilidade (HA), você se conecta usando o endereço IP virtual do grupo HA ou um domínio totalmente qualificado que mapeia para o endereço IP virtual. O nó de administração primário deve ser selecionado como a interface primária do grupo, para que, ao acessar o Grid Manager, você o acesse no nó de administração primário, a menos que o nó de administração primário não esteja disponível. Consulte ["Gerenciar grupos de alta disponibilidade"](#).

Use o SSO

Os passos para iniciar sessão são ligeiramente diferentes se ["O single sign-on \(SSO\) foi configurado"](#).

Faça login no Grid Manager no primeiro nó de administração

Antes de começar

- Você já possui suas credenciais de login.
- Você está usando um ["navegador web compatível"](#).
- Os cookies estão ativados no seu navegador.
- Você pertence a um grupo de usuários que possui pelo menos uma permissão.
- Você tem a URL do Grid Manager:

```
https://FQDN_or_Admin_Node_IP/
```

Você pode usar o domínio totalmente qualificado, o endereço IP de um nó de administração ou o endereço IP virtual de um grupo de HA de nós de administração.

Para acessar o Gerenciador de Grade em uma porta diferente da porta padrão para HTTPS (443), inclua o número da porta na URL:

```
https://FQDN_or_Admin_Node_IP:port/
```



O SSO não está disponível na porta restrita do Grid Manager. Você deve usar a porta 443.

Passos

1. Inicie um navegador web compatível.
2. Na barra de endereços do navegador, digite a URL do Grid Manager.
3. Se você receber um alerta de segurança, instale o certificado usando o assistente de instalação do navegador. Veja ["Gerenciar certificados de segurança"](#).

4. Faça login no Grid Manager.

A tela de login que aparece depende se o single sign-on (SSO) foi configurado para StorageGRID.

Não usar SSO

- a. Insira seu nome de usuário e senha para o Grid Manager.
- b. Selecione **Entrar**.

Utilizando SSO

- Se StorageGRID estiver usando SSO e esta for a primeira vez que você acessa a URL neste navegador:
 - i. Selecione **Entrar**. Você pode deixar o 0 no campo Conta.
 - ii. Insira suas credenciais padrão de SSO na página de SSO da sua organização.

Por exemplo, se StorageGRID estiver usando SSO e você já tiver acessado o Grid Manager ou uma conta de tenant:

- A. Digite **0** (o ID da conta do Grid Manager) ou selecione **Grid Manager** se ele aparecer na lista de contas recentes.
- B. Selecione **Sign in**.
- C. Faça login com suas credenciais SSO padrão na página de login SSO da sua organização.

Ao iniciar sessão, a página inicial do Grid Manager é exibida, incluindo o dashboard. Para saber quais informações são fornecidas, consulte "[Visualize e gerencie o painel de controle](#)".

Faça login em outro nó de administração

Siga estas etapas para entrar em outro nó de administração.

Não usar SSO

Passos

1. Na barra de endereços do navegador, digite o domínio totalmente qualificado ou o endereço IP do outro nó de administração. Inclua o número da porta, se necessário.
2. Insira seu nome de usuário e senha para o Grid Manager.
3. Selecione **Entrar**.

Utilizando SSO

Se StorageGRID estiver usando SSO e você já tiver feito login em um nó de administração, você pode acessar outros nós de administração sem precisar fazer login novamente.

Passos

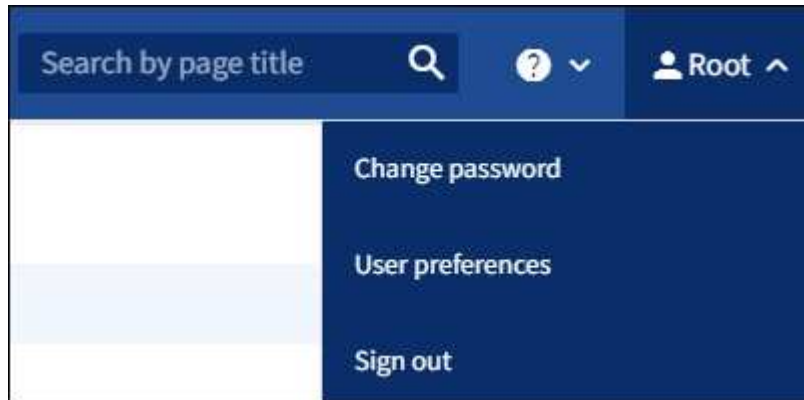
1. Digite o domínio totalmente qualificado ou endereço IP do outro nó de administração na barra de endereços do navegador.
2. Se a sua sessão SSO expirou, insira suas credenciais novamente.

Saia do StorageGRID Grid Manager

Ao terminar de usar o Grid Manager, você deve sair para garantir que usuários não autorizados não acessem o sistema StorageGRID. Fechar o navegador pode não encerrar sua sessão no sistema, dependendo das configurações de cookies do navegador.

Passos

1. Selecione seu nome de usuário no canto superior direito.



2. Selecione **Sair**.

Opção	Descrição
SSO não está em uso	Você foi desconectado do nó de administração. A página de login do Grid Manager é exibida. Nota: Se você fez login em mais de um nó de administração, você deve sair de cada um deles.
SSO ativado	Você foi desconectado de todos os Admin Nodes que estava acessando. A página de login do StorageGRID é exibida. Grid Manager está listado como padrão na lista suspensa Contas Recentes, e o campo Account ID mostra 0. Nota: Se o SSO estiver ativado e você também estiver conectado ao Gerenciador de Locatários, você também deve "sair da conta do tenant" para "sair do SSO".

Altere sua senha do StorageGRID Grid Manager

Se você for um usuário local do Grid Manager, poderá alterar sua própria senha.

Antes de começar

Você está conectado ao Gerenciador de Grade usando um "[navegador web compatível](#)".

Sobre esta tarefa

Se você fizer login no StorageGRID como um usuário federado ou se o logon único (SSO) estiver habilitado,

não poderá alterar sua senha no Grid Manager. Em vez disso, você deve alterar sua senha na fonte de identidade externa, por exemplo, Active Directory ou OpenLDAP.

Passos

1. No cabeçalho do Grid Manager, selecione **seu nome** > **Alterar senha**.
2. Digite sua senha atual.
3. Digite uma nova senha.

Sua senha deve conter no mínimo 8 e no máximo 32 caracteres. As senhas diferenciam maiúsculas de minúsculas.

4. Digite novamente a nova senha.
5. Selecione **Salvar**.

Veja as informações da licença do StorageGRID

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

Antes de começar

Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).

Sobre esta tarefa

Se houver algum problema com a licença de software deste sistema StorageGRID, o cartão de status de integridade no painel inclui um ícone de status da licença e um link **Licença**. O número indica o número de problemas relacionados à licença.



Passos

1. Acesse a página de Licença realizando um dos seguintes procedimentos:
 - Selecione **Manutenção** > **Sistema** > **Licença**.
 - No cartão de status de saúde no painel de controle, selecione o ícone de status da licença ou o link **Licença**.

Este link só aparece se houver algum problema com a licença.

2. Veja os detalhes somente leitura da licença atual:

- ID do sistema StorageGRID, que é o número de identificação exclusivo desta instalação do StorageGRID
- Número de série da licença
- Tipo de licença, **Perpétua** ou **Assinatura**
- Capacidade de storage licenciada da grid
- Capacidade de storage suportada
- Data de término da licença. **N/A** indica uma licença perpétua.
- Data de término do suporte

Esta data é lida do arquivo de licença atual e pode estar desatualizada se você tiver estendido ou renovado o contrato de serviço de suporte após obter o arquivo de licença. Para atualizar este valor, consulte "[Atualizar informações de licença do StorageGRID](#)". Você também pode visualizar a data real de término do contrato usando Active IQ.

- Conteúdo do arquivo de texto da licença

Atualizar informações de licença do StorageGRID

Você deve atualizar as informações de licença do seu sistema StorageGRID sempre que os termos da sua licença forem alterados. Por exemplo, você deve atualizar as informações de licença se adquirir capacidade de storage adicional para seu grid.

Antes de começar

- Você tem um novo arquivo de licença para aplicar ao seu sistema StorageGRID.
- Você tem "[permissões de acesso específicas](#)".
- Você possui a senha de provisionamento.

Passos

1. Selecione **Manutenção > Sistema > Licença**.
2. Na seção Atualizar licença, selecione **Procurar**.
3. Localize e selecione o novo arquivo de licença (.txt).

O novo arquivo de licença é validado e exibido.

4. Digite a senha de provisionamento.
5. Selecione **Salvar**.

Use o API

Use a API de gerenciamento de grid do StorageGRID

Você pode executar tarefas de gerenciamento do sistema usando a API REST de gerenciamento do Grid 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 alto nível

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

- `/grid`: O acesso é restrito aos usuários do Grid Manager e baseia-se nas permissões de grupo configuradas.
- `/org`: O acesso é restrito a usuários que pertencem a um grupo LDAP local ou federado para uma conta de locatário. Para obter detalhes, consulte ["Use uma conta de tenant"](#).
- `/private`: O acesso é restrito a 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 Grid utiliza 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 de usuário Swagger fornece detalhes completos e documentação para cada operação da API.

Antes de começar

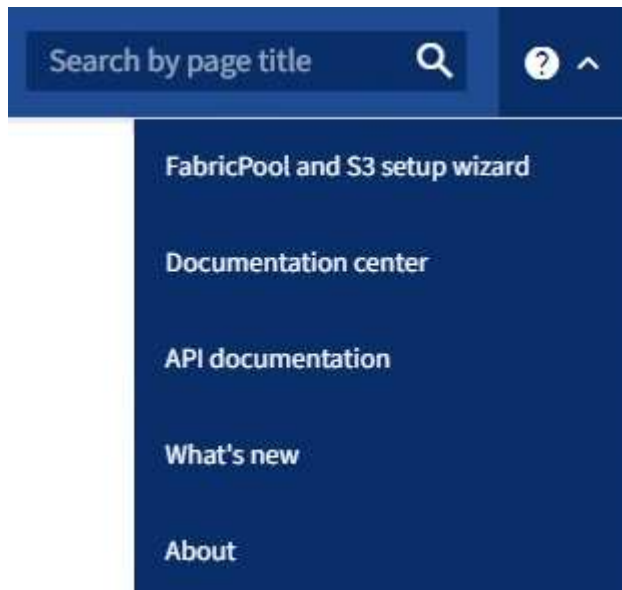
- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).



Qualquer operação de API realizada por meio da página de documentação da API é uma operação em tempo real. 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 **API documentation**.



2. Para executar uma operação com a API privada, selecione **Acessar 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 da API, você pode visualizar 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 parâmetros obrigatórios 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 25
marker string (query)	marker-style pagination offset (value is Group's URN) marker - marker-style pagination offset (value
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 <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers", </pre>

5. Determine se a solicitação requer parâmetros adicionais, como um ID de grupo ou de usuário. Em

seguida, obtenha esses valores. Pode ser necessário fazer uma solicitação de API diferente primeiro para obter as informações de que você precisa.

6. Determine se você precisa modificar o corpo da solicitação de exemplo. Caso precise, selecione **Model** para conhecer os requisitos de cada campo.
7. Selecione **Experimentar**.
8. Forneça todos os parâmetros necessários ou modifique o corpo da solicitação conforme necessário.
9. Selecione **Executar**.
10. Analise o código de resposta para determinar se a solicitação foi bem-sucedida.

Operações da API de gerenciamento de grid no StorageGRID

A API de Gerenciamento de Grid organiza as operações disponíveis nas seguintes seções.



Esta lista inclui apenas as operações disponíveis na API pública.

- **contas**: Operações para gerenciar contas de locatários de armazenamento, incluindo criar novas contas e recuperar o uso de armazenamento para uma determinada conta.
- **histórico de alertas**: operações em alertas resolvidos.
- **receptores de alertas**: Operações em receptores de notificações de alerta (email).
- **alert-rules**: Operações em regras de alerta.
- **alert-silences**: Operações em silêncios de alerta.
- **alertas**: Operações em alertas.
- **auditoria**: Operações para listar e atualizar a configuração de auditoria.
- **auth**: Operações para realizar autenticação de sessão do usuário.

A API de gerenciamento de grid suporta o esquema de autenticação Bearer Token. Para fazer login, você fornece um nome de usuário e uma senha no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com sucesso, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho das solicitações de API subsequentes ("Authorization: Bearer *token*"). O token expira após 16 horas.



Se o single sign-on estiver habilitado para o StorageGRID, você deve executar etapas diferentes para autenticar. Consulte "Autenticando na API se o single sign-on estiver habilitado".

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

- **client-certificates**: Operações para configurar certificados de cliente para que StorageGRID possa ser acessado com segurança usando ferramentas de monitoramento externas.
- **config**: Operações relacionadas ao lançamento do produto e às versões da API de Gerenciamento de Grid. Você pode listar a versão de lançamento do produto e as principais versões da API de Gerenciamento de Grid suportadas por esse lançamento, além de desativar versões obsoletas da API.
- **recursos-desativados**: operações para visualizar recursos que podem ter sido desativados.
- **servidores-dns**: Operações para listar e alterar servidores DNS externos configurados.

- **drive-details**: Operações em unidades para modelos específicos de dispositivos de storage.
- **endpoint-domain-names**: Operações para listar e alterar nomes de domínio de endpoint do S3.
- **erasure-coding**: Operações em perfis de codificação de apagamento.
- **expansão**: operações de expansão (nível de procedimento).
- **expansion-nodes**: Operações em expansão (nível de nó).
- **locais de expansão**: Operações em expansão (nível do local).
- **grid-networks**: Operações para listar e alterar a Lista de Redes da Grid.
- **grid-passwords**: operações para gerenciamento de senhas em grid.
- **grupos**: Operações para gerenciar grupos de administradores de Grid locais e para recuperar grupos de administradores de Grid federados de um servidor LDAP externo.
- **identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo e usuário federados.
- **ilm**: Operações de gerenciamento do ciclo de vida das informações (ILM).
- **procedimentos-em-andamento**: Recupera os procedimentos de manutenção que estão atualmente em andamento.
- **licença**: Operações para recuperar e atualizar a licença do StorageGRID.
- **logs**: Operações para coletar e baixar arquivos de log.v
- **metrics**: Operações em métricas do StorageGRID, incluindo consultas instantâneas de métricas em um ponto único no tempo e consultas de métricas de intervalo ao longo de um período de tempo. A Grid Management API utiliza a ferramenta de monitoramento de sistemas Prometheus como fonte de dados de backend. Para obter informações sobre como construir consultas Prometheus, consulte o site do Prometheus.



As métricas que incluem *private* em seus nomes destinam-se apenas ao uso interno. Essas métricas estão sujeitas a alterações entre versões do StorageGRID sem aviso prévio.

- **node-details**: Operações nos detalhes do nó.
- **node-health**: Operações sobre o status de integridade do nó.
- **node-storage-state**: Operações no status de armazenamento do nó.
- **ntp-servers**: Operações para listar ou atualizar servidores externos do Protocolo de Tempo de Rede (NTP).
- **objetos**: Operações em objetos e metadados de objetos.
- **recuperação**: Operações para o procedimento de recuperação.
- **pacote de recuperação**: operações para baixar o pacote de recuperação.
- **regiões**: Operações para visualizar e criar regiões.
- **s3-object-lock**: Operações nas configurações globais de S3 Object Lock.
- **server-certificate**: Operações para visualizar e atualizar os certificados do servidor Grid Manager.
- **snmp**: Operações na configuração SNMP atual.
- **storage-watermarks**: Marcas d'água de nós de storage.
- **classes-de-tráfego**: Operações para políticas de classificação de tráfego.

- **rede-cliente-não-confiável**: Operações na configuração da rede de cliente não confiável.
- **usuários**: Operações para visualizar e gerenciar usuários do Grid Manager.

Controle de versão da Grid Management API no StorageGRID

A API de gerenciamento de grid utiliza versionamento para suportar atualizações não disruptivas.

Por exemplo, esta URL de solicitação especifica a versão 4 da API.

`https://hostname_or_ip_address/api/v4/authorize`

A versão principal da API é atualizada quando são feitas alterações que *não são compatíveis* com versões anteriores. A versão secundária da API é atualizada quando são feitas alterações que *são compatíveis* com versões anteriores. Alterações compatíveis incluem a adição de novos endpoints ou novas propriedades.

O exemplo a seguir ilustra como a versão da API é atualizada com base no tipo de alterações realizadas.

Tipo de alteração na API	Versão antiga	Nova versão
Compatível com versões anteriores	2,1	2,2
Não é compatível com versões antigas	2,1	3,0

Ao instalar o software StorageGRID pela primeira vez, apenas a versão mais recente da API é habilitada. No entanto, ao atualizar para uma nova versão de recursos do StorageGRID, você continua tendo acesso à versão anterior da API por pelo menos uma versão de recursos do StorageGRID.



Você pode configurar as versões suportadas. Consulte a seção **config** da documentação da API Swagger para o "[API de gerenciamento de grid](#)" para mais informações. Você deve desativar o suporte para a versão antiga após atualizar todos os clientes da API para usar a versão mais recente.

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho da resposta é "Deprecated: true"
- O corpo da resposta JSON inclui "deprecated": true
- Um aviso de descontinuação é adicionado ao nms.log. Por exemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determine quais versões da API são compatíveis na versão atual

Use a solicitação GET `/versions` à API para retornar uma lista das versões principais da API suportadas. Essa solicitação está localizada na seção **config** da documentação da API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Especifique uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (/api/v4) ou um cabeçalho (Api-Version: 4). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Proteja contra ataques de falsificação de solicitação entre sites (CSRF) no StorageGRID

Você pode ajudar a proteger contra ataques de Cross-Site Request Forgery (CSRF) ao StorageGRID usando tokens CSRF para aprimorar a autenticação que utiliza cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes da API podem escolher se desejam habilitá-lo ao fazer login.

Um atacante capaz de enviar uma solicitação para um site diferente (como por meio de um formulário HTTP POST) pode fazer com que determinadas solicitações sejam realizadas usando os cookies do usuário autenticado.

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 no corpo de uma POST.

Para ativar o recurso, defina o `csrfToken`parâmetro` como ``true` durante a autenticação. O padrão 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 cookie `GridCsrfToken` é definido com um valor aleatório para autenticações no Grid Manager, e o cookie `AccountCsrfToken` é definido com um valor aleatório para autenticações no Tenant Manager.

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

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

Consulte a documentação da API online para obter exemplos e detalhes adicionais.



As solicitações que possuem um cookie de token CSRF definido também imporão o cabeçalho `"Content-Type: application/json"` para qualquer solicitação que espere um corpo de solicitação JSON como proteção adicional contra ataques CSRF.

Use a API se o single sign-on estiver ativado

Use a API do StorageGRID se o login único estiver habilitado (Active Directory)

Se você tem ["configurou e ativou o single sign-on \(SSO\)"](#) e utiliza o Active Directory como provedor de SSO, é necessário emitir uma série de solicitações de API para obter um token de autenticação válido para a Grid Management API ou a Tenant Management API.

Faça login na API se o single sign-on estiver ativado

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

Antes de começar

- Você conhece o nome de usuário e a senha do SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você deseja acessar a API de Gerenciamento de Tenant, você sabe o ID da conta do tenant.

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 de arquivos de instalação do StorageGRID (`./rpms` para RHEL, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).

- Um exemplo de fluxo de trabalho com requisições curl.

O fluxo de trabalho curl pode expirar se você o executar muito lentamente. Você poderá 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 seguinte erro: Unsupported SAML version.

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
 - Use o `storagegrid-ssoauth.py` script Python. Vá para o passo 2.
 - Use requisições curl. Vá 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. Digite ADFS ou adfs.
- O nome de usuário SSO
- O domínio onde StorageGRID está instalado
- O endereço do StorageGRID
- O ID da conta do locatário, caso você queira acessar a Tenant Management API.

```
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 do StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.

3. Se você deseja usar solicitações curl, use o procedimento a seguir.
 - a. Declare as variáveis necessárias para efetuar o login.


```
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 Grid, use 0 como TENANTACCOUNTID.

- b. Para receber uma URL de autenticação assinada, envie 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 uma URL assinada que está codificada em 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 uma URL completa que inclua o ID da solicitação do cliente do AD FS.

Uma opção é solicitar o formulário de login usando a 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 da solicitação do cliente:

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

e. Salve o ID da solicitação do cliente a partir da resposta.

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

f. Envie suas credenciais para a ação do 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 habilitada para o seu sistema SSO, o formulário enviado 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=fZHRTOMwFIZfhh...UJikvo77sXPw%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='AAEADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

- h. Envie uma solicitação GET para o local especificado com os cookies da autenticação POST.

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

Os cabeçalhos da resposta conterão informações da sessão do AD FS para uso posterior no logout, e o corpo da resposta conterá 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
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThtMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

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

- i. Salve o SAMLResponse do campo oculto:

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

- j. Utilizando o valor salvo SAMLResponse, faça uma solicitação StorageGRID/api/saml-response

para gerar um token de autenticação do StorageGRID.

Para RelayState, use o ID da conta do tenant ou use 0 se você quiser fazer login na Grid Management API.

```
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, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.

Saia da API se o single sign-on estiver ativado

Se o login único (SSO) estiver habilitado, você deve emitir uma série de solicitações de API para sair da Grid Management API ou da Tenant Management API. Essas instruções se aplicam se você estiver usando Active Directory como provedor de identidade SSO

Sobre esta tarefa

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

Passos

1. Para gerar uma solicitação de logout assinada, passe o 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
```

Uma URL de logout é retornada:

```
{
  "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 a 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 StorageGRID.

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

A resposta 302 é retornada. O local de redirecionamento não se aplica ao logout somente via API.

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

4. Exclua o token de portador do StorageGRID.

Excluir o token de portador do StorageGRID funciona da mesma forma que sem SSO. Se o cookie `sso=true` não for fornecido, o usuário será desconectado do StorageGRID sem afetar o estado do 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 agora está desconectado.

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

Use a API do StorageGRID se o single sign-on estiver ativado (Entra ID)

Se você possui "[configurou e ativou o single sign-on \(SSO\)](#)" e utiliza o Entra ID como provedor de SSO, pode usar dois scripts de exemplo para obter um token de autenticação válido para a Grid Management API ou para a Tenant Management API.

Faça login na API se o single sign-on do Entra ID estiver ativado

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

Antes de começar

- Você conhece o endereço de e-mail e a senha de SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você deseja acessar a API de Gerenciamento de Tenant, você sabe o ID da conta do tenant.

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 de arquivos de instalação do StorageGRID (`./rpms` para RHEL, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).

Para criar sua própria integração de API com o Entra ID, consulte o `storagegrid-ssoauth-azure.py` script. O script em Python faz duas requisições diretamente ao StorageGRID (primeiro para obter o SAMLRequest e, posteriormente, para obter o token de autorização) e também chama o script em Node.js para interagir com o Entra ID e realizar as operações de SSO.

As operações de SSO podem ser executadas usando uma série de solicitações de API, mas isso não é trivial. O módulo Puppeteer para Node.js é usado para extrair dados da interface Entra ID SSO.

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

Passos

1. Instale as dependências necessárias, conforme a seguir:
 - a. Instale o Node.js (consulte "<https://nodejs.org/en/download/>").

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 então chamará o script Node.js correspondente para executar as interações de SSO do Entra ID.

3. Quando solicitado, insira os valores para os seguintes argumentos (ou passe-os usando parâmetros):

- O endereço de e-mail SSO usado para fazer login no Entra ID
- O endereço do StorageGRID
- O ID da conta do locatário, caso você queira acessar a API de gerenciamento de locatários

4. Quando solicitado, insira a senha e esteja preparado para fornecer uma autorização MFA ao Entra ID, caso seja 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 pressupõe que a autenticação multifator (MFA) seja feita usando o Microsoft Authenticator. Pode ser necessário modificar o script para suportar outras formas de MFA (como inserir um código recebido por mensagem de texto).

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

Use a API do StorageGRID se o login único estiver ativado (PingFederate)

Se você tem "[configurou e ativou o single sign-on \(SSO\)](#)" e utiliza PingFederate como provedor de SSO, é necessário emitir uma série de solicitações de API para obter um token de autenticação válido para a Grid Management API ou a Tenant Management API.

Faça login na API se o single sign-on estiver ativado

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

Antes de começar

- Você conhece o nome de usuário e a senha do SSO de um usuário federado que pertence a um grupo de usuários do StorageGRID.
- Se você deseja acessar a API de Gerenciamento de Tenant, você sabe o ID da conta do tenant.

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 de arquivos de instalação do StorageGRID (`./rpms` para RHEL, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).
- Um exemplo de fluxo de trabalho com requisições curl.

O fluxo de trabalho curl pode expirar se você o executar muito lentamente. Você poderá 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 seguinte erro: `Unsupported SAML version.`

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
 - Use o `storagegrid-ssoauth.py` script Python. Vá para o passo 2.
 - Use requisições curl. Vá 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 StorageGRID está instalado. Este campo não é utilizado para PingFederate. Você pode deixá-lo em branco ou inserir qualquer valor.
- O endereço do StorageGRID
- O ID da conta do locatário, caso você queira acessar a Tenant Management API.

```
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 do StorageGRID é fornecido na saída. Agora você pode usar o token para outras solicitações, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.

3. Se você deseja usar solicitações curl, use o procedimento a seguir.
 - a. Declare as variáveis necessárias para efetuar o login.


```
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 Grid, use 0 como TENANTACCOUNTID.

- b. Para receber uma URL de autenticação assinada, envie 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 uma URL assinada que está codificada em 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 exiba 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 exiba a resposta:

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

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

f. Exporte o valor 'href' (remova a barra final /) e exiba a resposta:

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

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

g. Exporte o valor de "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. Utilizando o valor salvo SAMLResponse, faça uma solicitação StorageGRID/api/saml-response para gerar um token de autenticação do StorageGRID.

Para RelayState, use o ID da conta do tenant ou use 0 se você quiser fazer login na Grid Management API.

```
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, de forma semelhante a como usaria a API se o SSO não estivesse sendo utilizado.

Saia da API se o single sign-on estiver ativado

Se o login único (SSO) estiver habilitado, você deve emitir uma série de solicitações de API para sair da API de Gerenciamento de Grid ou da API de Gerenciamento de Locatários. Essas instruções se aplicam se você estiver usando PingFederate como provedor de identidade SSO

Sobre esta tarefa

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

Passos

1. Para gerar uma solicitação de logout assinada, passe o 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
```

Uma URL de logout é retornada:

```
{
  "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 a 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 StorageGRID.

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

A resposta 302 é retornada. O local de redirecionamento não se aplica ao logout somente via 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 de portador do StorageGRID.

Excluir o token de portador do StorageGRID funciona da mesma forma que sem SSO. Se o cookie `sso=true` não for fornecido, o usuário será desconectado do StorageGRID sem afetar o estado do 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 agora está desconectado.

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

Desative os recursos do StorageGRID com a API

Você pode usar a API de Gerenciamento de Grid 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 Recursos Desativados permite impedir o acesso a determinados recursos no sistema StorageGRID. Desativar um recurso é a única maneira de impedir que o usuário raiz ou usuários pertencentes a grupos de administradores com permissão de **acesso à raiz** possam usar esse recurso.

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

A Company A é uma prestadora de serviços que aluga a capacidade de storage do seu sistema StorageGRID criando contas de locatário. Para proteger a segurança dos objetos dos seus locatários, a Company A deseja garantir que seus próprios funcionários nunca possam acessar nenhuma conta de locatário após a implantação da conta.

A Company A pode atingir esse objetivo usando o sistema Deactivate Features na Grid Management API. Ao desativar completamente o recurso **Change tenant root password** no Grid Manager (tanto na interface de usuário quanto na API), a Company A garante que usuários Admin — incluindo o usuário raiz e usuários pertencentes a grupos com a permissão **Root access** — não possam alterar a senha do usuário raiz de nenhuma conta de tenant.

Passos

1. Acesse a documentação Swagger para a API de Gerenciamento de Grid. Veja ["Use a API de gerenciamento de grid"](#).
2. Localize o endpoint Desativar recursos.
3. Para desativar um recurso, como Alterar a senha raiz do locatário, envie um corpo para a API assim:

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

Quando a solicitação for concluída, o recurso Alterar senha raiz do locatário será desativado. A permissão de gerenciamento **Alterar senha raiz do locatário** não aparece mais na interface de usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário falha com "403 Forbidden".

Reativar funcionalidades desativadas

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



O recurso **activateFeatures** não pode ser reativado. Se você decidir desativar este recurso, esteja ciente de que 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 Swagger para a API de gerenciamento de Grid.
2. Localize o endpoint Desativar recursos.
3. Para reativar todas as funcionalidades, envie um corpo para a API da seguinte forma:

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

Quando esta solicitação for concluída, todos os recursos, incluindo o recurso Alterar senha raiz do locatário, serão reativados. A permissão de gerenciamento **Alterar senha raiz do locatário** agora aparece na interface de usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário será bem-sucedida, assumindo que o usuário tenha a permissão de gerenciamento **Acesso à raiz** ou **Alterar senha raiz do locatário**.



O exemplo anterior faz com que *todos* os recursos desativados sejam reativados. Se outros recursos foram desativados e devem permanecer desativados, você deve especificá-los explicitamente na solicitação PUT. Por exemplo, para reativar o recurso Alterar senha raiz do locatário e continuar a desativar a permissão de gerenciamento storageAdmin, envie esta solicitação PUT:

```
{ "grid": {"storageAdmin": true} }
```

Controle o acesso ao StorageGRID

Controlar o acesso ao StorageGRID

Você controla quem pode acessar StorageGRID e quais tarefas os usuários podem executar, criando ou importando grupos e usuários e atribuindo permissões a cada grupo. Opcionalmente, você pode habilitar o logon único (SSO), criar certificados de cliente e alterar as senhas do grid.

Controle o acesso ao Grid Manager

Você determina quem pode acessar o Gerenciador de Grid e a API de Gerenciamento de Grid importando grupos e usuários de um serviço de federação de identidades ou configurando grupos e usuários locais.

Usar "[federação de identidade](#)" torna a configuração de "[grupos](#)" e "[usuários](#)" mais rápida e permite que os usuários façam login no StorageGRID usando credenciais já conhecidas. Você pode configurar a federação de identidades se usar Active Directory, OpenLDAP ou Oracle Directory Server.



Contate o suporte técnico se você quiser usar outro serviço LDAP v3.

Você determina quais tarefas cada usuário pode executar atribuindo diferentes "[permissões](#)" a cada grupo. Por exemplo, você pode querer que os usuários de um grupo possam gerenciar regras de ILM e os usuários de outro grupo possam executar tarefas de manutenção. Um usuário deve pertencer a pelo menos um grupo para acessar o sistema.

Opcionalmente, você pode configurar um grupo como somente leitura. Usuários em um grupo somente leitura podem apenas visualizar configurações e recursos. Eles não podem fazer alterações nem executar operações no Grid Manager ou na Grid Management API.

Ativar single sign-on

O sistema StorageGRID suporta autenticação única (SSO) usando o padrão Security Assertion Markup Language 2.0 (SAML 2.0). Após você "[configurar e habilitar SSO](#)", todos os usuários devem ser autenticados por um provedor de identidade externo antes de poderem acessar o Grid Manager, o Tenant Manager, a API de gerenciamento do Grid ou a API de gerenciamento do Tenant. Usuários locais não podem fazer login no StorageGRID.

Alterar senha de provisionamento

A senha de provisionamento é necessária para muitos procedimentos de instalação e manutenção, e para baixar o pacote de recuperação do StorageGRID. A senha também é necessária para baixar backups das informações de topologia da grade e das chaves de criptografia do sistema StorageGRID. Você pode ["alterar a frase secreta"](#) conforme necessário.

Alterar senhas do console do nó

Cada nó em sua grade possui uma senha de console do nó, que você precisa para fazer login no nó como "admin" usando SSH ou como usuário raiz em uma conexão de console física/VM. Conforme necessário, você pode ["alterar a senha do console do nó"](#) para cada nó.

Alterar a senha de provisionamento do StorageGRID

Use este procedimento para alterar a senha de provisionamento do StorageGRID. A senha é necessária para procedimentos de recuperação, expansão e manutenção. A senha também é necessária para baixar backups do pacote de recuperação que incluem as informações de topologia da grade, as senhas do console do nó da grade e as chaves de criptografia do sistema StorageGRID.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você possui permissões de acesso de manutenção ou root.
- Você possui a senha de provisionamento atual.

Sobre esta tarefa

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

Passos

1. Selecione **Configuração > Controle de acesso > Senhas da grade**.
2. Em **Alterar senha de provisionamento**, selecione **Fazer uma alteração**
3. Digite sua senha de provisionamento atual.
4. Digite a nova senha. A senha deve conter no mínimo 8 e no máximo 32 caracteres. Senhas diferenciam maiúsculas de minúsculas.



Guarde a senha de provisionamento em um local seguro. Ela é necessária para os procedimentos de instalação, expansão e manutenção.

5. Digite novamente a nova senha e selecione **Salvar**.

O sistema exibe uma faixa verde de sucesso quando a alteração da senha de provisionamento é concluída.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

6. Selecione **Recovery Package**.

7. Insira a nova senha de provisionamento para baixar o novo pacote de recuperação.



Após alterar a senha de provisionamento, você deve baixar imediatamente um novo pacote de recuperação. O arquivo do pacote de recuperação permite restaurar o sistema em caso de falha.

Alterar senhas do console do nó em StorageGRID

Cada nó em sua grade possui uma senha de console do nó, que você usa para fazer login no nó. Por padrão, cada nó tem uma senha única. Você pode alterar cada senha para uma nova senha única ou pode alterar a senha de todos os nós para usar uma senha global. As senhas são armazenadas no pacote de recuperação.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso de manutenção ou root"](#).
- Você possui a senha de provisionamento atual.

Sobre esta tarefa

Você usa a senha do console do nó para fazer login em um nó como "admin" usando SSH ou como usuário raiz em uma conexão de console de VM/física. Você pode alterar as senhas do console do nó usando uma destas opções:

- Aplicar automaticamente senhas aleatórias a cada nó
- Especifique e aplique uma senha global a todos os nós
- Especifique e aplique uma senha exclusiva a um ou mais nós

As senhas são armazenadas em um arquivo `Passwords.txt` atualizado no pacote de recuperação. As senhas estão listadas na coluna "Senha" no arquivo.



O ["Senhas de acesso SSH"](#) das chaves SSH usadas para comunicação entre os nós é separado das senhas do console do nó. Este procedimento não altera as senhas de acesso SSH.

Acesse o assistente

Passos

1. Selecione **Configuração > Controle de acesso > Senhas da grid**.
2. Em **Alterar senhas do console do nó**, selecione **Fazer uma alteração**.

Baixe o pacote de recuperação atual

Antes de alterar as senhas do console do nó, baixe o pacote de recuperação atual. Você pode usar as senhas contidas neste arquivo caso o processo de alteração de senha falhe em qualquer nó.

Passos

1. Insira a senha de provisionamento para seu grid.
2. Selecione **Baixar pacote de recuperação**.

3. Copie o arquivo do pacote de recuperação (.zip para dois locais seguros, protegidos 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.

4. Selecione **Continue**.

Forneça novas senhas

1. Selecione o método de alteração de senha que você deseja usar.
 - **Automático**: StorageGRID atribui automaticamente uma nova senha de console aleatória a todos os nós.
 - **Personalizado**: Você fornece as senhas do console.

Automático

1. Selecione **Continue**.

Personalizado

1. Selecione uma das seguintes opções:
 - **Senha global do console**: aplique a mesma senha do console a todos os nós.
 - **Senhas de console exclusivas**: aplique uma senha diferente em um ou mais nós.
2. Se você selecionou **Senha do console global**, insira a senha que você deseja usar para todos os nós.
3. Se você selecionou **Senhas exclusivas do console**, insira uma senha exclusiva para um ou mais nós.
4. Selecione **Continue**.

Conclua a alteração de senha

1. Quando a caixa de diálogo de confirmação aparecer, selecione **Sim** se você estiver pronto para que StorageGRID comece a alterar as senhas do console do nó.



Não é possível cancelar esse processo depois que ele for iniciado.

StorageGRID gera um novo pacote de recuperação contendo a nova senha.

2. Quando o novo pacote de recuperação estiver pronto, selecione **Baixar novo pacote de recuperação** e salve o pacote de recuperação.
3. Abra o arquivo .zip.
4. Confirme se você tem acesso ao conteúdo, incluindo o Passwords.txt arquivo, que contém as novas senhas do console do nó.
5. Copie o novo arquivo do pacote de recuperação (.zip para dois locais seguros, protegidos e separados.



Não sobrescreva o pacote de recuperação antigo.

Você deve proteger o arquivo de recuperação, pois ele contém chaves de criptografia e senhas que

podem ser usadas para obter dados do sistema StorageGRID.

6. Selecione a caixa de seleção para indicar que você baixou o novo pacote de recuperação e verificou o conteúdo.
7. Selecione **Continue**.

StorageGRID atualiza a senha de cada nó.

Se ocorrer um erro durante o processo de atualização, a barra de progresso exibirá o número de nós que não tiveram suas senhas alteradas. O sistema tentará novamente o processo automaticamente em qualquer nó que não teve sua senha alterada. Se o processo terminar com alguns nós ainda sem a senha alterada, o botão **Retry** será exibido.

8. Se a atualização da senha falhar em um ou mais nós:
 - a. Analise as mensagens de erro listadas na tabela.
 - b. Resolva os problemas.
 - c. Selecione **Tentar novamente**.



A nova tentativa altera apenas as senhas do console dos nós que falharam durante as tentativas anteriores de alteração de senha.

9. Quando a barra de progresso indicar que não há mais atualizações restantes, selecione **Concluir**.
10. Após alterar as senhas do console de todos os nós, exclua o [primeiro pacote de recuperação que você baixou](#).

Alterar as senhas de acesso SSH para os nós de administração do StorageGRID

Alterar as senhas de acesso SSH para os Nós de Administração também atualiza os conjuntos exclusivos de chaves SSH internas para cada nó na grade. O Nó de Administração principal usa essas chaves SSH para acessar os nós usando autenticação segura sem senha.

Utilize uma chave SSH para fazer login em um nó como `admin` ou como usuário raiz em uma máquina virtual ou conexão de console físico.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso de manutenção ou root"](#).
- Você possui a senha de provisionamento atual.

Sobre esta tarefa

As novas senhas de acesso para os Nós de Administração e as novas chaves internas para cada nó estão armazenadas no `Passwords.txt` arquivo no pacote de recuperação. As chaves estão listadas na coluna Senha desse arquivo.

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

Acesse o assistente

Passos

1. Selecione **Configuração > Controle de acesso > Senhas da grid.**
2. Em **Alterar chaves SSH**, selecione **Fazer uma alteração.**

Baixe o pacote de recuperação atual

Antes de alterar as chaves de acesso SSH, baixe o pacote de recuperação atual. Você pode usar as chaves neste arquivo caso o processo de alteração de chaves falhe em qualquer nó.

Passos

1. Insira a senha de provisionamento para seu grid.
2. Selecione **Baixar pacote de recuperação.**
3. Copie o arquivo do pacote de recuperação (.zip para dois locais seguros, protegidos 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.

4. Selecione **Continue.**
5. Quando a caixa de diálogo de confirmação aparecer, selecione **Sim** se você estiver pronto para começar a alterar as chaves de acesso SSH.



Não é possível cancelar esse processo depois que ele for iniciado.

Alterar chaves de acesso SSH

Quando o processo de alteração das chaves de acesso SSH é iniciado, um novo pacote de recuperação é gerado, incluindo as novas chaves. Em seguida, as chaves são atualizadas em cada nó.

Passos

1. Aguarde a geração do novo pacote de recuperação, o que pode levar alguns minutos.
2. Quando o botão "Baixar novo pacote de recuperação" estiver habilitado, selecione **Baixar novo pacote de recuperação** e salve o arquivo do novo pacote de recuperação (.zip em dois locais seguros, protegidos e separados.
3. Quando o download for concluído:
 - a. Abra o arquivo .zip.
 - b. Confirme se você tem acesso ao conteúdo, incluindo o `Passwords.txt` arquivo, que contém as novas chaves de acesso SSH.
 - c. Copie o novo arquivo do pacote de recuperação (.zip para dois locais seguros, protegidos e separados.



Não sobrescreva 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. Aguarde a atualização das chaves em cada nó, o que pode levar alguns minutos.

Se as chaves forem alteradas para todos os nós, uma faixa verde de sucesso aparece.

Se ocorrer um erro durante o processo de atualização, uma mensagem em destaque lista o número de nós que não tiveram suas chaves alteradas. O sistema tentará automaticamente repetir o processo em qualquer nó que não teve sua chave alterada. Se o processo terminar com alguns nós ainda sem a chave alterada, o botão **Retry** será exibido.

Se a atualização da chave falhar em um ou mais nós:

- a. Analise as mensagens de erro listadas na tabela.
- b. Resolva os problemas.
- c. Selecione **Tentar novamente**.

A nova tentativa altera apenas as chaves de acesso SSH nos nós que falharam durante as tentativas anteriores de alteração de chave.

5. Após as chaves de acesso SSH terem sido alteradas para todos os nós, exclua o [primeiro pacote de recuperação que você baixou](#).

6. Opcionalmente, selecione **Manutenção > Sistema > Pacote de recuperação** para baixar uma cópia adicional do novo pacote de recuperação.

Use a federação de identidades no StorageGRID

Utilizar a federação de identidades torna a configuração de grupos e usuários mais rápida e permite que os usuários façam login no StorageGRID usando credenciais familiares.

Configurar a federação de identidades para o Grid Manager

Você pode configurar a federação de identidades no Grid Manager se você quiser que grupos de administradores e usuários sejam gerenciados em outro sistema, como Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador web compatível"](#).
- Você ["permissões de acesso específicas"](#).
- Você está usando Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server como provedor de identidade.



Se você deseja usar um serviço LDAP v3 que não esteja listado, entre em contato com o suporte técnico.

- Se você planeja usar o OpenLDAP, você deve configurar o servidor OpenLDAP. Veja [Diretrizes para configurar um servidor OpenLDAP](#).
- Se você planeja habilitar o login único (SSO), você revisou o ["Requisitos e considerações para single sign-on"](#).
- Se você planeja usar o Transport Layer Security (TLS) para comunicações com o servidor LDAP, o provedor de identidade está usando TLS 1.2 ou 1.3. Consulte ["Cifras suportadas para conexões TLS de](#)

saída".

Sobre esta tarefa

Você pode configurar uma fonte de identidade para o Grid Manager se desejar importar grupos de outro sistema, como Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server. Você pode importar os seguintes tipos de grupos:

- Grupos de administradores. Os usuários em grupos de administradores podem entrar no Gerenciador de Grade e executar tarefas, com base nas permissões de gerenciamento atribuídas ao grupo.
- Grupos de usuários de locatários para locatários que não usam sua própria fonte de identidade. Usuários em grupos de locatários podem fazer login no Tenant Manager e executar tarefas, com base nas permissões atribuídas ao grupo no Tenant Manager. Consulte ["Criar conta de locatário"](#) e ["Use uma conta de tenant"](#) para obter detalhes.

Insira a configuração

Passos

1. Selecione **Configuração > Controle de acesso > Federação de identidades**.
2. Selecione **Ativar federação de identidades**.
3. Na seção tipo de serviço LDAP, selecione o tipo de serviço LDAP que você deseja configurar.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other

Selecione **Outro** para configurar valores de um servidor LDAP que utiliza o Oracle Directory Server.

4. Se você selecionou **Outro**, preencha os campos na seção Atributos LDAP. Caso contrário, vá para a próxima etapa.
 - **Nome Único do Usuário:** O nome do atributo que contém o identificador único de um usuário LDAP. Este atributo é equivalente a `sAMAccountName` para Active Directory e `uid` para OpenLDAP. Se você estiver configurando o Oracle Directory Server, insira `uid`.
 - **UUID do usuário:** O nome do atributo que contém o identificador único permanente de um usuário LDAP. Este atributo é equivalente a `objectGUID` para Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando Oracle Directory Server, insira `nsuniqueid`. O valor de cada usuário para o atributo especificado deve ser um número hexadecimal de 32 dígitos, em formato de 16 bytes ou string, onde os hífen são ignorados.
 - **Nome Único do Grupo:** O nome do atributo que contém o identificador único de um grupo LDAP. Este atributo é equivalente a `sAMAccountName` para Active Directory e `cn` para OpenLDAP. Se você estiver configurando Oracle Directory Server, insira `cn`.
 - **UUID do Grupo:** O nome do atributo que contém o identificador único permanente de um grupo LDAP. Este atributo é equivalente a `objectGUID` para Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando Oracle Directory Server, insira `nsuniqueid`. O valor de cada grupo para o atributo especificado deve ser um número hexadecimal de 32 dígitos, em formato de 16 bytes ou

string, onde os hífen são ignorados.

5. Para todos os tipos de serviço LDAP, insira as informações necessárias do servidor LDAP e da conexão de rede na seção Configurar servidor LDAP.

- **Nome do host:** O domínio totalmente qualificado (FQDN) ou endereço IP do servidor LDAP.
- **Porta:** A porta usada para 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 diferenciado (DN) do usuário que vai se conectar ao servidor LDAP.

Para o Active Directory, você também pode especificar o Down-Level Logon Name ou o User Principal Name.

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`
 - **Entra ID:** `accountEnabled` e `userPrincipalName`
- **Senha:** a senha associada ao nome de usuário.



Se você alterar a senha no futuro, você deve atualizá-la nesta página.

- **DN Base do Grupo:** O caminho completo do nome diferenciado (DN) de uma subárvore LDAP na qual você deseja pesquisar grupos. No exemplo do Active Directory (abaixo), todos os grupos cujo nome diferenciado é relativo ao DN base (`DC=storagegrid,DC=example,DC=com`) podem ser usados como grupos federados.



Os valores do **Nome único do grupo** devem ser únicos dentro do **DN base do grupo** ao qual pertencem.

- **DN Base do Usuário:** O caminho completo do nome diferenciado (DN) de uma subárvore LDAP na qual você deseja pesquisar usuários.



Os valores do **Nome único do usuário** devem ser únicos dentro do **DN base do usuário** ao qual pertencem.

- **Formato de nome de usuário de vinculação** (opcional): o padrão de nome de usuário que StorageGRID deve usar se o padrão não puder ser determinado automaticamente.

É recomendável fornecer o **formato de nome de usuário de vinculação**, pois isso pode permitir que os usuários façam login caso o StorageGRID não consiga se vincular à conta de serviço.

Insira um destes padrões:

- **UserPrincipalName padrão (AD e Entra ID):** [USERNAME]@example.com
- **Padrão de nome de logon de nível inferior (AD e Entra ID):** example\[USERNAME]
- **Padrão de nome diferenciado:** CN=[USERNAME], CN=Users, DC=example, DC=com

Inclua [USERNAME] exatamente como está escrito.

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

- **Usar STARTTLS:** Use STARTTLS para proteger as comunicações com o servidor LDAP. Esta é a opção recomendada para Active Directory, OpenLDAP ou outros, mas esta opção não é compatível com Microsoft Entra ID.
- **Usar LDAPS:** A opção LDAPS (LDAP sobre SSL) usa TLS para estabelecer uma conexão com o servidor LDAP. Você deve selecionar esta opção para Microsoft Entra ID.
- **Não utilize TLS:** O tráfego de rede entre o sistema StorageGRID e o servidor LDAP não será seguro. Esta opção não é compatível com Microsoft Entra ID.



A opção **Não usar TLS** não é compatível se o seu servidor Active Directory exigir assinatura LDAP. Você deve usar STARTTLS ou LDAPS.

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

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

Se você selecionar esta opção, copie e cole o certificado de segurança personalizado na caixa de texto do certificado da CA.

Teste a conexão e salve a configuração

Após inserir todos os valores, você deve testar a conexão antes de salvar a configuração. StorageGRID verifica as configurações de conexão para o servidor LDAP e o formato do nome de usuário de bind, caso você tenha fornecido um.

Passos

1. Selecione **Test connection**.
2. Se você não forneceu um formato de nome de usuário de vinculação:
 - Uma mensagem "Conexão testada com sucesso" é exibida se as configurações de conexão forem válidas. Selecione **Salvar** para salvar a configuração.
 - A mensagem "Não foi possível estabelecer a conexão de teste" será exibida se as configurações de conexão forem inválidas. Selecione **Fechar**. Em seguida, resolva quaisquer problemas e teste a conexão novamente.
3. Se você forneceu um formato de nome de usuário de vinculação, 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 @ ou /.

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

[Cancel](#) [Test Connection](#)

- Uma mensagem "Conexão testada com sucesso" é exibida se as configurações de conexão forem válidas. Selecione **Salvar** para salvar a configuração.
- Uma mensagem de erro será exibida se as configurações de conexão, o formato do nome de usuário de vinculação ou o nome de usuário e senha de teste forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

Forçar a sincronização com a fonte de identidade

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

Passos

1. Acesse a página de federação de identidades.
2. Selecione **Sync server** na parte superior da página.

O processo de sincronização pode demorar algum tempo dependendo do seu ambiente.



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

Desativar federação de identidade

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

Sobre esta tarefa

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

- Usuários federados não poderão fazer login.
- Os usuários federados que estiverem conectados no momento manterão o acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login após a expiração da sessão.

- A sincronização entre o sistema StorageGRID e a fonte de identidade não ocorrerá e alertas não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Habilitar federação de identidades** fica desabilitada se o status de logon único (SSO) for **Habilitado** ou **Modo Sandbox**. O status do SSO na página de logon único deve ser **Desabilitado** antes que você possa desabilitar a federação de identidades. Consulte ["Desativar single sign-on"](#).

Passos

1. Acesse a página de federação de identidades.
2. Desmarque a caixa de seleção **Ativar federação de identidades**.

Diretrizes para configurar um servidor OpenLDAP

Se você deseja usar um servidor OpenLDAP para federação de identidades, você deve configurar definições específicas no servidor OpenLDAP.



Para fontes de identidade que não sejam o Active Directory ou o Microsoft Entra ID, StorageGRID não bloqueará automaticamente o acesso S3 para usuários que estejam desabilitados externamente. Para bloquear o acesso S3, exclua quaisquer chaves S3 do usuário ou remova o usuário de todos os grupos.

Memberof e sobreposições refint

As sobreposições memberof e refint devem estar habilitadas. Para obter mais informações, consulte as instruções para manutenção reversa de associação de grupo no ["Documentação do OpenLDAP: Guia do administrador da versão 2.4"](#).

Indexação

Você deve configurar os seguintes atributos do 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 para Username estejam indexados para um desempenho ideal.

Consulte as informações sobre a manutenção reversa da associação a grupos no ["Documentação do OpenLDAP: Guia do administrador da versão 2.4"](#).

Gerenciar grupos de administradores no StorageGRID

Você pode criar grupos de administradores para gerenciar as permissões de segurança de um ou mais usuários administradores. Os usuários precisam pertencer a um grupo para receber acesso ao sistema StorageGRID.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).

- Você tem "[permissões de acesso específicas](#)".
- Se você planeja importar um grupo federado, você configurou a federação de identidades e o grupo federado já existe na fonte de identidade configurada.

Criar um grupo de administradores

Os grupos de administradores permitem que você determine quais usuários podem acessar quais recursos e operações no Gerenciador de Grade e na API de Gerenciamento de Grade.

Acesse o assistente

Passos

1. Selecione **Configuração > Controle de acesso > Grupos de administradores**.
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 você quiser atribuir permissões a usuários locais.
- Crie um grupo federado para importar usuários da fonte de identidade.

Grupo local

Passos

1. Selecione **Grupo local**.
2. Insira um nome de exibição para o grupo, que você poderá atualizar posteriormente, conforme necessário. Por exemplo, "Usuários de Manutenção" ou "Administradores do ILM".
3. Insira um nome exclusivo para o grupo, que você não poderá atualizar depois.
4. Selecione **Continue**.

Grupo federado

Passos

1. Selecione **Grupo federado**.
2. Insira o nome do grupo que você deseja importar, exatamente como aparece na fonte de identidade configurada.
 - Para Active Directory e Microsoft Entra ID, use o sAMAccountName.
 - Para o OpenLDAP, use o CN (Common Name).
 - Para outro LDAP, use o nome exclusivo apropriado para o servidor LDAP.
3. Selecione **Continue**.

Gerenciar permissões de grupo

Passos

1. Em **Modo de acesso**, selecione se os usuários do grupo podem alterar configurações e executar operações no Grid Manager e na Grid Management API ou se podem apenas visualizar configurações e recursos.

- **Leitura e gravação** (padrão): Os usuários podem alterar as configurações e executar as operações permitidas por suas permissões de gerenciamento.
- **Somente leitura**: Os usuários podem apenas visualizar as configurações e os recursos. Eles não podem fazer alterações nem executar operações no Grid Manager ou Grid Management API. Usuários locais com permissão somente leitura podem alterar suas próprias senhas.



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

2. Selecione uma ou mais ["permissões do grupo de administradores"](#).

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

3. Se estiver criando um grupo local, selecione **Continuar**. Se estiver criando um grupo federado, selecione **Criar grupo e Concluir**.

Adicionar usuários (somente grupos locais)

Passos

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

Se você ainda não criou usuários locais, pode salvar o grupo sem adicionar usuários. Você pode adicionar este grupo ao usuário na página Usuários. Veja ["Gerenciar usuários"](#) para mais detalhes.

2. Selecione **Criar grupo** e **Concluir**.

Visualizar e editar grupos de administradores

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

- Para visualizar informações básicas sobre todos os grupos, consulte a tabela na página Groups.
- Para visualizar todos os detalhes de um grupo específico ou editar um grupo, use o menu **Ações** ou a página de detalhes.

Tarefa	Menu de ações	Página de detalhes
Ver detalhes do grupo	a. Selecione a caixa de seleção do grupo. b. Selecione Ações > Ver detalhes do grupo .	Selecione o nome do grupo na tabela.
Editar nome de exibição (apenas grupos locais)	a. Selecione a caixa de seleção do grupo. b. Selecione Ações > Editar nome do grupo . c. Digite o novo nome. d. Selecione Save changes .	a. Selecione o nome do grupo para exibir os detalhes. b. Selecione o ícone de edição  . c. Digite o novo nome. d. Selecione Save changes .

Tarefa	Menu de ações	Página de detalhes
Editar modo de acesso ou permissões	a. Selecione a caixa de seleção do grupo. b. Selecione Ações > Ver detalhes do grupo . c. Opcionalmente, altere o modo de acesso do grupo. d. Opcionalmente, selecione ou desmarque "permissões do grupo de administradores". e. Selecione Save changes .	a. Selecione o nome do grupo para exibir os detalhes. b. Opcionalmente, altere o modo de acesso do grupo. c. Opcionalmente, selecione ou desmarque "permissões do grupo de administradores". d. Selecione Save changes .

Duplicar um grupo

Passos

1. Selecione a caixa de seleção do grupo.
2. Selecione **Ações > Duplicar grupo**.
3. Conclua o assistente Duplicate group.

Excluir um grupo

Você pode excluir um grupo de administradores quando quiser remover o grupo do sistema e remover todas as permissões associadas ao grupo. Excluir um grupo de administradores remove todos os usuários do grupo, mas não exclui os usuários.

Passos

1. Na página Groups, selecione a caixa de seleção de cada grupo que você deseja remover.
2. Selecione **Ações > Excluir grupo**.
3. Selecione **Excluir grupos**.

Permissões do grupo de administradores no StorageGRID

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

Você deve atribuir pelo menos uma permissão a cada grupo; caso contrário, os usuários pertencentes a esse grupo não poderão fazer login no Grid Manager ou na Grid Management API.

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

- Faça login no Grid Manager
- Veja o dashboard
- Veja as páginas de nós

- Veja os alertas atuais e resolvidos
- Alterar a própria senha (somente para usuários locais)
- Veja determinadas informações fornecidas nas páginas de 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 podem apenas visualizar as configurações e recursos relacionados. Se um usuário pertencer a vários grupos e algum 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 de **Root access**.

Acesso à raiz

Esta permissão concede acesso a todos os recursos de administração do grid.

Alterar senha raiz do tenant

Essa permissão concede acesso à opção **Alterar senha de root** na página de Locatários, permitindo que você controle quem pode alterar a senha do usuário raiz do locatário. Essa permissão também é usada para migrar chaves do S3 quando o recurso de importação de chaves do S3 está habilitado. Usuários que não possuem essa permissão não podem ver a opção **Alterar senha de root**.



Para conceder acesso à página Tenants, que contém a opção **Change root password**, atribua também a permissão **Tenant accounts**.

ILM

Esta permissão concede acesso às seguintes opções de menu do **ILM**:

- Regras
- Políticas
- Etiquetas de política
- Pools de storage
- Classes de storage
- Regiões
- Pesquisa de metadados de objetos



Os usuários devem ter a permissão **Other grid configuration** para gerenciar os storage grades.

Manutenção

Os usuários precisam ter a permissão de Maintenance para usar essas opções:

- **Configuração > Controle de acesso:**
 - Senhas do grid

- **Configuração > Rede:**
 - Nomes de domínio de endpoint S3
- **Manutenção > Tarefas:**
 - Descomissionar
 - Expansão
 - Verificação de existência de objeto
 - Recuperação
- **Manutenção > Sistema:**
 - Pacote de recuperação
 - Atualização de software
- **Suporte > Ferramentas:**
 - Registros

Usuários que não possuem a permissão de Maintenance podem visualizar, mas não editar, estas páginas:

- **Manutenção > Rede:**
 - Servidores DNS
 - Rede de grid
 - Servidores NTP
- **Manutenção > Sistema:**
 - Licença
- **Configuração > Rede:**
 - Nomes de domínio de endpoint S3
- **Configuração > Segurança:**
 - Certificados
- **Configuração > Monitoramento:**
 - Servidor de auditoria e syslog

Gerenciar alertas

Essa permissão concede acesso às opções de gerenciamento de alertas. Os usuários precisam dessa permissão para gerenciar silenciamentos, notificações de alerta e regras de alerta.

Consulta de métricas

Esta permissão concede acesso a:

- **Suporte > Ferramentas > Métricas**
- Consultas de métricas personalizadas do Prometheus usando a seção **Métricas** da Grid Management API
- Cartões do painel do Grid Manager que contêm métricas

Pesquisa de metadados de objetos

Esta permissão concede acesso à página **ILM > Pesquisa de metadados de objetos**.

Outra configuração de grid

Esta permissão concede acesso a estas opções adicionais de configuração da grid:

- **ILM:**
 - Classes de storage
- **Configuração > Sistema:**
- **Suporte > Outros:**
 - Custo do link

Administrador de appliance de armazenamento

Esta permissão concede:

- Acesso ao E-Series SANtricity System Manager em dispositivos de armazenamento através do Grid Manager.
- A capacidade de executar tarefas de solução de problemas e manutenção na guia Gerenciar unidades para appliances que suportam essas operações.

Contas de locatários

Esta permissão permite:

- Acesse a página de Tenants, onde você pode criar, editar e remover contas de tenant
- Consulte as políticas de classificação de tráfego existentes
- Visualize os cartões do painel do Grid Manager que contêm detalhes do tenant

Gerenciar usuários no StorageGRID

Você pode visualizar usuários locais e federados. Você também pode criar usuários locais e atribuí-los a grupos de administradores locais para determinar a quais recursos do Grid Manager esses usuários podem acessar.

Antes de começar

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

Criar 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 Grid Manager e da Grid Management API o usuário pode acessar.

Você só pode criar 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 single sign-on (SSO) estiver ativado, os usuários locais não poderão fazer login no StorageGRID.

Acesse o assistente

Passos

1. Selecione **Configuração > Controle de acesso > Usuários administradores**.
2. Selecione **Criar usuário**.

Insira as credenciais do usuário

Passos

1. Insira o nome completo do usuário, um nome de usuário exclusivo e uma senha.
2. Opcionalmente, selecione **Sim** se este usuário não deve ter acesso ao Grid Manager ou à Grid Management API.
3. Selecione **Continue**.

Atribuir a grupos

Passos

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

Se você ainda não criou grupos, pode salvar o usuário sem selecionar grupos. Você pode adicionar este usuário a um grupo na página Grupos.

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

2. Selecione **Criar usuário** e selecione **Concluir**.

Visualizar e editar usuários locais

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

Você só pode editar usuários locais. Use a fonte de identidade externa para gerenciar usuários federados.

- Para visualizar informações básicas sobre todos os usuários locais e federados, consulte 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.

Quaisquer alterações são aplicadas na próxima vez que o usuário sair e entrar novamente no Grid Manager.



Os usuários locais podem alterar suas próprias senhas usando a opção **Alterar senha** no banner do Grid Manager.

Tarefa	Menu de ações	Página de detalhes
Ver detalhes do usuário	a. Selecione a caixa de seleção para o usuário. b. Selecione Ações > Ver detalhes do usuário.	Selecione o nome do usuário na tabela.
Editar nome completo (somente usuários locais)	a. Selecione a caixa de seleção para o usuário. b. Selecione Ações > Editar nome completo. c. Digite o novo nome. d. Selecione Save changes.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione o ícone de edição . c. Digite o novo nome. d. Selecione Save changes.
Negar ou permitir acesso ao StorageGRID	a. Selecione a caixa de seleção para o usuário. b. Selecione Ações > Ver detalhes do usuário. c. Selecione a guia Acesso. d. Selecione Sim para impedir que o usuário faça login no Grid Manager ou na Grid Management API, ou selecione Não para permitir que o usuário faça login. e. Selecione Save changes.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Acesso. c. Selecione Sim para impedir que o usuário faça login no Grid Manager ou na Grid Management API, ou selecione Não para permitir que o usuário faça login. d. Selecione Save changes.
Alterar senha (somente para usuários locais)	a. Selecione a caixa de seleção para o usuário. b. Selecione Ações > Ver detalhes do usuário. c. Selecione a guia Senha. d. Digite uma nova senha. e. Selecione Alterar senha.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Senha. c. Digite uma nova senha. d. Selecione Alterar senha.

Tarefa	Menu de ações	Página de detalhes
Alterar grupos (somente usuários locais)	a. Selecione a caixa de seleção para o usuário. b. Selecione Ações > Ver detalhes do usuário . c. Selecione a guia Grupos. d. Opcionalmente, selecione o link após o nome do grupo para visualizar os detalhes do grupo em uma nova guia do navegador. e. Selecione Editar grupos para selecionar grupos diferentes. f. Selecione Save changes .	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a guia Grupos. c. Opcionalmente, selecione o link após o nome do grupo para visualizar os detalhes do grupo em uma nova guia do navegador. d. Selecione Editar grupos para selecionar grupos diferentes. e. Selecione Save changes .

Importar usuários federados

Você pode importar um ou mais usuários federados, até um máximo de 100 usuários, diretamente na página Usuários.

Passos

1. Selecione **Configuração > Controle de acesso > Usuários administradores**.
2. Selecione **Import federated users**.
3. Insira o UUID ou nome de usuário de um ou mais usuários federados.

Para múltiplas entradas, adicione cada UUID ou nome de usuário em uma nova linha.

4. Selecione **Import**.

Se a importação para o campo Usuários falhar para um ou mais usuários, execute as seguintes etapas:

- a. Expanda **Usuários não importados** e selecione **Copiar usuários**.
- b. Tente importar novamente selecionando **Anterior** e colando os usuários copiados na caixa de diálogo **Importar usuários federados**.

Após fechar a caixa de diálogo **Importar usuários federados**, as informações dos usuários federados são exibidas na página Usuários para os usuários importados com sucesso.

Duplicar um usuário

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

Passos

1. Selecione a caixa de seleção para o usuário.
2. Selecione **Ações > Duplicar usuário**.
3. Conclua o assistente de duplicar usuário.

Excluir um usuário

Você pode excluir um usuário local para removê-lo permanentemente do sistema.



Você não pode excluir o usuário raiz.

Passos

1. Na página Usuários, selecione a caixa de seleção de cada usuário que você deseja remover.
2. Selecione **Ações > Excluir usuário**.
3. Selecione **Excluir usuário**.

Use o single sign-on (SSO)

Saiba mais sobre StorageGRID SSO

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

O sistema StorageGRID suporta autenticação única (SSO) usando o padrão Security Assertion Markup Language 2.0 (SAML 2.0).

Antes de habilitar o single sign-on (SSO), verifique como os processos de login e logout do StorageGRID são afetados quando o SSO está habilitado.

Faça login quando o SSO estiver ativado

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

Passos

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

A página de login do StorageGRID é exibida.

- Se esta for a primeira vez que você acessa a URL neste navegador, será solicitado que você insira um ID de conta.
- Se você já acessou o Grid Manager ou o Tenant Manager anteriormente, será solicitado que selecione uma conta recente ou insira um ID de conta.



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

2. Indique se você deseja acessar o Grid Manager ou o Tenant Manager:

- Para acessar o Grid Manager, deixe o campo **Account ID** em branco, digite **0** como account ID ou selecione **Grid Manager** se ele aparecer na lista de contas recentes.
- Para acessar o Gerenciador de Inquilinos, insira o ID da conta do inquilino de 20 dígitos ou selecione um inquilino pelo nome se ele aparecer na lista de contas recentes.

3. Selecione **Sign in**

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

4. Faça login com suas credenciais de SSO.

Se suas credenciais de SSO estiverem corretas:

- O provedor de identidade (IdP) fornece uma resposta de autenticação ao StorageGRID.
- 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 Grid Manager ou ao Tenant Manager, dependendo da conta que você selecionou.



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

5. Opcionalmente, acesse outros Nós de Administração ou acesse o Grid Manager ou o Tenant Manager, caso você tenha permissões adequadas.

Você não precisa inserir suas credenciais de SSO novamente.

Saia quando o SSO estiver ativado

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

Passos

- Localize o link **Sair** no canto superior direito da interface de usuário.
- Selecione **Sair**.

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



A tabela resume o que acontece ao sair da sua conta se você estiver usando uma única sessão do navegador. Se você estiver conectado ao StorageGRID em várias sessões do navegador, você deve sair de cada sessão separadamente.

Se você estiver conectado a...	E você sai de...	Você está desconectado(a) de...
Gerenciador de grade em um ou mais nós de administração	Gerenciador de grade em qualquer nó de administração	Gerenciador de grade em todos os nós de administração Observação: Se você usar o Entra ID para SSO, pode levar alguns minutos para que a sessão seja encerrada em todos os Admin Nodes.
Gerenciador de locatários em um ou mais nós de administração	Gerenciador de locatários em qualquer nó administrativo	Gerenciador de Inquilinos em todos os nós administrativos
Tanto o Grid Manager quanto o Tenant Manager	Grid Manager	Somente o Grid Manager. Você também precisa sair do Tenant Manager para sair do SSO.

Requisitos e considerações para SSO do StorageGRID

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

Requisitos do provedor de identidade

StorageGRID é compatível com os seguintes provedores de identidade SSO (IdP):

- Serviço de Federação do Active Directory (AD FS)
- Microsoft Entra ID
- PingFederate

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

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

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



Windows Server 2016 deve usar a "[Atualização KB3201845](#)", ou superior.

Requisitos adicionais

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

Considerações sobre Entra ID

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

Requisitos de certificado do servidor

Por padrão, StorageGRID usa um certificado de interface de gerenciamento em cada nó administrativo para proteger o acesso ao Grid Manager, ao Tenant Manager, à API de Gerenciamento de Grid e à API de Gerenciamento de Locatários. Ao configurar relações de confiança de terceiros (AD FS), aplicativos corporativos (Entra ID) ou conexões de provedor de serviços (PingFederate) para StorageGRID, você usa o certificado do servidor como o certificado de assinatura para as solicitações do StorageGRID.

Se você ainda não "[configurou um certificado personalizado para a interface de gerenciamento](#)", deve fazer isso agora. Ao instalar um certificado de servidor personalizado, ele é usado em todos os Admin Nodes e você pode usá-lo em todas as relações de confiança de relying party do StorageGRID, aplicações empresariais ou conexões SP.



Não é recomendável usar o certificado de servidor padrão de um nó de administração em uma relação de confiança com terceiros, aplicativo corporativo ou conexão SP. Se o nó falhar e você o recuperar, um novo certificado de servidor padrão será gerado. Antes de fazer login no nó recuperado, você deve atualizar a relação de confiança com terceiros, o aplicativo corporativo ou a conexão SP com o novo certificado.

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

Requisitos de porta

O login único (SSO) não está disponível nas portas restritas do Grid Manager ou do Tenant Manager. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autentiquem com login único. Consulte "[Controle de acesso no firewall externo](#)".

Confirme se os usuários federados podem fazer login no StorageGRID

Antes de ativar o login único (SSO), você deve confirmar que pelo menos um usuário federado consegue acessar o Grid Manager e o Tenant Manager para quaisquer contas de locatário existentes.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Você já configurou a federação de identidades.

Passos

1. Caso existam contas de inquilinos, confirme que nenhum dos inquilinos está usando sua própria fonte de identidade.



Ao ativar o SSO, a origem de identidade configurada no Gerenciador de Locatários é substituída pela origem de identidade configurada no Grid Manager. Os usuários pertencentes à origem de identidade do locatário não poderão mais fazer login, a menos que possuam uma conta com a origem de identidade do Grid Manager.

- a. Faça login no Tenant Manager para cada conta de tenant.
 - b. Selecione **Gerenciamento de acesso > Federação de identidades**.
 - c. Confirme se a caixa de seleção **Ativar federação de identidades** não está selecionada.
 - d. Caso afirmativo, confirme se os grupos federados que possam estar em uso para esta conta de locatário não são mais necessários, desmarque a caixa de seleção e selecione **Salvar**.
2. Confirme se um usuário federado pode acessar o Grid Manager:
 - a. No Grid Manager, selecione **Configuração > Controle de acesso > Grupos de administradores**.
 - b. Certifique-se de que pelo menos um grupo federado tenha sido importado da fonte de identidade do Active Directory e que a ele tenha sido atribuída a permissão de acesso raiz.
 - c. Sair.
 - d. Confirme se você consegue acessar novamente o Grid Manager como um usuário do grupo federado.
 3. Caso existam contas de locatário, confirme que um usuário federado com permissão de acesso Root pode fazer login:
 - a. No Grid Manager, selecione **Tenants**.
 - b. Selecione a conta do locatário e selecione **Ações > Editar**.
 - c. Na guia Inserir detalhes, selecione **Continuar**.
 - d. Se a caixa de seleção **Usar fonte de identidade própria** estiver marcada, desmarque-a e selecione **Salvar**.

A página do tenant é exibida.

 - e. Selecione a conta do locatário, selecione **Entrar** e faça login na conta do locatário como usuário raiz.
 - f. No Tenant Manager, selecione **Gerenciamento de Acesso > Grupos**.
 - g. Certifique-se de que pelo menos um grupo federado do Grid Manager tenha recebido a permissão de acesso Root para este tenant.
 - h. Sair.
 - i. Confirme se você consegue entrar novamente no tenant como um usuário do grupo federado.

Informações relacionadas

- ["Requisitos e considerações para single sign-on"](#)

- ["Gerenciar grupos de administradores"](#)
- ["Use uma conta de tenant"](#)

Configurar SSO no StorageGRID

Você pode seguir o assistente de configuração do SSO e entrar no modo sandbox para configurar e testar o logon único (SSO) antes de habilitá-lo para todos os usuários do StorageGRID. Após o SSO ter sido habilitado, você pode retornar ao modo sandbox quando necessário para alterar ou testar novamente a configuração.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).
- Você configurou a federação de identidades para o seu sistema StorageGRID.
- Para o tipo de serviço **LDAP** de federação de identidades, você selecionou Active Directory ou Entra ID, com base no provedor de identidade SSO que você pretende usar.

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Serviço de Federação do Active Directory (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

Sobre esta tarefa

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

- A resposta do Active Directory ou PingFederate inclui um identificador único universal (UUID) para o usuário.
- A resposta do Entra ID inclui um Nome Principal do Usuário (UPN).

Para permitir que StorageGRID (o provedor de serviços) e o provedor de identidade SSO se comuniquem com segurança sobre as solicitações de autenticação do usuário, você deverá concluir estas tarefas:

1. Configure as configurações no StorageGRID.
2. Use o software do provedor de identidade SSO para criar uma relação de confiança com a parte confiável (AD FS), Aplicativo Empresarial (Entra ID) ou Provedor de Serviços (PingFederate) para cada Admin Node.
3. Retorne ao StorageGRID para ativar o SSO.

O modo sandbox facilita a realização dessa configuração bidirecional e permite testar todas as suas configurações antes de ativar o SSO. Quando você está usando o modo sandbox, os usuários não podem fazer login usando o SSO.

Acesse o assistente

Passos

1. Selecione **Configuração > Controle de acesso > Single sign-on**. A página de Single sign-on é exibida.



Se o botão Configurar configurações de SSO estiver desativado, confirme se você configurou o provedor de identidade como a fonte de identidade federada. Consulte ["Requisitos e considerações para single sign-on"](#).

2. Selecione **Configurar definições de SSO**. A página Fornecer detalhes do provedor de identidade é exibida.

Forneça os detalhes do provedor de identidade

Passos

1. Selecione o **tipo de SSO** na lista suspensa.
2. Se você selecionou o Active Directory como o tipo de SSO, insira o **nome do serviço de federação** para o provedor de identidade, exatamente como aparece no Active Directory Federation Service (AD FS).



Para localizar o nome do serviço de federação, acesse o Windows Server Manager. Selecione **Tools > AD FS Management**. No menu Action, selecione **Edit Federation Service Properties**. O nome do serviço de federação é exibido no segundo campo.

3. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração SSO em resposta às solicitações do StorageGRID.
 - **Usar certificado CA do sistema operacional:** Use o certificado CA padrão instalado no sistema operacional para proteger a conexão.
 - **Usar certificado CA personalizado:** Use um certificado CA personalizado para proteger a conexão.

Se você selecionar essa configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **CA Certificate**.
 - **Não utilize TLS:** Não utilize um certificado TLS para proteger a conexão.



Se você alterar o certificado da CA, imediatamente ["reinicie o serviço mgmt-api nos nós de administração"](#) e teste se o SSO no Grid Manager foi bem-sucedido.

4. Selecione **Continuar**. A página Fornecer identificador da parte confiável é exibida.

Forneça o identificador da parte confiável

1. Preencha os campos na página "Fornecer identificador da parte confiável" com base no tipo de SSO que você selecionou.

Active Directory

- a. Especifique o **Identificador da parte confiável** para StorageGRID. Esse valor controla o nome que você usa para cada relação de confiança com a parte confiável no AD FS.
 - Por exemplo, se sua grade tiver apenas um Nó de Administração e você não prevê adicionar mais Nós de Administração no futuro, insira `SG` ou `StorageGRID`.
 - Se sua grid incluir mais de um Admin Node, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Incluir essa string resulta em uma tabela que mostra o identificador da relying party para cada Admin Node na grid, com base no hostname do nó.



Você deve criar uma relação de confiança de terceiros para cada Nó de Administração no seu sistema StorageGRID. Ter uma relação de confiança de terceiros para cada Nó de Administração garante que os usuários possam fazer login e logout com segurança em qualquer Nó de Administração.

- b. Selecione **Salvar e entrar no modo sandbox**.

Entra ID

- a. Na seção Aplicativo Empresarial, especifique o **nome do aplicativo empresarial** para StorageGRID. Esse valor controla o nome que você usa para cada aplicativo empresarial no Entra ID.
 - Por exemplo, se sua grade tiver apenas um Nó de Administração e você não prevê adicionar mais Nós de Administração no futuro, insira `SG` ou `StorageGRID`.
 - Se a sua grid incluir mais de um Admin Node, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Incluir essa string resulta em uma tabela que mostra o nome do aplicativo corporativo para cada Admin Node em seu sistema, com base no hostname do nó.



Você deve criar um aplicativo corporativo para cada Nó de Administração em seu sistema StorageGRID. Ter um aplicativo corporativo para cada Nó de Administração garante que os usuários possam entrar e sair de qualquer Nó de Administração com segurança.

- b. Siga os passos descritos em "[Crie aplicativos empresariais no Entra ID](#)" para criar uma aplicação empresarial para cada Admin Node listado na tabela.
- c. No Entra ID, copie a URL dos metadados de federação para cada aplicação empresarial. Em seguida, cole essa URL no campo **Federation metadata URL** correspondente no StorageGRID.
- d. Depois de copiar e colar uma URL de metadados de federação para todos os Admin Nodes, selecione **Salvar e entrar no modo sandbox**.

PingFederate

- a. Na seção Provedor de Serviços (SP), especifique o **SP connection ID** para StorageGRID. Esse valor controla o nome que você usa para cada conexão SP em PingFederate.
 - Por exemplo, se sua grade tiver apenas um Nó de Administração e você não prevê adicionar mais Nós de Administração no futuro, insira `SG` ou `StorageGRID`.
 - Se sua grid incluir mais de um Nó de Administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Incluir essa string resulta em uma tabela que mostra o ID de conexão do SP para cada Nó de Administração em seu sistema, com base no

hostname do nó.



Você deve criar uma conexão SP para cada Nó de Administração no seu sistema StorageGRID. Ter uma conexão SP para cada Nó de Administração garante que os usuários possam fazer login e logout com segurança em qualquer Nó de Administração.

- b. Especifique a URL de metadados de federação para cada Nó de Administração no campo **URL de metadados de federação**.

Utilize o seguinte formato:

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

- c. Selecione **Salvar e entrar no modo sandbox**.

Configurar relações de confiança com terceiros confiáveis, aplicativos corporativos ou conexões SP

Após salvar a configuração e entrar no modo sandbox, você pode concluir e testar a configuração do tipo de SSO que você selecionou.

StorageGRID pode permanecer em modo sandbox pelo tempo que for necessário. No entanto, somente usuários federados e usuários locais podem fazer login.

Active Directory

Passos

1. Acesse o Active Directory Federation Services (AD FS).
2. Crie uma ou mais relações de confiança de terceiros para StorageGRID, usando cada identificador de terceiro exibido na tabela na página Configurar SSO.

Você deve criar uma relação de confiança para cada Admin Node mostrado na tabela.

Para obter instruções, acesse ["Crie relações de confiança de terceiros no AD FS"](#).

Entra ID

Passos

1. Na página de login único do nó de administração em que você está conectado, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para quaisquer outros nós de administração em sua grade, repita estas etapas:
 - a. Faça login no nó.
 - b. Selecione **Configuração > Controle de acesso > Single sign-on**.
 - c. Baixe e salve os metadados SAML para esse nó.
3. Acesse o portal do Azure.
4. Siga os passos em ["Crie aplicativos empresariais no Entra ID"](#) para carregar o arquivo de metadados SAML de cada Nó de Administração em seu respectivo aplicativo corporativo Entra ID.

PingFederate

Passos

1. Na página de login único do nó de administração em que você está conectado, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para quaisquer outros nós de administração em sua grade, repita estas etapas:
 - a. Faça login no nó.
 - b. Selecione **Configuração > Controle de acesso > 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 StorageGRID"](#). Use o ID de conexão do SP para cada Nó de Administração (mostrado na tabela na página Configurar SSO) e os metadados SAML que você baixou para esse Nó de Administração.

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

Testar configuração

Antes de impor o uso de single sign-on para todo o seu sistema StorageGRID, confirme que o single sign-on e o single logout estão configurados corretamente para cada Admin Node.

Active Directory

Passos

1. Na página Configurar SSO, localize o link na etapa Testar configuração do assistente.

A URL é derivada do valor que você inseriu no campo **Nome do serviço de federação**.

2. Selecione o link ou copie e cole a URL em um navegador para acessar a página de login do seu provedor de identidade.
3. Para confirmar que você pode usar o SSO para entrar no StorageGRID, selecione **Entrar em um dos seguintes sites**, selecione o identificador da parte confiável para seu nó de administração principal e selecione **Entrar**.
4. Insira seu nome de usuário federado e sua senha.
 - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.
 - Se a operação de SSO falhar, uma mensagem de erro será exibida. Corrija o problema, limpe os cookies do navegador e tente novamente.
5. Repita estes passos para verificar a conexão SSO de cada Admin Node em sua grid.

Entra ID

Passos

1. Acesse a página de login único no portal do Azure.
2. Selecione **Test this application**.
3. Insira as credenciais de um usuário federado.
 - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.
 - Se a operação de SSO falhar, uma mensagem de erro será exibida. Corrija o problema, limpe os cookies do navegador e tente novamente.
4. Repita estes passos para verificar a conexão SSO de cada Admin Node em sua grid.

PingFederate

Passos

1. Na página Configurar SSO, selecione o primeiro link na mensagem de modo Sandbox.

Selecione e teste um link de cada vez.

2. Insira as credenciais de um usuário federado.
 - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.
 - Se a operação de SSO falhar, uma mensagem de erro será exibida. Corrija o problema, limpe os cookies do navegador e tente novamente.
3. Selecione o link a seguir para verificar a conexão SSO de cada nó de administração em sua grade.

Se você vir a mensagem "Página Expirada", selecione o botão **Voltar** no seu navegador e envie suas credenciais novamente.

Ativar single sign-on

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



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

Passos

1. Na etapa Test configuration do assistente de configuração de SSO, selecione **Enable SSO**.
2. Analise a mensagem de aviso e selecione **Ativar SSO**.

O login único agora está ativado. A página de login único é exibida e agora inclui os detalhes do SSO que você acabou de configurar.

3. Para editar a configuração, selecione **Editar**.
4. Para desativar o single sign-on, selecione **Disable SSO**.



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

Crie relações de confiança com terceiros confiáveis no AD FS para StorageGRID

Você deve usar o Active Directory Federation Services (AD FS) para criar uma relação de confiança com outra parte para cada nó administrativo do seu sistema. Você pode criar relações de confiança com outra parte usando comandos do PowerShell, importando metadados SAML do StorageGRID ou inserindo os dados manualmente.

Antes de começar

- Você configurou o logon único para StorageGRID e selecionou **AD FS** como o tipo de SSO.
- Você tem ["entrou no modo sandbox"](#) no Grid Manager.
- Você conhece o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador da parte confiável para cada Admin Node em seu sistema. Você pode encontrar esses valores na tabela de detalhes dos Admin Nodes na página Configure SSO do StorageGRID.



Você deve criar uma relação de confiança de terceiros para cada Nó de Administração no seu sistema StorageGRID. Ter uma relação de confiança de terceiros para cada Nó de Administração garante que os usuários possam fazer login e logout com segurança em qualquer Nó de Administração.

- Você tem experiência na criação de relações de confiança de terceiros no AD FS ou tem acesso à documentação do Microsoft AD FS.
- Você está usando o snap-in de Gerenciamento do AD FS e pertence ao grupo Administradores.
- Se você estiver criando a relação de confiança com a parte confiável manualmente, você possui o certificado personalizado que foi carregado para a interface de gerenciamento do StorageGRID, ou sabe como fazer login em um Admin Node 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, notará pequenas diferenças no procedimento. Consulte a documentação do Microsoft AD FS se você tiver dúvidas.

Crie uma relação de confiança com terceiros usando Windows PowerShell

Você pode usar o Windows PowerShell para criar rapidamente uma ou mais relações de confiança com terceiros confiáveis.

Passos

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

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

- Para *Admin_Node_Identifer*, insira o Identificador da Parte Confiável para o Nó de Administração, exatamente como aparece na página de Single Sign-on. Por exemplo, SG-DC1-ADM1.
- Para *Admin_Node_FQDN*, insira o domínio totalmente qualificado para o mesmo Admin Node. (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 deverá atualizar ou recriar essa relying party trust caso esse endereço IP seja alterado.)

3. No Gerenciador do Servidor do Windows Server, selecione **Ferramentas > Gerenciamento do AD FS**.

A ferramenta de gerenciamento do AD FS é exibida.

4. Selecione **AD FS > Relying Party Trusts**.

A lista de relying party trusts é exibida.

5. Adicione uma política de controle de acesso à relação de confiança da parte confiável recém-criada:

- a. Localize a relação de confiança da parte confiável que você acabou de criar.
- b. Clique com o botão direito do mouse na relação de confiança e selecione **Editar Política de Controle de Acesso**.
- c. Selecione uma política de controle de acesso.
- d. Selecione **Aplicar** e selecione **OK**

6. Adicione uma política de emissão de declarações à nova relação de confiança de terceira parte criada:

- a. Localize a relação de confiança da parte confiável que você acabou de criar.
- b. Clique com o botão direito do mouse na trust e selecione **Editar política de emissão de declarações**.
- c. Selecione **Adicionar regra**.
- d. Na página Selecionar Modelo de Regra, selecione **Enviar Atributos LDAP como Declarações** na lista e selecione **Avançar**.
- e. Na página Configurar Regra, insira um nome de exibição para esta regra.

Por exemplo, **ObjectGUID para Name ID** ou **UPN para Name ID**.

- f. Para o Repositório de Atributos, selecione **Active Directory**.
 - g. Na coluna Atributo LDAP da tabela de Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.
 - h. Na coluna Tipo de Reivindicação de Saída da tabela de Mapeamento, selecione **Name ID** na lista suspensa.
 - i. Selecione **Concluir** e selecione **OK**.
7. Confirme se os metadados foram importados com sucesso.
- a. Clique com o botão direito do mouse na relação de confiança da parte confiável para abrir suas propriedades.
 - b. Confirme se os campos nas abas **Endpoints**, **Identifiers** e **Signature** estão preenchidos.
- Se os metadados estiverem ausentes, confirme se o endereço de metadados da Federação está correto ou insira os valores manualmente.
8. Repita estes passos para configurar uma relação de confiança da parte confiável para todos os nós de administração em seu sistema StorageGRID.
9. Ao concluir, retorne ao StorageGRID e "[testar todas as relações de confiança de terceiros](#)" para confirmar que estão configurados corretamente.

Crie uma relação de confiança de terceiros importando metadados de federação

Você pode importar os valores para cada relação de confiança com a parte confiável acessando os metadados SAML de cada Admin Node.

Passos

1. No Gerenciador do Servidor do Windows Server, selecione **Ferramentas** e, em seguida, selecione **Gerenciamento do AD FS**.
2. Em Ações, selecione **Adicionar Relying Party Trust**.
3. Na página de boas-vindas, escolha **Reconhecimento de reivindicações** e selecione **Iniciar**.
4. Selecione **Importar dados sobre a parte confiante publicados online 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 Admin Node:

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

Para *Admin_Node_FQDN*, insira o domínio totalmente qualificado para o mesmo Admin Node. (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 deverá atualizar ou recriar essa relying party trust caso esse endereço IP seja alterado.)

6. Conclua o assistente de Relying Party Trust, salve o relying party trust e feche o assistente.



Ao inserir o nome de exibição, use o Identificador da Parte Confiável para o Nó de Administração, exatamente como aparece na página de Single Sign-on no Grid Manager. Por exemplo, SG-DC1-ADM1.

7. Adicione uma regra de reivindicação:
 - a. Clique com o botão direito do mouse na trust e selecione **Editar política de emissão de declarações**.

b. Selecione **Adicionar regra**:

c. Na página Selecionar Modelo de Regra, selecione **Enviar Atributos LDAP como Declarações** na lista e selecione **Avançar**.

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

Por exemplo, **ObjectGUID para Name ID** ou **UPN para Name ID**.

e. Para o Repositório de Atributos, selecione **Active Directory**.

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

g. Na coluna Tipo de Reivindicação de Saída da tabela de Mapeamento, selecione **Name ID** na lista suspensa.

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

8. Confirme se os metadados foram importados com sucesso.

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

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

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

9. Repita estes passos para configurar uma relação de confiança da parte confiável para todos os nós de administração em seu sistema StorageGRID.

10. Ao concluir, retorne ao StorageGRID e ["testar todas as relações de confiança de terceiros"](#) para confirmar se estão configuradas corretamente.

Criar manualmente uma relação de confiança de terceiros

Caso opte por não importar os dados para os relying part trusts, você pode inserir os valores manualmente.

Passos

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

2. Em Ações, selecione **Adicionar Relying Party Trust**.

3. Na página de boas-vindas, escolha **Reconhecimento de reivindicações** e selecione **Iniciar**.

4. Selecione **Inserir manualmente os dados da parte confiante** e selecione **Avançar**.

5. Conclua o assistente de Confiança da Parte Confiável:

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

Para manter a consistência, use o Identificador da Parte Confiável para o Nó de Administração, exatamente como aparece na página de Autenticação Única no Gerenciador de Grade. Por exemplo, SG-DC1-ADM1.

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

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

- d. Digite a URL do endpoint do serviço SAML para o Admin Node:

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

Para *Admin_Node_FQDN*, insira o nome de domínio totalmente qualificado do Nó de Administração. (Se necessário, você pode usar o endereço IP do nó em vez disso. No entanto, se você inserir um endereço IP aqui, esteja ciente de que será necessário atualizar ou recriar essa relação de confiança com a parte confiável caso esse endereço IP seja alterado.)

- e. Na página Configurar Identificadores, especifique o Identificador da Parte Confiável para o mesmo Admin Node:

Admin_Node_Identifier

Para *Admin_Node_Identifier*, insira o Identificador da Parte Confiável para o Nó de Administração, exatamente como aparece na página de Single Sign-on. Por exemplo, SG-DC1-ADM1.

- f. Revise as configurações, salve a relação de confiança com a parte confiável e feche o assistente.

A caixa de diálogo Edit Claim Issuance Policy é exibida.



Se a caixa de diálogo não aparecer, clique com o botão direito do mouse na trust e selecione **Editar política de emissão de reivindicações**.

6. Para iniciar o assistente de regras de reivindicação, selecione **Adicionar regra**:

- a. Na página Selecionar Modelo de Regra, selecione **Enviar Atributos LDAP como Declarações** na lista e selecione **Avançar**.
b. Na página Configurar Regra, insira um nome de exibição para esta regra.

Por exemplo, **ObjectGUID para Name ID** ou **UPN para Name ID**.

- c. Para o Repositório de Atributos, selecione **Active Directory**.
d. Na coluna Atributo LDAP da tabela de Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.
e. Na coluna Tipo de Reivindicação de Saída da tabela de Mapeamento, selecione **Name ID** na lista suspensa.
f. Selecione **Concluir** e selecione **OK**.

7. Clique com o botão direito do mouse na relação de confiança da parte confiável para abrir suas propriedades.

8. Na aba **Endpoints**, configure o endpoint para logout único (SLO):

- a. Selecione **Adicionar SAML**.
b. Selecione **Tipo de Endpoint > Logout SAML**.
c. Selecione **Associação > Redirecionamento**.
d. No campo **URL confiável**, insira a URL usada para logout único (SLO) deste Admin Node:

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

Para *Admin_Node_FQDN*, insira o domínio totalmente qualificado do nó de administração. (Se necessário,

you can use the IP address of the node instead of this. However, if you enter an IP address here, be aware that you will need to update or recreate this trust relationship with the other party in case this IP address is changed.)

a. Select **OK**.

9. In the **Assinatura** guide, specify the certificate of signature for this trust relationship with the trusted party:

a. Add the custom certificate:

- If you have the custom certificate of management that you uploaded to StorageGRID, select this certificate.
- If you do not have the custom certificate, log in to the Administration Node, access `/var/local/mgmt-api` directory of the Administration Node and add the `custom-server.crt` certificate file.



It is not recommended to use the default certificate of the administration node (`server.crt`). If the administration node fails, the default certificate will be regenerated when you recover the node, and you will need to update the relying party trust.

b. Select **Aplicar** and select **OK**.

The properties of the Relying Party are saved and closed.

10. Repeat these steps to configure a trust relationship of the trusted party for all administration nodes in your StorageGRID system.

11. After completion, return to StorageGRID and **"testar todas as relações de confiança de terceiros"** to confirm that they are configured correctly.

Create corporate applications in Entra ID for StorageGRID

You use Entra ID to create a corporate application for each Admin Node in your system.

Before you begin

- You initiated the configuration of single sign-on for StorageGRID and selected **Entra ID** as the SSO type.
- You have **"entra no modo sandbox"** in Grid Manager.
- You have the **nome do aplicativo corporativo** for each Admin Node in your system. You can copy these values from the details table of the Admin Node on the Configure SSO page.



You must create a corporate application for each Administration Node in your StorageGRID system. Having a corporate application for each Administration Node ensures that users can log in and out of any Administration Node securely.

- You have experience creating corporate applications in Entra ID.
- You have an active Entra ID account.
- You have one of the following roles in your Entra ID account: Global Administrator, Cloud Application Administrator, Application Administrator or owner of the service principal.

Acessar Entra ID

Passos

1. Faça login no "Portal do Azure".
2. Navegue até "Entra ID".
3. Selecione "Aplicações empresariais".

Crie aplicativos corporativos e salve a configuração do StorageGRID SSO

Para salvar a configuração de SSO para o Entra ID no StorageGRID, você deve usar o Entra ID para criar um aplicativo corporativo para cada Admin Node. Você copiará os URLs de metadados de federação do Entra ID e os colará nos campos **URL de metadados de federação** correspondentes na página Configurar SSO.

Passos

1. Repita as seguintes etapas para cada Admin Node.
 - a. No painel de aplicações do Entra ID Enterprise, selecione **New application**.
 - b. Selecione **Criar sua própria aplicação**.
 - c. No campo "Nome", insira o **Nome do aplicativo corporativo** que você copiou da tabela de detalhes do nó de administração na página "Configurar SSO".
 - d. Deixe a opção **Integrar qualquer outro aplicativo que você não encontrar na galeria (Não pertencente à galeria)** selecionada.
 - e. Selecione **Create**.
 - f. Selecione o link **Começar** na **2. Configurar login único** ou selecione o link **Login único** na margem esquerda.
 - g. Selecione a caixa **SAML**.
 - h. Copie o **App Federation Metadata Url**, que você pode encontrar em **Etapas 3 SAML Signing Certificate**.
 - i. Acesse a página Configurar SSO e cole a URL no campo **URL de metadados de federação** que corresponde ao **nome do aplicativo corporativo** que você utilizou.
2. Depois de colar uma URL de metadados de federação para cada nó de administração e fazer todas as outras alterações necessárias na configuração do SSO, selecione **Salvar** na página Configurar SSO.

Baixe os metadados SAML para cada nó de administração

Após salvar a configuração do SSO, você pode baixar um arquivo de metadados SAML para cada nó de administração em seu sistema StorageGRID.

Passos

1. Repita estas etapas para cada Admin Node.
 - a. Faça login no StorageGRID a partir do nó de administração.
 - b. Selecione **Configuração > Controle de acesso > Single sign-on**.
 - c. Selecione o botão para baixar os metadados SAML desse nó administrativo.
 - d. Salve o arquivo, que você irá carregar no Entra ID.

Faça o upload dos metadados SAML para cada aplicativo corporativo

Após baixar um arquivo de metadados SAML para cada nó de administração do StorageGRID, execute as seguintes etapas no Entra ID:

Passos

1. Retorne ao Portal do Azure.
2. Repita estas etapas para cada aplicação empresarial:



Pode ser necessário atualizar a página de aplicativos corporativos para ver os aplicativos que você adicionou anteriormente na lista.

- a. Acesse a página Propriedades do aplicativo corporativo.
 - b. Defina **Atribuição necessária** como **Não** (a menos que você queira configurar atribuições separadamente).
 - c. Vá para a página de login único.
 - d. Conclua a configuração SAML.
 - e. Selecione o botão **Carregar arquivo de metadados** e selecione o arquivo de metadados SAML que você baixou para o nó de administração correspondente.
 - f. Após o carregamento do arquivo, selecione **Salvar** e, em seguida, selecione **X** para fechar o painel. Você retorna à página Configurar Single Sign-On com SAML.
3. ["Teste cada aplicação"](#).

Crie conexões de provedor de serviços em PingFederate para StorageGRID

Você usa o PingFederate para criar uma conexão de provedor de serviços (SP) para cada nó de administração em seu sistema. Para acelerar o processo, você importará os metadados SAML do StorageGRID.

Antes de começar

- Você configurou o logon único para StorageGRID e selecionou **Ping Federate** como o tipo de SSO.
- Você tem ["entrou no modo sandbox"](#) no Grid Manager.
- Você possui o **ID de conexão SP** para cada Nó de Administração em seu sistema. Você pode encontrar esses valores na tabela de detalhes dos Nós de Administração na página Configurar SSO.
- Você baixou os **metadados SAML** para cada nó de administração em seu sistema.
- Você tem experiência em criar conexões SP no PingFederate Server.
- Você tem o ["Guia de Referência do Administrador"](#) para o PingFederate Server. A documentação do PingFederate fornece instruções detalhadas passo a passo e explicações.
- Você tem o ["Permissão de administrador"](#) para o PingFederate Server.

Sobre esta tarefa

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

Conclua os pré-requisitos em PingFederate

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

Criar armazenamento de dados

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

- **Tipo:** Diretório (LDAP)
- **Tipo LDAP:** Active Directory
- **Nome do Atributo Binário:** insira **objectGUID** na guia Atributos Binários do LDAP exatamente como mostrado.

Criar validador de credencial de senha

Se ainda não fez isso, crie um validador de credencial de senha.

- **Tipo:** Validador de credencial LDAP com nome de usuário e senha
- **Armazenamento de dados:** selecione o armazenamento de dados que você criou.
- **Base de pesquisa:** Insira informações do LDAP (por exemplo, DC=saml,DC=sgws).
- **Filtro de pesquisa:** sAMAccountName=\${username}
- **Escopo:** Subárvore

Criar instância do adaptador IdP

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

Passos

1. Acesse **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 credencial'**.
5. Selecione o [validador de credencial de senha](#) que você criou.
6. Na guia Atributos do Adaptador, selecione o atributo **username** para **Pseudonym**.
7. Selecione **Salvar**.

Criar ou importar certificado de assinatura

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

Passos

1. Acesse **Segurança > Chaves e certificados de assinatura e descryptografia**.
2. Crie ou importe o certificado de assinatura.

Crie uma conexão SP em PingFederate

Ao criar uma conexão SP em PingFederate, você importa os metadados SAML que baixou do StorageGRID para o Nó de Administração. O arquivo de metadados contém muitos dos valores específicos de que você precisa.



Você deve criar uma conexão SP para cada nó de administração no seu sistema StorageGRID, para que os usuários possam entrar e sair de qualquer nó com segurança. Use estas instruções para criar a primeira conexão SP. Em seguida, acesse [Criar conexões SP adicionais](#) para criar as conexões adicionais necessárias.

Escolha o tipo de conexão SP

Passos

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

Importar metadados do SP

Passos

1. Na guia Importar Metadados, selecione **Arquivo**.
2. Selecione o arquivo de metadados SAML que você baixou da página Configurar SSO para o Admin Node.
3. Analise o Resumo de Metadados e as informações fornecidas na aba Informações Gerais.

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

4. Selecione **Next**.

Configurar SSO do navegador IdP

Passos

1. Na guia SSO do navegador, selecione **Configurar SSO do navegador**.
2. Na guia Perfis SAML, selecione as opções **SSO iniciado pelo SP**, **SLO iniciado pelo SP**, **SSO iniciado pelo IdP** e **SLO iniciado pelo IdP**.
3. Selecione **Next**.
4. Na aba "Tempo de Vida da Asserção", não faça alterações.
5. Na guia Criação de Asserção, selecione **Configurar Criação de Asserção**.
 - a. Na guia Mapeamento de Identidade, selecione **Standard**.
 - b. Na guia Contrato de Atributo, use **SAML_SUBJECT** como Contrato de Atributo e o formato de nome não especificado que foi importado.
6. Para prorrogar o contrato, selecione **Excluir** para remover o `urn:oid`, que não está sendo usado.

Mapear instância do adaptador

Passos

1. Na guia Mapeamento da Fonte de Autenticação, selecione **Mapear nova instância do adaptador**.
2. Na guia Instância do Adaptador, selecione a **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 & Pesquisa de Usuário, selecione **Adicionar Origem do Atributo**.
5. Na aba "Data Store", forneça uma descrição e selecione o **armazenamento de dados** que você adicionou.
6. Na guia Pesquisa de diretório LDAP:
 - Insira o **DN base**, que deve corresponder exatamente ao valor que você inseriu no StorageGRID para o servidor LDAP.
 - Para o escopo de pesquisa, selecione **Subárvore**.
 - Para a classe de objeto raiz, procure e adicione um destes atributos: **objectGUID** ou **userPrincipalName**.
7. Na guia Tipos de codificação de atributos binários LDAP, selecione **Base64** para o atributo **objectGUID**.
8. Na guia Filtro LDAP, insira **sAMAccountName=\${username}**.
9. Na guia Cumprimento do Contrato de Atributo, selecione **LDAP (atributo)** na lista suspensa Origem e selecione **objectGUID** ou **userPrincipalName** na lista suspensa Valor.
10. Revise e depois salve a fonte de atributos.
11. Na guia Origem do atributo Failsave, selecione **Abort the SSO Transaction**.
12. Revise o resumo e selecione **Concluído**.
13. Selecione **Concluído**.

Configurar as configurações do protocolo

Passos

1. Na guia **Conexão SP > SSO do navegador > Configurações de protocolo**, selecione **Configurar configurações de protocolo**.
2. Na guia URL do serviço de consumo de asserção, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**POST** para Binding e `/api/saml-response` para Endpoint URL).
3. Na guia URLs do serviço SLO, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**REDIRECT** para Binding e `/api/saml-logout` para Endpoint URL).
4. Na aba "Associações SAML Permitidas", desmarque **ARTIFACT** e **SOAP**. Somente **POST** e **REDIRECT** são obrigatórios.
5. Na guia Política de Assinatura, deixe as caixas de seleção **Exigir que as solicitações de autenticação sejam assinadas** e **Sempre assinar a declaração** marcadas.
6. Na guia Política de Criptografia, selecione **None**.
7. Analise o resumo e selecione **Concluído** para salvar as configurações do protocolo.
8. Analise o resumo e selecione **Concluído** para salvar as configurações de SSO do navegador.

Configurar credenciais

Passos

1. Na guia Conexão do SP, selecione **Credenciais**.
2. Na aba Credenciais, selecione **Configurar Credenciais**.
3. Selecione o [certificado de assinatura](#) que você criou ou importou.
4. Selecione **Avançar** para ir para **Gerenciar configurações de verificação de assinatura**.
 - a. Na aba Trust Model, selecione **Unanchored**.
 - b. Na aba Certificado de Verificação de Assinatura, revise as informações do certificado de assinatura, que foram importadas dos metadados SAML do StorageGRID.
5. Analise as telas de resumo e selecione **Salvar** para salvar a conexão SP.

Criar conexões SP adicionais

Você pode copiar a primeira conexão SP para criar as conexões SP necessárias para cada Nó de Administração em sua grade. Você carrega novos metadados para cada cópia.



As conexões 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.

Passos

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

Desativar SSO no StorageGRID

Você pode desativar o single sign-on (SSO) se não quiser mais usar essa funcionalidade. Você deve desativar o single sign-on antes de desativar a federação de identidades.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).

- Você tem "[permissões de acesso específicas](#)".

Passos

1. Selecione **Configuração > Controle de acesso > Single sign-on**.

A página de Single Sign-on é exibida.

2. Selecione **Desativar SSO**.
3. Selecione **Sim**.

Uma mensagem de aviso é exibida indicando que os usuários locais agora poderão fazer login.

Na próxima vez que você acessar o StorageGRID, a página de login do StorageGRID será exibida e você deverá inserir o nome de usuário e a senha de um usuário local ou federado do StorageGRID.

Desative e reative temporariamente o SSO para um nó de administração do StorageGRID

Você pode não conseguir acessar o Grid Manager se o sistema de autenticação única (SSO) estiver inativo. Nesse caso, você pode desativar e reativar temporariamente o SSO para um Admin Node. Para desativar e depois reativar o SSO, você deve acessar o shell de comando do nó.

Antes de começar

- Você tem "[permissões de acesso específicas](#)".
- Você tem o arquivo `Passwords.txt`.
- Você sabe a senha do usuário raiz local.

Sobre esta tarefa

Após desativar o SSO para um Nó de Administração, você pode fazer login no Grid Manager como o usuário raiz. Para proteger seu sistema StorageGRID, você deve usar o shell de comando do nó para reativar o SSO no Nó de Administração assim que sair.



Desativar o SSO para um nó de administração não afeta as configurações de SSO de outros nós de administração na grade. A caixa de seleção **Ativar SSO** na página de Single Sign-on do Grid Manager permanece marcada e todas as configurações de SSO existentes são mantidas, a menos que você as atualize.

Passos

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

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

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

Uma mensagem indica que o comando se aplica somente a este Admin Node.

3. Confirme que você deseja desativar o SSO.

Uma mensagem indica que o single sign-on está desativado no nó.

4. A partir de um navegador web, acesse o Grid Manager no mesmo Admin Node.

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

5. Faça login com o nome de usuário root e a senha do usuário raiz local.
6. Se você desativou o SSO temporariamente porque precisava corrigir a configuração do SSO:
 - a. Selecione **Configuração > Controle de acesso > Single sign-on**.
 - b. Altere as configurações de SSO incorretas ou desatualizadas.
 - c. Selecione **Salvar**.

Selecionar **Salvar** na página de Single Sign-on reativa automaticamente o SSO para toda a grid.

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 precise executar.
 - b. Selecione **Sair** e feche o Grid Manager.
 - c. Reative o SSO no nó de administração. Você pode executar uma das seguintes etapas:
 - Execute o seguinte comando: `enable-saml`

Uma mensagem indica que o comando se aplica somente a este Admin Node.

Confirme que você deseja ativar o SSO.

Uma mensagem indica que o single sign-on está ativado no nó.

- Reinicie o nó da grade: `reboot`

8. A partir de um navegador web, acesse o Grid Manager no mesmo nó de administração.
9. Confirme que a página de login do StorageGRID aparece e que você precisa inserir suas credenciais de SSO para acessar o Grid Manager.

Use a federação de grid

Saiba mais sobre a federação de grids StorageGRID

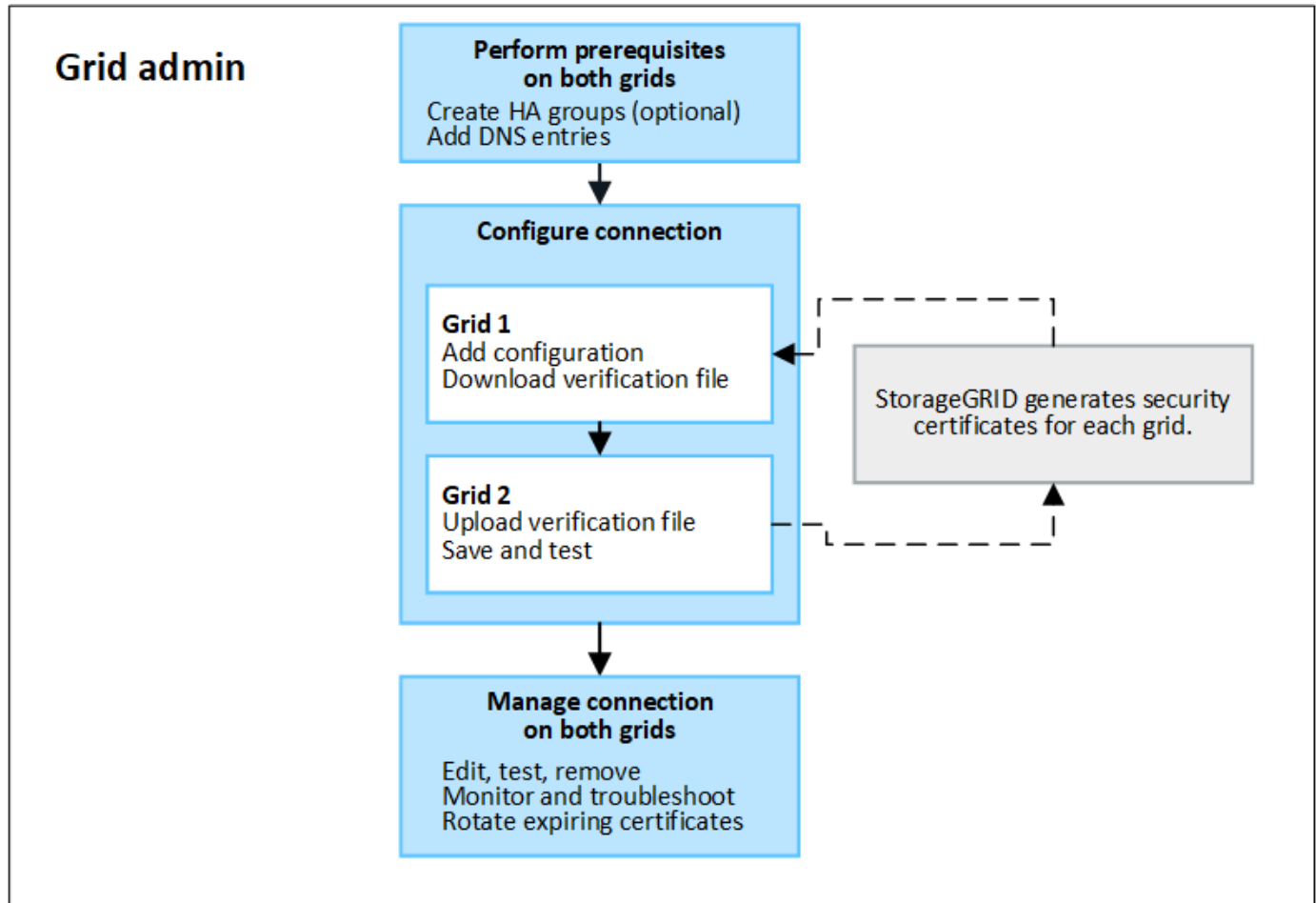
Você pode usar a federação de grids para clonar tenants e replicar seus objetos entre dois sistemas StorageGRID para recuperação de desastres.

O que é uma conexão de federação de grid?

Uma conexão de federação de grid é uma conexão bidirecional, confiável e segura entre Admin Nodes e Gateway Nodes em dois sistemas StorageGRID.

Fluxo de trabalho para federação de grids

O diagrama de fluxo de trabalho resume as etapas para configurar uma conexão de federação de grid entre dois grids.



Considerações e requisitos para conexões de federação de grid

- Os grids usados para a federação de grids devem estar executando versões do StorageGRID que sejam idênticas ou que tenham no máximo uma diferença de uma versão principal entre si.

Para obter detalhes sobre os requisitos de versão, consulte a ["Notas de lançamento"](#). Você precisa fazer login com sua NetApp conta ou criar uma conta para acessar as notas de versão.

- Uma grid pode ter uma ou mais conexões de federação com outras grids. Cada conexão de federação é independente de quaisquer outras conexões. Por exemplo, se a Grid 1 tiver uma conexão com a Grid 2 e uma segunda conexão com a Grid 3, não há nenhuma conexão implícita entre a Grid 2 e a Grid 3.
- As conexões de federação de grids são bidirecionais. Após a conexão ser estabelecida, você pode monitorar e gerenciar a conexão a partir de qualquer um dos grids.
- É necessário que exista pelo menos uma conexão de federação de grade antes de você poder usar ["clone de conta"](#) ou ["replicação entre grids"](#).

Requisitos de rede e endereço IP

- As conexões de federação de Grid podem ocorrer na Grid Network, na Admin Network ou na Client Network.

- Uma conexão de federação de grids conecta um grid a outro grid. A configuração de cada grid especifica um endpoint de federação de grid no outro grid, que consiste em Admin Nodes, Gateway Nodes ou ambos.
- A melhor prática é conectar "[grupos de alta disponibilidade \(HA\)](#)" os nós de Gateway e de Admin em cada grid. Usar grupos de HA ajuda a garantir que as conexões de federação de grid permaneçam online se os nós ficarem indisponíveis. Se a interface ativa em qualquer um dos grupos de HA falhar, a conexão pode usar uma interface de backup.
- Não é recomendável criar uma conexão de federação de grid que utilize o endereço IP de um único nó de administração ou nó de gateway. Se o nó ficar indisponível, a conexão de federação de grid também ficará indisponível.
- "[Replicação entre grades](#)" O armazenamento de objetos requer que os Nós de Armazenamento em cada grid possam acessar os Nós de Administração e de Gateway configurados no outro grid. Para cada grid, confirme que todos os Nós de Armazenamento tenham uma rota de alta largura de banda até os Nós de Administração ou Nós de Gateway usados para a conexão.

Use FQDNs para balancear a conexão

Para um ambiente de produção, utilize nomes de domínio totalmente qualificados (FQDNs) para identificar cada grid na conexão. Em seguida, crie as entradas DNS apropriadas, conforme descrito a seguir:

- O FQDN para Grid 1 mapeado para um ou mais endereços IP virtuais (VIP) para grupos HA em Grid 1 ou para o endereço IP de um ou mais nós Admin ou Gateway em Grid 1.
- O FQDN para Grid 2 mapeado para um ou mais endereços VIP do Grid 2 ou para o endereço IP de um ou mais nós de administração ou gateway no Grid 2.

Ao usar várias entradas DNS, as solicitações para usar a conexão são balanceadas por carga, da seguinte forma:

- As entradas DNS que correspondem aos endereços VIP de vários grupos HA têm sua carga balanceada entre os nós ativos nos grupos HA.
- As entradas DNS que correspondem aos endereços IP de vários Nós de Administração ou Nós de Gateway têm sua carga balanceada entre os nós mapeados.

Requisitos de porta

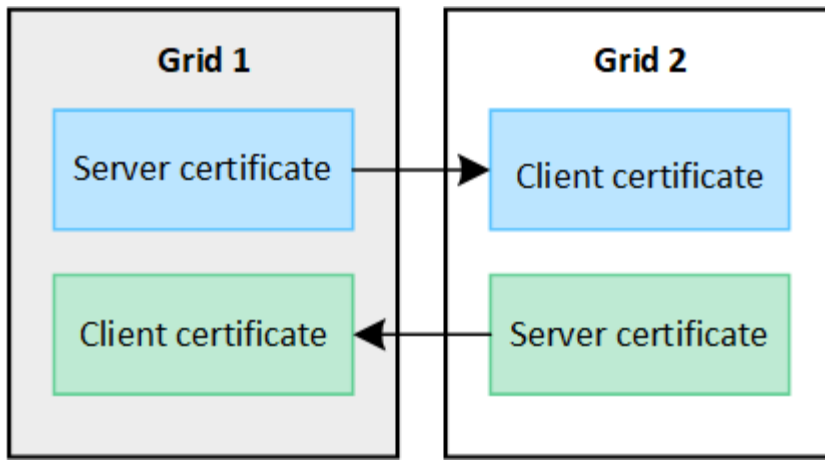
Ao criar uma conexão de federação de grids, você pode especificar qualquer número de porta não utilizado entre 23000 e 23999. Ambos os grids nessa conexão usarão a mesma porta.

Você deve garantir que nenhum nó em nenhuma das grids utilize esta porta para outras conexões.

Requisitos de certificado

Ao configurar uma conexão de federação de grid, StorageGRID gera automaticamente quatro certificados SSL:

- Certificados de servidor e cliente para autenticar e criptografar informações enviadas da grid 1 para a grid 2
- Certificados de servidor e cliente para autenticar e criptografar informações enviadas da grid 2 para a grid 1



Por padrão, os certificados são válidos por 730 dias (2 anos). Quando esses certificados se aproximam da data de expiração, o alerta **Expiração do certificado de federação de grid** lembra você de rotacionar os certificados, o que você pode fazer usando o Grid Manager.



Se os certificados em qualquer uma das extremidades da conexão expirarem, a conexão deixará de funcionar. A replicação de dados ficará pendente até que os certificados sejam atualizados.

Saiba mais

- ["Criar conexões de federação de grid"](#)
- ["Gerenciar conexões de federação de grid"](#)
- ["Solucionar problemas de erros de federação de grid"](#)

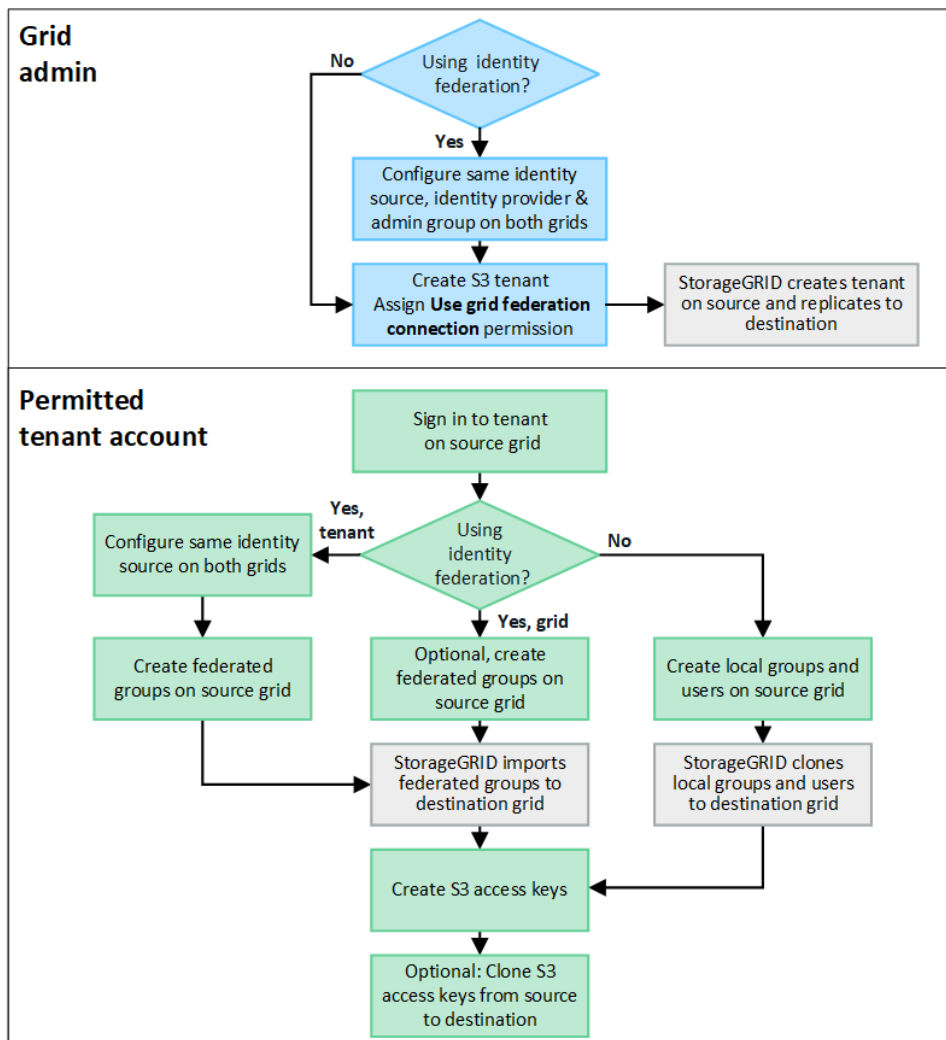
Saiba mais sobre clonagem de contas no StorageGRID

A clonagem de conta é a replicação automática de uma conta de locatário, grupos de locatários, usuários de locatários e, opcionalmente, chaves de acesso S3 entre os sistemas StorageGRID em um ["conexão de federação de grid"](#).

A clonagem de contas é necessária para ["replicação entre grids"](#). Clonar as informações da conta de um sistema StorageGRID de origem para um sistema StorageGRID de destino garante que os usuários e grupos do locatário possam acessar os buckets e objetos correspondentes em qualquer um dos grids.

Fluxo de trabalho para clonagem de conta

O diagrama de fluxo de trabalho mostra as etapas que os administradores da grade e os locatários autorizados executarão para configurar a clonagem de contas. Essas etapas são executadas após a ["A conexão de federação de grid está configurada"](#).



Fluxo de trabalho de administração do Grid

Os passos que os administradores da grade executam dependem de os sistemas StorageGRID na "[conexão de federação de grid](#)" utilizarem autenticação única (SSO) ou federação de identidades.

Configurar SSO para clonagem de conta (opcional)

Se qualquer sistema StorageGRID na conexão de federação de grids usar SSO, ambos os grids devem usar SSO. Antes de criar as contas de locatário para a federação de grids, os administradores dos grids de origem e destino do locatário devem executar estas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grids. Consulte "[Use federação de identidades](#)".
2. Configure o mesmo provedor de identidade SSO (IdP) para ambas as grids. Consulte "[Configure o single sign-on \(SSO\)](#)".
3. "[Crie o mesmo grupo de administradores](#)" em ambas as grades, importando o mesmo grupo federado.

Ao criar o locatário, você selecionará este grupo para ter a permissão inicial de acesso à raiz tanto para as contas de locatário de origem quanto de destino.



Se esse grupo de administradores não existir em ambas as grades antes de você criar o locatário, o locatário não será replicado para o destino.

Configurar federação de identidade em nível de grid para account clone (opcional)

Se qualquer um dos sistemas StorageGRID usar federação de identidade sem SSO, ambos os grids devem usar federação de identidade. Antes de criar as contas de locatário para a federação de grids, os administradores dos grids de origem e destino do locatário devem executar estas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grids. Consulte ["Use federação de identidades"](#).
2. Opcionalmente, se um grupo federado tiver permissão inicial de acesso Root para ambas as contas de locatário de origem e destino, ["crie o mesmo grupo de administradores"](#) em ambos os grids importando o mesmo grupo federado.



Se você atribuir permissão de acesso de usuário raiz a um grupo federado que não existe em ambas as grids, o locatário não será replicado para a grid de destino.

3. Se você não deseja que um grupo federado tenha permissão de acesso inicial de root para ambas as contas, especifique uma senha para o usuário raiz.

Criar conta de locatário S3 permitida

Após configurar opcionalmente o SSO ou a federação de identidades, um administrador de grid executa estas etapas para determinar quais tenants podem replicar objetos de bucket para outros sistemas StorageGRID.

Passos

1. Determine qual grid você deseja que seja o grid de origem do tenant para operações de clonagem de conta.

A grade onde o locatário é originalmente criado é conhecida como a *grade de origem* do locatário. A grade onde o locatário é replicado é conhecida como a *grade de destino* do locatário.

2. Nessa grade, crie uma nova conta de tenant do S3 ou edite uma conta existente.
3. Atribua a permissão **Usar conexão de federação de grid**.
4. Se a conta do locatário for gerenciar seus próprios usuários federados, atribua a permissão **Usar a própria fonte de identidade**.

Se essa permissão for atribuída, tanto as contas de locatário de origem quanto as de destino devem configurar a mesma fonte de identidade antes de criar grupos federados. Os grupos federados adicionados ao locatário de origem não podem ser clonados para o locatário de destino, a menos que ambas as grids usem a mesma fonte de identidade.

5. Selecione uma conexão de federação de grid específica.
6. Salve o novo ou o inquilino modificado.

Quando um novo locatário com a permissão **Usar conexão de federação de grid** é salvo, StorageGRID cria automaticamente uma réplica desse locatário na outra grid, da seguinte forma:

- Ambas as contas de locatário têm o mesmo ID de conta, nome, cota de armazenamento e permissões atribuídas.

- Se você selecionou um grupo federado para ter permissão de acesso de usuário raiz para o locatário, esse grupo é clonado para o locatário de destino.
- Se você selecionou um usuário local com permissão de acesso de usuário raiz para o locatário, esse usuário será clonado para o locatário de destino. No entanto, a senha desse usuário não será clonada.

Para obter detalhes, consulte ["Gerenciar locatários permitidos para federação de grid"](#).

Fluxo de trabalho permitido para conta de tenant

Após um locatário com a permissão **Usar conexão de federação de grid** ser replicado para a grid de destino, as contas de locatário permitidas podem executar estas etapas para clonar grupos de locatários, usuários e chaves de acesso S3.

Passos

1. Faça login na conta do locatário na grid de origem do locatário.
2. Se permitido, configure a federação de identidade nas contas de locatário de origem e de destino.
3. Crie grupos e usuários no locatário de origem.

Quando novos grupos ou usuários são criados no locatário de origem, StorageGRID os clona automaticamente para o locatário de destino, mas não ocorre clonagem do destino de volta para a origem.

4. Crie chaves de acesso S3.
5. Opcionalmente, clone as chaves de acesso S3 do locatário de origem para o locatário de destino.

Para obter detalhes sobre o fluxo de trabalho permitido para contas de locatários e para saber como grupos, usuários e chaves de acesso do S3 são clonados, consulte ["Clonar grupos de tenants e usuários"](#) e ["Clonar chaves de acesso S3 usando a API"](#).

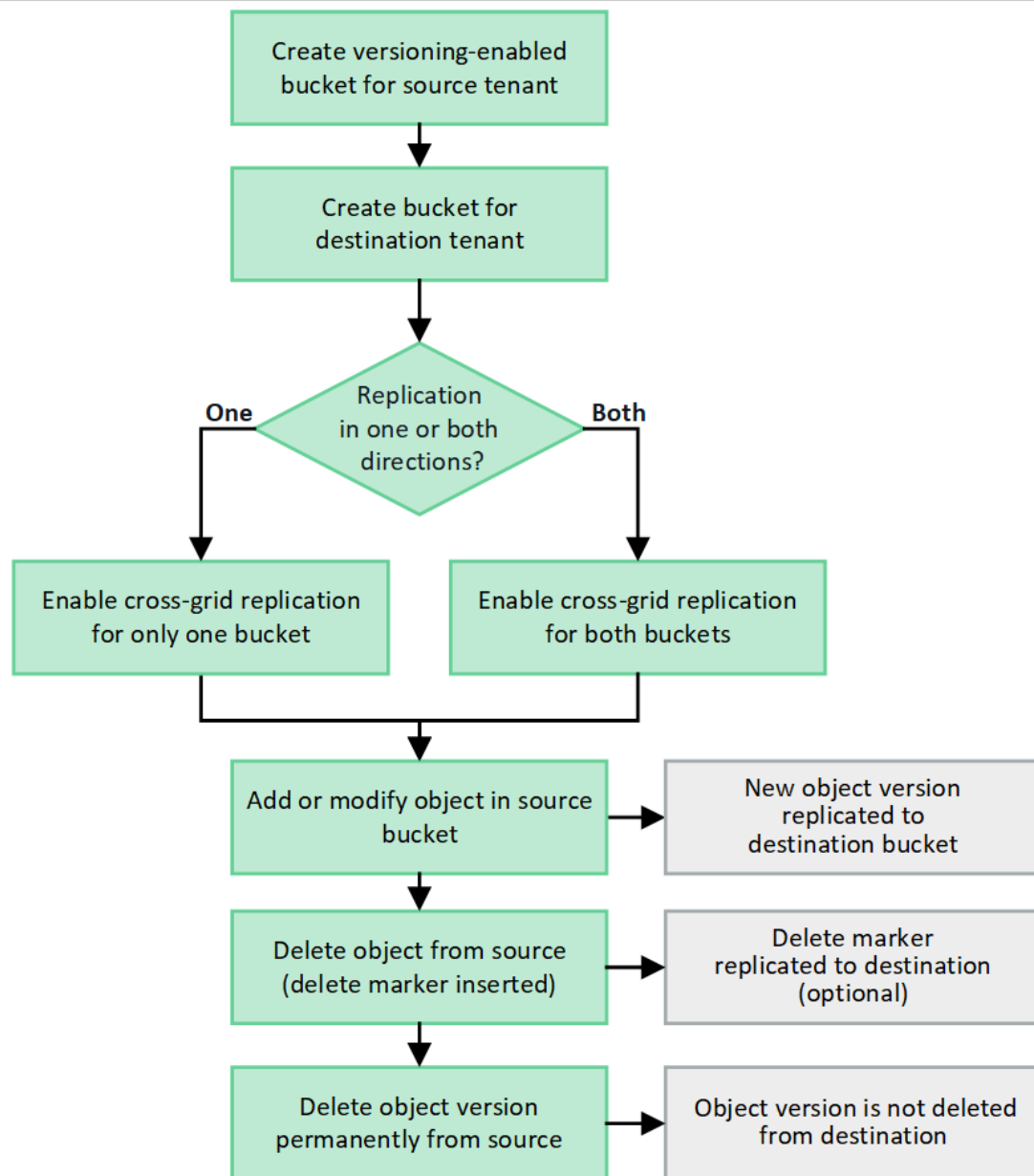
Saiba mais sobre replicação entre grids no StorageGRID

A replicação entre grades é a replicação automática de objetos entre buckets S3 selecionados em dois sistemas StorageGRID conectados em uma ["conexão de federação de grid"](#). ["Clonagem de conta"](#) é necessário para a replicação entre grades.

Fluxo de trabalho para replicação entre grids

O diagrama de fluxo de trabalho resume as etapas para configurar a replicação entre buckets em duas grids.

Tenant user



Requisitos para replicação entre grids

Se uma conta de locatário tiver a permissão **Usar conexão de federação de grade** para usar uma ou mais "conexões de federação de grid" grades, um usuário de locatário com permissão de acesso root pode criar buckets nas contas de locatário correspondentes em cada grade. Esses buckets:

- Podem ter nomes diferentes entre si
- Pode ter regiões diferentes
- É necessário ter o versionamento ativado
- Deve estar vazio

Após a criação de ambos os buckets, a replicação entre grades pode ser configurada para um ou ambos os buckets.

Saiba mais

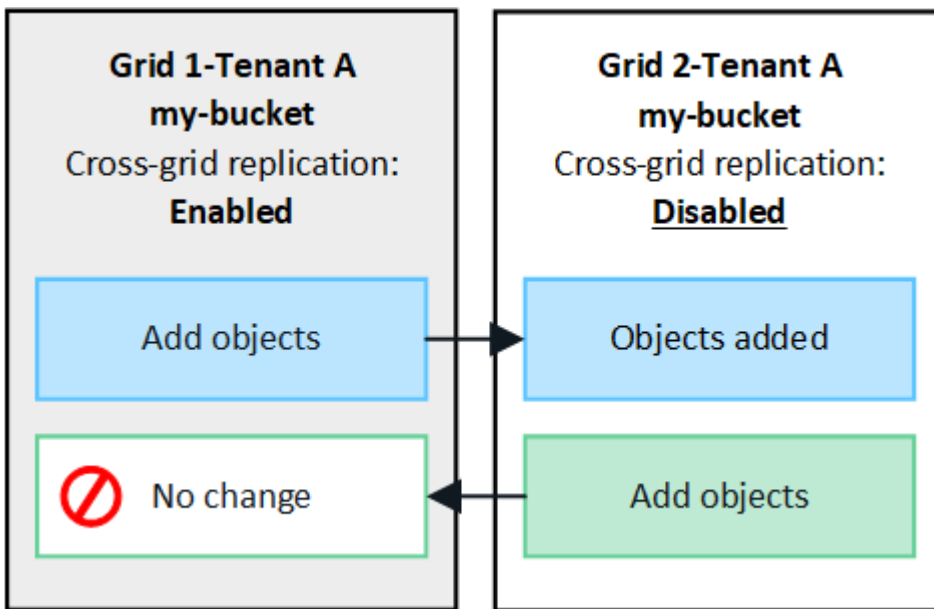
"Gerencie a replicação entre grades"

Como funciona a replicação entre grades

Você pode configurar a replicação entre grades para ocorrer em uma direção ou em ambas as direções.

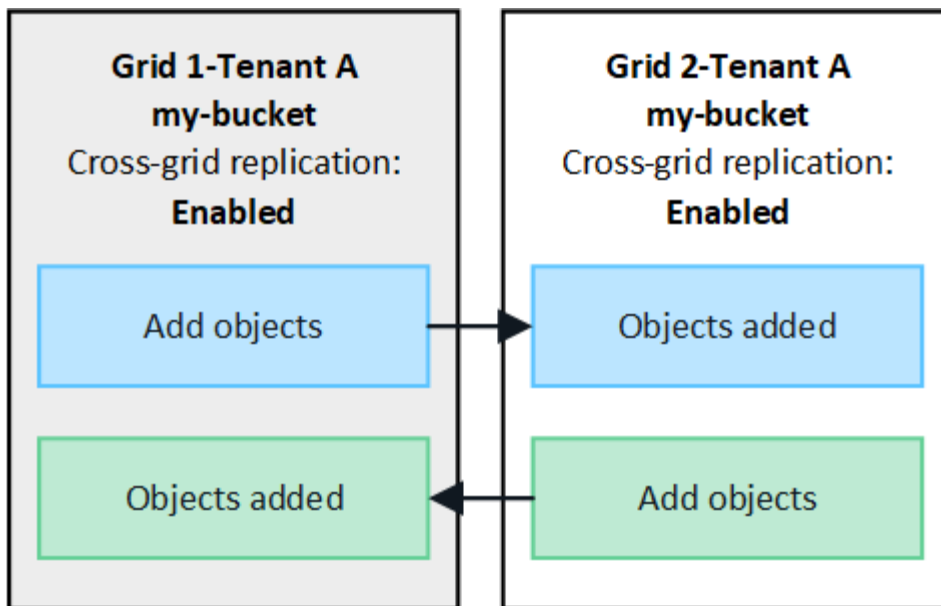
Replicação em uma direção

Se você habilitar a replicação entre grades para um bucket em apenas uma grade, os objetos adicionados a esse bucket (o bucket de origem) serão replicados para o bucket correspondente na outra grade (o bucket de destino). No entanto, os objetos adicionados ao bucket de destino não são replicados de volta para a origem. Na figura, a replicação entre grades está habilitada `my-bucket` da Grid 1 para a Grid 2, mas não está habilitada na direção oposta.



Replicação em ambas as direções

Se você habilitar a replicação entre grades para o mesmo bucket em ambas as grades, os objetos adicionados a qualquer um dos buckets serão replicados para a outra grade. Na figura, a replicação entre grades está habilitada para `my-bucket` em ambas as direções.



O que acontece quando objetos são ingeridos?

Quando um cliente S3 adiciona um objeto a um bucket com replicação entre grades habilitada, ocorre o seguinte:

1. StorageGRID replica automaticamente o objeto do bucket de origem para o bucket de destino. O tempo necessário para executar essa operação de replicação em segundo plano depende de vários fatores, incluindo o número de outras operações de replicação pendentes.

O cliente S3 pode verificar o status de replicação de um objeto emitindo uma solicitação `GetObject` ou `HeadObject`. A resposta inclui um cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que possui um dos seguintes valores:

Grid	Status de replicação
Fonte	• CONCLUÍDO: A replicação foi bem-sucedida para todas as conexões do grid. • PENDENTE: O objeto ainda não foi replicado para pelo menos uma conexão de grid. • FALHA: A replicação não está pendente para nenhuma conexão de grid e pelo menos uma falhou com uma falha permanente. Você deve resolver o erro.
Destino	RÉPLICA: O objeto foi replicado da grid de origem.



StorageGRID não suporta o `x-amz-replication-status` cabeçalho.

2. StorageGRID utiliza as políticas ILM ativas de cada grid para gerenciar os objetos, da mesma forma que faria com qualquer outro objeto. Por exemplo, o Objeto A no Grid 1 pode ser armazenado como duas cópias replicadas e mantido indefinidamente, enquanto a cópia do Objeto A que foi replicada para o Grid 2 pode ser armazenada usando codificação de apagamento 2+1 e excluída após três anos.

O que acontece quando os objetos são excluídos?

Conforme descrito em ["Excluir fluxo de dados"](#), StorageGRID pode excluir um objeto por qualquer um destes motivos:

- O cliente S3 emite uma solicitação de exclusão.
- Um usuário do Tenant Manager seleciona a opção ["Excluir objetos no bucket"](#) para remover todos os objetos de um bucket.
- O bucket possui uma configuração de ciclo de vida, que expira.
- O último período de tempo na regra ILM para o objeto termina e não há mais posicionamentos especificados.

Quando StorageGRID exclui um objeto devido a uma operação de exclusão de objetos no bucket, expiração do ciclo de vida do bucket ou expiração do posicionamento ILM, o objeto replicado nunca é excluído do outro grid em uma conexão de federação de grids. No entanto, marcadores de exclusão adicionados ao bucket de origem por exclusões do cliente S3 podem, opcionalmente, ser replicados para o bucket de destino.

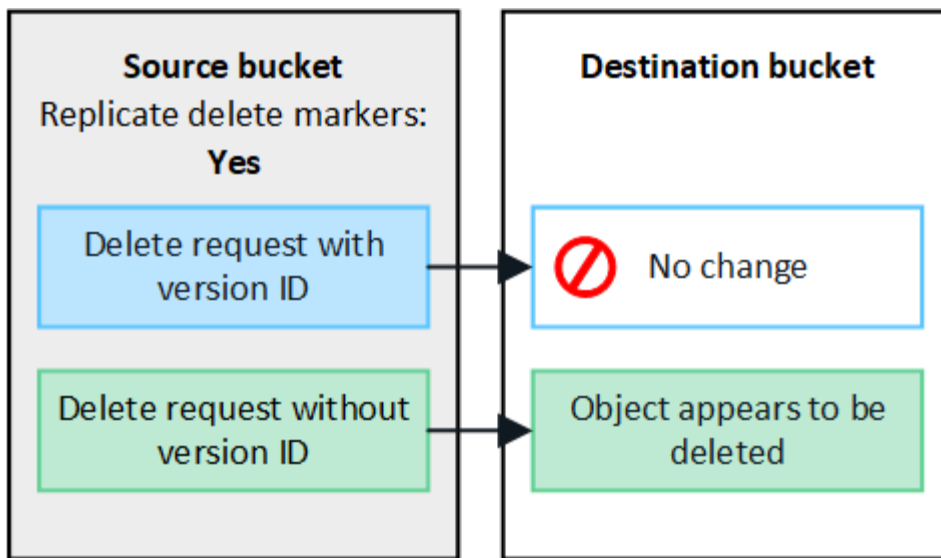
Para entender o que acontece quando um cliente S3 exclui objetos de um bucket com replicação entre grades habilitada, revise como os clientes S3 excluem objetos de buckets com versionamento habilitado, conforme descrito a seguir:

- Se um cliente S3 emitir uma solicitação de exclusão que inclua um ID de versão, essa versão do objeto será removida permanentemente. Nenhum marcador de exclusão é adicionado ao bucket.
- Se um cliente S3 emitir uma solicitação de exclusão que não inclua um ID de versão, StorageGRID não exclui nenhuma versão do objeto. Em vez disso, ele adiciona um marcador de exclusão ao bucket. O marcador de exclusão faz com que o StorageGRID aja como se o objeto tivesse sido excluído:
 - Uma solicitação `GetObject` sem um ID de versão falha com `404 No Object Found`
 - Uma solicitação `GetObject` com um ID de versão válido é bem-sucedida e retorna a versão do objeto solicitada.

Quando um cliente S3 exclui um objeto de um bucket que possui replicação entre grades habilitada, StorageGRID determina se deve replicar a solicitação de exclusão para o destino, da seguinte forma:

- Se a solicitação de exclusão incluir um ID de versão, essa versão do objeto será removida permanentemente da grid de origem. No entanto, StorageGRID não replica solicitações de exclusão que incluem um ID de versão, portanto, a mesma versão do objeto não é excluída do destino.
- Se a solicitação de exclusão não incluir um ID de versão, StorageGRID pode, opcionalmente, replicar o marcador de exclusão, dependendo de como a replicação entre grids está configurada para o bucket:
 - Se você optar por replicar os marcadores de exclusão (padrão), um marcador de exclusão será adicionado ao bucket de origem e replicado para o bucket de destino. Na prática, o objeto parecerá ter sido excluído em ambas as grids.
 - Se você optar por não replicar os marcadores de exclusão, um marcador de exclusão será adicionado ao bucket de origem, mas não será replicado para o bucket de destino. Na prática, os objetos excluídos na grid de origem não serão excluídos na grid de destino.

Na figura, **Replicar marcadores de exclusão** foi definido como **Sim** quando ["A replicação entre grades foi ativada"](#). As solicitações de exclusão para o bucket de origem que incluem um ID de versão não excluem objetos do bucket de destino. As solicitações de exclusão para o bucket de origem que não incluem um ID de versão parecem excluir objetos no bucket de destino.



Se você deseja manter as exclusões de objetos sincronizadas entre as grades, crie "[Configurações de ciclo de vida S3](#)" correspondentes para os buckets em ambas as grades.

Como os objetos criptografados são replicados

Ao usar a replicação entre grades para replicar objetos entre grades, você pode criptografar objetos individuais, usar a criptografia padrão do bucket ou configurar a criptografia em toda a grade. Você pode adicionar, modificar ou remover as configurações de criptografia padrão do bucket ou da grade antes ou depois de habilitar a replicação entre grades para um bucket.

Para criptografar objetos individuais, você pode usar SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID) ao adicionar os objetos ao bucket de origem. Use o `x-amz-server-side-encryption` cabeçalho da solicitação e especifique `AES256`. Consulte "[Use criptografia do lado do servidor](#)".



O uso de SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente) não é compatível com a replicação entre grids. A operação de ingestão falhará.

Para usar a criptografia padrão para um bucket, use uma solicitação `PutBucketEncryption` e defina o parâmetro `SSEAlgorithm` como `AES256`. A criptografia no nível do bucket se aplica a quaisquer objetos ingeridos sem o cabeçalho `x-amz-server-side-encryption` da solicitação. Consulte "[Operações em buckets](#)".

Para usar a criptografia em nível de grid, defina a opção **Criptografia de objeto armazenado** como **AES-256**. A criptografia em nível de grid se aplica a quaisquer objetos que não estejam criptografados no nível do bucket ou que sejam ingeridos sem o cabeçalho de solicitação `x-amz-server-side-encryption`. Consulte "[Configurar as opções de rede e de objeto](#)".



O SSE não suporta AES-128. Se a opção **Criptografia de objeto armazenado** estiver habilitada para o grid de origem usando a opção **AES-128**, o uso do algoritmo AES-128 não é propagado para o objeto replicado. Em vez disso, o objeto replicado usa a configuração de criptografia padrão do bucket ou do grid de destino, se disponível.

Ao determinar como criptografar objetos de origem, StorageGRID aplica estas regras:

1. Use o ``x-amz-server-side-encryption`` cabeçalho de ingestão, se presente.

2. Caso não haja um cabeçalho de ingestão, utilize a configuração de criptografia padrão do bucket, se configurada.
3. Se uma configuração de bucket não estiver definida, use a configuração de criptografia de toda a grade, se estiver configurada.
4. Se não houver uma configuração para toda a grade, não criptografe o objeto de origem.

Ao determinar como criptografar objetos replicados, StorageGRID aplica estas regras nesta ordem:

1. Use a mesma criptografia do objeto de origem, a menos que esse objeto use criptografia AES-128.
2. Se o objeto de origem não estiver criptografado ou usar AES-128, use a configuração de criptografia padrão do bucket de destino, se configurada.
3. Se o bucket de destino não tiver uma configuração de criptografia, use a configuração de criptografia de toda a grid de destino, se configurada.
4. Se não houver uma configuração para toda a grid, não criptografe o objeto de destino.

Replicação entre grades com S3 Object Lock

Você pode configurar a replicação entre grids entre buckets do StorageGRID com o S3 Object Lock ativado nas seguintes circunstâncias.

Quando o S3 Object Lock no bucket de origem está...	E o S3 Object Lock no bucket de destino é...
Habilitado	Habilitado
Desabilitado	Habilitado

Quando o S3 Object Lock no bucket de origem estiver ativado:

- Os objetos são bloqueados com configurações de retenção no destino nesta ordem:

- a. Os valores do cabeçalho de retenção do objeto de origem para:

`x-amz-object-lock-mode`

`x-amz-object-lock-retain-until-date`

- b. A retenção padrão do bucket de origem, se definida.
- c. A retenção padrão do bucket de destino, se definida.

A configuração de retenção padrão do bucket de destino não substitui as configurações de retenção replicadas do objeto de origem.

- Você pode definir o status de guarda legal para o objeto de destino usando `x-amz-object-lock-legal-hold` ao fazer o upload do objeto.
- Ocorre um erro se o locatário ou bucket de destino não for compatível com as configurações de S3 Object Lock do objeto de origem. Consulte ["Alertas e erros de replicação entre grids."](#)

Quando o bloqueio de objeto S3 no bucket de origem está desativado:

- Você pode configurar a retenção padrão no bucket de destino para aplicar as configurações de retenção do S3 Object Lock ao objeto de destino.
- O objeto de destino não pode definir um status de guarda legal.

PutObjectTagging e DeleteObjectTagging não são suportados

PutObjectTagging e DeleteObjectTagging solicitações não são suportadas para objetos em buckets que tenham replicação entre grades ativada.

Se um cliente S3 emitir uma solicitação PutObjectTagging ou DeleteObjectTagging, 501 Not Implemented é retornado. A mensagem é Put (Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured.

PutObjectRetention e PutObjectLegalHold não são suportados

PutObjectRetention e PutObjectLegalHold solicitações não são totalmente compatíveis com objetos em buckets que têm replicação entre grids ativada.

Se um cliente S3 emitir uma solicitação PutObjectRetention ou PutObjectLegalHold, as configurações do objeto de origem serão modificadas, mas as alterações não serão aplicadas ao destino.

Como os objetos segmentados são replicados

O tamanho máximo do segmento da grid de origem se aplica aos objetos replicados para a grid de destino. Quando os objetos são replicados para outra grid, a configuração **Tamanho Máximo do Segmento (Configuração > Sistema > Opções de armazenamento)** da grid de origem é usada em ambas as grids. Por exemplo, suponha que o tamanho máximo do segmento para a grid de origem seja 1 GB, enquanto o tamanho máximo do segmento da grid de destino seja 50 MB. Se você ingerir um objeto de 2 GB na grid de origem, esse objeto será salvo como dois segmentos de 1 GB. Ele também é replicado para a grid de destino como dois segmentos de 1 GB, mesmo que o tamanho máximo do segmento dessa grid seja 50 MB.

Compare a replicação entre grades e a replicação CloudMirror no StorageGRID

Ao começar a usar a federação de grade, revise as semelhanças e diferenças entre ["replicação entre grids"](#) e ["Serviço de replicação StorageGRID CloudMirror"](#).



Não é possível usar CloudMirror em um bucket replicado por replicação entre grades, e vice-versa.

	Replicação entre grades	CloudMirror serviço de replicação
Qual é o objetivo principal?	Um sistema StorageGRID funciona como um sistema de recuperação de desastres. Os objetos em um bucket podem ser replicados entre os grids em uma ou ambas as direções.	Permite que um locatário replique automaticamente objetos de um bucket no StorageGRID (origem) para um bucket S3 externo (destino). CloudMirror replication cria uma cópia independente de um objeto em uma infraestrutura S3 independente. Essa cópia independente não é usada como backup, mas geralmente é processada posteriormente na nuvem.

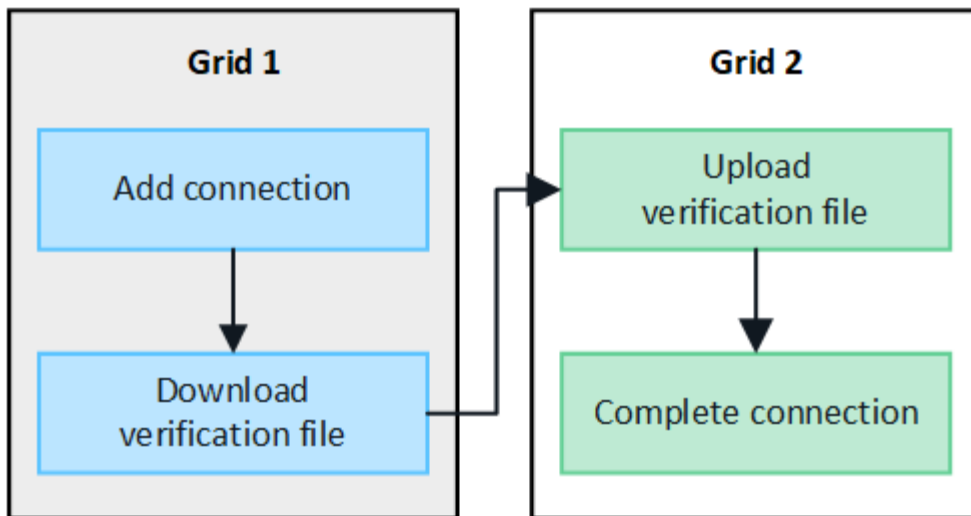
	Replicação entre grades	CloudMirror serviço de replicação
Como é configurado?	1. Configurar uma conexão de federação de grids entre dois grids. 2. Adicione novas contas de locatário, que são clonadas automaticamente para a outra grid. 3. Adicione novos grupos de locatários e usuários, que também são clonados. 4. Crie buckets correspondentes em cada grid e habilite a replicação entre grids para ocorrer em uma ou ambas as direções.	1. Um usuário locatário configura a replicação CloudMirror definindo um endpoint CloudMirror (endereço IP, credenciais e assim por diante) usando o Tenant Manager ou a S3 API. 2. Qualquer bucket pertencente a essa conta de locatário pode ser configurado para apontar para o endpoint CloudMirror.
Quem é responsável por configurá-lo?	• Um administrador de grid configura a conexão e os locatários. • Os usuários locatários configuram os grupos, usuários, chaves e buckets.	Normalmente, um usuário locatário.
Qual é o destino?	Um bucket S3 correspondente e idêntico no outro sistema StorageGRID na conexão de federação de grid.	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3). • Google Cloud Platform (GCP)
O versionamento de objetos é necessário?	Sim, tanto o bucket de origem quanto o de destino devem ter o versionamento de objetos ativado.	Não, a replicação CloudMirror suporta qualquer combinação de buckets não versionados e versionados, tanto na origem quanto no destino.
O que faz com que os objetos sejam movidos para o destino?	Os objetos são replicados automaticamente quando são adicionados a um bucket que tem a replicação entre grades habilitada.	Os objetos são replicados automaticamente quando são adicionados a um bucket que foi configurado com um endpoint CloudMirror. Os objetos que já existiam no bucket de origem antes de o bucket ser configurado com o endpoint CloudMirror não são replicados, a menos que sejam modificados.
Como os objetos são replicados?	A replicação entre grids cria objetos versionados e replica o ID da versão do bucket de origem para o bucket de destino. Isso permite que a ordem das versões seja mantida em ambos os grids.	CloudMirror replication não exige buckets com controle de versão habilitado, então o CloudMirror só pode manter a ordem de uma chave dentro de um site. Não há garantias de que a ordem será mantida para solicitações a um objeto em sites diferentes.
E se um objeto não puder ser replicado?	O objeto é enfileirado para replicação, sujeito aos limites de armazenamento de metadados.	O objeto é enfileirado para replicação, sujeito aos limites dos serviços da plataforma (veja "Recomendações para o uso de serviços de plataforma").

	Replicação entre grades	CloudMirror serviço de replicação
Os metadados do sistema do objeto são replicados?	Sim, quando um objeto é replicado para a outra grid, seus metadados do sistema também são replicados. Os metadados serão idênticos em ambas as grids.	Não, quando um objeto é replicado para o bucket externo, seus metadados do sistema são atualizados. Os metadados podem variar entre locais, dependendo do horário de ingestão e do comportamento da infraestrutura S3 independente.
Como os objetos são recuperados?	Os aplicativos podem recuperar ou ler objetos fazendo uma solicitação ao bucket em qualquer um dos grids.	Os aplicativos podem recuperar ou ler objetos fazendo uma solicitação ao StorageGRID ou ao destino S3. Por exemplo, suponha que você use a replicação CloudMirror para espelhar objetos em uma organização parceira. O parceiro pode usar seus próprios aplicativos para ler ou atualizar objetos diretamente do destino S3. Não é necessário usar o StorageGRID.
O que acontece se um objeto for excluído?	• As solicitações de exclusão que incluem um ID de versão nunca são replicadas para o grid de destino. • As solicitações de exclusão que não incluem um ID de versão adicionam um marcador de exclusão ao bucket de origem, que pode opcionalmente ser replicado para o grid de destino. • Se a replicação entre grades estiver configurada apenas em uma direção, os objetos no bucket de destino poderão ser excluídos sem afetar a origem.	Os resultados podem variar dependendo do estado de versionamento dos buckets de origem e destino (que não precisam ser iguais): • Se ambos os buckets estiverem versionados, uma solicitação de exclusão adicionará um marcador de exclusão em ambos os locais. • Se apenas o bucket de origem estiver versionado, uma solicitação de exclusão adicionará um marcador de exclusão à origem, mas não ao destino. • Se nenhum dos buckets estiver versionado, uma solicitação de exclusão excluirá o objeto da origem, mas não do destino. Da mesma forma, os objetos no bucket de destino podem ser excluídos sem afetar a origem.

Criar conexões de federação de grids StorageGRID

Você pode criar uma conexão de federação de grid entre dois sistemas StorageGRID se desejar clonar detalhes de locatários e replicar dados de objetos.

Conforme ilustrado na figura, a criação de uma conexão de federação de grades inclui etapas em ambas as grades. Você adiciona a conexão em uma grade e a conclui na outra. Você pode começar por qualquer uma das grades.



Antes de começar

- Você revisou o "[Considerações e requisitos](#)" para configurar conexões de federação de grid.
- Se você planeja usar nomes de domínio totalmente qualificados (FQDNs) para cada grid em vez de endereços IP ou VIP, você sabe quais nomes usar e confirmou que o servidor DNS de cada grid possui as entradas apropriadas.
- Você está usando um "[navegador web compatível](#)".
- Você possui permissão de acesso Root e a senha de provisionamento para ambas as grids.

Adicionar conexão

Execute estas etapas em qualquer um dos dois sistemas StorageGRID.

Passos

1. Faça login no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **Configuração > Sistema > Grid federation**.
3. Selecione **Adicionar conexão**.
4. Insira os detalhes da conexão.

Campo	Descrição
Nome da conexão	Um nome único para ajudar você a reconhecer essa conexão, por exemplo, "Grid 1-Grid 2".
FQDN ou IP para esta grid	Uma das seguintes opções: • O FQDN da grid na qual você está conectado no momento • Um endereço VIP de um grupo HA neste grid • Um endereço IP de um Nó de Administração ou Nó de Gateway neste grid. O IP pode estar em qualquer rede que o grid de destino possa alcançar.

Campo	Descrição
Porta	A porta que você deseja usar para esta conexão. Você pode inserir qualquer número de porta não utilizado entre 23000 e 23999. Ambas as grids nesta conexão usarão a mesma porta. Você deve garantir que nenhum nó em nenhuma das grids use esta porta para outras conexões.
Dias de validade do certificado para este grid	O número de dias que você deseja que os certificados de segurança para esta grid na conexão sejam válidos. O valor padrão é 730 dias (2 anos), mas você pode inserir qualquer valor de 1 a 762 dias. StorageGRID gera automaticamente certificados de cliente e servidor para cada grid quando você salva a conexão.
Senha de provisionamento para esta grid	A senha de provisionamento para o grid no qual você está conectado.
FQDN ou IP para a outra grid	Uma das seguintes opções: • O FQDN do grid ao qual você deseja se conectar • Um endereço VIP de um grupo HA em outra grid • Um endereço IP de um Nó de Administração ou Nó de Gateway na outra grid. O IP pode estar em qualquer rede que a grid de origem possa alcançar.

5. Selecione **Salvar e continuar**.

6. Na etapa "Baixar arquivo de verificação", selecione "Baixar arquivo de verificação".

Após a conexão ser concluída na outra grid, você não poderá mais baixar o arquivo de verificação de nenhuma das grids.

7. Localize o arquivo baixado (*connection-name.grid-federation*) e salve-o em um local seguro.



Este arquivo contém segredos (mascarados como *) e outros detalhes sensíveis e deve ser armazenado e transmitido com segurança.

8. Selecione **Fechar** para retornar à página de federação da Grid.

9. Confirme que a nova conexão está sendo exibida e que o seu **Status de conexão** é **Aguardando conexão**.

10. Forneça o arquivo *connection-name.grid-federation* ao administrador da outra grid.

Conexão completa

Execute estas etapas no sistema StorageGRID ao qual você está se conectando (a outra grid).

Passos

1. Faça login no Grid Manager a partir do nó de administração principal.

2. Selecione **Configuração > Sistema > Grid federation**.
3. Selecione **Carregar arquivo de verificação** para acessar a página de Upload.
4. Selecione **Carregar arquivo de verificação**. Em seguida, localize e selecione o arquivo baixado na primeira grade (`connection-name.grid-federation`).

Os detalhes da conexão são exibidos.

5. Opcionalmente, insira um número diferente de dias de validade para os certificados de segurança desta grid. A entrada **Dias de validade do certificado** assume por padrão o valor que você inseriu na primeira grid, mas cada grid pode usar datas de expiração diferentes.

Em geral, utilize o mesmo número de dias para os certificados em ambos os lados da conexão.



Se os certificados em qualquer uma das extremidades da conexão expirarem, a conexão deixará de funcionar e as replicações ficarão pendentes até que os certificados sejam atualizados.

6. Insira a senha de provisionamento do grid no qual você está conectado.
7. Selecione **Salvar e testar**.

Os certificados são gerados e a conexão é testada. Se a conexão for válida, uma mensagem de sucesso é exibida e a nova conexão é listada na página de Grid federation. O **Connection status** será **Connected**.

Se aparecer uma mensagem de erro, resolva os problemas. Consulte "[Solucionar problemas de erros de federação de grid](#)".

8. Acesse a página de federação do Grid no primeiro grid e atualize o navegador. Confirme que o **Status da conexão** agora é **Conectado**.
9. Após a conexão ser estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

Ao editar esta conexão, um novo arquivo de verificação será criado. O arquivo original não pode ser reutilizado.

Depois que você terminar

- Analise as considerações para "[gerenciando locatários permitidos](#)".
- "[Crie uma ou mais novas contas de locatário](#)", atribua a permissão **Usar conexão de federação de grid** e selecione a nova conexão.
- "[Gerenciar a conexão](#)" conforme necessário. Você pode editar os valores de conexão, testar uma conexão, rotacionar os certificados de conexão ou remover uma conexão.
- "[Monitore a conexão](#)" como parte das suas atividades normais de monitoramento do StorageGRID.
- "[Solucione problemas de conexão](#)", incluindo a resolução de quaisquer alertas e erros relacionados à clonagem de contas e à replicação entre grids.

Gerenciar conexões de federação de grids do StorageGRID

O gerenciamento de conexões de federação de grid entre StorageGRID systems inclui editar detalhes da conexão, rotacionar os certificados, remover permissões de tenant e remover conexões não utilizadas.

Antes de começar

- Você está conectado ao Grid Manager em qualquer uma das grids usando um ["navegador web compatível"](#).
- Você tem ["Permissão de acesso root"](#) para a grid na qual você está conectado.

Editar uma conexão de federação de grid

Você pode editar uma conexão de federação de grids fazendo login no nó de administração principal em qualquer um dos grids da conexão. Depois de fazer alterações no primeiro grid, você deve baixar um novo arquivo de verificação e carregá-lo no outro grid.



Enquanto a conexão estiver sendo editada, as solicitações de clonagem de conta ou replicação entre grades continuarão usando as configurações de conexão existentes. Quaisquer edições que você fizer na primeira grade serão salvas localmente, mas não serão usadas até que tenham sido carregadas na segunda grade, salvas e testadas.

Comece a editar a conexão

Passos

1. Faça login no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **Nós** e confirme se todos os outros Admin Nodes em seu sistema estão online.



Ao editar uma conexão de federação de grid, StorageGRID tenta salvar um arquivo de "configuração candidata" em todos os nós de administração do primeiro grid. Se esse arquivo não puder ser salvo em todos os nós de administração, uma mensagem de aviso aparece ao selecionar **Salvar e testar**.

3. Selecione **Configuração > Sistema > Grid federation**.
4. Edite os detalhes da conexão usando o menu **Ações** na página de federação do Grid ou na página de detalhes de uma conexão específica. Veja ["Criar conexões de federação de grid"](#) o que inserir.

Menu de ações

- a. Selecione o botão de opção para a conexão.
- b. Selecione **Ações > Editar**.
- c. Insira as novas informações.

Página de detalhes

- a. Selecione o nome da conexão para exibir seus detalhes.
- b. Selecione **Editar**.
- c. Insira as novas informações.

5. Insira a senha de provisionamento da grid na qual você está conectado.
6. Selecione **Salvar e continuar**.

Os novos valores são salvos, mas não serão aplicados à conexão até que você carregue o novo arquivo de verificação na outra grid.

7. Selecione **Download verification file**.

Para baixar este arquivo posteriormente, acesse a página de detalhes da conexão.

8. Localize o arquivo baixado (*connection-name.grid-federation*) e salve-o em um local seguro.



O arquivo de verificação contém segredos e deve ser armazenado e transmitido com segurança.

9. Selecione **Fechar** para retornar à página de federação da Grid.

10. Confirme se o **Status da conexão** está como **Edição pendente**.



Se o status da conexão era diferente de **Conectado** quando você começou a editar a conexão, ele não mudará para **Edição pendente**.

11. Forneça o arquivo *connection-name.grid-federation* ao administrador da outra grid.

Finalize a edição da conexão

Finalize a edição da conexão carregando o arquivo de verificação na outra grid.

Passos

1. Faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **Configuração > Sistema > Grid federation**.
3. Selecione **Carregar arquivo de verificação** para acessar a página de upload.
4. Selecione **Carregar arquivo de verificação**. Em seguida, localize e selecione o arquivo que foi baixado do primeiro grid.
5. Insira a senha de provisionamento do grid no qual você está conectado.
6. Selecione **Salvar e testar**.

Se a conexão puder ser estabelecida usando os valores editados, uma mensagem de sucesso será exibida. Caso contrário, uma mensagem de erro será exibida. Analise a mensagem e resolva quaisquer problemas.

7. Feche o assistente para retornar à página de federação do Grid.
8. Confirme se o **Status da conexão** é **Conectado**.
9. Acesse a página de federação do Grid no primeiro grid e atualize o navegador. Confirme que o **Status da conexão** agora é **Conectado**.
10. Após a conexão ser estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

Testar uma conexão de federação de grid

Passos

1. Faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **Configuração > Sistema > Grid federation**.
3. Teste a conexão usando o menu **Actions** na página de Grid federation ou na página de detalhes de uma conexão específica.

Menu de ações

- a. Selecione o botão de opção para a conexão.
- b. Selecione **Ações > Testar**.

Página de detalhes

- a. Selecione o nome da conexão para exibir seus detalhes.
- b. Selecione **Test connection**.

4. Verifique o status da conexão:

Status da conexão	Descrição
Conectado	Ambas as grids estão conectadas e comunicando-se normalmente.
Erro	A conexão está em estado de erro. Por exemplo, um certificado expirou ou um valor de configuração não é mais válido.
Edição pendente	Você editou a conexão nesta grid, mas ela ainda está usando a configuração existente. Para concluir a edição, carregue o novo arquivo de verificação na outra grid.
Aguardando conexão	Você configurou a conexão nesta grid, mas a conexão ainda não foi concluída na outra grid. Baixe o arquivo de verificação desta grid e carregue-o na outra grid.
Desconhecido	A conexão está em um estado desconhecido, possivelmente devido a um problema de rede ou a um nó offline.

5. Se o status da conexão for **Erro**, resolva quaisquer problemas. Em seguida, selecione **Testar conexão** novamente para confirmar que o problema foi resolvido.

Rotacionar certificados de conexão

Cada conexão de federação de grids utiliza quatro certificados SSL gerados automaticamente para proteger a conexão. Quando os dois certificados de cada grid estiverem próximos da data de expiração, o alerta **Expiração do certificado de federação de grids** lembra você de rotacionar os certificados.



Se os certificados em qualquer uma das extremidades da conexão expirarem, a conexão deixará de funcionar e as replicações ficarão pendentes até que os certificados sejam atualizados.

Passos

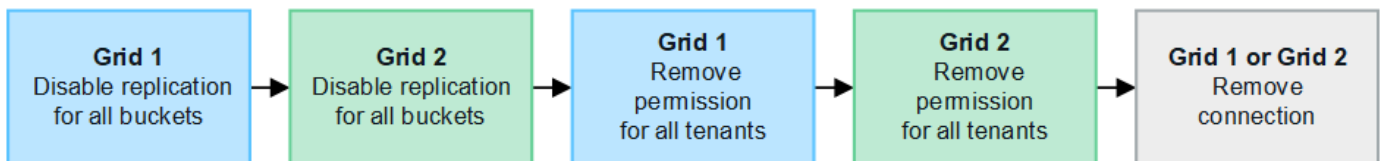
1. Faça login no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **Configuração > Sistema > Grid federation**.
3. Em qualquer uma das abas da página de federação do Grid, selecione o nome da conexão para exibir seus detalhes.

4. Selecione a guia **Certificados**.
5. Selecione **Girar certificados**.
6. Especifique por quantos dias os novos certificados devem ser válidos.
7. Insira a senha de provisionamento da grid na qual você está conectado.
8. Selecione **Girar certificados**.
9. Se necessário, repita estas etapas na outra grid da conexão.

Em geral, utilize o mesmo número de dias para os certificados em ambos os lados da conexão.

Remover uma conexão de federação de grid

Você pode remover uma conexão de federação de grid de qualquer um dos grids na conexão. Como mostrado na figura, você deve executar etapas prévias em ambos os grids para confirmar que a conexão não está sendo usada por nenhum tenant em nenhum dos grids.



Antes de remover uma conexão, observe o seguinte:

- Remover uma conexão não exclui nenhum item que já tenha sido copiado entre grids. Por exemplo, usuários, grupos e objetos do tenant que existem em ambos os grids não são excluídos de nenhum dos grids quando a permissão do tenant é removida. Se você quiser excluir esses itens, você deve excluí-los manualmente de ambos os grids.
- Ao remover uma conexão, quaisquer objetos que estejam com replicação pendente (ingeridos, mas ainda não replicados para a outra grid) terão sua replicação permanentemente falhada.

Desative a replicação para todos os buckets de locatários

Passos

1. A partir de qualquer uma das grades, faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **Configuração > Sistema > Grid federation**.
3. Selecione o nome da conexão para exibir seus detalhes.
4. Na aba **Inquilinos permitidos**, determine se a conexão está sendo usada por algum inquilino.
5. Se houver inquilinos listados, instrua todos os inquilinos a "[desativar a replicação entre grids](#)" para todos os seus buckets em ambas as grades da conexão.



Não é possível remover a permissão **Usar conexão de federação de grid** se algum bucket de locatário tiver a replicação entre grids ativada. Cada conta de locatário deve desativar a replicação entre grids para seus buckets em ambas as grids.

Remover permissão para cada tenant

Após desativar a replicação entre grades para todos os buckets de locatários, remova a permissão **Usar federação de grid** de todos os locatários em ambas as grids.

Passos

1. Selecione **Configuração > Sistema > Grid federation**.
2. Selecione o nome da conexão para exibir seus detalhes.
3. Para cada locatário na guia **Locatários permitidos**, remova a permissão **Usar conexão de federação de grid** de cada locatário. Consulte "[Gerenciar locatários permitidos](#)".
4. Repita estas etapas para os tenants permitidos na outra grid.

Remover conexão

Passos

1. Quando nenhum locatário em nenhuma das grids estiver usando a conexão, selecione **Remover**.
2. Analise a mensagem de confirmação e selecione **Remover**.
 - Se a conexão puder ser removida, uma mensagem de sucesso será exibida. A conexão de federação de grids agora foi removida de ambos os grids.
 - Se a conexão não puder ser removida (por exemplo, se ainda estiver em uso ou se houver um erro de conexão), uma mensagem de erro será exibida. Você pode fazer o seguinte:
 - Corrija o erro (recomendado). Consulte "[Solucionar problemas de erros de federação de grid](#)".
 - Remova a conexão à força. Veja a próxima seção.

Remova uma conexão de federação de grid à força

Se necessário, você pode forçar a remoção de uma conexão que não tenha o status **Connected**.

A remoção forçada exclui apenas a conexão da grid local. Para remover completamente a conexão, execute os mesmos passos em ambas as grids.

Passos

1. Na caixa de diálogo de confirmação, selecione **Forçar remoção**.

Uma mensagem de sucesso é exibida. Esta conexão de federação de grids não pode mais ser usada. No entanto, os buckets dos tenants ainda podem ter a replicação entre grids habilitada e algumas cópias de objetos podem já ter sido replicadas entre os grids na conexão.

2. A partir da outra grid na conexão, faça login no Grid Manager a partir do nó de administração primário.
3. Selecione **Configuração > Sistema > Grid federation**.
4. Selecione o nome da conexão para exibir seus detalhes.
5. Selecione **Remover** e **Sim**.
6. Selecione **Remover à força** para remover a conexão deste grid.

Gerencie os locatários permitidos para a federação de grids do StorageGRID

Você pode permitir que contas de locatários do S3 usem uma conexão de federação de grid entre dois sistemas StorageGRID. Quando os locatários têm permissão para usar uma conexão, etapas especiais são necessárias para editar os detalhes do locatário ou para remover permanentemente a permissão de um locatário para usar a conexão.

Antes de começar

- Você está conectado ao Grid Manager em qualquer uma das grids usando um ["navegador web compatível"](#).
- Você tem ["Permissão de acesso root"](#) para a grid na qual você está conectado.
- Você tem ["Criou uma conexão de federação de grid"](#) entre duas grades.
- Você analisou os fluxos de trabalho para ["clone de conta"](#) e ["replicação entre grids"](#).
- Conforme necessário, você já configurou o login único (SSO) ou a federação de identidade para ambas as grids na conexão. Consulte ["O que é clonagem de conta"](#).

Criar um tenant permitido

Se você deseja permitir que uma conta de locatário nova ou existente use uma conexão de federação de grade para clonagem de conta e replicação entre grades, siga as instruções gerais em ["crie um novo locatário S3"](#) ou ["editar uma conta de tenant"](#) e observe o seguinte:

- Você pode criar o locatário a partir de qualquer uma das grades na conexão. A grade onde um locatário é criado é a *grade de origem do locatário*.
- O status da conexão deve ser **Conectado**.
- Quando o locatário é criado ou editado para habilitar a permissão **Usar conexão de federação de grid** e, em seguida, salvo na primeira grid, um locatário idêntico é replicado automaticamente para a outra grid. A grid na qual o locatário é replicado é a *grid de destino do locatário*.
- Os locatários em ambas as grades terão o mesmo ID de conta de 20 dígitos, nome, descrição, cota e permissões. Opcionalmente, você pode usar o campo **Descrição** para ajudar a identificar qual é o locatário de origem e qual é o locatário de destino. Por exemplo, esta descrição para um locatário criado na Grade 1 também aparecerá para o locatário replicado na Grade 2: "Este locatário foi criado na Grade 1."
- Por motivos de segurança, a senha do usuário raiz local não é copiada para a grid de destino.



Antes que um usuário raiz local possa fazer login no locatário replicado na grade de destino, um administrador dessa grade deve ["alterar a senha do usuário raiz local"](#).

- Após o novo locatário ou o locatário editado estar disponível em ambas as grades, os usuários do locatário podem realizar estas operações:
 - A partir da grid de origem do tenant, crie grupos e usuários locais, que são clonados automaticamente para a grid de destino do tenant. Consulte ["Clonar grupos de tenants e usuários"](#).
 - Crie novas chaves de acesso S3, que podem ser opcionalmente clonadas para o grid de destino do locatário. Consulte ["Clonar chaves de acesso S3 usando a API"](#).
 - Crie buckets idênticos em ambas as grades na conexão e habilite a replicação entre grades em uma direção ou em ambas as direções. Consulte ["Gerencie a replicação entre grades"](#).

Visualize um tenant permitido

Você pode ver detalhes de um locatário que tem permissão para usar uma conexão de federação de grid.

Passos

1. Selecione **Tenants**.
2. Na página de Tenants, selecione o nome do tenant para visualizar a página de detalhes do tenant.

Se esta for a grid de origem do tenant (ou seja, se o tenant foi criado nesta grid), um banner será exibido

para lembrar você de que o tenant foi clonado para outra grid. Se você editar ou excluir este tenant, suas alterações não serão sincronizadas com a outra grid.

Tenants > tenant A for grid federation

tenant A for grid federation

Tenant ID: 0899 6970 1700 0930 0009

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Description: this tenant was created on Grid 1

Sign in

Edit

Actions

This tenant has been cloned to another grid. If you edit or delete this tenant, your changes will not be synced to the other grid.

Space breakdown

Allowed features

Grid federation

Remove permission

Clear error

Search...

Displaying one result

Connection name	Connection status	Remote grid hostname	Last error
Grid 1 to Grid 2	Connected	10.96.106.230	Check for errors

3. Opcionalmente, selecione a guia **Federação de grade** para "monitorar a conexão da federação da grid".

Editar um tenant permitido

Se precisar editar um locatário que tenha a permissão **Usar conexão de federação de grade**, siga as instruções gerais "editar uma conta de tenant" e observe o seguinte:

- Se um locatário tiver a permissão **Usar conexão de federação de grades**, você pode editar os detalhes do locatário em qualquer uma das grades da conexão. No entanto, quaisquer alterações que você fizer não serão copiadas para a outra grade. Se você quiser manter os detalhes do locatário sincronizados entre as grades, deverá fazer as mesmas edições em ambas as grades.
- Você não pode remover a permissão **Usar conexão de federação de grid** ao editar um tenant.
- Não é possível selecionar uma conexão de federação de grid diferente ao editar um tenant.

Excluir um tenant permitido

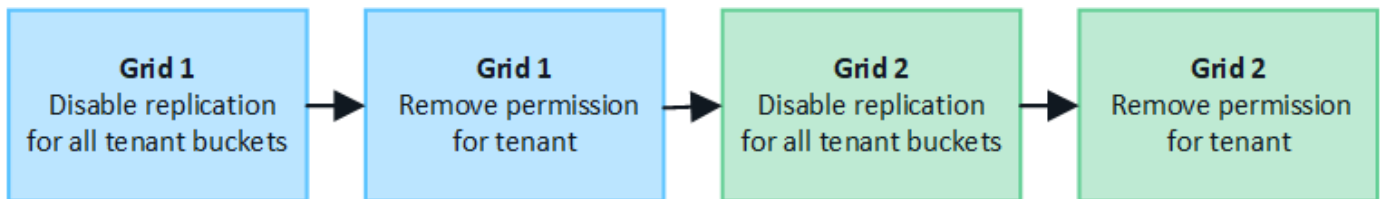
Se precisar remover um locatário que tenha a permissão **Usar conexão de federação de grade**, siga as instruções gerais "Excluindo uma conta de locatário" e observe o seguinte:

- Antes de remover o locatário original na grid de origem, você deve remover todos os buckets da conta na grid de origem.
- Antes de remover o locatário clonado na grid de destino, você deve remover todos os buckets da conta na grid de destino.
- Se você remover o locatário original ou o locatário clonado, a conta não poderá mais ser usada para replicação entre grids.
- Se você estiver removendo o locatário original na grade de origem, quaisquer grupos de locatários, usuários ou chaves que foram clonados para a grade de destino permanecerão inalterados. Você pode excluir o locatário clonado ou permitir que ele gerencie seus próprios grupos, usuários, chaves de acesso e buckets.
- Se você estiver removendo o locatário clonado na grade de destino, ocorrerão erros de clonagem caso novos grupos ou usuários sejam adicionados ao locatário original.

Para evitar esses erros, remova a permissão do locatário para usar a conexão de federação da grid antes de excluir o locatário desta grid.

Remover permissão Usar conexão de federação de grid

Para impedir que um locatário use uma conexão de federação de grid, você deve remover a permissão **Usar conexão de federação de grid**.



Antes de remover a permissão de um locatário para usar uma conexão de federação de grid, observe o seguinte:

- Não é possível remover a permissão **Usar conexão de federação de grid** se algum dos buckets do locatário tiver a replicação entre grids ativada. A conta do locatário deve desativar a replicação entre grids para todos os seus buckets primeiro.
- Remover a permissão **Usar conexão de federação de grid** não exclui nenhum item que já tenha sido replicado entre os grids. Por exemplo, quaisquer usuários, grupos e objetos do tenant que existam em ambos os grids não são excluídos de nenhum dos grids quando a permissão do tenant é removida. Se você quiser excluir esses itens, deve excluí-los manualmente de ambos os grids.
- Se você deseja reativar essa permissão com a mesma conexão de federação de grid, exclua primeiro esse locatário na grid de destino; caso contrário, reativar essa permissão resultará em um erro.



Reativar a permissão **Usar conexão de federação de grid** torna o grid local o grid de origem e aciona a clonagem para o grid remoto especificado pela conexão de federação de grid selecionada. Se a conta do tenant já existir no grid remoto, a clonagem resultará em um erro de conflito.

Antes de começar

- Você está usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#) para ambas as grades.

Desative a replicação para buckets de locatários

Como primeiro passo, desative a replicação entre grids para todos os buckets de locatários.

Passos

1. A partir de qualquer uma das grades, faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **Configuração > Sistema > Grid federation**.
3. Selecione o nome da conexão para exibir seus detalhes.
4. Na aba **Inquilinos permitidos**, verifique se o inquilino está usando a conexão.
5. Se o inquilino estiver listado, instrua-o a "[desativar a replicação entre grids](#)" para todos os seus buckets em ambas as grids na conexão.



Não é possível remover a permissão **Usar conexão de federação de grid** se algum bucket do locatário tiver a replicação entre grids ativada. O locatário deve desativar a replicação entre grids para seus buckets em ambas as grids.

Remover permissão para tenant

Após desativar a replicação entre grids para buckets de locatários, você pode remover a permissão do locatário para usar a conexão de federação de grid.

Passos

1. Faça login no Grid Manager a partir do nó de administração principal.
2. Remova a permissão da página de federação do Grid ou da página de Tenants.

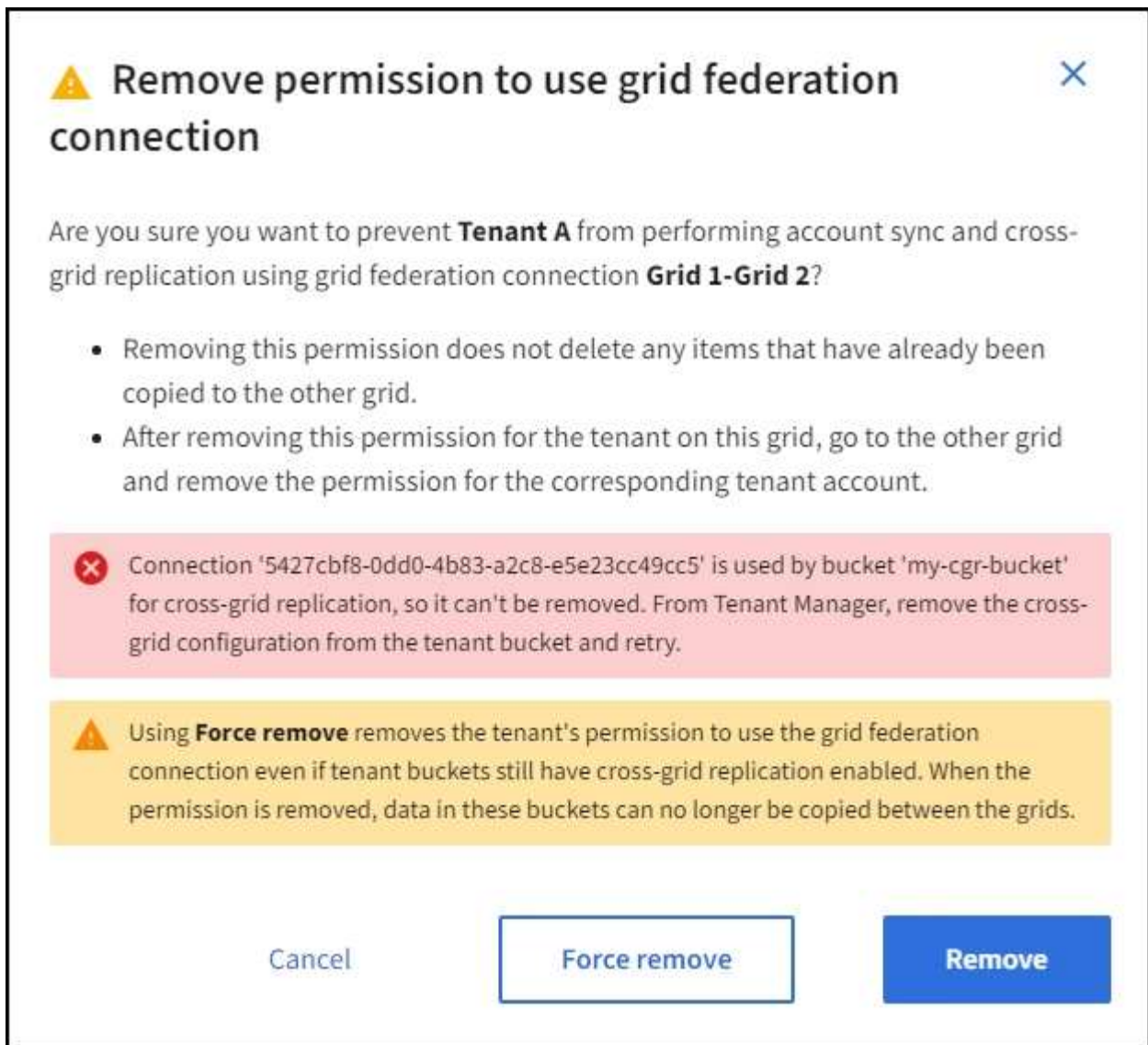
Página de federação de grid

- a. Selecione **Configuração > Sistema > Grid federation**.
- b. Selecione o nome da conexão para exibir a página de detalhes.
- c. Na aba **Inquilinos permitidos**, selecione o botão de opção correspondente ao tenant.
- d. Selecione **Remover permissão**.

Página de locatários

- a. Selecione **Tenants**.
- b. Selecione o nome do tenant para exibir a página de detalhes.
- c. Na aba **Federação de grid**, selecione o botão de opção para a conexão.
- d. Selecione **Remover permissão**.

3. Analise os avisos na caixa de diálogo de confirmação e selecione **Remover**.
 - Se a permissão puder ser removida, você retornará à página de detalhes e uma mensagem de sucesso será exibida. Este locatário não poderá mais usar a conexão de federação de grid.
 - Se um ou mais buckets de locatários ainda tiverem a replicação entre grids ativada, um erro será exibido.



Você pode fazer o seguinte:

- (Recomendado.) Faça login no Tenant Manager e desative a replicação para cada um dos buckets do tenant. Veja ["Gerencie a replicação entre grades"](#). Em seguida, repita os passos para remover a permissão **Use grid connection**.
- Remova a permissão à força. Veja a próxima seção.

4. Acesse a outra grid e repita estes passos para remover a permissão do mesmo tenant na outra grid.

Remover a permissão à força

Se necessário, você pode forçar a remoção da permissão de um locatário para usar uma conexão de federação de grid, mesmo que os buckets do locatário tenham a replicação entre grids habilitada.

Antes de revogar a permissão de um inquilino à força, observe as considerações gerais para [removendo a permissão](#) assim como estas considerações adicionais:

- Se você remover a permissão **Usar conexão de federação de grid** à força, quaisquer objetos que estejam pendentes de replicação para a outra grid (ingeridos, mas ainda não replicados) continuarão sendo replicados. Para impedir que esses objetos em processo cheguem ao bucket de destino, você também deve remover a permissão do locatário na outra grid.

- Quaisquer objetos inseridos no bucket de origem após você remover a permissão **Usar conexão de federação de grid** nunca serão replicados para o bucket de destino.

Passos

1. Faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **Configuração > Sistema > Grid federation**.
3. Selecione o nome da conexão para exibir a página de detalhes.
4. Na aba **Inquilinos permitidos**, selecione o botão de opção correspondente ao tenant.
5. Selecione **Remover permissão**.
6. Analise os avisos na caixa de diálogo de confirmação e selecione **Forçar remoção**.

Uma mensagem de sucesso é exibida. Este locatário não pode mais usar a conexão de federação de grid.

7. Conforme necessário, acesse a outra grid e repita esses passos para forçar a remoção da permissão para a mesma conta de tenant na outra grid. Por exemplo, você deve repetir esses passos na outra grid para impedir que objetos em processamento cheguem ao bucket de destino.

Solucionar problemas de erros de federação de grid no StorageGRID

Você pode precisar solucionar problemas relacionados a alertas e erros referentes a conexões de federação de grid, clonagem de contas e replicação entre grids.

Alertas e erros de conexão da federação de grid

Você pode receber alertas ou encontrar erros com suas conexões de federação de grid.

Após efetuar quaisquer alterações para resolver um problema de conexão, teste a conexão para garantir que o status da conexão retorne a **Conectado**. Para obter instruções, consulte ["Gerenciar conexões de federação de grid"](#).

Alerta de falha na conexão da federação de grid

Problema

O alerta **Falha na conexão da federação de grid** foi acionado.

Detalhes

Este alerta indica que a conexão de federação de grid entre os grids não está funcionando.

Ações recomendadas

1. Analise as configurações na página de Federação de Grades para ambas as grades. Confirme se todos os valores estão corretos. Consulte ["Gerenciar conexões de federação de grid"](#).
2. Analise os certificados usados para a conexão. Certifique-se de que não haja alertas para certificados de federação de grid expirados e que os detalhes de cada certificado sejam válidos. Veja as instruções para rotacionar certificados de conexão em ["Gerenciar conexões de federação de grid"](#).
3. Confirme se todos os nós de administração e gateway em ambas as grids estão online e disponíveis. Resolva quaisquer alertas que possam estar afetando esses nós e tente novamente.
4. Se você forneceu um domínio totalmente qualificado (FQDN) para a grid local ou remota, confirme se o servidor DNS está online e disponível. Consulte ["O que é federação de grid?"](#) para os requisitos de rede, endereço IP e DNS.

Alerta de expiração do certificado de federação de grid

Problema

O alerta **Expiração do certificado de federação de grid** foi acionado.

Detalhes

Este alerta indica que um ou mais certificados de federação de grid estão prestes a expirar.

Ações recomendadas

Consulte as instruções para rotacionar certificados de conexão em "[Gerenciar conexões de federação de grid](#)".

Erro ao editar uma conexão de federação de grid

Problema

Ao editar uma conexão de federação de grid, você verá a seguinte mensagem de aviso ao selecionar **Salvar e testar**: "Falha ao criar um arquivo de configuração candidato em um ou mais nós."

Detalhes

Ao editar uma conexão de federação de grid, StorageGRID tenta salvar um arquivo de "configuração candidata" em todos os nós de administração do primeiro grid. Uma mensagem de aviso é exibida se esse arquivo não puder ser salvo em todos os nós de administração, por exemplo, porque um nó de administração está offline.

Ações recomendadas

1. Na grade que você está usando para editar a conexão, selecione **Nodes**.
2. Confirme se todos os nós de administração dessa grid estão online.
3. Se algum nó estiver offline, coloque-o novamente online e tente editar a conexão novamente.

Erros de clonagem de conta

Não é possível iniciar sessão em uma conta de locatário clonada

Problema

Você não pode fazer login em uma conta de locatário clonada. A mensagem de erro na página de login do Tenant Manager é: "Suas credenciais para esta conta são inválidas. Tente novamente."

Detalhes

Por motivos de segurança, quando uma conta de locatário é clonada da grid de origem para a grid de destino, a senha que você definiu para o usuário raiz local do locatário não é clonada. Da mesma forma, quando um locatário cria usuários locais em sua grid de origem, as senhas dos usuários locais não são clonadas para a grid de destino.

Ações recomendadas

Antes que o usuário raiz possa fazer login no grid de destino do locatário, um administrador do grid deve primeiro "[alterar a senha do usuário raiz local](#)" no grid de destino.

Antes que um usuário local clonado possa fazer login na grade de destino do locatário, o usuário raiz do locatário clonado deve adicionar uma senha para o usuário na grade de destino. Para obter instruções, consulte "[Gerenciar usuários](#)" nas instruções para usar o Tenant Manager.

Tenant criado sem um clone

Problema

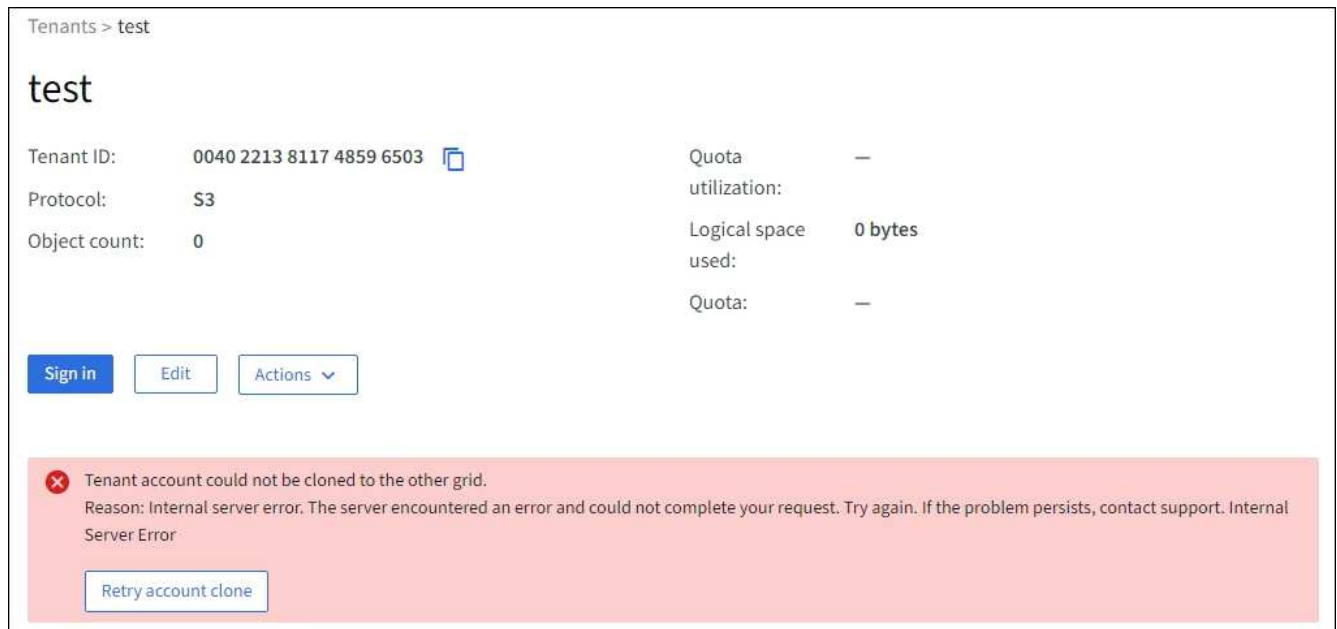
Você vê a mensagem "Tenant created without a clone" após criar um novo tenant com a permissão **Use grid federation connection**.

Detalhes

Esse problema pode ocorrer se as atualizações do status da conexão forem atrasadas, o que pode fazer com que uma conexão instável seja listada como **Connected**.

Ações recomendadas

1. Analise o motivo listado na mensagem de erro e resolva quaisquer problemas de rede ou outros que possam estar impedindo a conexão de funcionar. Consulte [Alertas e erros de conexão da federação de grid](#).
2. Siga as instruções para testar uma conexão de federação de grid em "[Gerenciar conexões de federação de grid](#)" para confirmar que o problema foi corrigido.
3. Na grid de origem do tenant, selecione **Tenants**.
4. Localize a conta do tenant que não pôde ser clonada.
5. Selecione o nome do tenant para exibir a página de detalhes.
6. Selecione **Retry account clone**.



Tenants > test

test

Tenant ID:	0040 2213 8117 4859 6503	Quota utilization:	—
Protocol:	S3	Logical space used:	0 bytes
Object count:	0	Quota:	—

[Sign in](#) [Edit](#) [Actions](#) ▼

✖ Tenant account could not be cloned to the other grid.
Reason: Internal server error. The server encountered an error and could not complete your request. Try again. If the problem persists, contact support. Internal Server Error

[Retry account clone](#)

Se o erro tiver sido resolvido, a conta do locatário agora será clonada para a outra grade.

Alertas e erros de replicação entre grids

Último erro exibido para conexão ou locatário

Problema

Quando "[Visualizando uma conexão de federação de grid](#)" (ou quando "[gerenciando os tenants permitidos](#)" para uma conexão), você nota um erro na coluna **Último erro** na página de detalhes da conexão. Por exemplo:

Grid 1 - Grid 2

Local hostname (this grid): 10.115.96.170
Port: 23000
Remote hostname (other grid): 10.115.96.175
Connection status:  Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

[Permitted tenants](#) [Certificates](#)

[Remove permission](#) [Clear error](#) 

Displaying one result

Tenant name	Last error
 Tenant A	2025-03-13 15:54:59 PDT Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-bucket' to destination bucket 'my-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled. (logID 13371653720226059496) Check for errors

Detalhes

Para cada conexão de federação de grids, a coluna **Último erro** mostra o erro mais recente ocorrido, se houver, quando os dados de um tenant estavam sendo replicados para o outro grid. Esta coluna exibe apenas o último erro de replicação entre grids; erros anteriores que possam ter ocorrido não são mostrados. Um erro nesta coluna pode ocorrer por um dos seguintes motivos:

- A versão do objeto de origem não foi encontrada.
- O bucket de origem não foi encontrado.
- O bucket de destino foi excluído.
- O bucket de destino foi recriado por uma conta diferente.
- O bucket de destino está com o controle de versão suspenso.
- O bucket de destino foi recriado pela mesma conta, mas agora está sem versionamento.
- O objeto de origem possui configurações de bloqueio de objeto S3 que não estão em conformidade com as configurações de retenção em nível de locatário da grade de destino.
- O objeto de origem possui configurações de Bloqueio de Objeto S3 e o Bloqueio de Objeto S3 está desativado no bucket de destino.

Ações recomendadas

Se uma mensagem de erro aparecer na coluna **Último erro**, siga estes passos:

1. Analise o texto da mensagem.
2. Execute as ações recomendadas. Por exemplo, se o versionamento foi suspenso no bucket de destino para replicação entre grids, reative o versionamento para esse bucket.
3. Selecione a conexão ou a conta de locatário na tabela.
4. Selecione **Limpar erro**.
5. Selecione **Sim** para limpar a mensagem e atualizar o status do sistema.
6. Aguarde de 5 a 6 minutos e, em seguida, insira um novo objeto no bucket. Confirme que a mensagem de erro não reaparece.



Para garantir que a mensagem de erro seja eliminada, aguarde pelo menos 5 minutos após o horário indicado na mensagem antes de inserir um novo objeto.



Após a correção do erro, um novo **Último erro** poderá aparecer se objetos forem ingeridos em um bucket diferente que também apresente um erro.

7. Para determinar se algum objeto não foi replicado devido a um erro no bucket, consulte ["Identifique e repita operações de replicação com falha"](#).

Alerta de falha permanente de replicação entre grids

Problema

O alerta **Falha permanente na replicação entre grades** foi acionado.

Detalhes

Este alerta indica que os objetos do locatário não podem ser replicados entre os buckets em duas grades por um motivo que requer intervenção do usuário para ser resolvido. Normalmente, esse alerta é causado por uma alteração no bucket de origem ou no bucket de destino.

Ações recomendadas

1. Faça login na grid onde o alerta foi acionado.
2. Acesse **Configuração > Sistema > Federação de grade** e localize o nome da conexão listado no alerta.
3. Na aba "Inquilinos permitidos", observe a coluna "Último erro" para determinar quais contas de inquilinos apresentam erros.
4. Para obter mais informações sobre a falha, consulte as instruções em ["Monitorar conexões de federação de grid"](#) para revisar as métricas de replicação entre grades.
5. Para cada conta de inquilino afetada:
 - a. Consulte as instruções em ["Monitorar a atividade do locatário"](#) para confirmar que o locatário não excedeu sua cota na grid de destino para replicação entre grids.
 - b. Conforme necessário, aumente a cota do locatário na grid de destino para permitir que novos objetos sejam salvos.
6. Para cada locatário afetado, faça login no Gerenciador de Locatários em ambas as grids para que você possa comparar a lista de buckets.
7. Para cada bucket com replicação entre grades ativada, confirme o seguinte:
 - Existe um bucket correspondente para o mesmo locatário na outra grid (deve-se usar o nome exato).
 - Ambos os buckets têm o versionamento de objetos ativado (o versionamento não pode ser suspenso em nenhum dos grids).
 - Nenhum dos buckets está no estado **Excluindo objetos: somente leitura**.
8. Para confirmar se o problema foi resolvido, consulte as instruções em ["Monitorar conexões de federação de grid"](#) para revisar as métricas de replicação entre grids ou execute estas etapas:
 - a. Volte para a página de federação Grid.
 - b. Selecione o locatário afetado e selecione **Limpar erro** na coluna **Último erro**.
 - c. Selecione **Sim** para limpar a mensagem e atualizar o status do sistema.
 - d. Aguarde de 5 a 6 minutos e, em seguida, insira um novo objeto no bucket. Confirme que a mensagem de erro não reaparece.



Para garantir que a mensagem de erro seja eliminada, aguarde pelo menos 5 minutos após o horário indicado na mensagem antes de inserir um novo objeto.



Pode levar até um dia para o alerta desaparecer após ele ser resolvido.

- a. Acesse "[Identifique e repita operações de replicação com falha](#)" para identificar quaisquer objetos ou marcadores de exclusão que não foram replicados para a outra grid e para tentar a replicação novamente, se necessário.

Alerta de recurso de replicação entre grades indisponível

Problema

O alerta **Recurso de replicação entre grades indisponível** foi acionado.

Detalhes

Este alerta indica que existem solicitações de replicação entre grades pendentes porque um recurso está indisponível. Por exemplo, pode haver um erro de rede.

Ações recomendadas

1. Monitore o alerta para verificar se o problema se resolve sozinho.
2. Se o problema persistir, verifique se alguma das grades apresenta um alerta de **Falha na conexão de federação da grade** para a mesma conexão ou um alerta de **Não foi possível se comunicar com o nó** para um nó. Esse alerta pode ser resolvido quando você resolver esses alertas.
3. Para obter mais informações sobre a falha, consulte as instruções em "[Monitorar conexões de federação de grid](#)" para revisar as métricas de replicação entre grades.
4. Se não conseguir resolver o alerta, entre em contato com o suporte técnico.

A replicação entre grades prosseguirá normalmente após a resolução do problema.

Identifique e repita operações de replicação do StorageGRID que falharam

Após resolver o alerta **Falha permanente na replicação entre grades**, você deve determinar se algum objeto ou marcador de exclusão não foi replicado para a outra grade. Em seguida, você pode reingerir esses objetos ou usar a Grid Management API para tentar a replicação novamente.

O alerta **Falha permanente na replicação entre grades** indica que os objetos do locatário não podem ser replicados entre os buckets em duas grades por um motivo que requer intervenção do usuário para ser resolvido. Esse alerta geralmente é causado por uma alteração no bucket de origem ou de destino. Para obter detalhes, consulte "[Solucionar problemas de erros de federação de grid](#)".

Determine se algum objeto falhou ao ser replicado

Para determinar se algum objeto ou marcador de exclusão não foi replicado para o outro grid, você pode pesquisar o log de auditoria por mensagens "[CGRR \(Solicitação de Replicação entre Grids\)](#)". Essa mensagem é adicionada ao log quando StorageGRID não consegue replicar um objeto, objeto multipart ou marcador de exclusão para o bucket de destino.

Você pode usar o "[ferramenta audit-explain](#)" para traduzir os resultados para um formato mais fácil de ler.

Antes de começar

- Você tem permissão de acesso root.
- Você tem o arquivo `Passwords.txt`.
- Você sabe o endereço IP do nó de administração principal.

Passos

1. Faça login no nó de administração principal:

- a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- b. Digite a senha listada no arquivo `Passwords.txt`.
- c. Digite o seguinte comando para alternar para root: `su -`
- d. Digite a senha listada no arquivo `Passwords.txt`.

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

2. Procure por mensagens CGRR no `audit.log` e use a ferramenta `audit-explain` para formatar os resultados.

Por exemplo, este comando busca todas as mensagens CGRR dos últimos 30 minutos e utiliza a ferramenta `audit-explain`.

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {  
print }' audit.log | grep CGRR | audit-explain
```

Os resultados do comando serão semelhantes a este exemplo, que contém entradas para seis mensagens CGRR. No exemplo, todas as solicitações de replicação entre grades retornaram um erro geral porque o objeto não pôde ser replicado. Os três primeiros erros são de operações de "replicate object" e os três últimos erros são de operações de "replicate delete marker".

```

CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error

```

Cada entrada contém as seguintes informações:

Campo	Descrição
Solicitação de replicação entre grades CGRR	O nome da solicitação
inquilino	O ID da conta do tenant
conexão	O ID da conexão da federação de grid
operação	O tipo de operação de replicação que estava sendo tentada: • replicar objeto • replicar marcador de exclusão • replicar objeto multipart
bucket	O nome do bucket
objeto	O nome do objeto
versão	O ID da versão do objeto

Campo	Descrição
erro	O tipo de erro. Se a replicação entre grades falhar, o erro será "Erro geral".

Tentar novamente as replicações com falha

Após gerar uma lista de objetos e marcadores de exclusão que não foram replicados para o bucket de destino e resolver os problemas subjacentes, você pode tentar a replicação novamente de duas maneiras:

- Reingira cada objeto no bucket de origem.
- Utilize a API privada de Gerenciamento de Grid, conforme descrito.

Passos

1. Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **API documentation**.
2. Selecione **Ir para a documentação da API privada**.



Os endpoints da API StorageGRID marcados como "Privados" estão sujeitos a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

3. Na seção **cross-grid-replication-advanced**, selecione o seguinte endpoint:

```
POST /private/cross-grid-replication-retry-failed
```

4. Selecione **Experimentar**.
5. Na caixa de texto **body**, substitua a entrada de exemplo para **versionID** por um ID de versão do log de auditoria que corresponda a uma solicitação de replicação entre grades com falha.

Certifique-se de manter as aspas duplas em torno da string.
6. Selecione **Executar**.
7. Confirme se o código de resposta do servidor é **204**, indicando que o objeto ou marcador de exclusão foi marcado como pendente para replicação entre grades para a outra grade.



"Pendente" significa que a solicitação de replicação entre grades foi adicionada à fila interna para processamento.

Monitorar novas tentativas de replicação

Você deve monitorar as operações de repetição de replicação para garantir que elas sejam concluídas.



Pode levar várias horas ou mais para que um objeto ou marcador de exclusão seja replicado para a outra grid.

Você pode monitorar as operações de repetição de duas maneiras:

- Use uma solicitação S3 "[HeadObject](#)" ou "[GetObject](#)". A resposta inclui o cabeçalho de resposta específico do StorageGRID `x-ntap-sg-cgr-replication-status`, que terá um dos seguintes

valores:

Grid	Status de replicação
Fonte	• CONCLUÍDO: A replicação foi bem-sucedida. • PENDENTE: O objeto ainda não foi replicado. • FALHA: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	RÉPLICA : O objeto foi replicado da grid de origem.

- Utilize a API privada de Gerenciamento de Grid, conforme descrito.

Passos

1. Na seção **cross-grid-replication-advanced** da documentação da API privada, selecione o seguinte endpoint:

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Selecione **Experimentar**.
3. Na seção Parâmetros, insira o ID da versão que você usou na `cross-grid-replication-retry-failed` solicitação.
4. Selecione **Executar**.
5. Confirme se o código de resposta do servidor é **200**.
6. Verifique o status da replicação, que será um dos seguintes:
 - **PENDENTE**: O objeto ainda não foi replicado.
 - **CONCLUÍDO**: A replicação foi bem-sucedida.
 - **FALHA**: A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.

Gerenciar segurança

Gerenciar a segurança no StorageGRID

Você pode configurar diversas opções de segurança no Gerenciador de Grade para ajudar a proteger seu sistema StorageGRID.

Gerenciar criptografia

StorageGRID oferece diversas opções para criptografar dados. Você deve ["revisar os métodos de criptografia disponíveis"](#) determinar quais delas atendem aos seus requisitos de proteção de dados.

Gerenciar certificados

Você pode ["configurar e gerenciar os certificados do servidor"](#) usá-los para conexões HTTP ou os certificados de cliente usados para autenticar a identidade de um cliente ou usuário no servidor.

Configurar os servidores de gerenciamento de chaves

O uso de um "[servidor de gerenciamento de chaves](#)" permite proteger os dados do StorageGRID mesmo se um appliance for removido do data center. Depois que os volumes do appliance são criptografados, você não pode acessar nenhum dado no appliance, a menos que o nó consiga se comunicar com o KMS.



Para usar o gerenciamento de chaves de criptografia, você deve habilitar a configuração **Criptografia de Nó** para cada appliance durante a instalação, antes que o appliance seja adicionado à grid.

Gerenciar configurações de proxy

Se você estiver usando os serviços da plataforma S3 ou os Cloud Storage Pools, pode configurar um "[servidor proxy de storage](#)" entre os Storage Nodes e os endpoints externos do S3. Se você enviar pacotes AutoSupport usando HTTPS ou HTTP, pode configurar um "[servidor proxy de administração](#)" entre os Admin Nodes e o suporte técnico.

Controlar firewalls

Para aumentar a segurança do seu sistema, você pode controlar o acesso aos StorageGRID Admin Nodes abrindo ou fechando portas específicas no "[firewall externo](#)". Você também pode controlar o acesso à rede de cada nó configurando seu "[firewall interno](#)". Você pode bloquear o acesso em todas as portas, exceto aquelas necessárias para sua implantação.

Revise os métodos de criptografia do StorageGRID

StorageGRID oferece diversas opções para criptografar dados. Você deve analisar os métodos disponíveis para determinar quais atendem aos seus 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 " configurar um servidor de gerenciamento de chaves " para o site do StorageGRID e " Ative a criptografia de nó para o dispositivo ". Em seguida, um nó do 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.	Nós de dispositivos com Criptografia de Nó ativada durante a instalação. Todos os dados no dispositivo estão protegidos contra perda física ou remoção do data center. Nota: Gerenciar chaves de criptografia com um KMS é compatível apenas com Storage Nodes e dispositivos de serviço.

Opção de criptografia	Como funciona	Aplica-se a
Página de Criptografia de Unidade no Instalador do Dispositivo StorageGRID	Se o dispositivo contiver unidades que suportam criptografia de hardware, você pode definir uma senha de unidade durante a instalação. Ao definir uma senha de unidade, é impossível para qualquer pessoa recuperar dados válidos de unidades que foram removidas do sistema, a menos que saiba a senha. Antes de iniciar a instalação, acesse Configurar Hardware > Criptografia de Unidade para definir uma senha de unidade que se aplique a todas as unidades autcriptografáveis gerenciadas pelo StorageGRID em um nó.	Dispositivos que contêm unidades de armazenamento com criptografia automática. Todos os dados nessas unidades seguras são protegidos contra perda física ou remoção do data center. A criptografia de unidade não se aplica a unidades gerenciadas pelo SANtricity. Se você tiver um dispositivo de storage com unidades de autcriptografia e controladores SANtricity, poderá ativar a segurança da unidade no SANtricity.
Segurança de unidade no SANtricity System Manager	Se o recurso Drive Security estiver ativado para o seu StorageGRID appliance, você pode usar "SANtricity System Manager" para criar e gerenciar a chave de segurança. A chave é necessária para acessar os dados nas unidades protegidas.	Dispositivos de storage que possuem unidades de Full Disk Encryption (FDE) ou unidades com criptografia automática. Todos os dados nas unidades protegidas estão protegidos contra perda física ou remoção do data center. Não pode ser usado com alguns dispositivos de storage ou com nenhum dispositivo de serviço.
Criptografia de objeto armazenado	Você habilita a opção "Criptografia de objeto armazenado" no Grid Manager. Quando habilitada, quaisquer novos objetos que não estejam criptografados no nível do bucket ou no nível do objeto são criptografados durante a ingestão.	Dados de objetos S3 recém-ingерidos. Os objetos armazenados existentes não são criptografados. Os metadados dos objetos e outros dados confidenciais não são criptografados.
Criptografia de bucket S3	Você emite uma solicitação PutBucketEncryption para habilitar a criptografia para o bucket. Quaisquer novos objetos que não estejam criptografados no nível do objeto são criptografados durante a ingestão.	Somente dados de objetos S3 recém-ingерidos. A criptografia deve ser especificada para o bucket. Os objetos de bucket existentes não são criptografados. Os metadados dos objetos e outros dados confidenciais não são criptografados. "Operações em buckets"

Opção de criptografia	Como funciona	Aplica-se a
Criptografia do lado do servidor (SSE) de objetos S3	Você emite uma solicitação S3 para armazenar um objeto e inclui o <code>x-amz-server-side-encryption</code> cabeçalho da solicitação.	Somente dados de objetos S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Metadados do objeto e outros dados confidenciais não são criptografados. StorageGRID gerencia as chaves. "Use criptografia do lado do servidor"
Criptografia do lado do servidor S3 com chaves fornecidas pelo cliente (SSE-C)	Você emite uma solicitação S3 para armazenar um objeto e inclui três cabeçalhos de solicitação. <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>	Somente dados de objetos S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Metadados do objeto e outros dados confidenciais não são criptografados. As chaves são gerenciadas fora do StorageGRID. "Use criptografia do lado do servidor"
Criptografia de volume externo ou datastore	Você usa um método de criptografia externo ao StorageGRID para criptografar um volume ou datastore inteiro, se sua plataforma de implantação oferecer suporte a isso.	Todos os dados de objetos, metadados e dados de configuração do sistema, assumindo que cada volume ou datastore esteja criptografado. Um método de criptografia externa proporciona um controle mais rigoroso sobre os algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de objetos fora do StorageGRID	Você utiliza um método de criptografia externo ao StorageGRID para criptografar os dados e metadados antes que sejam inseridos no StorageGRID.	Apenas dados de objetos e metadados (os dados de configuração do sistema não são criptografados). Um método de criptografia externa proporciona um controle mais rigoroso sobre os algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados. "Amazon Simple Storage Service - Guia do Usuário: 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 ao mesmo tempo. Por exemplo:

- Você pode usar um KMS para proteger os nós do dispositivo e também usar o recurso de segurança de unidade no SANtricity System Manager para "duplamente criptografar" os dados nas unidades de criptografia automática nos mesmos dispositivos.
- Você pode usar um KMS para proteger os dados nos nós do dispositivo e também usar a opção de criptografia de objeto armazenado para criptografar todos os objetos quando forem inseridos.

Se apenas uma pequena parte dos seus objetos requer criptografia, considere controlar a criptografia no nível do bucket ou do objeto individual. Habilitar vários níveis de criptografia acarreta um custo adicional de desempenho.

Informações relacionadas

["Conheça as opções de criptografia com certificação FIPS"](#)

Gerenciar certificados

Gerenciar certificados de segurança no StorageGRID

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

StorageGRID utiliza dois tipos de certificados de segurança:

- Os **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 possuem cada um uma cópia do certificado.
- **Certificados de cliente** autenticam a identidade de um cliente ou usuário no servidor, proporcionando

uma autenticação mais segura do que apenas senhas. Certificados de cliente não criptografam 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 compara a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas coincidirem, o cliente inicia uma sessão com o servidor usando a mesma chave pública.

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

Certificado CA padrão do Grid

StorageGRID possui uma autoridade de certificação (CA) incorporada que gera um certificado interno do Grid CA durante a instalação do sistema. O certificado Grid CA é usado, por padrão, para proteger o tráfego interno do StorageGRID. Uma autoridade de certificação (CA) externa pode emitir certificados personalizados que estejam totalmente em conformidade com as políticas de segurança da informação da sua organização.

Use o certificado da Autoridade Certificadora (CA) do Grid para ambientes que não sejam de produção. Para produção, use certificados personalizados assinados por uma autoridade certificadora externa. Conexões não seguras sem certificado são suportadas, mas não recomendadas.

- Os certificados de CA personalizados não removem os certificados internos; no entanto, os certificados personalizados devem ser aqueles especificados para verificar as conexões do servidor.
- Todos os certificados personalizados devem atender aos ["Diretrizes de reforço do sistema para certificados de servidor"](#).
- StorageGRID suporta o agrupamento de certificados de uma CA em um único arquivo (conhecido como pacote de certificados de CA).



StorageGRID também inclui certificados de CA do sistema operacional que são os mesmos em todos os grids. Em ambientes de produção, certifique-se de especificar um certificado personalizado assinado por uma autoridade de certificação externa no lugar do certificado de CA do sistema operacional.

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

Certificados de segurança de acesso

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.

Passos

1. No Grid Manager, selecione **Configuração > 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).

Global

Grid CA

Client

Load balancer endpoints

Tenants

Other

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 aba na página Certificados para obter informações sobre cada categoria de certificado e acessar as configurações do certificado. Você pode acessar uma aba se tiver o "[permissão apropriada](#)".

- **Global:** protege o acesso ao StorageGRID a partir de navegadores web e clientes de API externos.
- **Grid CA:** protege o tráfego interno do StorageGRID.
- **Cliente:** Garante a segurança das conexões entre clientes externos e o banco de dados StorageGRID Prometheus.
- **Pontos de extremidade do balanceador de carga:** Garante a segurança das conexões entre os clientes S3 e o Load Balancer do StorageGRID.
- **Inquilinos:** Garante conexões seguras com servidores de federação de identidade ou de endpoints de serviço de plataforma para recursos de storage.
- **Outros:** Protege as conexões StorageGRID que exigem certificados específicos.

Cada aba é descrita abaixo com links para detalhes adicionais do certificado.

Global

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

- [Certificado da interface de gerenciamento](#): Protege as conexões do navegador web do cliente com as interfaces de gerenciamento do StorageGRID.
- [Certificado da API S3](#): Protege as conexões da API do cliente com os Nós de Armazenamento, Nós de Administração e Nós de Gateway, que os aplicativos cliente do S3 usam para fazer upload e download de 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 grid.
- **Data de expiração**: Se estiver usando o certificado padrão, nenhuma data de expiração é exibida.

Você pode:

- Substitua os certificados padrão por certificados personalizados assinados por uma autoridade certificadora externa para melhorar a segurança do grid:
 - ["Substitua o certificado de interface de gerenciamento padrão gerado pelo StorageGRID"](#) Usado para conexões do Grid Manager e do Tenant Manager.
 - ["Substitua o certificado da API S3"](#) Usado para conexões com o Storage Node e o endpoint do load balancer (opcional).
- ["Restaurar o certificado padrão da interface de gerenciamento"](#).
- ["Restaurar o certificado padrão da API S3"](#).
- ["Use um script para gerar um novo certificado de interface de gerenciamento autoassinado"](#).
- Copie ou baixe o ["certificado da interface de gerenciamento"](#) ou ["Certificado da API S3"](#).

Grid CA

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

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

Você pode ["Copie ou faça o download do certificado Grid CA"](#), mas não pode mudar.

Cliente

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

A tabela de certificados possui 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 expiração do certificado.

Você pode:

- ["Faça o upload ou gere um novo certificado de cliente."](#)
- Selecione o nome do certificado para exibir os detalhes do certificado, onde você pode:
 - ["Altere o nome do certificado do cliente."](#)
 - ["Defina a permissão de acesso do Prometheus."](#)
 - ["Faça o upload e substitua o certificado do cliente."](#)
 - ["Copie ou faça o download do certificado do cliente."](#)
 - ["Remova o certificado do cliente."](#)
- Selecione **Ações** para rapidamente ["editar"](#), ["anexar"](#) ou ["remover"](#) um certificado de cliente. Você pode selecionar até 10 certificados de cliente e removê-los de uma só vez usando **Ações > Remover**.

Pontos de extremidade do balanceador de carga

[Certificados de endpoint do balanceador de carga](#) Proteja as conexões entre os clientes S3 e o serviço StorageGRID Load Balancer nos nós de gateway e nos nós de administração.

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



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

Você pode:

- ["Visualizar um endpoint de balanceador de carga"](#), incluindo os detalhes do certificado.
- ["Especifique um certificado de endpoint do balanceador de carga para FabricPool."](#)
- ["Use o certificado global da API S3"](#) em vez de gerar um novo certificado de endpoint do balanceador de carga.

Locatários

Os inquilinos podem usar [certificados do servidor de federação de identidades](#) ou [certificados de endpoint de serviço da plataforma](#) para proteger suas conexões com StorageGRID.

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

Você pode:

- ["Selecione um nome de inquilino para entrar no Tenant Manager"](#)
- ["Selecione um nome de locatário para visualizar os detalhes da federação de identidade do locatário"](#)
- ["Selecione um nome de locatário para ver os detalhes dos serviços da plataforma do locatário"](#)
- ["Especifique um certificado de endpoint de serviço de plataforma durante a criação do endpoint"](#)

Outro

StorageGRID utiliza outros certificados de segurança para fins específicos. Esses certificados estão listados por seu nome funcional. Outros certificados de segurança incluem:

- [Certificados do Cloud Storage Pool](#)
- [Certificados de notificação de alerta por e-mail](#)
- [Certificados externos do servidor syslog](#)
- [Certificados de conexão de grid federation](#)
- [Certificados de federação de identidade](#)
- [Certificados do servidor de gerenciamento de chaves \(KMS\)](#)
- [Certificados de single sign-on](#)

As informações indicam o tipo de certificado que uma função utiliza e as datas de expiração dos certificados de servidor e cliente, quando aplicável. Selecionar o nome de uma função abre uma aba do navegador onde você pode visualizar e editar os detalhes do certificado.



Você só pode visualizar e acessar informações de outros certificados se tiver o "permissão apropriada".

Você pode:

- ["Especifique um certificado de Cloud Storage Pool para S3, C2S S3 ou Azure"](#)
- ["Especifique um certificado para notificações de alerta por e-mail"](#)
- ["Use um certificado para um servidor syslog externo"](#)
- ["Girar certificados de conexão da federação de grid"](#)
- ["Visualizar e editar um certificado de federação de identidades"](#)
- ["Carregar certificados do servidor de gerenciamento de chaves \(KMS\) e do cliente"](#)
- ["Especifique manualmente um certificado SSO para uma relação de confiança de terceiros"](#)

Detalhes do certificado de segurança

Cada tipo de certificado de segurança é descrito abaixo, com links para as instruções de implementação.

Certificado da interface de gerenciamento

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre os navegadores web do cliente e a interface de gerenciamento do StorageGRID, permitindo que você acesse o Grid Manager e o Tenant Manager sem avisos de segurança. Este certificado também autentica as conexões da Grid Management API e da Tenant Management API. Você pode usar o certificado padrão criado durante a instalação ou carregar um certificado personalizado.	Em Configuração > Segurança > Certificados , selecione a guia Global e, em seguida, selecione Certificado da interface de gerenciamento	"Configurar certificados da interface de gerenciamento"

Certificado da API S3

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica conexões seguras de clientes S3 a um nó de armazenamento e a endpoints de balanceamento de carga (opcional).	Configuração > Segurança > Certificados , selecione a guia Global e, em seguida, selecione S3 API certificate	"Configurar certificados da API S3"

Certificado CA da Grid

Consulte o [Descrição padrão do certificado CA do Grid](#).

Certificado de cliente administrador

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Cliente	Instalado em cada cliente, permitindo que StorageGRID autentique o acesso de clientes externos. • Permite que clientes externos autorizados acessem o banco de dados StorageGRID Prometheus. • Permite o monitoramento seguro do StorageGRID usando ferramentas externas.	Configuração > Segurança > Certificados e então selecione a guia Cliente	"Configurar certificados de cliente"

Certificado de endpoint do balanceador de carga

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre clientes S3 e o serviço StorageGRID Load Balancer nos nós de gateway e nós de administração. Você pode carregar ou gerar um certificado de balanceador de carga ao configurar um endpoint de balanceador de carga. Os aplicativos cliente usam o certificado do balanceador de carga ao se conectarem ao StorageGRID para salvar e recuperar dados de objetos. Você também pode usar uma versão personalizada do Certificado da API S3 certificado global para autenticar conexões com o serviço de Load Balancer. Se o certificado global for usado para autenticar conexões com o Load Balancer, você não precisa carregar ou gerar um certificado separado para cada endpoint do Load Balancer. Nota: O certificado usado para autenticação do balanceador de carga é o certificado mais utilizado durante a operação normal do StorageGRID.	Configuração > Rede > Pontos de extremidade do balanceador de carga	• "Configurar pontos de extremidade do balanceador de carga" • "Crie um ponto de extremidade de balanceamento de carga para FabricPool"

Certificado de endpoint do Cloud Storage Pool

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão de um StorageGRID Cloud Storage Pool para um local de armazenamento externo, como S3 Glacier ou Microsoft Azure Blob storage. É necessário um certificado diferente para cada tipo de provedor de nuvem.	ILM > Pools de armazenamento	"Criar um Cloud Storage Pool"

Certificado de notificação de alerta por e-mail

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre um servidor de e-mail SMTP e StorageGRID usado para notificações de alerta. • Se a comunicação com o servidor SMTP exigir Segurança da Camada de Transporte (TLS), você deve especificar o certificado da Autoridade Certificadora (CA) do servidor de e-mail. • Especifique um certificado de cliente somente se o servidor de e-mail SMTP exigir certificados de cliente para autenticação.	Alertas > Configuração de e-mail	"Configure notificações por e-mail para alertas"

Certificado de servidor syslog externo

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão TLS ou RELP/TLS entre um servidor syslog externo que registra eventos no StorageGRID. Nota: Não é necessário um certificado de servidor syslog externo para conexões TCP, RELP/TCP e UDP com um servidor syslog externo.	Configuração > Monitoramento > Servidor de auditoria e syslog	"Use um servidor syslog externo"

Certificado de conexão de federação de grid

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autenticar e criptografar informações enviadas entre o sistema StorageGRID atual e outra grade em uma conexão de federação de grades.	Configuração > Sistema > Grid federation	• "Criar conexões de federação de grid" • "Rotacionar certificados de conexão"

Certificado de federação de identidade

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre StorageGRID e um provedor de identidade externo, como Active Directory, OpenLDAP ou Oracle Directory Server. Usado para federação de identidades, que permite que grupos de administradores e usuários sejam gerenciados por um sistema externo.	Configuração > Controle de acesso > Federação de identidades	"Use federação de identidades"

Certificado do servidor de gerenciamento de chaves (KMS)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre StorageGRID e um servidor de gerenciamento de chaves externo (KMS), que fornece chaves de criptografia para os nós do dispositivo StorageGRID.	Configuração > Segurança > Servidor de gerenciamento de chaves	"Adicionar servidor de gerenciamento de chaves (KMS)"

Certificado de endpoint de serviços de plataforma

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão do serviço da plataforma StorageGRID com um recurso de armazenamento S3.	Gerenciador de Locatários > ARMAZENAMENTO (S3) > Pontos de extremidade de serviços da plataforma	"Criar endpoint de serviços de plataforma" "Editar endpoint de serviços da plataforma"

Certificado de single sign-on (SSO)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre serviços de federação de identidade, como Active Directory Federation Services (AD FS), e StorageGRID que são usados para solicitações de logon único (SSO).	Configuração > Controle de acesso > Autenticação única	"Configure o single sign-on (SSO)"

Exemplos de certificados

Exemplo 1: serviço de balanceador de carga

Neste exemplo, StorageGRID atua como o servidor.

1. Você configura um endpoint de balanceador de carga e carrega ou gera um certificado de servidor no StorageGRID.
2. Você configura uma conexão de cliente S3 com o endpoint do balanceador de carga e carrega o mesmo certificado no cliente.

3. Quando o cliente deseja salvar ou recuperar dados, ele se conecta ao endpoint do balanceador de carga usando HTTPS.
4. StorageGRID responde com o certificado do servidor, que contém uma chave pública, e com uma assinatura baseada na chave privada.
5. O cliente compara a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas coincidirem, o cliente inicia uma sessão usando a mesma chave pública.
6. O cliente envia dados de objetos para StorageGRID.

Exemplo 2: servidor externo de gerenciamento de chaves (KMS)

Neste exemplo, StorageGRID atua como o cliente.

1. Utilizando um software externo de Key Management Server, você configura o StorageGRID como um cliente KMS e obtém um certificado de servidor assinado por uma autoridade certificadora (CA), um certificado de cliente público e a chave privada para o certificado de cliente.
2. Utilizando o Grid Manager, você configura um servidor KMS e faz upload dos certificados do servidor e do cliente, além da chave privada do cliente.
3. Quando um nó do StorageGRID precisa de uma chave de criptografia, ele faz uma solicitação ao servidor KMS que inclui dados do certificado e uma assinatura baseada 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.

Tipos de certificados de servidor suportados no StorageGRID

O sistema StorageGRID suporta certificados personalizados criptografados com RSA ou ECDSA (Algoritmo de Assinatura Digital de Curva Elíptica).



O tipo de cifra para a política de segurança deve corresponder ao tipo de certificado do servidor. Por exemplo, cifras RSA exigem certificados RSA e cifras ECDSA exigem certificados ECDSA. Consulte ["Gerenciar certificados de segurança"](#). Se você configurar uma política de segurança personalizada que não seja compatível com o certificado do servidor, você pode ["reverter temporariamente para a política de segurança padrão"](#).

Para obter mais informações sobre como o StorageGRID protege as conexões do cliente, consulte ["Segurança para clientes S3"](#).

Configurar certificados da interface de gerenciamento no StorageGRID

Você pode substituir o certificado padrão da interface de gerenciamento por um único certificado personalizado que permite aos usuários acessar o Grid Manager e o Tenant Manager sem encontrar avisos de segurança. Você também pode reverter para o certificado padrão da interface de gerenciamento ou gerar um novo.

Sobre esta tarefa

Por padrão, cada nó administrativo recebe um certificado assinado pela CA da grid. Esses certificados assinados pela CA podem ser substituídos por um único certificado de interface de gerenciamento personalizado comum e a 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 de vários domínios se os clientes precisarem verificar o nome do host ao se conectarem ao Grid Manager e ao Tenant Manager. Defina o certificado personalizado de forma que ele corresponda a todos os Nós de Administração na grid.

Você precisa concluir a configuração no servidor e, dependendo da autoridade de certificação raiz (CA) que estiver usando, os usuários também podem precisar instalar o certificado da CA do Grid no navegador da web que usarão para acessar o Grid Manager e o Tenant Manager.



Para garantir que as operações não sejam interrompidas por uma falha no certificado do servidor, o alerta **Expiração do certificado do servidor para a interface de gerenciamento** é acionado quando este certificado está prestes a expirar. Se necessário, você pode verificar quando o certificado atual expira selecionando **Configuração > Segurança > Certificados** e consultando a data de expiração do certificado da interface de gerenciamento na guia Global.



Se você estiver acessando o Grid Manager ou o Tenant Manager usando um nome de domínio em vez de um endereço IP, o navegador exibirá um erro de certificado sem opção para ignorá-lo caso ocorra uma das seguintes situações:

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

Adicionar 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 Grid Manager.

Passos

1. Selecione **Configuração > Segurança > Certificados**.
2. Na guia **Global**, selecione **Certificado da interface de gerenciamento**.
3. Selecione **Usar certificado personalizado**.
4. Faça o upload ou gere o certificado.

Carregar certificado

Faça o upload dos arquivos de certificado do servidor necessários.

a. Selecione **Carregar certificado**.

b. Faça o upload dos arquivos de certificado de servidor necessários:

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



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

- **Pacote de CA:** Um único arquivo opcional contendo os certificados de cada autoridade certificadora (CA) intermediária. O arquivo deve conter cada um dos arquivos de certificado da CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote de CA opcional, cada certificado é 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 certificados.

Especifique o nome do arquivo do 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 CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Salvar**. + O certificado da interface de gerenciamento personalizada é usado para todas as novas conexões subsequentes com o Grid Manager, Tenant Manager, Grid Manager API ou Tenant Manager API.

Gerar certificado

Gere os arquivos de certificado do servidor.



A melhor prática para um ambiente de produção é usar um certificado de interface de gerenciamento personalizado, assinado por uma autoridade certificadora externa.

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados para incluir no certificado. Use um * como caractere curinga para representar vários nomes de domínio.

Campo	Descrição
IP	Um ou mais endereços IP para incluir no certificado.
Assunto (opcional)	Nome diferenciado (DN) ou subject X.509 do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usa o primeiro nome de domínio ou endereço IP como nome comum do sujeito (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. Nota: Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluírem essas extensões.

c. Selecione **Gerar**.

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

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

Por exemplo: `storagegrid_certificate.pem`

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

e. Selecione **Salvar**. + O certificado da interface de gerenciamento personalizada é usado para todas as novas conexões subsequentes com o Grid Manager, Tenant Manager, Grid Manager API ou Tenant Manager API.

5. Atualize a página para garantir que o navegador web esteja atualizado.



Após carregar ou gerar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados sejam resolvidos.

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

Restaurar o certificado padrão da interface de gerenciamento

Você pode voltar a usar o certificado de interface de gerenciamento padrão para conexões do Grid Manager e do Tenant Manager.

Passos

1. Selecione **Configuração > Segurança > Certificados**.
2. Na guia **Global**, selecione **Certificado da interface de gerenciamento**.
3. Selecione **Usar certificado padrão**.

Ao restaurar o certificado da interface de gerenciamento padrão, os arquivos de certificado de servidor personalizados que você configurou são excluídos e não podem ser recuperados do sistema. O certificado da interface de gerenciamento padrão é usado para todas as novas conexões de clientes subsequentes.

4. Atualize a página para garantir que o navegador web esteja atualizado.

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

Caso seja necessária uma validação rigorosa do nome do host, você pode usar um script para gerar o certificado da interface de gerenciamento.

Antes de começar

- Você tem "[permissões de acesso específicas](#)".
- Você tem o arquivo `Passwords.txt`.

Sobre esta tarefa

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

Passos

1. Obtenha o nome de domínio totalmente qualificado (FQDN) de cada nó administrativo.
2. Faça login no nó de administração principal:
 - a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
 - b. Digite a senha listada no arquivo `Passwords.txt`.
 - c. Digite o seguinte comando para alternar para root: `su -`
 - d. Digite a senha listada no arquivo `Passwords.txt`.

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

3. Configurar 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 Admin Nodes. Por exemplo, `*.ui.storagegrid.example.com` usa o curinga `*` para representar `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
- Defina `--type` para `management` configurar o certificado da interface de gerenciamento, que é usado pelo Grid Manager e pelo Tenant Manager.
- 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 StorageGRID; caso contrário, o cliente pode rejeitar o certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
```

O resultado obtido contém o certificado público necessário para o seu cliente da API de gerenciamento.

4. Selecione e copie o certificado.

Inclua as tags BEGIN e END na sua seleção.

5. Saia do terminal de comandos. `$ exit`

6. Confirme se o certificado foi configurado:

- a. Acesse o Grid Manager.
- b. Selecione **Configuração > Segurança > Certificados**
- c. Na guia **Global**, selecione **Certificado da interface de gerenciamento**.

7. Configure seu cliente de gerenciamento para usar o certificado público que você copiou. Inclua as tags BEGIN e END.

Baixe ou copie o certificado da interface de gerenciamento

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

Passos

1. Selecione **Configuração > Segurança > Certificados**.
2. Na guia **Global**, selecione **Certificado da interface de gerenciamento**.
3. Selecione a guia **Servidor** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Baixe o arquivo de certificado ou o pacote de CA

Faça o download do arquivo de certificado ou do pacote de CA .pem. Se você estiver usando um pacote de CA opcional, cada certificado do pacote é exibido em sua própria subguia.

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

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

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

Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote PEM da CA

Copie o texto do certificado para colar em outro local. Se você estiver usando um pacote de CA opcional, cada certificado do pacote será exibido em sua própria subguia.

a. Selecione **Copiar certificado PEM** ou **Copiar CA bundle PEM**.

Se você estiver copiando um pacote de certificados de autoridade de certificação (CA bundle), todos os certificados nas guias secundárias do pacote de CA são 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`

Configurar os certificados da API S3 no StorageGRID

Você pode substituir ou restaurar o certificado do servidor usado para conexões de clientes S3 com nós de armazenamento ou com endpoints de balanceadores de carga. O certificado de servidor personalizado de substituição é específico para sua organização.



Detalhes sobre o Swift foram removidos desta versão do site de documentação. Veja ["StorageGRID 11.8: Configurar certificados das APIs S3 e Swift"](#).

Sobre esta tarefa

Por padrão, cada Storage Node recebe um certificado de servidor X.509 assinado pela CA da grid. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e a chave privada correspondente.

Um único certificado de servidor personalizado é usado para todos os Storage Nodes, então você deve especificar o certificado como um curinga ou multi-domain certificate se os clientes precisarem verificar o hostname ao se conectarem ao endpoint de armazenamento. Defina o certificado personalizado de forma que ele corresponda a todos os Storage Nodes na grid.

Após concluir a configuração no servidor, você também poderá precisar instalar o certificado da Autoridade Certificadora (CA) do Grid no cliente da API S3 que você usará para acessar o sistema, dependendo da autoridade certificadora raiz (CA) que você estiver utilizando.



Para garantir que as operações não sejam interrompidas por uma falha no certificado do servidor, o alerta **Expiração do certificado global do servidor para a API do S3** é acionado quando o certificado raiz do servidor está prestes a expirar. Conforme necessário, você pode ver quando o certificado atual expira selecionando **Configuração > Segurança > Certificados** e consultando a data de expiração do certificado da API do S3 na guia Global.

Você pode carregar ou gerar um certificado de API S3 personalizado.

Adicionar um certificado de API S3 personalizado

Passos

1. Selecione **Configuração > Segurança > Certificados**.
2. Na aba **Global**, selecione **S3 API certificate**.
3. Selecione **Usar certificado personalizado**.
4. Faça o upload ou gere o certificado.

Carregar certificado

Faça o upload dos arquivos de certificado do servidor necessários.

a. Selecione **Carregar certificado**.

b. Faça o upload dos arquivos de certificado de servidor necessários:

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



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

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

Especifique o nome do arquivo do 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 CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Salvar**.

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

Gerar certificado

Gere os arquivos de certificado do servidor.

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados para incluir no certificado. Use um * como caractere curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP para incluir no certificado.

Campo	Descrição
Assunto (opcional)	Nome diferenciado (DN) ou subject X.509 do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usa o primeiro nome de domínio ou endereço IP como nome comum do sujeito (CN).
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. Nota: Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluírem essas extensões.

c. Selecione **Gerar**.

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

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

Por exemplo: `storagegrid_certificate.pem`

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

e. Selecione **Salvar**.

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

5. Selecione uma aba para exibir metadados do certificado padrão do servidor StorageGRID, de um certificado assinado por uma CA que foi carregado ou de um certificado personalizado que foi gerado.



Após carregar ou gerar um novo certificado, aguarde até um dia para que quaisquer alertas de expiração de certificado relacionados sejam resolvidos.

6. Atualize a página para garantir que o navegador web esteja atualizado.

7. Após adicionar um certificado de API S3 personalizado, a página de certificados da API S3 exibe informações detalhadas sobre o certificado personalizado em uso. Você pode baixar ou copiar o arquivo PEM do certificado conforme necessário.

Restaurar o certificado padrão da API S3

Você pode voltar a usar o certificado padrão da API S3 para conexões de clientes S3 com os nós de armazenamento. No entanto, você não pode usar o certificado padrão da API S3 para um endpoint de balanceador de carga.

Passos

1. Selecione **Configuração > Segurança > Certificados**.
2. Na aba **Global**, selecione **S3 API certificate**.
3. Selecione **Usar certificado padrão**.

Ao restaurar a versão padrão do certificado global da API S3, os arquivos de certificado de servidor personalizados que você configurou são excluídos e não podem ser recuperados do sistema. O certificado padrão da API S3 será usado para novas conexões de cliente S3 subsequentes com os Storage Nodes.

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

Se você tiver permissão de acesso Root e o certificado personalizado da API S3 tiver sido usado para conexões de endpoints do balanceador de carga, será exibida uma lista dos endpoints do balanceador de carga que não estarão mais acessíveis usando o certificado padrão da API S3. Vá para "[Configurar pontos de extremidade do balanceador de carga](#)" para editar ou remover os endpoints afetados.

5. Atualize a página para garantir que o navegador web esteja atualizado.

Baixe ou copie o certificado da API S3

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

Passos

1. Selecione **Configuração > Segurança > Certificados**.
2. Na aba **Global**, selecione **S3 API certificate**.
3. Selecione a guia **Servidor** ou **CA bundle** e, em seguida, baixe ou copie o certificado.

Baixe o arquivo de certificado ou o pacote de CA

Faça o download do arquivo de certificado ou do pacote de CA .pem. Se você estiver usando um pacote de CA opcional, cada certificado do pacote é exibido em sua própria subguia.

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

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

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

Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote PEM da CA

Copie o texto do certificado para colar em outro local. Se você estiver usando um pacote de CA opcional, cada certificado do pacote será exibido em sua própria subguia.

a. Selecione **Copiar certificado PEM** ou **Copiar CA bundle PEM**.

Se você estiver copiando um pacote de certificados de autoridade de certificação (CA bundle), todos os certificados nas guias secundárias do pacote de CA são 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

- ["Utilize a API REST S3"](#)
- ["Configurar nomes de domínio de endpoint S3"](#)

Copie o certificado CA do StorageGRID Grid

StorageGRID utiliza uma autoridade de certificação (CA) interna para proteger o tráfego interno. Este certificado não se altera caso você carregue seus próprios certificados.

Antes de começar

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

Sobre esta tarefa

Se um certificado de servidor personalizado tiver sido configurado, os aplicativos cliente deverão verificar o servidor usando o certificado de servidor personalizado. Eles não devem copiar o certificado da CA do StorageGRID.

Passos

1. Selecione **Configuração > Segurança > Certificados** e, em seguida, selecione a guia **Grid CA**.
2. Na seção **Certificado PEM**, faça o download ou copie o certificado.

Baixar arquivo de certificado

Baixe o arquivo de certificado .pem.

- a. Selecione **Baixar certificado**.
- b. Especifique o nome do arquivo do 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

Configure os certificados do StorageGRID para FabricPool

Para clientes S3 que realizam validação rigorosa de nome de host e não suportam a desativação dessa validação, como clientes ONTAP que utilizam FabricPool, você pode gerar ou carregar um certificado de servidor ao configurar o endpoint do balanceador de carga.

Antes de começar

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

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 certificadora (CA) reconhecida. Em ambientes de produção, você deve usar um certificado assinado por uma CA reconhecida. Certificados assinados por uma CA podem ser rotacionados sem interrupção. Eles também são mais seguros porque oferecem melhor proteção contra ataques man-in-the-middle.

Os passos a seguir fornecem diretrizes gerais para clientes S3 que utilizam FabricPool. Para obter informações e procedimentos mais detalhados, consulte ["Configurar o StorageGRID para FabricPool"](#).

Passos

1. Opcionalmente, configure um grupo de alta disponibilidade (HA) para o FabricPool usar.
2. Crie um endpoint de balanceador de carga S3 para FabricPool usar.

Ao criar um endpoint de balanceador de carga HTTPS, você será solicitado a carregar seu certificado do servidor, a chave privada do certificado e, opcionalmente, o pacote de CA.

3. Anexe StorageGRID como uma camada de nuvem no ONTAP.

Especifique a porta do 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 da CA.



Se o certificado StorageGRID foi emitido por uma autoridade certificadora intermediária, você deve fornecer o certificado dessa autoridade certificadora intermediária. Se o certificado StorageGRID foi emitido diretamente pela autoridade certificadora raiz, você deve fornecer o certificado dessa autoridade certificadora raiz.

Configurar certificados de cliente no StorageGRID

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

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

Veja ["Gerenciar certificados de segurança"](#) e ["Configurar certificados de servidor personalizados"](#).



Para garantir que as operações não sejam interrompidas por uma falha no certificado do servidor, o alerta **Expiração dos certificados do cliente configurados na página Certificados** é acionado quando este certificado do servidor está prestes a expirar. Se necessário, você pode verificar quando o certificado atual expira selecionando **Configuração > Segurança > Certificados** e consultando a data de expiração do certificado do cliente na guia Cliente.



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

Antes de começar

- Você tem permissão de acesso root.
- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Para configurar um certificado de cliente:
 - Você possui o endereço IP ou nome de domínio do Admin Node.
 - Se você configurou o certificado da interface de gerenciamento do StorageGRID, você possui a CA, o certificado do cliente e a chave privada usados para configurar o certificado da interface de gerenciamento.
 - Para carregar seu próprio certificado, a chave privada do certificado está disponível em seu computador local.
 - A chave privada deve ter sido salva ou registrada 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 possui o endereço IP ou nome de domínio do Admin Node.
 - Para carregar seu próprio certificado ou um novo certificado, a chave privada, o certificado do cliente e a CA (se utilizada) estão disponíveis em seu computador local.

Adicionar certificados de cliente

Para adicionar o certificado do cliente, utilize um destes procedimentos:

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

O certificado da interface de gerenciamento já está configurado

Utilize este procedimento para adicionar um certificado de cliente caso um certificado de interface de gerenciamento já esteja configurado utilizando uma CA fornecida pelo cliente, certificado de cliente e chave privada.

Passos

1. No Grid Manager, selecione **Configuração > Segurança > Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione **Add**.
3. Insira um nome de certificado.
4. Para acessar métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir prometheus**.
5. Selecione **Continue**.
6. Na etapa **Anexar certificados**, carregue o certificado da interface de gerenciamento.
 - a. Selecione **Carregar certificado**.
 - b. Selecione **Procurar** e selecione o arquivo de certificado da interface de gerenciamento (.pem).
 - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o certificado PEM.
 - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado para colar em outro lugar.
 - c. Selecione **Criar** para salvar o certificado no Grid Manager.

O novo certificado aparece na guia Cliente.

7. [Configurar uma ferramenta de monitoramento externa](#), como Grafana.

Certificado de cliente emitido pela CA

Use este procedimento para adicionar um certificado de cliente administrador caso um certificado de interface de gerenciamento não tenha sido configurado e você planeje adicionar um certificado de cliente para o Prometheus que utilize um certificado de cliente e uma chave privada emitidos por uma Autoridade Certificadora (CA).

Passos

1. Execute os passos para "[configurar um certificado de interface de gerenciamento](#)".
2. No Grid Manager, selecione **Configuração > Segurança > Certificados** e, em seguida, selecione a guia **Cliente**.
3. Selecione **Add**.
4. Insira um nome de certificado.
5. Para acessar métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir prometheus**.
6. Selecione **Continue**.
7. Na etapa **Anexar certificados**, carregue o certificado do cliente, a chave privada e os arquivos do pacote de certificados da autoridade certificadora (CA):
 - a. Selecione **Carregar certificado**.
 - b. Selecione **Procurar** e selecione o certificado do cliente, a chave privada e os arquivos do pacote da CA (.pem).
 - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o certificado PEM.
 - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado para colar em outro lugar.
 - c. Selecione **Criar** para salvar o certificado no Grid Manager.

Os novos certificados aparecem na guia Cliente.

8. [Configurar uma ferramenta de monitoramento externa](#), como Grafana.

Certificado gerado pelo Grid Manager

Utilize este procedimento para adicionar um certificado de cliente administrador caso um certificado de interface de gerenciamento não tenha sido configurado e você planeje adicionar um certificado de cliente para o Prometheus que utilize a função de gerar certificado no Grid Manager.

Passos

1. No Grid Manager, selecione **Configuração > Segurança > Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione **Add**.
3. Insira um nome de certificado.
4. Para acessar métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir prometheus**.
5. Selecione **Continue**.
6. Na etapa **Anexar certificados**, selecione **Gerar certificado**.
7. Especifique as informações do certificado:
 - **Assunto** (opcional): assunto X.509 ou nome diferenciado (DN) do proprietário do certificado.
 - **Dias de validade**: o número de dias que o certificado gerado é válido, a partir do momento em que é gerado.
 - **Adicionar extensões de uso de chave**: Se selecionado (padrão e recomendado), as extensões de uso de chave e de uso de chave estendido são adicionadas ao certificado gerado.

Essas extensões definem a finalidade da chave contida no certificado.



Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

8. Selecione **Gerar**.

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



Você não poderá visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou baixe a chave para um local seguro.

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- Selecione **Baixar certificado** para salvar o arquivo de certificado.

Especifique o nome do arquivo do 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 **Baixar chave privada** para salvar a chave privada como um arquivo.

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

10. Selecione **Criar** para salvar o certificado no Grid Manager.

O novo certificado aparece na guia Cliente.

11. No Grid Manager, selecione **Configuração > Segurança > Certificados** e, em seguida, selecione a guia **Global**.

12. Selecione **certificado da interface de gerenciamento**.

13. Selecione **Usar certificado personalizado**.

14. Faça o upload dos arquivos `certificate.pem` e `private_key.pem` da [detalhes do certificado do cliente](#) etapa. Não é necessário fazer o upload do CA bundle.

- Selecione **Carregar certificado** e depois selecione **Continuar**.
- Faça o upload de cada arquivo de certificado (`.pem`).
- Selecione **Salvar** para salvar o certificado no Grid Manager.

O novo certificado aparece na página de certificados da interface de gerenciamento.

15. [Configurar uma ferramenta de monitoramento externa](#), como Grafana.

Configurar uma ferramenta de monitoramento externa

Passos

- Configure as seguintes configurações na sua ferramenta de monitoramento externa, como o Grafana.
 - Nome:** Insira um nome para a conexão.

StorageGRID não exige essas informações, mas você precisa fornecer um nome para testar a conexão.

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

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

- c. Ative **Autenticação de Cliente TLS** e **Com Certificado CA**.

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

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

- e. **ServerName:** insira o nome de domínio do nó de administração.

ServerName deve corresponder ao nome de domínio conforme aparece no certificado da interface de gerenciamento.

2. 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 do Prometheus do StorageGRID com sua ferramenta de monitoramento externa.

Para obter informações sobre as métricas, consulte o "[Instruções para monitoramento do StorageGRID](#)".

Editar certificados de cliente

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

Passos

1. Selecione **Configuração > Segurança > Certificados** e, em seguida, selecione a guia **Cliente**.

As datas de expiração dos certificados e as permissões de acesso do Prometheus são listadas na tabela. Se um certificado estiver prestes a expirar ou já estiver expirado, uma mensagem aparece na tabela e um alerta é acionado.

2. Selecione o certificado que você deseja editar.
3. Selecione **Editar** e depois selecione **Editar nome e permissão**
4. Insira um nome de certificado.
5. Para acessar métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir prometheus**.
6. Selecione **Continuar** para salvar o certificado no Grid Manager.

O certificado atualizado é exibido na guia Cliente.

Anexar novo certificado de cliente

Você pode enviar um novo certificado quando o atual expirar.

Passos

1. Selecione **Configuração > Segurança > Certificados** e, em seguida, selecione a guia **Cliente**.

As datas de expiração dos certificados e as permissões de acesso do Prometheus são listadas na tabela. Se um certificado estiver prestes a expirar ou já estiver expirado, uma mensagem aparece na tabela e um alerta é acionado.

2. Selecione o certificado que você deseja 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 depois selecione **Continuar**.
- b. Faça upload do nome do certificado do cliente (.pem).

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

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

Por exemplo: storagegrid_certificate.pem

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado para colar em outro lugar.
- c. Selecione **Criar** para salvar o certificado no Grid Manager.

O certificado atualizado é exibido na guia Cliente.

Gerar certificado

Gere o texto do certificado para colar em outro lugar.

- a. Selecione **Gerar certificado**.
- b. Especifique as informações do certificado:

- **Assunto** (opcional): assunto X.509 ou nome diferenciado (DN) do proprietário do certificado.
- **Dias de validade**: o número de dias que o certificado gerado é válido, a partir do momento em que é gerado.
- **Adicionar extensões de uso de chave**: Se selecionado (padrão e recomendado), as extensões de uso de chave e de uso de chave estendido são adicionadas ao certificado gerado.

Essas extensões definem a finalidade da chave contida no certificado.



Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluírem essas extensões.

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



Você não poderá visualizar a chave privada do certificado depois de fechar a caixa de diálogo. Copie ou baixe a chave para um local seguro.

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado para colar em outro

lugar.

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

Especifique o nome do arquivo do 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 **Baixar chave privada** para salvar a chave privada como um arquivo.

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

e. Selecione **Criar** para salvar o certificado no Grid Manager.

O novo certificado aparece na guia Cliente.

Baixe ou copie os certificados do cliente

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

Passos

1. Selecione **Configuração > Segurança > Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione o certificado que você deseja copiar ou baixar.
3. Faça o download ou copie o certificado.

Baixar arquivo de certificado

Baixe o arquivo de certificado `.pem`.

- a. Selecione **Baixar certificado**.
- b. Especifique o nome do arquivo do 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 **Configuração > Segurança > Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione o certificado que você deseja remover.
3. Selecione **Excluir** e confirme.



Para remover até 10 certificados, selecione cada certificado que deseja remover na guia Cliente e selecione **Ações > Excluir**.

Após a remoção de um certificado, os clientes que o utilizavam devem especificar um novo certificado de cliente para acessar o banco de dados StorageGRID Prometheus.

Configurar as configurações de segurança

Gerencie a política de TLS e SSH no StorageGRID

A política de TLS e SSH determina quais protocolos e cifras são usados para estabelecer conexões TLS seguras com aplicativos cliente e conexões SSH seguras com serviços internos do StorageGRID.

A política de segurança controla como o TLS e o SSH criptografam os dados em trânsito. Em geral, use a política de compatibilidade Modern (padrão), a menos que seu sistema precise estar em conformidade com Common Criteria ou que você precise usar outros cifradores.



Alguns serviços do StorageGRID ainda não foram atualizados para usar as cifras presentes nessas políticas.

Antes de começar

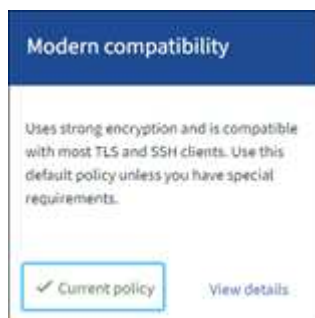
- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).

Selecione uma política de segurança

Passos

1. Selecione **Configuração > Segurança > Configurações de segurança**.

A aba **Políticas de TLS e SSH** mostra as políticas disponíveis. A política atualmente ativa é indicada por uma marca de seleção verde no bloco da política.



2. Consulte as abas para saber mais sobre as políticas disponíveis.

Compatibilidade moderna (padrão)

Use a política padrão se precisar de criptografia forte e não tiver requisitos especiais. Essa política é compatível com a maioria dos clientes TLS e SSH.

Compatibilidade com versões anteriores

Use a política de compatibilidade Legado se você precisar de opções de compatibilidade adicionais para clientes mais antigos. As opções adicionais desta política podem torná-la menos segura do que a política de compatibilidade Moderna.

Critérios Comuns

Utilize a política de Common Criteria se você precisar de certificação Common Criteria.

FIPS estrito

Use a política FIPS estrita se você precisar de certificação Common Criteria e precisar usar o NetApp Cryptographic Security Module (NCSM) 3.0.8 ou o módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 para conexões de clientes externos com os endpoints do balanceador de carga, Tenant Manager e Grid Manager. O uso dessa política pode reduzir o desempenho.

O NCSM 3.0.8 e o módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 são usados nas seguintes operações:

- NCSM
 - Conexões TLS entre os seguintes serviços: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw e cache-svc
 - Conexões TLS entre clientes e o serviço nginx-gw (endpoints do balanceador de carga)
 - Conexões TLS entre clientes e o serviço LDR
 - Criptografia de conteúdo de objeto para SSE-S3, SSE-C e a configuração de criptografia de objeto armazenado
 - Conexões SSH

Para obter mais informações, consulte o Programa de Validação de Algoritmos Criptográficos do NIST "[Certificado nº 4838](#)".

- NetApp StorageGRID módulo da API de criptografia do kernel

O módulo StorageGRID Kernel Crypto API da NetApp está presente apenas nas plataformas de VM e appliance StorageGRID.

- Coleta de entropia
- Criptografia de nó

Para obter mais informações, consulte o Programa de Validação de Algoritmos Criptográficos do NIST "[Certificados nº A6242 a nº A6257](#)" e "[Certificado de Entropia nº E223](#)".

Nota: Após selecionar esta política, "[execute uma reinicialização gradual](#)" para todos os nós para ativar o NCSM. Use **Manutenção > reinicialização em andamento** para iniciar e monitorar as reinicializações.

Personalizado

Crie uma política personalizada se você precisar aplicar seus próprios cifradores.

Opcionalmente, se o seu StorageGRID tiver requisitos de criptografia FIPS 140, habilite o recurso de modo FIPS para usar o NCSM 3.0.8 e o módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64:

- Defina o `fipsMode` parâmetro para `true`.
- Quando solicitado, **"execute uma reinicialização gradual"** ative os módulos de criptografia em todos os nós. Use **Manutenção > reinicialização contínua** para iniciar e monitorar as reinicializações.
- Selecione **Suporte > Diagnóstico** para visualizar as versões ativas do módulo FIPS.

3. Para ver detalhes sobre as cifras, protocolos e algoritmos de cada política, selecione **Ver detalhes**.

4. Para alterar a política atual, selecione **Usar política**.

Uma marca de seleção verde aparece ao lado de **Current policy** no bloco de políticas.

Criar uma política de segurança personalizada

Você pode criar uma política personalizada se precisar aplicar seus próprios cifradores.

Passos

- Na aba da política mais semelhante à política personalizada que você deseja criar, selecione **Ver detalhes**.
- Selecione **Copiar para a área de transferência** e, em seguida, selecione **Cancelar**.



3. No bloco **Política personalizada**, selecione **Configurar e usar**.

4. Cole o JSON que você copiou e faça as alterações necessárias.

5. Selecione **Usar política**.

Uma marca de seleção verde aparece ao lado de **Política atual** no bloco Política personalizada.

6. Opcionalmente, selecione **Editar configuração** para fazer mais alterações na nova política personalizada.

Reverter temporariamente para a política de segurança padrão

Se você configurou uma política de segurança personalizada, poderá não conseguir fazer login no Grid Manager se a política TLS configurada for incompatível com a ["certificado de servidor configurado"](#).

Você pode reverter temporariamente para a política de segurança padrão.

Passos

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

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

2. Execute o seguinte comando:

```
restore-default-cipher-configurations
```

3. A partir de um navegador web, acesse o Grid Manager no mesmo Admin Node.
4. Siga os passos em [Selecione uma política de segurança](#) para configurar a política novamente.

Configurar a segurança de rede e de objetos do StorageGRID

Você pode configurar a segurança de rede e de objetos para criptografar objetos armazenados, impedir determinadas solicitações S3 ou permitir que as conexões de clientes com os Storage Nodes usem HTTP em vez de HTTPS.

Criptografia de objeto armazenado

A criptografia de objetos armazenados permite a criptografia de todos os dados dos objetos à medida que são ingeridos pelo S3. Por padrão, os objetos armazenados não são criptografados, mas você pode optar por criptografar objetos usando o algoritmo de criptografia AES-128 ou AES-256. Quando você habilita essa configuração, todos os objetos recém-ingерidos são criptografados, mas nenhuma alteração é feita nos objetos armazenados existentes. Se você desabilitar a criptografia, os objetos atualmente criptografados permanecerão criptografados, mas os objetos recém-ingерidos não serão criptografados.

A configuração de criptografia de objetos armazenados aplica-se somente a objetos S3 que não foram criptografados por criptografia no nível do bucket ou no nível do objeto.

Para obter mais detalhes sobre os métodos de criptografia do StorageGRID, consulte ["Revise os métodos de criptografia do StorageGRID"](#).

Impedir modificação do cliente

Impedir modificação do cliente é uma configuração de todo o sistema. Quando a opção **Impedir modificação do cliente** está selecionada, as seguintes solicitações são negadas.

S3 API REST

- DeleteBucket solicitações
- Qualquer solicitação para modificar os dados de um objeto existente, metadados definidos pelo usuário ou marcação de objetos S3

Habilitar HTTP para conexões de nós de armazenamento

Por padrão, os aplicativos cliente usam o protocolo de rede HTTPS para quaisquer conexões diretas com os Storage Nodes. Você pode habilitar o HTTP opcionalmente para essas conexões, por exemplo, ao testar uma grid que não seja de produção.

Use HTTP para conexões com nós de armazenamento somente se os clientes S3 precisarem fazer conexões HTTP diretamente com os nós de armazenamento. Você não precisa usar essa opção para clientes que usam apenas conexões HTTPS ou para clientes que se conectam ao serviço de Load Balancer (porque você pode ["configurar cada endpoint do balanceador de carga"](#) usar HTTP ou HTTPS).

Consulte ["Resumo: endereços IP e portas para conexões de clientes"](#) para saber quais portas os clientes S3 usam ao se conectar aos nós de armazenamento usando HTTP ou HTTPS.

Selecione opções

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem permissão de acesso root.

Passos

1. Selecione **Configuração > Segurança > Configurações de segurança**.
2. Selecione a guia **Rede e objetos**.
3. Para a criptografia de objetos armazenados, use a configuração **Nenhuma** (padrão) se você não quiser que os objetos armazenados sejam criptografados ou selecione **AES-128** ou **AES-256** para criptografar os objetos armazenados.
4. Opcionalmente, selecione **Impedir modificação pelo cliente** se você quiser impedir que os clientes S3 façam solicitações específicas.



Se você alterar essa configuração, levará cerca de um minuto para que a nova configuração seja aplicada. O valor configurado é armazenado em cache para desempenho e escalabilidade.

5. Opcionalmente, selecione **Habilitar HTTP para conexões de nós de armazenamento** se os clientes se conectarem diretamente aos nós de armazenamento e você quiser usar conexões HTTP.



Tenha cuidado ao habilitar HTTP para uma grade de produção, pois as solicitações serão enviadas sem criptografia.

6. Selecione **Salvar**.

Alterar as configurações de segurança da interface StorageGRID

As configurações de segurança da interface permitem que você controle se os usuários serão desconectados caso fiquem inativos por mais tempo do que o período

especificado e se um rastreamento de pilha será incluído nas respostas de erro da API.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["Permissão de acesso root"](#).

Sobre esta tarefa

A página **Configurações de segurança** inclui as configurações **Tempo limite de inatividade do navegador** e **Rastreamento de pilha da Management API**.

Tempo limite de inatividade do navegador

Indica por quanto tempo o navegador de um usuário pode ficar inativo antes que o usuário seja desconectado. O padrão é 15 minutos.

O tempo limite de inatividade do navegador também é controlado pelos seguintes:

- Um timer StorageGRID separado e não configurável, incluído para a segurança do sistema. O token de autenticação de cada usuário expira 16 horas após o usuário fazer login. Quando a autenticação de um usuário expira, esse usuário é desconectado automaticamente, mesmo que o tempo limite de inatividade do navegador esteja desativado ou que o valor do tempo limite do navegador não tenha sido atingido. Para renovar o token, o usuário deve fazer login novamente.
- Configurações de tempo limite para o provedor de identidade, assumindo que o logon único (SSO) esteja habilitado para StorageGRID.

Se o SSO estiver ativado e o navegador de um usuário expirar, o usuário deverá inserir novamente suas credenciais de SSO para acessar o StorageGRID. Consulte ["Como funciona o SSO"](#).

Rastreamento de pilha da Management API

Controla se um rastreamento de pilha é retornado nas respostas de erro da API do Grid Manager e do Tenant Manager.

Essa opção está desativada por padrão, mas você pode querer habilitar essa funcionalidade para um ambiente de teste. Em geral, você deve manter o rastreamento de pilha desativado em ambientes de produção para evitar revelar detalhes internos do software quando ocorrerem erros de API.

Passos

1. Selecione **Configuração > Segurança > Configurações de segurança**.
2. Selecione a guia **Interface**.
3. Para alterar a configuração de tempo limite de inatividade do navegador:
 - a. Expanda o acordeão.
 - b. Para alterar o período de tempo limite, especifique um valor entre 60 segundos e 7 dias. O tempo limite padrão é de 15 minutos.
 - c. Para desativar essa função, desmarque a caixa de seleção.
 - d. Selecione **Salvar**.

A nova configuração não afeta os usuários que já estão conectados. Os usuários precisam fazer login novamente ou atualizar o navegador para que a nova configuração de timeout entre em vigor.

4. Para alterar a configuração do rastreamento de pilha da Management API:

- a. Expanda o acordeão.
- b. Selecione a caixa de seleção para retornar um rastreamento de pilha nas respostas de erro da API do Grid Manager e do Tenant Manager.



Deixe o rastreamento de pilha desativado em ambientes de produção para evitar a divulgação de detalhes internos do software quando ocorrerem erros na API.

- c. Selecione **Salvar**.

Gerenciar o acesso SSH externo no StorageGRID

Gerencie o acesso SSH para tráfego de entrada na grid bloqueando ou permitindo acesso externo. O gerenciamento do acesso SSH externo não afeta o tráfego entre os nós na grid.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["Permissão de acesso root"](#).

Sobre esta tarefa

Para aumentar a segurança do sistema, o acesso SSH externo é bloqueado por padrão. Se você precisar realizar tarefas que exigem acesso SSH de entrada, como solucionar problemas, permita temporariamente o acesso externo. Quando você terminar a tarefa, bloqueie o acesso externo.

Passos

1. Selecione **Configuração > Segurança > Configurações de segurança**.
2. Selecione a guia **Bloquear SSH**.
3. Use a opção **Bloquear acesso SSH de entrada** para gerenciar acesso SSH externo:
 - a. Selecione a caixa de seleção para bloquear o acesso (padrão).
 - b. Desmarque a caixa de seleção para permitir o acesso.



É necessário acesso à porta 22 entre o laptop de serviço e todos os outros nós da grade. Remova o acesso à porta 22 ao concluir a tarefa de manutenção.

4. Selecione **Salvar**.

Configurar os servidores de gerenciamento de chaves

Saiba mais sobre os principais servidores de gerenciamento no StorageGRID

Um servidor de gerenciamento de chaves (KMS) é um sistema externo de terceiro que fornece chaves de criptografia para os nós de appliance StorageGRID no site StorageGRID associado, usando o Key Management Interoperability Protocol (KMIP).

StorageGRID suporta apenas determinados servidores de gerenciamento de chaves. Para obter uma lista dos produtos e versões suportados, use o ["NetApp Ferramenta de Matriz de Interoperabilidade \(IMT\)"](#).

Você pode usar um ou mais servidores de gerenciamento de chaves para gerenciar as chaves de criptografia de nós para quaisquer nós de dispositivo StorageGRID que tenham a configuração **Criptografia de Nó**.

habilitada durante a instalação. Usar servidores de gerenciamento de chaves com esses nós de dispositivo permite que você proteja seus dados mesmo se um dispositivo for removido do data center. Depois que os volumes do dispositivo forem criptografados, você não poderá acessar nenhum dado no dispositivo, a menos que o nó consiga se comunicar com o KMS.

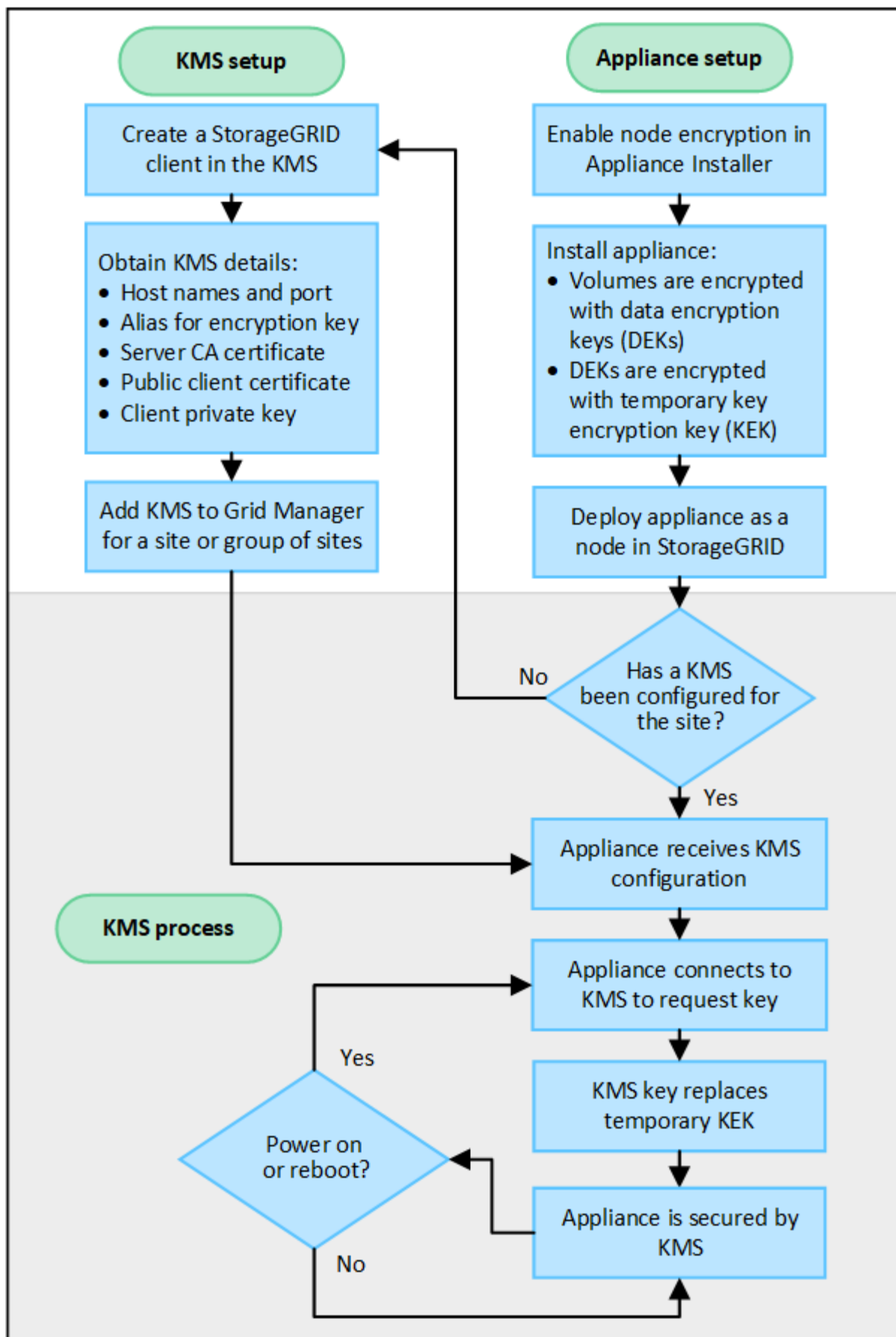


StorageGRID não cria nem gerencia as chaves externas usadas para criptografar e descriptografar os nós do appliance. Se você planeja usar um servidor de gerenciamento de chaves externo para proteger os dados do StorageGRID, você precisa entender como configurar esse servidor e como gerenciar as chaves de criptografia. A execução de tarefas de gerenciamento de chaves está além do escopo destas instruções. Se você precisar de ajuda, consulte a documentação do seu servidor de gerenciamento de chaves ou entre em contato com o suporte técnico.

Configuração do servidor de gerenciamento de chaves e do dispositivo StorageGRID

Antes de você poder usar um servidor de gerenciamento de chaves (KMS) para proteger os dados do StorageGRID nos nós do appliance, é necessário concluir duas tarefas de configuração: configurar um ou mais servidores KMS e habilitar a criptografia de nó para os nós do appliance. Quando essas duas tarefas de configuração estiverem concluídas, o processo de gerenciamento de chaves ocorrerá automaticamente.

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



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

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

Configurar o servidor de gerenciamento de chaves (KMS)

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

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

Configurar o appliance

Configurar um nó de appliance para uso com o KMS inclui as seguintes etapas de alto nível.

1. Durante a fase de configuração de hardware da instalação do appliance, use o StorageGRID Appliance Installer para ativar a configuração **Criptografia de Nó** para o appliance.



Não é possível ativar a configuração **Criptografia de Nó** depois que um appliance é adicionado à grid, e não é possível usar o gerenciamento de chaves externas para appliances que não têm criptografia de nó ativada.

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

Veja ["Habilitar criptografia do nó"](#) para obter detalhes.

Processo de criptografia com gerenciamento de chaves (ocorre automaticamente)

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

1. Ao instalar um dispositivo com criptografia de nó habilitada na grade, StorageGRID determina se existe uma configuração KMS para o site que contém o novo nó.
 - Se um KMS já tiver sido configurado para o site, o appliance recebe a configuração do KMS.

- Se um KMS ainda não tiver sido configurado para o site, os dados no appliance continuarão criptografados pela KEK temporária até que você configurar um KMS para o site e o appliance receba a configuração do KMS.
- 2. O dispositivo utiliza 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 a KEK temporária e agora é usada para criptografar e descriptografar as DEKs dos volumes do dispositivo.



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

- 4. Se o dispositivo for ligado ou reiniciado, ele se reconecta ao KMS para solicitar a chave. A chave, que é salva na memória volátil, não sobrevive a uma perda de energia ou a uma reinicialização.

Requisitos e considerações do servidor de gerenciamento de chaves do StorageGRID

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

Qual versão do KMIP é suportada?

StorageGRID é compatível com a versão 1.4 do KMIP.

["Especificação do Protocolo de Interoperabilidade de Gerenciamento de Chaves Versão 1.4"](#)

Quais são as considerações de rede?

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

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

Quais versões do TLS são suportadas?

A comunicação entre os nós do dispositivo e o KMS configurado utiliza conexões TLS seguras. StorageGRID pode suportar o protocolo TLS 1.2 ou TLS 1.3 ao estabelecer conexões KMIP com um KMS ou cluster KMS, dependendo do que o KMS suporta e de qual ["Política de TLS e SSH"](#) você está utilizando.

StorageGRID negocia o protocolo e a cifra (TLS 1.2) ou o conjunto de cifras (TLS 1.3) com o KMS ao estabelecer a conexão. Para verificar quais versões de protocolo e cifras/conjuntos de cifras estão disponíveis, consulte a seção `tlsOutbound` da política ativa de TLS e SSH do grid (**Configuração > Segurança > Configurações de segurança**).

Quais appliances são compatíveis?

Você pode usar um servidor de gerenciamento de chaves (KMS) para gerenciar as chaves de criptografia de qualquer appliance StorageGRID em sua grid que tenha a configuração **Criptografia de Nó** ativada. Essa configuração só pode ser ativada durante a etapa de configuração de hardware da instalação do appliance usando o StorageGRID Appliance Installer.



Você não pode ativar a criptografia de nó depois que um appliance é adicionado ao grid, e não pode usar o gerenciamento externo de chaves para appliances que não têm a criptografia de nó ativada.

Você pode usar o KMS configurado para StorageGRID appliances e nós de appliances.

Não é possível usar o KMS configurado para nós baseados em software (não appliance), incluindo os seguintes:

- Nós implantados como máquinas virtuais (VMs)
- Nós implantados em mecanismos de contêiner em hosts Linux

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

Quando devo configurar os servidores de gerenciamento de chaves?

Para uma nova instalação, geralmente é recomendável configurar um ou mais servidores de gerenciamento de chaves no Grid Manager antes de criar tenants. Essa ordem garante que os nós estejam protegidos antes que quaisquer dados de objetos sejam armazenados neles.

Você pode configurar os servidores de gerenciamento de chaves no Grid Manager antes ou depois de instalar os nós do appliance.

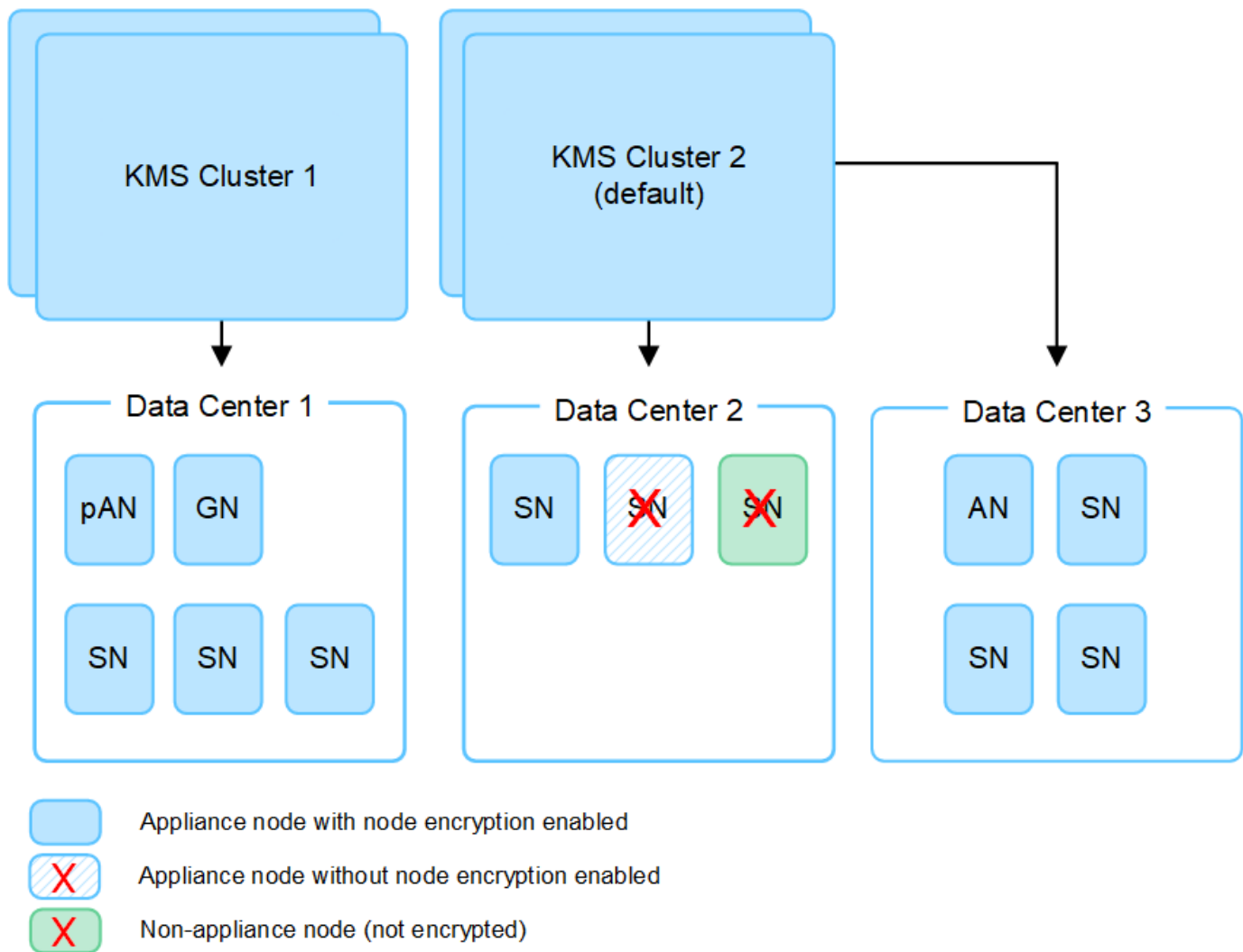
De quantos servidores de gerenciamento de chaves você precisa?

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

StorageGRID suporta 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 a capacidade de failover em uma configuração de alta disponibilidade.

Por exemplo, suponha que seu sistema StorageGRID tenha três sites de data center. Você pode configurar um cluster KMS para fornecer uma chave a todos os nós de appliance no Data Center 1 e um segundo cluster KMS para fornecer uma chave a todos os nós de appliance em todos os outros sites. 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 appliance ou para quaisquer nós appliance que não tenham a configuração **Criptografia de Nó** ativada durante a instalação.



O que acontece quando uma chave é rotacionada?

Como prática recomendada de segurança, você deve periodicamente ["girar a chave de criptografia"](#) usado por cada KMS configurado.

Quando a nova versão da chave estiver disponível:

- Ela é distribuída automaticamente para os nós de appliance criptografados no(s) site(s) associado(s) ao KMS. A distribuição deve ocorrer dentro de uma hora após a rotação da chave.
- Se o nó do appliance criptografado estiver offline quando a nova versão da chave for distribuída, o nó receberá a nova chave assim que for reiniciado.
- Se a nova versão da chave não puder ser usada para criptografar volumes do appliance por qualquer motivo, o alerta **KMS encryption key rotation failed** 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 após ele ter sido criptografado?

Se você precisar instalar um appliance criptografado em outro sistema StorageGRID, primeiro deve descomissionar o nó de grid para mover os dados de objeto para outro nó. Em seguida, você pode usar o StorageGRID Appliance Installer para ["Limpar a configuração do KMS"](#). Limpar a configuração do KMS desativa a configuração **Node Encryption** e remove a associação entre o nó do appliance e a configuração

do KMS para o site StorageGRID.



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

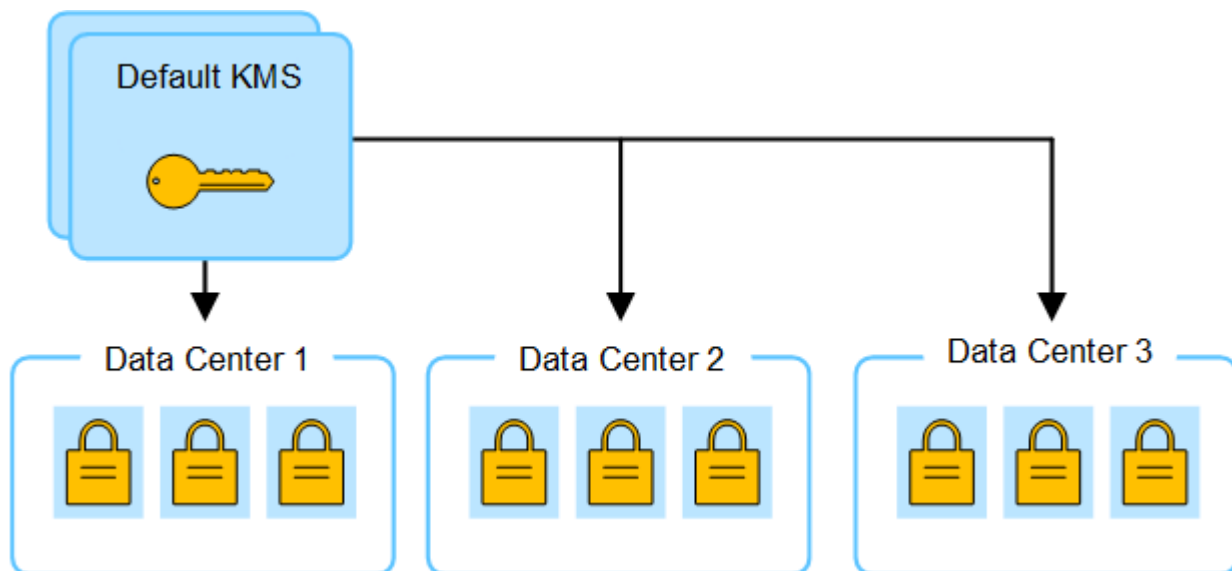
Considerações para a alteração do KMS em um site StorageGRID

Cada servidor de gerenciamento de chaves (KMS) ou cluster KMS fornece uma chave de criptografia para todos os nós do appliance em um único site 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.

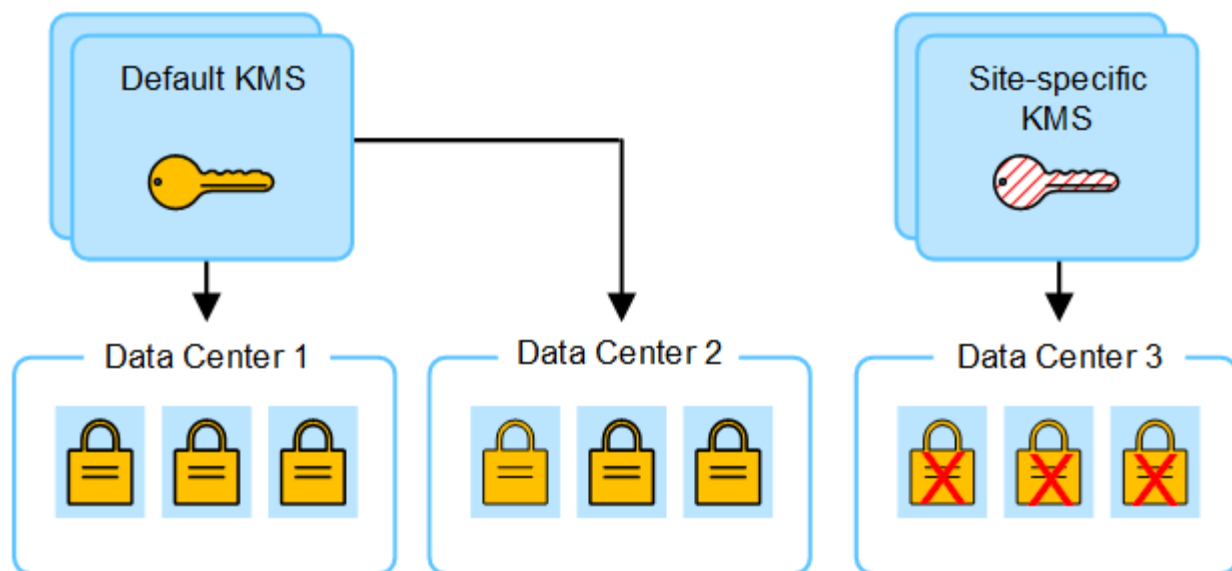
Se você alterar o KMS usado em um site, deverá garantir que os nós de appliance criptografados anteriormente nesse site possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, pode ser necessário copiar a versão atual da chave de criptografia do KMS original para o novo KMS.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

Por exemplo:

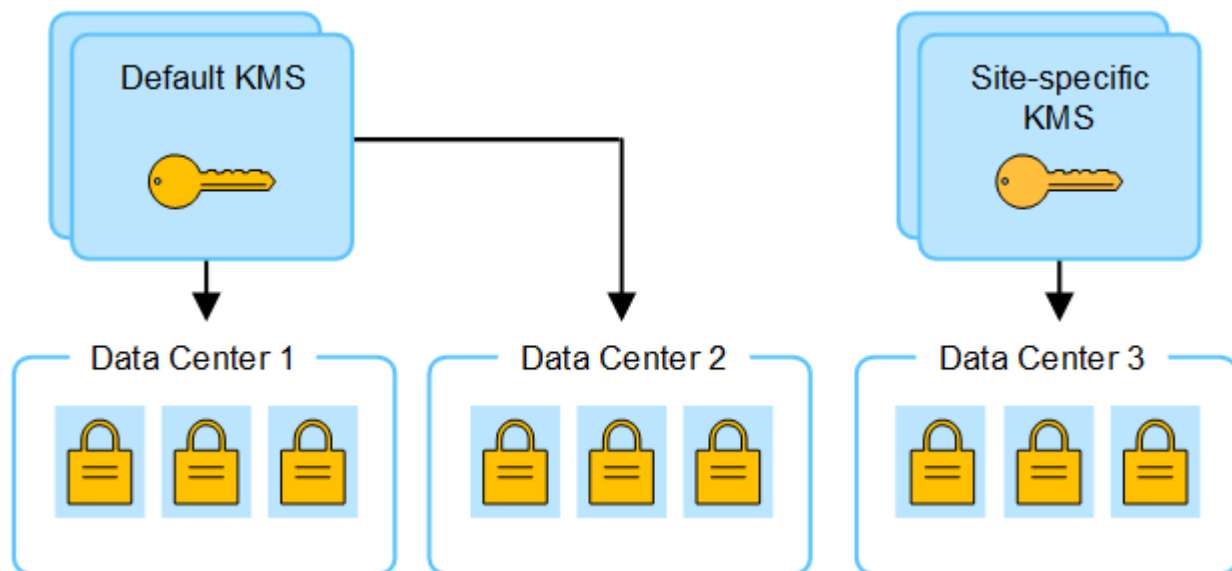
1. Inicialmente, você configura um KMS padrão que se aplica a todos os sites que não possuem um KMS dedicado.
2. Quando o KMS é salvo, todos os nós de appliance que têm a configuração **Criptografia de Nó** ativada se conectam ao KMS e solicitam a chave de criptografia. Essa chave é usada para criptografar os nós de appliance em todos os sites. Essa mesma chave também deve ser usada para descriptografar esses appliances.



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, ocorre um erro de validação ao tentar salvar a configuração do KMS específico para o site. O erro ocorre porque o KMS específico para o site não possui a chave correta para descriptografar os nós nesse site.



4. Para resolver o problema, você copia 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 se torna uma versão anterior da nova chave.) O KMS específico do site agora possui a chave correta para descriptografar os nós do appliance no data center 3, então ela pode ser salva 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 de alteração do KMS de um site.

Caso de uso para alterar o KMS de um site	Etapas necessárias
Você possui uma ou mais entradas KMS específicas do site e deseja usar uma delas como KMS padrão.	Edite o KMS específico do site. No campo Gerencia chaves para, selecione Sites não gerenciados por outro KMS (KMS padrão). O KMS específico do site agora será usado como o KMS padrão. Ele será aplicado a qualquer site que não tenha um KMS dedicado. "Editar um servidor de gerenciamento de chaves (KMS)"
Você possui um KMS padrão e adiciona um novo site em uma expansão. Você não deseja usar o KMS padrão para o novo site.	1. Se os nós do 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 Grid Manager, adicione o novo KMS e selecione o site. "Adicionar um servidor de gerenciamento de chaves (KMS)"
Você deseja que o KMS de um site utilize um servidor diferente.	1. Se os nós do dispositivo no local já tiverem sido criptografados pelo KMS existente, use o software KMS para copiar a versão atual da chave de criptografia do KMS existente para o novo KMS. 2. Utilizando o Gerenciador de Grade, edite a configuração KMS existente e insira o novo nome do host ou endereço IP. "Adicionar um servidor de gerenciamento de chaves (KMS)"

Configurar o StorageGRID como cliente no KMS

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



Estas instruções aplicam-se ao Thales CipherTrust Manager e ao Hashicorp Vault. Para obter uma lista de produtos e versões compatíveis, utilize o ["NetApp Ferramenta de Matriz de Interoperabilidade \(IMT\)"](#).

Passos

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

Cada KMS gerencia uma única chave de criptografia para os nós dos appliances StorageGRID em um único site ou em um grupo de sites.

2. Crie uma chave usando um dos dois métodos a seguir:

- Utilize a página de gerenciamento de chaves do seu produto KMS. Crie uma chave de criptografia AES para cada KMS ou cluster KMS.

A chave de criptografia deve ter 2.048 bits ou mais e deve ser exportável.

- Peça para o StorageGRID criar a chave. Você será solicitado quando testar e salvar após ["Carregando certificados de cliente"](#).

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

Você precisa dessas informações ao adicionar o KMS ao StorageGRID:

- Nome do host ou endereço IP para cada servidor.
 - Porta KMIP usada pelo KMS.
 - Alias da chave de criptografia no KMS.
4. Para cada KMS ou cluster KMS, obtenha um certificado de servidor assinado por uma autoridade certificadora (CA) ou um pacote de certificados que contenha cada um dos arquivos de certificado da CA codificados em PEM, concatenados na ordem da 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 em Base-64 Privacy Enhanced Mail (PEM).
- O campo Nome Alternativo do Assunto (SAN) em cada certificado de servidor deve incluir o domínio totalmente qualificado (FQDN) ou endereço IP ao qual o StorageGRID se conectará.



Ao configurar o KMS no StorageGRID, você deve inserir os mesmos domínios totalmente qualificados ou endereços IP no campo **Hostname**.

- O certificado do servidor deve corresponder ao certificado usado pela interface KMIP do KMS, que normalmente usa a porta 5696.
5. Obtenha o certificado público do cliente emitido para o StorageGRID pelo KMS externo e a chave privada do certificado do cliente.

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

Adicionar um servidor de gerenciamento de chaves no StorageGRID

Você usa o assistente do StorageGRID Key Management Server para adicionar cada KMS ou cluster KMS.

Antes de começar

- Você revisou o ["Considerações e requisitos para usar um servidor de gerenciamento de chaves"](#).
- Você tem ["configurou StorageGRID como cliente no KMS"](#) e as informações necessárias para cada KMS ou cluster KMS.
- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).

Sobre esta tarefa

Se possível, configure quaisquer servidores de gerenciamento de chaves específicos 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 appliances criptografados no nível do nó na grade serão criptografados pelo KMS padrão. Se você quiser criar um KMS específico do site depois, será necessário primeiro copiar a versão atual da chave de criptografia do KMS padrão para o novo KMS. Consulte ["Considerações para alterar o KMS de um site"](#) para obter detalhes.

Etapa 1: detalhes do KMS

Na Etapa 1 (detalhes do KMS) do assistente Adicionar um Servidor de Gerenciamento de Chaves, você fornece detalhes sobre o KMS ou cluster KMS.

Passos

1. Selecione **Configuração > Segurança > Servidor de gerenciamento de chaves**.

A página do servidor de gerenciamento de chaves é exibida com a guia Detalhes da configuração selecionada.

2. Selecione **Create**.

A etapa 1 (detalhes do KMS) do assistente Adicionar um Key Management Server é exibida.

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

Campo	Descrição
Nome da KMS	Um nome descritivo para ajudar você a identificar este KMS. Deve ter entre 1 e 64 caracteres.
Nome da chave	O alias de chave exato para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres. Observação: Se você ainda não criou uma chave usando seu produto KMS, será solicitado que StorageGRID crie a chave.
Gerencia chaves para	O site do StorageGRID que será associado a este KMS. Se possível, você deve configurar quaisquer servidores de gerenciamento de chaves específicos do site antes de configurar um KMS padrão que se aplique a todos os sites não gerenciados por outro KMS. • Selecione um site se este KMS for gerenciar as chaves de criptografia para os nós do dispositivo em um site específico. • Selecione Sites não gerenciados por outro KMS (KMS padrão) para configurar um KMS padrão que será aplicado a qualquer site que não tenha um KMS dedicado e a qualquer site que você adicionar em expansões subsequentes. Nota: Ocorrerá um erro de validação ao salvar a configuração do KMS se você selecionar um site que foi criptografado anteriormente pelo KMS padrão, mas não forneceu a versão atual da chave de criptografia original para o novo KMS.
Porta	A porta que o servidor KMS usa para comunicações do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). O padrão é 5696, que é a porta padrão do KMIP.
Nome do host	O nome de domínio totalmente qualificado ou endereço IP do KMS. Nota: O campo Nome Alternativo do Assunto (SAN) do certificado do servidor deve incluir o domínio totalmente qualificado ou endereço IP inserido aqui. Caso contrário, StorageGRID não conseguirá se conectar ao KMS ou a todos os servidores em um cluster KMS.

4. Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.
5. Selecione **Continue**.

Etapa 2: Carregar o certificado do 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 da **Etapa 2 (Carregar certificado do servidor)**, navegue até o local onde o certificado do servidor ou a cadeia de certificados foi salva.
2. Faça o upload do arquivo de certificado.

Os metadados do certificado do servidor são exibidos.



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

3. Selecione **Continue**.

Etapa 3: Carregar certificados do 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 da **Etapa 3 (Carregar certificados do cliente)**, navegue até o local do certificado do cliente.
2. Faça upload do arquivo de certificado do cliente.

Os metadados do certificado do cliente aparecem.

3. Navegue até a localização da chave privada para o certificado do cliente.
4. Faça o upload do arquivo de chave privada.
5. Selecione **Test and save**.

Se uma chave não existir, você será solicitado a permitir que o StorageGRID crie uma.

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



Imediatamente após você adicionar um KMS, o status do certificado na página Key Management Server aparece como Desconhecido. O StorageGRID pode levar até 30 minutos para obter o status real de cada certificado. Você deve atualizar seu navegador para ver o status atual.

6. Se uma mensagem de erro aparecer ao selecionar **Test and save**, revise os detalhes da mensagem e selecione **OK**.

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

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



Selecionar **Forçar salvamento** salva a configuração do KMS, mas não testa a conexão externa de cada appliance com esse KMS. Se houver algum problema com a configuração, você pode não conseguir reinicializar os nós de appliance que têm criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

8. Analise o aviso de confirmação e selecione **OK** se tiver certeza de que deseja forçar o salvamento da configuração.

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

Gerencie um servidor de gerenciamento de chaves no StorageGRID

Gerenciar um servidor de gerenciamento de chaves (KMS) envolve visualizar ou editar detalhes, gerenciar certificados, visualizar nós criptografados e remover um KMS quando ele não for mais necessário.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador web compatível](#)".
- Você tem o "[permissão de acesso necessária](#)".

Ver detalhes do KMS

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

Passos

1. Selecione **Configuração > Segurança > Servidor de gerenciamento de chaves**.

A página do servidor de gerenciamento de chaves é exibida e mostra as seguintes informações:

- A aba Detalhes da configuração lista todos os servidores de gerenciamento de chaves que estão configurados.
 - A aba "Nós criptografados" lista todos os nós que têm criptografia de nó ativada.
2. Para visualizar os detalhes de um KMS específico e realizar operações nesse KMS, selecione o nome do KMS. A página de detalhes do KMS lista as seguintes informações:

Campo	Descrição
Gerencia chaves para	O site StorageGRID associado ao KMS. Este campo exibe o nome de um site StorageGRID específico ou Sites não gerenciados por outro KMS (KMS padrão) .

Campo	Descrição
Nome do host	O domínio totalmente qualificado ou endereço IP do KMS. Se houver um cluster de dois servidores de gerenciamento de chaves, o domínio totalmente qualificado ou endereço IP de ambos os servidores será listado. Se houver mais de dois servidores de gerenciamento de chaves em um cluster, o domínio totalmente qualificado ou endereço IP do primeiro KMS será listado juntamente com o número de servidores de gerenciamento de chaves adicionais no cluster. Por exemplo: 10.10.10.10 and 10.10.10.11 ou 10.10.10.10 and 2 others. Para visualizar todos os nomes de host em um cluster, selecione um KMS e selecione Editar ou Ações > Editar.

3. Selecione uma aba na página de detalhes do KMS para visualizar as seguintes informações:

Aba	Campo	Descrição
Detalhes principais	Nome da chave	O alias principal para o cliente StorageGRID no KMS.
UID da chave	O identificador único da versão mais recente da chave.	Última modificação
A data e a hora da versão mais recente da chave.	Certificado do servidor	Metadados
Os metadados do certificado, como número de série, data e hora de expiração e o PEM do certificado.	Certificado PEM	O conteúdo do arquivo PEM (privacy enhanced mail) do certificado.
Certificado do cliente	Metadados	Os metadados do certificado, como número de série, data e hora de expiração e o PEM do certificado.

4. Sempre que as práticas de segurança da sua organização exigirem, selecione **Girar chave** ou use o software KMS para criar uma nova versão da chave.

Quando a rotação de chaves é bem-sucedida, os campos UID da chave e Última modificação são atualizados.

Se você rotacionar a chave de criptografia usando o software KMS, rotacione-a da última versão usada da chave para uma nova versão da mesma chave. Não rotacione para uma chave completamente diferente.



Nunca tente rotacionar uma chave alterando o nome da chave (alias) no KMS. StorageGRID exige 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, StorageGRID pode não conseguir descriptografar seus dados.

Gerenciar certificados

Resolva prontamente quaisquer problemas com certificados de servidor ou cliente. Se possível, substitua os certificados antes que expirem.



Você deve resolver quaisquer problemas com certificados o mais rápido possível para manter o acesso aos dados.

Passos

1. Selecione **Configuração > Segurança > Servidor de gerenciamento de chaves**.
2. Na tabela, observe o valor de validade do certificado para cada KMS.
3. Se a data de expiração do certificado de qualquer KMS for desconhecida, aguarde até 30 minutos e atualize seu navegador.
4. Se a coluna Validade do certificado indicar que um certificado expirou ou está perto de expirar, selecione o KMS para acessar a página de detalhes do KMS.
 - a. Selecione **Certificado do servidor** e verifique o valor do campo "Expira em".
 - b. Para substituir o certificado, selecione **Editar certificado** para carregar um novo certificado.
 - c. Repita esses subpassos e selecione **Certificado do cliente** em vez de Certificado do servidor.
5. Quando os alertas **Expiração do certificado da CA do KMS**, **Expiração do certificado do cliente KMS** e **Expiração do certificado do servidor KMS** forem acionados, anote a descrição de cada alerta e execute as ações recomendadas.

Pode levar até 30 minutos para o StorageGRID obter atualizações sobre a expiração do certificado. Atualize seu navegador para ver os valores atuais.



Se você receber o status **Status do certificado do servidor desconhecido**, verifique se o seu KMS permite obter um certificado de servidor sem exigir um certificado de cliente.

Visualizar nós criptografados

Você pode visualizar informações sobre os nós de appliance em seu sistema StorageGRID que têm a configuração **Criptografia de Nó** ativada.

Passos

1. Selecione **Configuração > Segurança > Servidor de gerenciamento de chaves**.

A página do Servidor de Gerenciamento de Chaves é exibida. A guia Detalhes da Configuração mostra quaisquer servidores de gerenciamento de chaves que foram configurados.

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

A aba "Nós criptografados" lista os nós do appliance no seu sistema StorageGRID que têm a configuração **Criptografia de nó** ativada.

3. Analise as informações na tabela para cada nó do appliance.

Coluna	Descrição
Nome do nó	O nome do nó do appliance.
Tipo de nó	O tipo de nó: Storage, Admin ou Gateway.
Site	O nome do site StorageGRID onde o nó está instalado.
Nome da KMS	O nome descritivo do KMS usado para o nó. Se nenhum KMS estiver listado, selecione a guia Detalhes da configuração para adicionar um KMS. "Adicionar um servidor de gerenciamento de chaves (KMS)"
UID da chave	O ID exclusivo da chave de criptografia usada para criptografar e descriptografar dados no nó do appliance. Para visualizar o UID completo de uma chave, selecione o texto. Um traço (--) indica que o UID da chave é desconhecido, possivelmente devido a um problema de conexão entre o nó do appliance e o KMS.
Status	O status da conexão entre o KMS e o nó do appliance. Se o nó estiver conectado, o registro de data e hora é atualizado a cada 30 minutos. Pode levar alguns minutos para o status da conexão ser atualizado após alterações na configuração do KMS. Nota: Atualize seu navegador para ver os novos valores.

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

Durante as operações normais do KMS, o status será **Conectado ao KMS**. Se um nó estiver desconectado do grid, o estado de conexão do nó será exibido (Administrativamente Inativo ou Desconhecido).

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

- Falha ao carregar a configuração do KMS
- Erro de conectividade KMS
- Nome da chave de criptografia KMS não encontrado
- Falha na rotação da chave de criptografia KMS
- A chave KMS não conseguiu descriptografar um volume do appliance.
- KMS não está configurado

Execute as ações recomendadas para esses alertas.



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

Editar um KMS

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

Antes de começar

- Se você planeja atualizar o site selecionado para um KMS, você revisou o ["Considerações para a alteração do KMS de um site"](#).
- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).

Passos

1. Selecione **Configuração > Segurança > Servidor de gerenciamento de chaves**.

A página do servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que você deseja editar e selecione **Ações > Editar**.

Você também pode editar um KMS selecionando o nome do KMS na tabela e selecionando **Editar** na página de detalhes do KMS.

3. Opcionalmente, atualize os detalhes na **Etapa 1 (detalhes do KMS)** do assistente Edit a Key Management Server.

Campo	Descrição
Nome da KMS	Um nome descritivo para ajudar você a identificar este KMS. Deve ter entre 1 e 64 caracteres.
Nome da chave	O alias de chave exato para o cliente StorageGRID no KMS. Deve ter entre 1 e 255 caracteres. 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.

Campo	Descrição
Gerencia chaves para	Se você estiver editando um KMS específico do site e ainda não tiver um KMS padrão, selecione opcionalmente Sites não gerenciados por outro KMS (KMS padrão). Essa seleção converte o KMS específico do site no KMS padrão, que será aplicado a todos os sites que não possuem um KMS dedicado e a quaisquer sites adicionados em uma expansão. Observação: Se você estiver editando um KMS específico de um site, não poderá selecionar outro site. Se você estiver editando o KMS padrão, não poderá selecionar um site específico.
Porta	A porta que o servidor KMS usa para comunicações do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). O padrão é 5696, que é a porta padrão do KMIP.
Nome do host	O nome de domínio totalmente qualificado ou endereço IP do KMS. Nota: O campo Nome Alternativo do Assunto (SAN) do certificado do servidor deve incluir o domínio totalmente qualificado ou endereço IP inserido aqui. Caso contrário, StorageGRID não conseguirá se conectar ao KMS ou a todos os servidores em um cluster KMS.

- Se você estiver configurando um cluster KMS, selecione **Adicionar outro nome de host** para adicionar um nome de host para cada servidor no cluster.

- Selecione **Continue**.

A etapa 2 (Carregar certificado do servidor) do assistente Editar um Key Management Server é exibida.

- Se você precisar substituir o certificado do servidor, selecione **Procurar** e carregue o novo arquivo.
- Selecione **Continue**.

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

- Se você precisar substituir o certificado do cliente e a chave privada do certificado do cliente, selecione **Procurar** e carregue os novos arquivos.
- Selecione **Test and save**.

As conexões entre o servidor de gerenciamento de chaves e todos os nós de dispositivos criptografados nos sites 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 é adicionado à tabela na página Key Management Server.

- Se aparecer uma mensagem de erro, revise os detalhes da mensagem e selecione **OK**.

Por exemplo, você pode receber um erro 422: Entidade não processável se o site que você selecionou para este KMS já for gerenciado por outro KMS ou se um teste de conexão falhar.

- Se você precisar salvar a configuração atual antes de resolver os erros de conexão, selecione **Forçar salvamento**.



Selecionar **Forçar salvamento** salva a configuração do KMS, mas não testa a conexão externa de cada appliance com esse KMS. Se houver algum problema com a configuração, você pode não conseguir reinicializar os nós de appliance que têm 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 foi salva.

12. Analise o aviso de confirmação e selecione **OK** se tiver certeza de que deseja forçar o salvamento da configuração.

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

Remover um servidor de gerenciamento de chaves (KMS)

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

Antes de começar

- Você revisou o "[Considerações e requisitos para usar um servidor de gerenciamento de chaves](#)".
- Você está conectado ao Gerenciador de Grade usando um "[navegador web compatível](#)".
- Você tem o "[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 appliance com criptografia de nó ativada.
- Você pode remover o KMS padrão se já existir um KMS específico para cada site que possua nós de appliance com criptografia ativada.

Passos

1. Selecione **Configuração > Segurança > Servidor de gerenciamento de chaves**.

A página do servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que você deseja remover e selecione **Ações > Remover**.

Você também pode remover um KMS selecionando o nome do KMS na tabela e selecionando **Remover** na página de detalhes do KMS.

3. Confirme se o seguinte é verdadeiro:

- Você está removendo um KMS específico do site para um site que não possui nenhum nó de appliance com criptografia de nó ativada.
- Você está removendo o KMS padrão, mas já existe um KMS específico para cada site com criptografia de nó.

4. Selecione **Sim**.

A configuração do KMS foi removida.

Gerenciar configurações de proxy

Configurar um proxy de armazenamento StorageGRID

Se você estiver usando serviços de plataforma ou Cloud Storage Pools, poderá configurar um proxy não transparente entre os Storage Nodes e os endpoints externos do S3. Por exemplo, você pode precisar de um proxy não transparente para permitir que mensagens dos serviços de plataforma sejam enviadas para endpoints externos, como um endpoint na internet.



As configurações de proxy de armazenamento configuradas não se aplicam aos endpoints dos serviços da plataforma Kafka.

Antes de começar

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

Sobre esta tarefa

Você pode configurar as definições para um único servidor proxy de armazenamento.

Passos

1. Selecione **Configuração > Segurança > Configurações de proxy**.
2. Na guia **Armazenamento**, selecione a caixa de seleção **Ativar proxy de armazenamento**.
3. Selecione o protocolo para o proxy de armazenamento.
4. Digite o nome do host ou o endereço IP do servidor proxy.
5. Opcionalmente, insira a porta usada para conectar-se ao servidor proxy.

Deixe este campo em branco para usar a porta padrão do protocolo: 80 para HTTP ou 1080 para SOCKS5.

6. Selecione **Salvar**.

Após salvar o proxy de armazenamento, novos endpoints para serviços de plataforma ou Cloud Storage Pools podem ser configurados e testados.



As alterações de proxy podem levar até 10 minutos para entrar em vigor.

7. Verifique as configurações do seu servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma StorageGRID não sejam bloqueadas.
8. Se você precisar desativar um proxy de armazenamento, desmarque a caixa de seleção e selecione **Salvar**.

Configurar as definições de proxy de administrador no StorageGRID

Se você enviar pacotes AutoSupport usando HTTP ou HTTPS, pode configurar um servidor proxy não transparente entre os Nós de Administração e o suporte técnico (AutoSupport).

Para obter mais informações sobre AutoSupport, consulte "[Configurar AutoSupport](#)".

Antes de começar

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

Sobre esta tarefa

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

Passos

1. Selecione **Configuração > Segurança > Configurações de proxy**.

A página Configurações de Proxy é exibida. Por padrão, Storage está selecionado no menu de abas.

2. Selecione a aba **Admin**.
3. Selecione a caixa de seleção **Enable Admin Proxy**.
4. Digite o nome do host ou o endereço IP do servidor proxy.
5. Digite a porta usada para conectar ao servidor proxy.
6. Opcionalmente, insira um nome de usuário e uma senha para o servidor proxy.

Deixe esses campos em branco se o seu servidor proxy não exigir um nome de usuário ou uma senha.

7. Selecione uma das seguintes opções:

- Se você deseja proteger a conexão com o proxy administrativo, selecione **Verificar certificado de proxy**. Carregue um pacote de certificados de autoridade certificadora (CA) para verificar a autenticidade dos certificados SSL apresentados pelo servidor proxy administrativo.



AutoSupport on Demand, E-Series AutoSupport através do StorageGRID e a determinação do caminho de atualização na página de upgrade do StorageGRID não funcionarão se um certificado de proxy for verificado.

Após o upload do pacote CA, seus metadados aparecem.

- Se você não quiser validar certificados ao se comunicar com o servidor proxy, selecione **Não verificar certificado de proxy**.

8. Selecione **Salvar**.

Após salvar o proxy administrativo, o servidor proxy entre os nós administrativos e o suporte técnico é configurado.



As alterações de proxy podem levar até 10 minutos para entrar em vigor.

9. Se você precisar desativar o proxy administrativo, desmarque a caixa de seleção **Ativar proxy administrativo** e selecione **Salvar**.

Controlar firewalls

Controlar o acesso ao StorageGRID em um firewall externo

Você pode abrir ou fechar portas específicas 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 querer impedir que os tenants se conectem ao Grid Manager no firewall, além de usar outros métodos para controlar o acesso ao sistema.

Se você deseja configurar o firewall interno do StorageGRID, consulte "[Configurar firewall interno](#)".

Porta	Descrição	Se a porta estiver aberta...
443	Porta HTTPS padrão para Admin Nodes	Navegadores web e clientes de API de gerenciamento podem acessar o Grid Manager, a Grid Management API, o Tenant Manager e a Tenant Management API. Nota: A porta 443 também é usada para algum tráfego interno.
8443	Porta do Grid Manager restrita em nós de administração	• Navegadores web e clientes da API de gerenciamento podem acessar o Grid Manager e a Grid Management API usando HTTPS. • Navegadores web e clientes da API de gerenciamento não podem acessar o Tenant Manager nem a Tenant Management API. • Solicitações de conteúdo interno serão rejeitadas.
9443	Porta do Tenant Manager restrita em Admin Nodes	• Navegadores web e clientes da API de gerenciamento podem acessar o Tenant Manager e a Tenant Management API usando HTTPS. • Navegadores web e clientes da API de gerenciamento não podem acessar o Grid Manager nem a Grid Management API. • Solicitações de conteúdo interno serão rejeitadas.



O login único (SSO) não está disponível nas portas restritas do Grid Manager ou do Tenant Manager. Você deve usar a porta HTTPS padrão (443) se quiser que os usuários se autenticuem com login único.

Informações relacionadas

- "[Faça login no Grid Manager](#)"
- "[Criar conta de locatário](#)"
- "[Comunicação externa](#)"

Gerencie os controles internos do firewall no StorageGRID

StorageGRID inclui um firewall interno em cada nó que aumenta a segurança do seu grid, permitindo que você controle o acesso à rede do nó. Use o firewall para impedir o acesso à rede em todas as portas, exceto aquelas necessárias para a sua implementação específica do grid. As alterações de configuração que você faz na página

de controle do firewall são aplicadas a cada nó.

Utilize as três abas na página de controle do Firewall para personalizar o acesso necessário para seu grid.

- **Lista de endereços privilegiados:** Use esta aba para permitir acesso selecionado a portas fechadas. Você pode adicionar endereços IP ou sub-redes na notação CIDR que podem acessar portas fechadas usando a aba Gerenciar acesso externo.
- **Gerenciar acesso externo:** Use esta aba para fechar portas que estão abertas por padrão ou reabrir portas previamente fechadas.
- **Rede de cliente não confiável:** Use esta aba para especificar se um nó confia no tráfego de entrada da rede de cliente.

As configurações desta guia substituem as configurações da guia Gerenciar acesso externo.

- Um nó com uma Client Network não confiável aceitará apenas conexões nas portas de endpoint do balanceador de carga configuradas nesse nó (globais, de interface de nó e vinculadas ao tipo de nó).
- As portas dos endpoints do balanceador de carga *são as únicas portas abertas* em redes de clientes não confiáveis, independentemente das configurações na guia Manage external networks.
- Quando confiáveis, todas as portas abertas na guia Gerenciar acesso externo ficam acessíveis, assim como quaisquer endpoints de balanceamento de carga abertos na Client Network.



As configurações que você define em uma guia podem afetar as alterações de acesso que você faz em outra guia. Certifique-se de verificar as configurações em todas as guias para garantir que sua rede se comporte da maneira que você espera.

Para configurar os controles internos do firewall, consulte ["Configurar controles de firewall"](#).

Para obter mais informações sobre firewalls externos e segurança de rede, consulte ["Controle de acesso no firewall externo"](#).

Guias Lista de endereços privilegiados e Gerenciar acesso externo

A aba Lista de endereços privilegiados permite que você registre um ou mais endereços IP que têm acesso a portas do grid que estão fechadas. A aba Gerenciar acesso externo permite que você feche o acesso externo a portas externas selecionadas ou a todas as portas externas abertas (portas externas são portas acessíveis por nós que não fazem parte do grid por padrão). Essas duas abas geralmente podem ser usadas juntas para personalizar exatamente o acesso à rede que você precisa permitir para seu grid.



Endereços IP privilegiados não possuem acesso à porta interna da grid por padrão.

Exemplo 1: use um servidor de salto para tarefas de manutenção

Suponha que você queira usar um jump host (um host com segurança reforçada) para administração de rede. Você pode seguir estes passos gerais:

1. Utilize a aba Lista de endereços privilegiados para adicionar o endereço IP do jump host.
2. Use a guia Gerenciar acesso externo para bloquear todas as portas.



Adicione o endereço IP privilegiado antes de bloquear as portas 443 e 8443. Qualquer usuário conectado a uma porta bloqueada, incluindo você, perderá o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Após salvar sua configuração, todas as portas externas no Admin Node do seu grid serão bloqueadas para todos os hosts, exceto o jump host. Você poderá então usar o jump host para realizar tarefas de manutenção no seu grid com mais segurança.

Exemplo 2: bloqueio de portas sensíveis

Suponha que você queira bloquear portas sensíveis e o serviço nessa porta. Você pode seguir os seguintes passos gerais:

1. Use a guia Lista de endereços privilegiados para conceder acesso somente aos hosts que precisam acessar o serviço.
2. Use a guia Gerenciar acesso externo para bloquear todas as portas.



Adicione o endereço IP privilegiado antes de bloquear o acesso a quaisquer portas atribuídas ao Grid Manager e ao Tenant Manager (as portas predefinidas são 443 e 8443). Qualquer usuário conectado a uma porta bloqueada, incluindo você, perderá o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.

Após salvar sua configuração, a porta sensível e o serviço nessa porta ficam disponíveis para os hosts na lista de endereços privilegiados. Todos os outros hosts são impedidos de acessar o serviço, independentemente da interface de origem da solicitação.

Exemplo 3: desativar o acesso a serviços não utilizados

Em nível de rede, você pode desativar alguns serviços que não pretende usar. Por exemplo, para bloquear o tráfego de cliente HTTP S3, você usaria a opção na guia Gerenciar acesso externo para bloquear a porta 18084.

Aba Redes de Clientes Não Confiáveis

Se você estiver usando uma Client Network, poderá ajudar a proteger o StorageGRID contra ataques hostis, aceitando o tráfego de entrada de clientes somente em endpoints explicitamente configurados.

Por padrão, a Rede do Cliente em cada nó da grade é *confiável*. Ou seja, por padrão, StorageGRID confia nas conexões de entrada para cada nó da grade em todos os ["portas externas disponíveis"](#).

Você pode reduzir a ameaça de ataques hostis ao seu StorageGRID especificando que a Client Network em cada nó seja *não confiável*. Se a Client Network de um nó for não confiável, o nó aceita apenas conexões de entrada em portas explicitamente configuradas como endpoints do balanceador de carga. Consulte ["Configurar pontos de extremidade do balanceador de carga"](#) e ["Configurar controles de firewall"](#).

Exemplo 1: o nó de gateway aceita apenas solicitações HTTPS S3

Suponha que você queira que um nó de gateway rejeite todo o tráfego de entrada na Client Network, exceto solicitações HTTPS S3. Você executaria estas etapas gerais:

1. Na página ["Pontos de extremidade do balanceador de carga"](#), configure um endpoint de balanceador de carga para S3 sobre HTTPS na porta 443.
2. Na página de controle do Firewall, selecione Não confiável para especificar que a Client Network no Gateway Node não é confiável.

Após salvar sua configuração, todo o tráfego de entrada na rede cliente do nó de gateway é bloqueado, exceto as solicitações HTTPS S3 na porta 443 e as solicitações de eco ICMP (ping).

Exemplo 2: nó de armazenamento envia solicitações de serviços da plataforma S3

Suponha que você queira habilitar o tráfego de saída dos serviços da plataforma S3 a partir de um Storage Node, mas queira impedir quaisquer conexões de entrada para esse Storage Node na Client Network. Você executaria esta etapa geral:

- Na guia "Redes de Clientes Não Confiáveis" da página de controle do Firewall, indique que a Rede de Clientes no Nó de Armazenamento não é confiável.

Após salvar sua configuração, o Nó de Armazenamento deixa de aceitar qualquer tráfego de entrada na Rede do Cliente, mas continua permitindo solicitações de saída para os destinos de serviços de plataforma configurados.

Exemplo 3: limitar o acesso ao Grid Manager a uma sub-rede

Suponha que você queira permitir o acesso do Grid Manager apenas em uma sub-rede específica. Você executaria os seguintes passos:

1. Conecte a rede do cliente dos seus nós de administração à subnet.
2. Utilize a guia Rede de Cliente Não Confiável para configurar a Rede de Cliente como não confiável.
3. Ao criar um endpoint de balanceador de carga da interface de gerenciamento, insira a porta e selecione a interface de gerenciamento que a porta acessará.
4. Selecione **Sim** para Rede de Cliente Não Confiável.
5. Use a guia Gerenciar acesso externo para bloquear todas as portas externas (com ou sem endereços IP privilegiados definidos para hosts fora dessa sub-rede).

Após salvar sua configuração, somente os hosts na sub-rede que você especificou poderão acessar o Grid Manager. Todos os outros hosts são bloqueados.

Configurar o firewall interno do StorageGRID

Você pode configurar o firewall do StorageGRID para controlar o acesso à rede a portas específicas nos seus nós do StorageGRID.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Você analisou as informações em ["Gerenciar controles de firewall"](#) e ["Diretrizes de networking"](#).
- Se você deseja que um Nó de Administração ou um Nó de Gateway aceite tráfego de entrada somente em endpoints explicitamente configurados, você definiu os endpoints do balanceador de carga.



Ao alterar a configuração da Rede do Cliente, as conexões de clientes existentes podem falhar se os endpoints do balanceador de carga não estiverem configurados.

Sobre esta tarefa

StorageGRID inclui um firewall interno em cada nó que permite abrir ou fechar algumas portas nos nós da sua grade. Você pode usar as abas de controle do Firewall para abrir ou fechar portas que estão abertas por padrão na Grid Network, Admin Network e Client Network. Você também pode criar uma lista de endereços IP privilegiados que podem acessar portas da grade que estão fechadas. Se você estiver usando uma Client Network, pode especificar se um nó confia no tráfego de entrada da Client Network e configurar o acesso a

portas específicas na Client Network.

Limitar o número de portas abertas para endereços IP externos à sua grid apenas àquelas absolutamente necessárias aumenta a segurança da sua grid. Você usa as configurações em cada uma das três guias de controle do Firewall para garantir que somente as portas necessárias estejam abertas.

Para obter mais informações sobre como usar os controles de firewall, incluindo exemplos, consulte ["Gerenciar controles de firewall"](#).

Para obter mais informações sobre firewalls externos e segurança de rede, consulte ["Controle de acesso no firewall externo"](#).

Acessar controles de firewall

Passos

1. Selecione **Configuração > Segurança > Controle de firewall**.

As três abas desta página são descritas em ["Gerenciar controles de firewall"](#).

2. Selecione qualquer aba para configurar os controles do firewall.

Você pode usar essas abas em qualquer ordem. As configurações definidas em uma aba não limitam o que você pode fazer nas outras abas; no entanto, as alterações de configuração feitas em uma aba podem alterar o comportamento das portas configuradas em outras abas.

Lista de endereços privilegiados

Você usa a guia Lista de endereços privilegiados para conceder acesso a hosts a portas que estão fechadas por padrão ou fechadas pelas configurações na guia Gerenciar acesso externo.

Endereços IP e sub-redes privilegiados não têm acesso interno à grid por padrão. Além disso, os endpoints do balanceador de carga e as portas adicionais abertas na guia Lista de endereços privilegiados são acessíveis mesmo que estejam bloqueados na guia Gerenciar acesso externo.



As configurações na guia Lista de endereços privilegiados não podem substituir as configurações na guia Rede de cliente não confiável.

Passos

1. Na guia Lista de endereços privilegiados, insira o endereço ou a sub-rede IP à qual você deseja conceder acesso às portas fechadas.
2. Opcionalmente, selecione **Adicionar outro endereço IP ou sub-rede na notação CIDR** para adicionar clientes privilegiados adicionais.



Adicione o mínimo possível de endereços à lista de privilegiados.

3. Opcionalmente, selecione **Permitir que endereços IP privilegiados acessem as portas internas do StorageGRID**. Consulte ["Portas internas do StorageGRID"](#).



Esta opção remove algumas proteções para serviços internos. Se possível, deixe-a desativada.

4. Selecione **Salvar**.

Gerenciar acesso externo

Quando uma porta é fechada na guia Gerenciar acesso externo, ela não pode ser acessada por nenhum endereço IP fora da grid, a menos que você adicione o endereço IP à lista de endereços privilegiados. Você só pode fechar portas que estejam abertas por padrão e só pode abrir portas que você tenha fechado.



As configurações na guia Gerenciar acesso externo não podem substituir as configurações na guia Rede de clientes não confiáveis. Por exemplo, se um nó não for confiável, a porta SSH/22 será bloqueada na Rede de clientes, mesmo que esteja aberta na guia Gerenciar acesso externo. As configurações na guia Rede de clientes não confiáveis substituem as portas fechadas (como 443, 8443, 9443) na Rede de clientes.

Passos

1. Selecione **Gerenciar acesso externo**. A guia exibe uma tabela com todas as portas externas (portas que são acessíveis por nós que não fazem parte da grade por padrão) para os nós em sua grade.
2. Configure as portas que você deseja abrir e fechar usando as seguintes opções:
 - Utilize o botão ao lado de cada porta para abrir ou fechar a porta selecionada.
 - Selecione **Abrir todas as portas exibidas** para abrir todas as portas listadas na tabela.
 - Selecione **Fechar todas as portas exibidas** para fechar todas as portas listadas na tabela.



Se você fechar as portas 443 ou 8443 do Grid Manager, todos os usuários atualmente conectados a uma porta bloqueada, incluindo você, perderão o acesso ao Grid Manager, a menos que seu endereço IP tenha sido adicionado à lista de endereços privilegiados.



Use a barra de rolagem à direita da tabela para garantir que você visualizou todas as portas disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer porta externa digitando um número de porta. Você pode digitar um número de porta parcial. Por exemplo, se você digitar **2**, todas as portas que têm a sequência "2" como parte do nome serão exibidas.

3. Selecione **Save**

Rede de cliente não confiável

Se a Rede Cliente de um nó não for confiável, o nó aceitará tráfego de entrada apenas nas portas configuradas como endpoints do balanceador de carga e, opcionalmente, em portas adicionais que você selecionar nesta guia. Você também pode usar esta guia para especificar a configuração padrão para novos nós adicionados em uma expansão.



As conexões de clientes existentes podem falhar se os endpoints do balanceador de carga não estiverem configurados.

As alterações de configuração que você faz na guia **Rede de Clientes Não Confiáveis** substituem as configurações da guia **Gerenciar acesso externo**.

Passos

1. Selecione **Rede de Cliente Não Confiável**.
2. Na seção Definir padrão para novos nós, especifique qual deve ser a configuração padrão quando novos

nós forem adicionados à grid em um procedimento de expansão.

- **Confiável** (padrão): Quando um nó é adicionado em uma expansão, sua Client Network é confiável.
- **Não confiável**: Quando um nó é adicionado em uma expansão, sua rede de clientes é não confiável.

Se necessário, você pode retornar a esta aba para alterar a configuração de um novo nó específico.



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

3. Utilize as seguintes opções para selecionar os nós que devem permitir conexões de clientes somente em endpoints de balanceador de carga explicitamente configurados ou em portas adicionais selecionadas:

- Selecione **Não confiar nos nós exibidos** para adicionar todos os nós exibidos na tabela à lista de Rede de Cliente Não Confiável.
- Selecione **Confiar nos nós exibidos** para remover todos os nós exibidos na tabela da lista de Rede de Cliente Não Confiável.
- Use o botão ao lado de cada nó para definir a Client Network como confiável ou não confiável para o nó selecionado.

Por exemplo, você pode selecionar **Não confiar nos nós exibidos** para adicionar todos os nós à lista de Rede de Clientes Não Confiáveis e, em seguida, usar a opção ao lado de um nó individual para adicionar esse nó específico à lista de Rede de Clientes Confiáveis.



Use a barra de rolagem à direita da tabela para garantir que você visualizou todos os nós disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer nó digitando o nome do nó. Você pode inserir um nome parcial. Por exemplo, se você digitar **GW**, todos os nós que têm a sequência "GW" como parte do nome serão exibidos.

4. Selecione **Salvar**.

As novas configurações do firewall são aplicadas e entram em vigor imediatamente. As conexões de cliente existentes podem falhar se os endpoints do balanceador de carga não tiverem sido configurados.

Gerenciar locatários

Contas de locatário no StorageGRID

Uma conta de locatário permite que você use a API REST do Simple Storage Service (S3) para armazenar e recuperar objetos em um sistema StorageGRID.



Detalhes sobre o Swift foram removidos desta versão do site de documentação. Veja ["StorageGRID 11.8: gerenciar locatários"](#).

Como administrador de grid, você cria e gerencia as contas de locatário que os clientes S3 usam para armazenar e recuperar objetos.

Cada conta de locatário possui grupos federados ou locais, usuários, buckets S3 e objetos.

As contas de locatário podem ser usadas para segregar objetos armazenados por diferentes entidades. Por exemplo, várias contas de locatário podem ser usadas para qualquer um destes casos de uso:

- **Caso de uso empresarial:** Se você administra um sistema StorageGRID em uma aplicação empresarial, pode ser interessante segregar o storage de objetos pelos diferentes departamentos da sua organização. Nesse caso, você poderia criar contas de locatário para o departamento de Marketing, o departamento de Suporte ao Cliente, o departamento de Recursos Humanos e assim por diante.



Se você utiliza o protocolo de cliente S3, pode usar buckets e políticas de buckets do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa usar contas de locatário. Consulte as instruções para implementar "[Buckets S3 e políticas de bucket](#)" para obter mais informações.

- **Caso de uso do provedor de serviços:** Se você está administrando um sistema StorageGRID como provedor de serviços, pode segregar o storage de objetos pelas diferentes entidades que irão alugar o storage na sua grid. Nesse caso, você criaria contas de locatário para Company A, Company B, Company C e assim por diante.

Para obter mais informações, consulte "[Use uma conta de tenant](#)".

Como faço para criar uma conta de locatário?

Use o Grid manager para criar uma conta de tenant. Ao criar uma conta de tenant, você especifica as seguintes informações:

- Informações básicas, incluindo o nome do locatário, o tipo de cliente (S3) e a cota de armazenamento opcional.
- Permissões para a conta do locatário, como se a conta do locatário pode usar serviços de plataforma S3, configurar sua própria fonte de identidade, usar S3 Select ou usar uma conexão de federação de grid.
- O acesso inicial à raiz para o locatário, dependendo se o sistema StorageGRID usa grupos e usuários locais, federação de identidade ou logon único (SSO).

Além disso, você pode habilitar a configuração de S3 Object Lock para o StorageGRID se as contas de locatário do S3 precisarem atender a requisitos regulatórios. Quando o S3 Object Lock está habilitado, todas as contas de locatário do S3 podem criar e gerenciar buckets em conformidade.

Para que serve o Tenant Manager?

Após você criar a conta de locatário, os usuários do locatário podem fazer login no Tenant Manager para executar tarefas como as seguintes:

- Configure a federação de identidades (a menos que a fonte de identidade seja compartilhada com o grid)
- Gerenciar grupos e usuários
- Use a federação de grids para clonagem de contas e replicação entre grids
- Gerenciar chaves de acesso S3
- Criar e gerenciar buckets S3
- Use os serviços da plataforma S3
- Use o S3 Select
- Monitorar o uso de armazenamento



Embora os usuários de locatários do S3 possam criar e gerenciar chaves de acesso e buckets do S3 com o Gerenciador de Locatários, eles precisam usar um aplicativo cliente S3 para ingerir e gerenciar objetos. Veja "[Utilize a API REST S3](#)" para mais detalhes.

Crie uma conta de locatário do StorageGRID

Você precisa criar pelo menos uma conta de locatário para controlar o acesso ao armazenamento no seu sistema StorageGRID.

Os passos para criar uma conta de locatário variam dependendo de ["federação de identidade"](#) e ["autenticação única"](#) estarem configurados e se a conta do Grid Manager que você usa para criar a conta de locatário pertence a um grupo de administradores com a permissão de acesso à raiz.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Acesso à raiz ou permissão para contas de locatário"](#).
- Se a conta do locatário usar a fonte de identidade configurada para o Grid Manager e você quiser conceder permissão de acesso à raiz para a conta do locatário a um grupo federado, você já importou esse grupo federado para o Grid Manager. Você não precisa atribuir nenhuma permissão do Grid Manager a esse grupo de administradores. Consulte ["Gerenciar grupos de administradores"](#).
- Se você deseja permitir que um locatário do S3 clone dados de conta e replique objetos de bucket para outra grid usando uma conexão de federação de grids:
 - Você tem ["configurou a conexão de federação de grid"](#).
 - O status da conexão é **Conectado**.
 - Você tem permissão de acesso root.
 - Você analisou as considerações para ["Gerenciando os tenants permitidos para a federação de grid"](#).
 - Se a conta do locatário usar a fonte de identidade que foi configurada para o Grid Manager, você importou o mesmo grupo federado para o Grid Manager em ambas as grids.

Ao criar o locatário, você selecionará este grupo para ter a permissão inicial de acesso à raiz tanto para as contas de locatário de origem quanto de destino.



Se esse grupo de administradores não existir em ambas as grades antes de você criar o locatário, o locatário não será replicado para o destino.

Acesse o assistente

Passos

1. Selecione **Tenants**.
2. Selecione **Create**.

Insira os detalhes

Passos

1. Insira os detalhes do tenant.

Campo	Descrição
Nome	Um nome para a conta do locatário. Os nomes dos locatários não precisam ser exclusivos. Quando a conta do locatário é criada, ela recebe um ID de conta exclusivo de 20 dígitos.

Campo	Descrição
Descrição (opcional)	Uma descrição para ajudar a identificar o tenant. Se você estiver criando um locatário que usará uma conexão de federação de grid, opcionalmente, use este campo para ajudar a identificar qual é o locatário de origem e qual é o locatário de destino. Por exemplo, esta descrição para um locatário criado no Grid 1 também aparecerá para o locatário replicado no Grid 2: "Este locatário foi criado no Grid 1."
Tipo de cliente	Deve ser S3 .
Cota de armazenamento (opcional)	Se você deseja que este tenant tenha uma cota de armazenamento, um valor numérico para a cota e as unidades.

2. Selecione **Continue**.

Selecione permissões

Passos

1. Opcionalmente, selecione as permissões básicas que você deseja que este locatário tenha.



Algumas dessas permissões têm requisitos adicionais. Para obter detalhes, selecione o ícone de ajuda para cada permissão.

Permissão	Se selecionado...
Permitir serviços de plataforma	O locatário pode usar serviços da plataforma S3, como CloudMirror. Veja "Gerencie serviços de plataforma para contas de locatário do S3" .
Use sua própria fonte de identidade	O locatário pode configurar e gerenciar sua própria fonte de identidade para grupos e usuários federados. Essa opção fica desabilitada se você tiver "SSO configurado" para o seu sistema StorageGRID.
Permitir S3 Select	O locatário pode emitir solicitações de API S3 SelectObjectContent para filtrar e recuperar dados de objetos. Consulte "Gerencie o S3 Select para contas de locatário". Importante: as solicitações SelectObjectContent podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Habilite esse recurso somente quando necessário e apenas para locatários confiáveis.

2. Opcionalmente, selecione as permissões avançadas que você deseja que este locatário tenha.

Permissão	Se selecionado...
Conexão de federação de grid	O tenant pode usar uma conexão de federação de grid, que: - Faz com que este locatário e todos os grupos de locatários e usuários adicionados à conta sejam clonados desta grid (a <i>grid de origem</i>) para a outra grid na conexão selecionada (a <i>grid de destino</i>). - Permite que este locatário configure a replicação entre grades (cross-grid) entre buckets correspondentes em cada grade. Consulte "Gerenciar os inquilinos permitidos para a federação de grid".
Bloqueio de objeto S3	Permitir que o locatário utilize recursos específicos do S3 Object Lock: Definir período máximo de retenção define por quanto tempo os novos objetos adicionados a este bucket devem ser retidos, a partir do momento em que são ingeridos. Permitir modo de conformidade impede que os usuários sobrescrevam ou excluam versões de objetos protegidos durante o período de retenção.

3. Selecione **Continue**.

Defina acesso à raiz e crie um locatário

Passos

1. Defina acesso à raiz para a conta do locatário, com base em se o seu sistema StorageGRID usa federação de identidade, single sign-on (SSO) ou ambos.

Opção	Faça isso
Se a federação de identidades não estiver ativada	Especifique a senha a ser usada ao fazer login no tenant como usuário raiz.
Se a federação de identidades estiver ativada	a. Selecione um grupo federado existente para ter permissão de acesso à raiz para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no tenant como usuário raiz.
Se a federação de identidades e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter permissão de acesso à raiz para o locatário. Nenhum usuário local pode fazer login.

2. Selecione **Criar locatário**.

Uma mensagem de sucesso é exibida e o novo tenant é listado na página de Tenants. Para saber como visualizar os detalhes do tenant e monitorar a atividade do tenant, consulte ["Monitorar a atividade do locatário"](#).



A aplicação das configurações de locatário em toda a grid pode levar 15 minutos ou mais, dependendo da conectividade da rede, do status do nó e das operações do Cassandra.

3. Se você selecionou a permissão **Usar conexão de federação de grid** para o locatário:

- a. Confirme se um locatário idêntico foi replicado para a outra grid na conexão. Os locatários em ambas as grids terão o mesmo ID de conta de 20 dígitos, nome, descrição, cota e permissões.



Se você vir a mensagem de erro "Tenant created without a clone", consulte as instruções em ["Solucionar problemas de erros de federação de grid"](#).

- b. Se você forneceu uma senha de usuário raiz local ao definir acesso à raiz, ["alterar a senha do usuário raiz local"](#) para o locatário replicado.



Um usuário raiz local não consegue fazer login no Tenant Manager na grade de destino até que a senha seja alterada.

Faça login no tenant (opcional)

Conforme necessário, você pode entrar no novo locatário agora para concluir a configuração ou pode entrar no locatário mais tarde. As etapas de login dependem se você está conectado ao Grid Manager usando a porta padrão (443) ou uma porta restrita. Consulte ["Controle de acesso no firewall externo"](#).

Faça login agora

Se você estiver usando...	Faça isso...
Porta 443 e você define uma senha para o usuário raiz local	1. Selecione Entrar como root. Ao iniciar sessão, aparecem links para configurar buckets, federação de identidade, grupos e usuários. 2. Selecione os links para configurar a conta do locatário. Cada link abre a página correspondente no Tenant Manager. Para concluir a página, consulte o "Instruções para usar contas de tenant".
Porta 443 e você não definiu uma senha para o usuário raiz local	Selecione Entrar e insira as credenciais de um usuário no grupo federado de acesso à raiz.

Se você estiver usando...	Faça isso...
Uma porta restrita	1. Selecione Concluir 2. Selecione Restrito na tabela de tenant para saber mais sobre como acessar esta conta de tenant. A URL do Tenant Manager tem este formato: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> ◦ <i>FQDN_or_Admin_Node_IP</i> é um domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ <i>port</i> é a porta exclusiva para tenants ◦ <i>20-digit-account-id</i> é o ID de conta exclusivo do locatário

Entrar mais tarde

Se você estiver usando...	Faça uma destas opções...
Porta 443	• No Grid Manager, selecione Tenants e, em seguida, selecione Sign in à direita do nome do tenant. • Digite a URL do locatário em um navegador da web: <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> ◦ <i>FQDN_or_Admin_Node_IP</i> é um domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ <i>20-digit-account-id</i> é o ID de conta exclusivo do locatário
Uma porta restrita	• No Grid Manager, selecione Inquilinos e selecione Restrito. • Digite a URL do locatário em um navegador da web: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> ◦ <i>FQDN_or_Admin_Node_IP</i> é um domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ <i>port</i> é a porta restrita exclusiva para tenant ◦ <i>20-digit-account-id</i> é o ID de conta exclusivo do locatário

Configurar o locatário

Siga as instruções em ["Use uma conta de tenant"](#) para gerenciar grupos de locatários e usuários, chaves de

acesso S3, buckets, serviços de plataforma, clonagem de contas e replicação entre grids.

Editar uma conta de locatário do StorageGRID

Você pode editar uma conta de locatário para alterar o nome de exibição, a cota de armazenamento ou as permissões do locatário.



Se um locatário tiver a permissão **Usar conexão de federação de grid**, você pode editar os detalhes do locatário em qualquer uma das grids da conexão. No entanto, quaisquer alterações que você fizer em uma grid da conexão não serão copiadas para a outra grid. Se você quiser manter os detalhes do locatário exatamente sincronizados entre as grids, faça as mesmas edições em ambas as grids. Consulte ["Gerencie os locatários permitidos para conexão de federação de grid"](#).

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Acesso à raiz ou permissão para contas de locatário"](#).



A aplicação das configurações de locatário em toda a grid pode levar 15 minutos ou mais, dependendo da conectividade da rede, do status do nó e das operações do Cassandra.

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

2. Localize a conta do locatário que você deseja editar.

Utilize a caixa de pesquisa para procurar um tenant pelo nome ou pelo ID do tenant.

3. Selecione o tenant. Você pode fazer uma das seguintes ações:

- Selecione a caixa de seleção do tenant e selecione **Actions > Edit**.
- Selecione o nome do locatário para exibir a página de detalhes e selecione **Editar**.

4. Opcionalmente, altere os valores destes campos:

- **Nome**
- **Descrição**
- **Cota de armazenamento**

5. Selecione **Continue**.

6. Selecione ou limpe as permissões da conta do tenant.

- Se você desativar os **Serviços da Plataforma** para um locatário que já os utiliza, os serviços que ele configurou para seus buckets S3 deixarão de funcionar. Nenhuma mensagem de erro é enviada ao locatário. Por exemplo, se o locatário configurou a replicação CloudMirror para um bucket S3, ele ainda poderá armazenar objetos no bucket, mas cópias desses objetos não serão mais feitas no bucket S3 externo que ele configurou como endpoint. Consulte ["Gerencie serviços de plataforma para contas de locatário do S3"](#).
- Altere a configuração de **Usar a própria fonte de identidade** para determinar se a conta do locatário usará sua própria fonte de identidade ou a fonte de identidade configurada para o Grid Manager.

Se **Usar a própria fonte de identidade** estiver:

- Desativado e selecionado, o locatário já habilitou sua própria fonte de identidade. Um locatário deve desativar sua fonte de identidade antes de poder usar a fonte de identidade configurada para o Grid Manager.
- Desativado e não selecionado, o SSO está habilitado para o sistema StorageGRID. O locatário deve usar a fonte de identidade que foi configurada para o Grid Manager.
- Selecione ou desmarque a permissão **Permitir seleção S3** conforme necessário. Consulte ["Gerencie o S3 Select para contas de locatário"](#).
- Para remover a permissão **Usar conexão de federação de grid**:
 - i. Selecione a guia **Federação de grid**.
 - ii. Selecione **Remover permissão**.
- Para adicionar a permissão **Usar conexão de federação de grid**:
 - i. Selecione a guia **Federação de grid**.
 - ii. Selecione a caixa de seleção **Usar conexão de federação de grid**.
 - iii. Opcionalmente, selecione **Clonar usuários e grupos locais existentes** para cloná-los para a grid remota. Se desejar, você pode interromper a clonagem em andamento ou tentar novamente a clonagem caso alguns usuários ou grupos locais não tenham sido clonados após a conclusão da última operação de clonagem.
- Para definir um período máximo de retenção ou permitir o modo de conformidade:



O bloqueio de objetos S3 deve estar ativado na grid antes que você possa usar essas configurações.

- i. Selecione a aba **Bloqueio de Objeto S3**.
- ii. Em **Definir período máximo de retenção**, insira um valor e selecione o período de tempo no menu suspenso.
- iii. Para **Permitir modo de conformidade**, selecione a caixa de seleção.

Alterar a senha do usuário raiz local do StorageGRID tenant

Você pode precisar alterar a senha do usuário raiz local de um locatário se o usuário raiz estiver bloqueado na conta.

Antes de começar

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

Sobre esta tarefa

Se o login único (SSO) estiver habilitado para o seu sistema StorageGRID, o usuário raiz não poderá acessar a conta do tenant. Para executar tarefas de usuário raiz, os usuários devem pertencer a um grupo federado que tenha permissão de acesso root para o tenant.

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		
☐	Name ? ↕	Logical space used ? ↕	Quota utilization ? ↕	Quota ? ↕	Object count ? ↕	Sign in/Copy URL ?	
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄	
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄	
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄	
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄	
☐	Tenant 05	5.00 GB	—	—	500	→ 📄	

2. Selecione a conta do locatário. Você pode fazer uma das seguintes ações:
 - Selecione a caixa de seleção do locatário e selecione **Ações > Alterar senha de root**.
 - Selecione o nome do locatário para exibir a página de detalhes e selecione **Ações > Alterar senha root**.
3. Digite a nova senha para a conta do tenant.
4. Selecione **Salvar**.

Excluir uma conta de locatário do StorageGRID

Você pode excluir a conta de um locatário se desejar remover permanentemente o acesso desse locatário ao sistema.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Você removeu todos os buckets e objetos S3 associados à conta do locatário.
- Se o inquilino tiver permissão para usar uma conexão de federação de grid, você analisou as considerações para ["excluindo um locatário com a permissão "Usar conexão de federação de grid""](#).

Passos

1. Selecione **Tenants**.
2. Localize a(s) conta(s) do locatário que você deseja excluir.

Utilize a caixa de pesquisa para procurar um tenant pelo nome ou pelo ID do tenant.

3. Para excluir vários tenants, selecione as caixas de seleção e selecione **Ações > Excluir**.
4. Para excluir um único locatário, faça um dos seguintes:
 - Selecione a caixa de seleção e selecione **Ações > Excluir**.
 - Selecione o nome do locatário para exibir a página de detalhes e, em seguida, selecione **Actions > Delete**.
5. Selecione **Sim**.

Gerenciar serviços de plataforma

Saiba mais sobre os serviços da plataforma StorageGRID

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

Se você habilitar os serviços de plataforma para contas de locatários do S3, deverá configurar sua grid para que os locatários possam acessar os recursos externos necessários para usar esses serviços.

Os serviços de plataforma não são suportados para ["buckets de branch"](#).

CloudMirror replicação

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

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

CloudMirror replication apresenta algumas semelhanças e diferenças importantes em relação ao recurso de replicação entre grades. Para saber mais, consulte ["Compare a replicação entre grades e a replicação CloudMirror"](#).



CloudMirror replication 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 realizadas em objetos para um cluster Kafka externo especificado, um endpoint de webhook ou o Amazon Simple Notification Service.

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 seja possível configurar a notificação de eventos em um bucket com o S3 Object Lock ativado, os metadados do S3 Object Lock (incluindo Retain Until Date e o status de Legal Hold) 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 específico, onde os metadados podem ser pesquisados ou analisados usando o serviço externo.

Por exemplo, você pode configurar seus buckets para enviar metadados de objetos S3 para um serviço Elasticsearch remoto. Em seguida, você pode usar o Elasticsearch para realizar buscas em todos os buckets e executar análises sofisticadas de padrões presentes nos metadados dos seus objetos.



Embora a integração com o Elasticsearch possa ser configurada em um bucket com o S3 Object Lock ativado, os metadados do S3 Object Lock (incluindo Retain Until Date e o status de Legal Hold) dos objetos não serão incluídos nas mensagens de notificação.

Os serviços de plataforma permitem que os locatários usem recursos de storage externos, serviços de notificação e serviços de pesquisa ou análise com seus dados. Como o local de destino dos serviços de plataforma geralmente é externo à sua implantação do StorageGRID, você deve decidir se deseja permitir que os locatários usem esses serviços. Se permitir, você deve habilitar o uso dos serviços de plataforma ao criar ou editar contas de locatário. Você também deve configurar sua rede para que as mensagens dos serviços de plataforma geradas pelos locatários possam chegar aos seus destinos.

Recomendações para o uso de serviços de plataforma

Antes de utilizar os serviços da plataforma, esteja ciente das seguintes recomendações:

- Se um bucket S3 no sistema StorageGRID tiver tanto o versionamento quanto a replicação CloudMirror ativados, você também deve ativar o versionamento do bucket S3 para o endpoint de destino. Isso permite que a replicação CloudMirror gere versões de objetos semelhantes no endpoint.
- Você não deve usar mais de 100 tenants ativos com solicitações S3 que exigem CloudMirror para replicação, notificações e integração de pesquisa. Ter mais de 100 tenants ativos pode resultar em desempenho mais lento do cliente S3.
- As solicitações para um endpoint que não puderem ser concluídas serão enfileiradas até um máximo de 500.000 solicitações. Esse limite é compartilhado igualmente entre os tenants ativos. Novos tenants podem exceder temporariamente esse limite de 500.000 para que não sejam penalizados injustamente.

Informações relacionadas

- ["Gerenciar serviços de plataforma"](#)
- ["Configurar as configurações de proxy de storage"](#)
- ["Monitorar o StorageGRID"](#)

Rede e portas para serviços de plataforma StorageGRID

Se você permitir que um locatário do S3 use os serviços da plataforma, deverá

configurar a rede do grid para garantir que as mensagens dos serviços da plataforma possam ser entregues aos seus destinos.

Você pode habilitar os serviços de plataforma para uma conta de locatário S3 ao criar ou atualizar a conta do locatário. Se os serviços de plataforma estiverem habilitados, o locatário pode criar endpoints que servem como destino para replicação CloudMirror, notificações de eventos ou mensagens de integração de pesquisa de seus buckets S3. Essas mensagens de serviços de plataforma são enviadas dos Storage Nodes 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 que oferece suporte ao recebimento de mensagens do Amazon Simple Notification Service
- Um cluster Kafka hospedado localmente
- Um endpoint webhook externo ou hospedado localmente que suporta solicitações de notificação HTTP POST.

Este endpoint pode ser hospedado em diversos servidores web, frameworks ou ferramentas de processamento de dados, como o Fluentd.

- Um bucket S3 hospedado localmente na mesma instância ou em outra instância do StorageGRID
- Um endpoint externo, como um endpoint na Amazon Web Services.

Para garantir que as mensagens dos serviços da plataforma possam ser entregues, você deve configurar a(s) rede(s) que contém(êm) os Nós de Armazenamento do ADC. Você deve garantir que as seguintes portas possam ser usadas para enviar mensagens dos serviços da plataforma aos 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 (a maioria dos endpoints)
- **443**: Para URIs de endpoint que começam com https (a maioria dos endpoints)
- **9092**: Para URIs de endpoint que começam com http ou https (somente endpoints Kafka)

Os locatários podem especificar uma porta diferente ao criar ou editar um endpoint.



Se uma implementação do StorageGRID for usada como destino para a replicação do CloudMirror, as mensagens de replicação poderão ser recebidas em uma porta diferente de 80 ou 443. Certifique-se de que a porta usada para o S3 pela implementação do StorageGRID de destino esteja especificada no endpoint.

Se você utiliza um servidor proxy não transparente, também precisa ["configurar as configurações de proxy de armazenamento"](#) permitir que mensagens sejam enviadas para endpoints externos, como um endpoint na internet.

Informações relacionadas

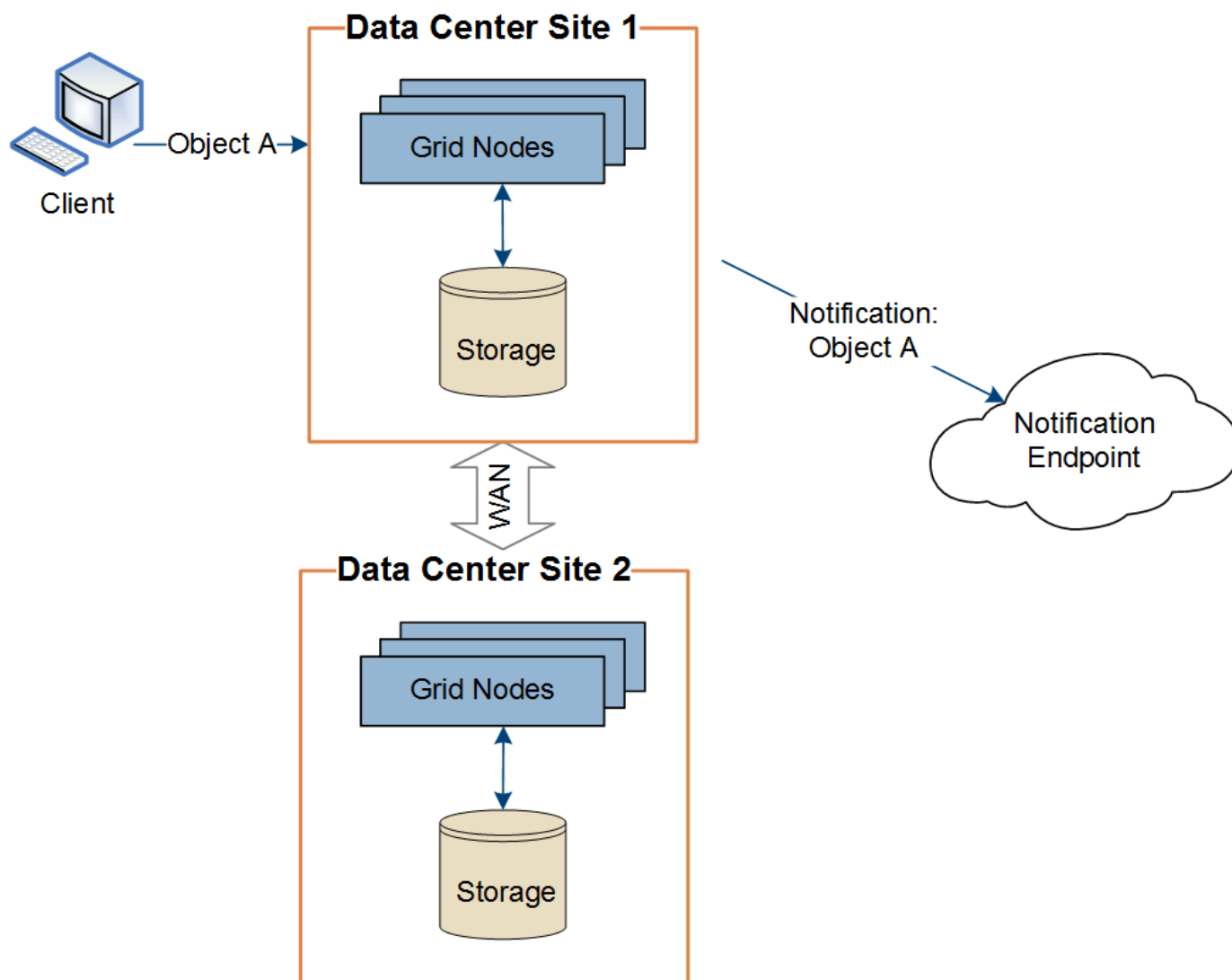
["Use uma conta de tenant"](#)

Entrega por local de mensagens dos serviços da plataforma StorageGRID

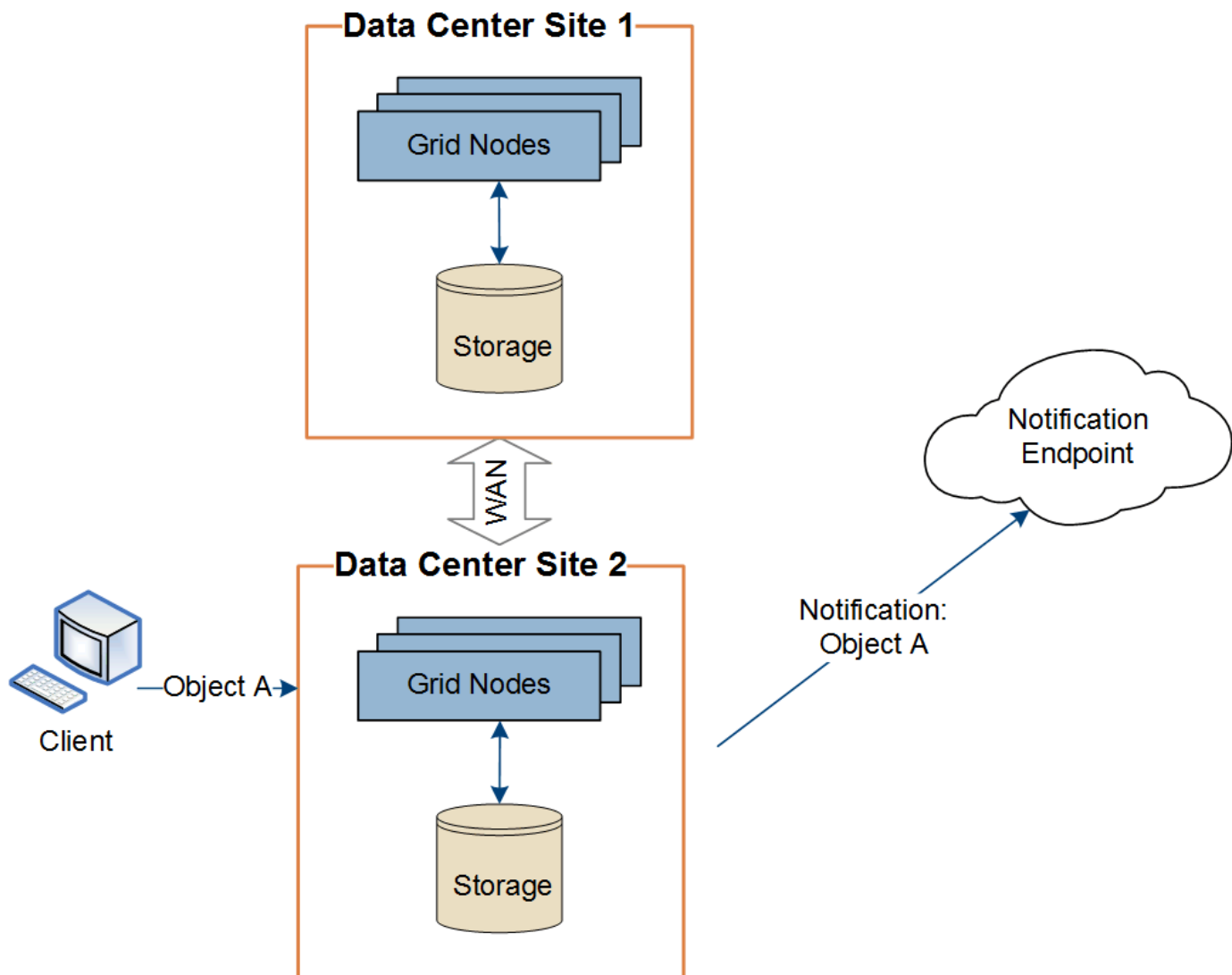
Todas as operações de serviços da plataforma são realizadas individualmente em cada

site.

Ou seja, se um locatário usar um cliente para executar uma operação Create da API S3 em um objeto, conectando-se a um Gateway Node no Data Center Site 1, a notificação sobre essa ação será acionada e enviada do Data Center Site 1.



Se o cliente posteriormente executar uma operação de exclusão da API S3 nesse mesmo objeto a partir 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 esteja configurada de forma que as mensagens dos serviços da plataforma possam ser entregues aos seus destinos.

Solucione problemas dos serviços da plataforma StorageGRID

Os endpoints usados nos serviços da plataforma são criados e mantidos pelos usuários do tenant no Tenant Manager. No entanto, se um tenant tiver problemas para configurar ou usar os serviços da plataforma, você pode usar o Grid Manager 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 endpoints usando o Tenant Manager. Cada endpoint representa um destino externo para um serviço da plataforma, como um bucket do StorageGRID S3, um bucket do Amazon Web Services, um tópico do Amazon Simple Notification Service, um tópico do Kafka ou um cluster do Elasticsearch hospedado localmente ou na AWS. Cada endpoint inclui tanto a localização do recurso externo quanto as credenciais necessárias para acessar esse recurso.

Quando um locatário cria um endpoint, o StorageGRID valida se o endpoint existe e se pode ser acessado 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 tenant.

Problemas com os endpoints existentes

Se ocorrer um erro quando StorageGRID tentar acessar um endpoint existente, uma mensagem será exibida no painel do Tenant Manager.



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 locatários podem acessar a página de Endpoints para revisar a mensagem de erro mais recente de cada endpoint e determinar há quanto tempo o erro ocorreu. A coluna **Último erro** exibe a mensagem de erro mais recente de cada endpoint e indica há quanto tempo 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

☐	Display name  	Last error  	Type  	URI  	URN  
☐	my-endpoint-2	 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
☐	my-endpoint-3	 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
☐	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
☐	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
☐	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 da grade ou suporte técnico pode usar esse ID para localizar informações mais detalhadas sobre o erro no bycast.log.

Problemas relacionados a servidores proxy

Se você configurou um "proxy de armazenamento" entre os nós de armazenamento e os endpoints do serviço da plataforma, podem ocorrer erros se o seu serviço de proxy não permitir mensagens do StorageGRID. Para resolver esses problemas, verifique as configurações do seu servidor proxy para garantir que as mensagens relacionadas ao serviço da plataforma não estejam sendo bloqueadas.

Determine se ocorreu um erro

Se ocorrerem erros de endpoint nos últimos 7 dias, o painel do Tenant Manager exibirá uma mensagem de alerta. Você pode acessar a página Endpoints para ver mais detalhes sobre o erro.

As operações do cliente falham

Alguns problemas nos serviços da plataforma podem causar falhas nas operações do cliente no bucket S3. Por exemplo, as operações do cliente S3 falharão se o serviço interno de Replicated State Machine (RSM) for interrompido ou se houver muitas mensagens dos serviços da plataforma enfileiradas para entrega.

Para verificar o status dos serviços:

1. Selecione **Nós > site > Nó de armazenamento > Visão geral**.
2. Verifique se há alertas ativos na tabela de Alertas.
3. Resolva quaisquer alertas ativos. Se necessário, entre em contato com o suporte técnico.

Erros de endpoint recuperáveis e irre recuperáveis

Após a criação dos endpoints, erros nas solicitações de serviço da plataforma podem ocorrer por diversos 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 bucket de destino não existe.
- A notificação não pôde ser entregue.

Caso StorageGRID encontre um erro recuperável, a solicitação de serviço da plataforma será repetida até que seja bem-sucedida.

Outros erros são irre recuperáveis. Por exemplo, erros irre recuperáveis podem ocorrer pelos seguintes motivos:

- O endpoint foi excluído.
- Um endpoint de webhook destino responde a uma solicitação de notificação com um 400 Bad Request erro.

Se StorageGRID encontrar um erro de endpoint irre recuperável:

- No Grid Manager, acesse **Suporte > Ferramentas > Métricas > Grafana > Platform Services Overview** para visualizar os detalhes do erro.
- No Gerenciador de Locatários, vá para **STORAGE (S3) > Platform Services Endpoints** para visualizar os detalhes do erro.
- Verifique o `/var/local/log/bycast-err.log` para erros relacionados. Os nós de armazenamento que possuem o serviço ADC contêm este arquivo de log.

Não foi possível entregar as mensagens dos serviços da plataforma

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

Verifique se há alertas relacionados.

Desempenho mais lento para solicitações de serviço da plataforma

O software StorageGRID pode limitar as solicitações S3 recebidas para um bucket se a taxa de envio das solicitações exceder a taxa na qual o endpoint de destino pode recebê-las. A limitação só ocorre quando há um acúmulo de solicitações aguardando para serem enviadas ao endpoint de destino.

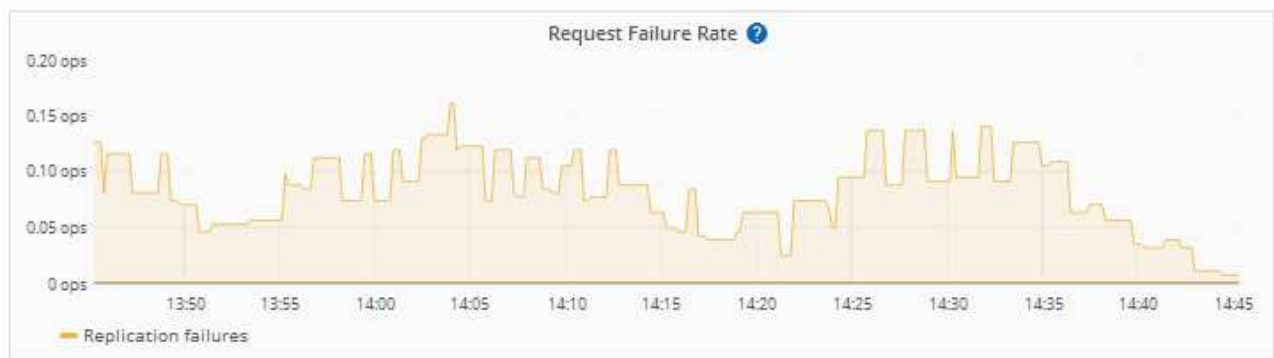
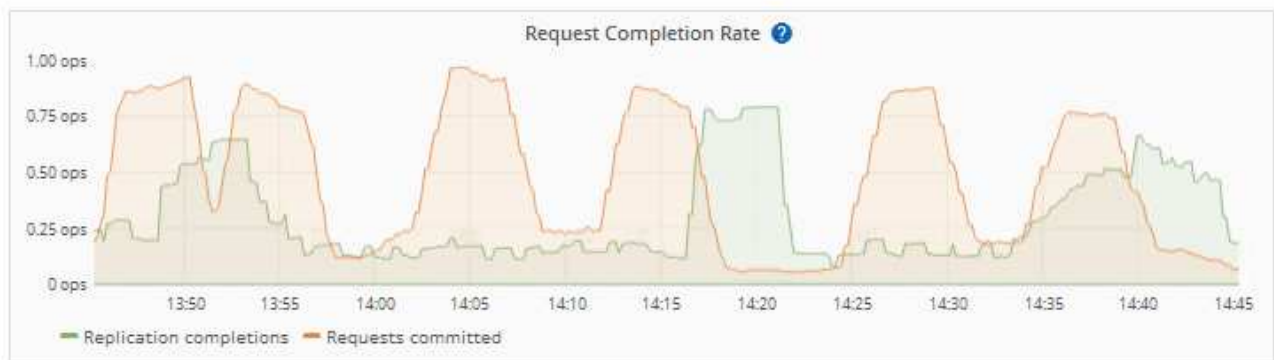
O único efeito visível é que as solicitações S3 recebidas levarão mais tempo para serem executadas. Se você começar a detectar um desempenho significativamente mais lento, você deve reduzir a taxa de ingestão ou usar um endpoint com maior capacidade. Se o acúmulo de solicitações continuar crescendo, as operações do cliente S3 (como solicitações PUT) eventualmente falharão.

As solicitações do CloudMirror têm mais probabilidade de serem afetadas pelo desempenho do endpoint de destino, porque normalmente envolvem mais transferência de dados do que as solicitações de integração de pesquisa ou de notificação de eventos.

As solicitações de serviço da plataforma falham

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

1. Selecione **Nós**.
2. Selecione **site > Serviços da Plataforma**.
3. Veja o gráfico da taxa de erros de solicitação.



Alerta de indisponibilidade dos serviços da plataforma

O alerta **Serviços da plataforma indisponíveis** indica que nenhuma operação de serviço da plataforma pode ser executada em um site porque há poucos Storage Nodes com o serviço RSM em execução ou disponíveis.

O serviço RSM garante que as solicitações de serviço da plataforma sejam enviadas aos seus respectivos endpoints.

Para resolver este alerta, determine quais Storage Nodes no site incluem o serviço RSM. (O serviço RSM está presente nos Storage Nodes que também incluem o serviço ADC.) Em seguida, certifique-se de que a maioria simples desses Storage Nodes esteja em execução e disponível.



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

Orientações adicionais para resolução de problemas nos endpoints dos serviços da plataforma

Para obter informações adicionais, consulte [Usar uma conta de locatário](#) > [Solucionar problemas de endpoints de serviços da plataforma](#).

Informações relacionadas

["Solucione problemas do sistema StorageGRID"](#)

Gerenciar o S3 Select para contas de locatário no StorageGRID

Você pode permitir que determinados tenants do S3 usem o S3 Select para emitir solicitações `SelectObjectContent` em objetos individuais.

O S3 Select oferece uma maneira eficiente de pesquisar grandes quantidades de dados sem a necessidade de implantar um banco de dados e os recursos associados para viabilizar as pesquisas. Ele também reduz o custo e a latência da recuperação de dados.

O que é S3 Select?

O S3 Select permite que os clientes S3 usem solicitações `SelectObjectContent` para filtrar e recuperar apenas os dados necessários de um objeto. A implementação do S3 Select no StorageGRID inclui um subconjunto de comandos e recursos do S3 Select.

Considerações e requisitos para usar o S3 Select

Requisitos de administração do grid

O administrador da grade deve conceder aos locatários a permissão S3 Select. Selecione **Permitir S3 Select** quando ["criando um tenant"](#) ou ["editar um tenant"](#).

Requisitos de formato de objeto

O objeto que você deseja consultar deve estar em um dos seguintes formatos:

- **CSV**. Pode ser usado como está ou compactado em arquivos GZIP ou BZIP2.
- **Parquet**. Requisitos adicionais para objetos Parquet:
 - O S3 Select suporta apenas compressão colunar usando GZIP ou Snappy. O S3 Select não suporta compressão de objeto inteiro para objetos Parquet.
 - O S3 Select não suporta saída em Parquet. Você deve especificar o formato de saída como CSV ou JSON.
 - O tamanho máximo de um grupo de linhas não compactadas é de 512 MB.
 - Você deve usar os tipos de dados especificados no esquema do objeto.
 - Não é possível usar os tipos lógicos INTERVAL, JSON, LIST, TIME ou UUID.

Requisitos do endpoint

A solicitação `SelectObjectContent` deve ser enviada para um ["Endpoint do balanceador de carga"](#)

[StorageGRID](#)".

Os nós de administração e de gateway usados pelo endpoint devem ser um dos seguintes:

- Um nó de appliance de serviços
- Um nó de software baseado em VMware
- Um nó bare metal executando um kernel com cgroup v2 habilitado

Considerações gerais

Não é possível enviar consultas diretamente para os Storage Nodes.



SelectObjectContent requests podem diminuir o desempenho do balanceador de carga para todos os clientes S3 e todos os locatários. Habilite esse recurso somente quando necessário e apenas para locatários confiáveis.

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

Para visualizar "[Gráficos do Grafana](#)" para operações do S3 Select ao longo do tempo, selecione **Suporte > Ferramentas > Métricas** no Gerenciador de Grade.

Configurar conexões de cliente

Configurar conexões do cliente S3 ao StorageGRID

Como administrador de grid, você gerencia as opções de configuração que controlam como os aplicativos cliente S3 se conectam ao seu sistema StorageGRID para armazenar e recuperar dados.



Detalhes sobre o Swift foram removidos desta versão do site de documentação. Veja "[StorageGRID 11.8: Configurar conexões de cliente S3 e Swift](#)".

Tarefas de configuração

1. Execute as tarefas pré-requisito no StorageGRID, com base em como o aplicativo cliente se conectará ao StorageGRID.

Tarefas necessárias

Você deve obter:

- Endereços IP
- Nomes de domínio
- Certificado SSL

Tarefas opcionais

Opcionalmente, configure:

- Federação de identidades
- SSO

1. Use StorageGRID para obter os valores necessários para que o aplicativo se conecte à grid. Você pode usar o assistente de instalação S3 ou configurar cada entidade do StorageGRID manualmente. +

Use o assistente de instalação S3

Siga os passos no assistente de instalação S3.

Configurar manualmente

1. Criar grupo de alta disponibilidade
2. Criar endpoint de balanceador de carga
3. Criar conta de locatário
4. Criar bucket e chaves de acesso
5. Configurar regra e política do ILM

1. Utilize o aplicativo S3 para concluir a conexão com StorageGRID. Crie entradas DNS para associar endereços IP a quaisquer nomes de domínio que você planeje usar.

Se necessário, realize configurações adicionais do aplicativo.

2. Execute tarefas contínuas no aplicativo e no StorageGRID para gerenciar e monitorar storage de objetos ao longo do tempo.

Informações necessárias para conectar StorageGRID a um aplicativo cliente

Antes de conectar StorageGRID a um aplicativo cliente S3, você deve executar etapas de configuração no StorageGRID e obter determinados valores.

Quais valores você precisa?

A tabela a seguir mostra os valores que você deve configurar no StorageGRID e onde esses valores são usados pelo aplicativo S3 e pelo servidor DNS.

Valor	Onde o valor é configurado	Onde o valor é usado
Endereços IP virtuais (VIP)	StorageGRID > Grupo HA	Entrada DNS
Porta	StorageGRID > Ponto final do balanceador de carga	Aplicativo do cliente
Certificado SSL	StorageGRID > Ponto final do balanceador de carga	Aplicativo do cliente
Nome do servidor (FQDN)	StorageGRID > Ponto final do balanceador de carga	• Aplicativo do cliente • Entrada DNS
ID da chave de acesso S3 e chave de acesso secreta	StorageGRID > Locatário e bucket	Aplicativo do cliente
Nome do bucket/container	StorageGRID > Locatário e bucket	Aplicativo do cliente

Como obtenho esses valores?

Dependendo das suas necessidades, você pode fazer o seguinte para obter as informações de que precisa:

- **Use o "Assistente de instalação S3".** O assistente de instalação S3 ajuda você a configurar rapidamente os valores necessários no StorageGRID e gera um ou dois arquivos que você pode usar ao configurar o aplicativo S3. O assistente orienta você pelas etapas necessárias e ajuda a garantir que suas configurações estejam em conformidade com as melhores práticas do StorageGRID.



Se você estiver configurando um aplicativo S3, recomenda-se usar o assistente de instalação do S3, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá personalização significativa.

- **Use o "FabricPool assistente de instalação".** Semelhante ao assistente de instalação S3, o assistente de instalação FabricPool ajuda você a configurar rapidamente os valores necessários e gera um arquivo que você pode usar ao configurar uma camada de nuvem FabricPool no ONTAP.



Se você planeja usar StorageGRID como o storage de objetos para uma camada de nuvem FabricPool, é recomendado usar o assistente de instalação FabricPool, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá personalização significativa.

- **Configurar itens manualmente.** Se você estiver se conectando a um aplicativo S3 e preferir não usar o assistente de instalação, você pode obter os valores necessários realizando a configuração manualmente. Siga estas etapas:
 - a. Configure o grupo de alta disponibilidade (HA) que você deseja usar para o aplicativo S3. Consulte ["Configurar grupos de alta disponibilidade"](#).
 - b. Crie o endpoint do balanceador de carga que o aplicativo S3 usará. Consulte ["Configurar pontos de extremidade do balanceador de carga"](#).
 - c. Crie a conta de locatário que o aplicativo S3 usará. Consulte ["Crie uma conta de locatário"](#).

- d. Para um locatário S3, faça login na conta do locatário e gere um ID de chave de acesso e uma chave de acesso secreta para cada usuário que acessará o aplicativo. Consulte ["Crie suas próprias chaves de acesso"](#).
- e. Crie um ou mais buckets do S3 na conta do locatário. Para S3, veja ["Criar bucket S3"](#).
- f. Para adicionar instruções específicas de posicionamento para os objetos pertencentes ao novo locatário ou bucket/container, crie uma nova regra ILM e ative uma nova política ILM para usar essa regra. Consulte ["Criar regra ILM"](#) e ["Criar política de ILM"](#).

Segurança para clientes S3 no StorageGRID

As contas de tenant do StorageGRID usam aplicativos cliente S3 para salvar dados de objetos no StorageGRID. Você deve revisar as medidas de segurança implementadas para aplicativos cliente.

Resumo

A lista a seguir resume como a segurança é implementada para a S3 API REST:

Segurança da conexão

TLS

Autenticação do servidor

Certificado de servidor X.509 assinado pela CA do sistema ou certificado de servidor personalizado fornecido pelo administrador

Autenticação do cliente

ID da chave de acesso da conta S3 e chave de acesso secreta

Autorização do cliente

Propriedade do bucket e todas as políticas de controle de acesso aplicáveis

Como StorageGRID fornece segurança para aplicativos de cliente

Os aplicativos cliente S3 podem se conectar ao serviço Load Balancer em Gateway Nodes, Admin Nodes ou diretamente aos Storage Nodes.

- Os clientes que se conectam ao serviço Load Balancer podem usar HTTPS ou HTTP, dependendo de como você ["configurar o endpoint do balanceador de carga"](#).

O HTTPS oferece comunicação segura e criptografada por TLS e é recomendado. Você deve anexar um certificado de segurança ao endpoint.

O HTTP oferece comunicação menos segura e não criptografada, devendo ser usado apenas para grids de teste ou que não sejam de produção.

- Os clientes que se conectam aos nós de armazenamento também podem usar HTTPS ou HTTP.

O HTTPS é o padrão e é recomendado.

O HTTP oferece comunicação menos segura e não criptografada, mas pode ser opcionalmente ["habilitado"](#) para grids de teste ou que não sejam de produção.

- As comunicações entre StorageGRID e o cliente são criptografadas usando TLS.
- As comunicações entre o serviço Load Balancer e os nós de armazenamento na grade são criptografadas, independentemente de o endpoint do Load Balancer estar configurado para aceitar conexões HTTP ou HTTPS.
- Os clientes devem fornecer "[Cabeçalhos de autenticação HTTP](#)" ao StorageGRID para executar operações da API REST.

Certificados de segurança e aplicativos de cliente

Em todos os casos, os aplicativos cliente podem estabelecer conexões TLS usando um certificado de servidor personalizado carregado pelo administrador da grid ou um certificado gerado pelo sistema StorageGRID:

- Quando os aplicativos cliente se conectam ao serviço Load Balancer, eles usam o certificado que foi configurado para o endpoint do balanceador de carga. Cada endpoint do balanceador de carga tem seu próprio certificado—seja um certificado de servidor personalizado carregado pelo administrador do grid ou um certificado que o administrador do grid gerou no StorageGRID ao configurar o endpoint.

Consulte "[Considerações sobre balanceamento de carga](#)".

- Quando os aplicativos cliente se conectam diretamente a um Nó de Armazenamento, eles usam os certificados de servidor gerados pelo sistema para os Nós de Armazenamento quando o sistema StorageGRID foi instalado (que são assinados pela autoridade certificadora do sistema), ou um único certificado de servidor personalizado fornecido para a grid por um administrador da grid. Consulte "[Adicionar um certificado de API S3 personalizado](#)".

Os clientes devem ser configurados para confiar na autoridade certificadora que assinou o certificado que utilizam para estabelecer conexões TLS.

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID suporta um conjunto de suítes de cifras que os aplicativos cliente podem usar ao estabelecer uma sessão TLS. Para configurar as cifras, vá em **Configuração > Segurança > Configurações de segurança** e selecione **Políticas de TLS e SSH**.

Versões compatíveis do TLS

StorageGRID suporta TLS 1.2 e TLS 1.3.



SSLv3 e TLS 1.1 (ou versões anteriores) não são mais suportados.

Use o assistente de instalação S3

Considerações e requisitos do assistente de instalação do StorageGRID S3

Você pode usar o assistente de instalação S3 para configurar o StorageGRID como o storage de objetos para um aplicativo S3.

Quando usar o assistente de instalação S3

O assistente de instalação S3 orienta você em cada etapa da configuração do StorageGRID para uso com um aplicativo S3. Como parte da conclusão do assistente, você faz o download de arquivos que pode usar para inserir valores no aplicativo S3. Use o assistente para configurar seu sistema mais rapidamente e para garantir que suas configurações estejam em conformidade com as melhores práticas do StorageGRID.

Se você tiver "[Permissão de acesso root](#)", poderá concluir o assistente de instalação do S3 ao começar a usar o StorageGRID Grid Manager ou poderá acessá-lo e concluí-lo posteriormente. Dependendo dos seus requisitos, você também pode configurar alguns ou todos os itens necessários manualmente e, em seguida, usar o assistente para reunir os valores que um aplicativo S3 precisa.

Antes de usar o assistente

Antes de usar o assistente, confirme que você concluiu esses pré-requisitos.

Obtenha endereços IP e configure interfaces VLAN

Se você for configurar um grupo de alta disponibilidade (HA), saberá a quais nós o aplicativo S3 se conectará e qual rede StorageGRID será usada. Você também saberá quais valores inserir para o CIDR da sub-rede, endereço IP do gateway e endereços IP virtuais (VIP).

Se você planeja usar uma LAN virtual para segregar o tráfego do aplicativo S3, você já configurou a interface VLAN. Consulte "[Configurar interfaces VLAN](#)".

Configurar a federação de identidades e o SSO (Single Sign-On)

Se você planeja usar federação de identidade ou logon único (SSO) para seu sistema StorageGRID, você habilitou esses recursos. Você também sabe qual grupo federado deve ter acesso à raiz para a conta do tenant que o aplicativo S3 usará. Consulte "[Use federação de identidades](#)" e "[Configure o single sign-on \(SSO\)](#)".

Obtenha e configure nomes de domínio

Você sabe qual domínio totalmente qualificado (FQDN) usar para StorageGRID. As entradas do servidor de nomes (DNS) mapearão esse FQDN para os endereços VIP do grupo de HA que você criar usando o assistente.

Se você planeja usar solicitações virtuais no estilo de hospedagem do S3, você deve ter "[nomes de domínio de endpoint S3 configurados](#)". O uso de solicitações virtuais no estilo de hospedagem é recomendado.

Analise os requisitos do balanceador de carga e do certificado de segurança

Se você planeja usar o balanceador de carga StorageGRID, já deve ter revisado as considerações gerais sobre balanceamento de carga. Você já possui os certificados que irá carregar ou os valores necessários para gerar um certificado.

Se você planeja usar um endpoint de balanceador de carga externo (terceiro), você precisa ter o domínio totalmente qualificado (FQDN), a porta e o certificado desse balanceador de carga.

Configurar quaisquer conexões de federação de grid

Se você deseja permitir que o locatário do S3 clone dados da conta e replique objetos do bucket para outra grid usando uma conexão de federação de grid, confirme o seguinte antes de iniciar o assistente:

- Você tem "[configurou a conexão de federação de grid](#)".
- O status da conexão é **Conectado**.
- Você tem permissão de acesso root.

Acesse e conclua o assistente de instalação no StorageGRID

Você pode usar o assistente de instalação S3 para configurar StorageGRID para uso com um aplicativo S3. O assistente de instalação fornece os valores necessários para

que o aplicativo acesse um bucket do StorageGRID e salve objetos.

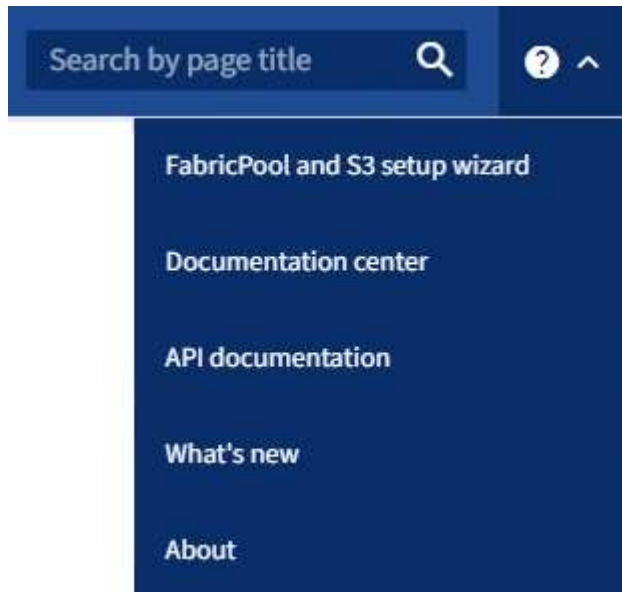
Antes de começar

- Você tem o ["Permissão de acesso root"](#).
- Você já revisou as ["Considerações e requisitos"](#) instruções para usar o assistente.

Acesse o assistente

Passos

1. Faça login no Grid Manager usando um ["navegador web compatível"](#).
2. Se o banner **FabricPool and S3 assistente de instalação** aparecer no painel, selecione o link no banner. Se o banner não aparecer mais, selecione o ícone de ajuda na barra de cabeçalho no Grid Manager e selecione **FabricPool and S3 assistente de instalação**.



3. Na seção de aplicativos S3 da página do assistente de instalação do FabricPool e S3, selecione **Configurar agora**.

Etapa 1 de 6: configurar grupo de alta disponibilidade

Um grupo de alta disponibilidade (HA) é uma coleção de nós, cada um contendo o serviço StorageGRID Load Balancer. Um grupo HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo de alta disponibilidade (HA) para ajudar a manter as conexões de dados do S3 disponíveis. Se a interface ativa no grupo HA falhar, uma interface de backup poderá gerenciar a carga de trabalho com pouco impacto nas operações do S3.

Para obter detalhes sobre esta tarefa, consulte ["Gerenciar grupos de alta disponibilidade"](#).

Passos

1. Se você planeja usar um balanceador de carga externo, não precisa criar um grupo de alta disponibilidade. Selecione **Ignorar esta etapa** e vá para [Etapa 2 de 6: Configurar o endpoint do balanceador de carga](#).
2. Para usar o balanceador de carga StorageGRID, você pode criar um novo grupo de alta disponibilidade (HA) ou usar um grupo HA existente.

Criar grupo HA

- Para criar um novo grupo HA, selecione **Criar grupo HA**.
- Na etapa **Inserir detalhes**, preencha os seguintes campos.

Campo	Descrição
Nome do grupo HA	Um nome de exibição exclusivo para este grupo HA.
Descrição (opcional)	A descrição deste grupo HA.

- Na etapa **Adicionar interfaces**, selecione as interfaces de nó que você deseja usar neste grupo de alta disponibilidade.

Use os cabeçalhos das colunas para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

Você pode selecionar um ou mais nós, mas só pode selecionar uma interface para cada nó.

- Na etapa **Priorizar interfaces**, determine a interface principal e quaisquer interfaces de backup para este grupo de alta disponibilidade.

Arraste as linhas para alterar os valores na coluna **Ordem de prioridade**.

A primeira interface da lista é a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.

Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços VIP (VIP) são movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP são movidos para a próxima interface de backup e assim por diante. Quando as falhas forem resolvidas, os endereços VIP retornam para a interface de maior prioridade disponível.

- Na etapa **Inserir endereços IP**, preencha os seguintes campos.

Campo	Descrição
CIDR da sub-rede	O endereço da sub-rede VIP na notação CIDR — um endereço IPv4 seguido por 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.
Endereço IP do gateway (opcional)	Se os endereços IP do S3 usados para acessar o StorageGRID não estiverem na mesma sub-rede que os endereços VIP do StorageGRID, insira o endereço IP do gateway local do VIP do StorageGRID. O endereço IP do gateway local deve estar dentro da sub-rede VIP.

Campo	Descrição
Endereço IP virtual	Insira pelo menos um e no máximo dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP. Pelo menos um endereço deve ser IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

f. Selecione **Criar grupo HA** e, em seguida, selecione **Concluir** para retornar ao assistente de instalação do S3.

g. Selecione **Continuar** para ir para a etapa do balanceador de carga.

Usar grupo HA existente

a. Para usar um grupo HA existente, selecione o nome do grupo HA em **Selecionar um grupo HA**.

b. Selecione **Continuar** para ir para a etapa do balanceador de carga.

Etapa 2 de 6: Configurar o endpoint do balanceador de carga

StorageGRID utiliza um balanceador de carga para gerenciar a carga de trabalho dos aplicativos cliente. O balanceamento de carga maximiza a velocidade e a capacidade de conexão entre vários Storage Nodes.

Você pode usar o serviço StorageGRID Load Balancer, que existe em todos os nós Gateway e Admin, ou pode se conectar a um balanceador de carga externo (de terceiro). Recomenda-se usar o balanceador de carga StorageGRID.

Para obter detalhes sobre esta tarefa, consulte "[Considerações sobre balanceamento de carga](#)".

Para usar o serviço StorageGRID Load Balancer, selecione a guia **StorageGRID load balancer** e, em seguida, crie ou selecione o endpoint do balanceador de carga que você deseja usar. Para usar um balanceador de carga externo, selecione a guia **External load balancer** e forneça detalhes sobre o sistema que você já configurou.

Criar endpoint

Passos

1. Para criar um endpoint de balanceador de carga, selecione **Criar endpoint**.
2. Na etapa **Inserir detalhes do endpoint**, preencha os seguintes campos.

Campo	Descrição
Nome	Um nome descritivo para o endpoint.
Porta	A porta do StorageGRID que você deseja usar para balanceamento de carga. Este campo tem como padrão 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada. Se você inserir 80 ou 443, o endpoint será configurado apenas nos nós de Gateway, pois essas portas são reservadas nos nós de Admin. Nota: Portas usadas por outros serviços de grid não são permitidas. Consulte "Portas internas do StorageGRID".
Tipo de cliente	Deve ser S3 .
Protocolo de rede	Selecione HTTPS. Nota: A comunicação com StorageGRID sem criptografia TLS é suportada, mas não recomendada.

3. Na etapa **Selecionar modo de vinculação**, especifique o modo de vinculação. O modo de vinculação controla como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

Modo	Descrição
Global (padrão)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer Gateway Node ou Admin Node, o endereço IP virtual (VIP) de qualquer grupo HA em qualquer rede ou um FQDN correspondente. Use a configuração Global (padrão), a menos que precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este endpoint. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA que você selecionar para os endpoints não se sobreponham.
Interfaces de nó	Os clientes devem usar os endereços IP (ou os FQDNs correspondentes) das interfaces de nó selecionadas para acessar este endpoint.

Modo	Descrição
Tipo de nó	Dependendo do tipo de nó que você selecionar, os clientes devem usar o endereço IP (ou o FQDN correspondente) de qualquer Nó de Administração ou o endereço IP (ou o FQDN correspondente) de qualquer Nó de Gateway para acessar este endpoint.

4. Na etapa de acesso do locatário, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de locatário podem usar este endpoint para acessar seus buckets.
Permitir locatários selecionados	Somente as contas de locatário selecionadas podem usar este endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar este endpoint para acessar seus buckets. Todos os outros locatários podem usar este endpoint.

5. Na etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Fazer upload do certificado (recomendado)	Use esta opção para carregar um certificado de servidor assinado por uma CA, a chave privada do certificado e, opcionalmente, um pacote de CA.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Veja "Configurar pontos de extremidade do balanceador de carga" para obter detalhes sobre o que inserir.
Use o certificado StorageGRID S3	Use esta opção somente se você já tiver carregado ou gerado uma versão personalizada do certificado global do StorageGRID. Veja "Configurar certificados da API S3" para detalhes.

6. Selecione **Concluir** para retornar ao assistente de instalação do S3.

7. Selecione **Continuar** para ir para a etapa de tenant e bucket.



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

Usar o endpoint do balanceador de carga existente

Passos

1. Para usar um endpoint existente, selecione o nome dele em **Selecionar um endpoint do balanceador de carga**.
2. Selecione **Continuar** para ir para a etapa de tenant e bucket.

Use um balanceador de carga externo

Passos

1. Para usar um balanceador de carga externo, preencha os seguintes campos.

Campo	Descrição
FQDN	O domínio totalmente qualificado (FQDN) do balanceador de carga externo.
Porta	O número da porta que o aplicativo S3 usará para se conectar ao balanceador de carga externo.
Certificado	Copie o certificado do servidor para o balanceador de carga externo e cole-o neste campo.

2. Selecione **Continuar** para ir para a etapa de tenant e bucket.

Etapa 3 de 6: criar locatário e bucket

Um locatário é uma entidade que pode usar aplicativos S3 para armazenar e recuperar objetos no StorageGRID. Cada locatário possui seus próprios usuários, chaves de acesso, buckets, objetos e um conjunto específico de recursos.

Um bucket é um contêiner usado para armazenar os objetos e os metadados de um locatário. Embora os locatários possam ter vários buckets, o assistente ajuda você a criar um locatário e um bucket da maneira mais rápida e fácil. Se você precisar adicionar buckets ou definir opções depois, pode usar o Tenant Manager.

Para obter detalhes sobre esta tarefa, consulte ["Criar conta de locatário"](#) e ["Criar bucket S3"](#).

Passos

1. Insira um nome para a conta do locatário.

Os nomes dos inquilinos não precisam ser únicos. Quando a conta do inquilino é criada, ela recebe um ID de conta numérico exclusivo.

2. Defina acesso à raiz para a conta do locatário, com base em se o seu sistema StorageGRID usa ["federação de identidade"](#), ["autenticação única \(SSO\)"](#) ou ambos.

Opção	Faça isso
Se a federação de identidades não estiver ativada	Especifique a senha a ser usada ao fazer login no tenant como usuário raiz.
Se a federação de identidades estiver ativada	a. Selecione um grupo federado existente para "Permissão de acesso root" para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no tenant como usuário raiz.

Opção	Faça isso
Se a federação de identidades e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter " Permissão de acesso root " para o locatário. Nenhum usuário local pode fazer login.

- Se você deseja que o assistente crie o ID da chave de acesso e a chave de acesso secreta para o usuário raiz, selecione **Criar chave de acesso S3 do usuário raiz automaticamente**.

Selecione esta opção se o único usuário do locatário for o usuário raiz. Se outros usuários utilizarem este locatário, "[Use o Tenant Manager](#)" para configurar as chaves e permissões.

- Se você deseja criar um bucket para este tenant agora, selecione **Create bucket for this tenant**.



Se o S3 Object Lock estiver habilitado para a grid, o bucket criado nesta etapa não terá o S3 Object Lock habilitado. Se você precisar usar um bucket com S3 Object Lock para este aplicativo S3, não selecione criar um bucket agora. Em vez disso, use o Tenant Manager para "[criar o bucket](#)" mais tarde.

- Insira o nome do bucket que o aplicativo S3 usará. Por exemplo, `s3-bucket`.

Não é possível alterar o nome do bucket depois de criá-lo.

- Selecione a **Região** para este bucket.

Use a região padrão (`us-east-1`) a menos que você pretenda usar o ILM no futuro para filtrar objetos com base na região do bucket.

- Selecione **Criar e continuar**.

Etapa 4 de 6: baixar dados

Na etapa de download de dados, você pode baixar um ou dois arquivos para salvar os detalhes do que você acabou de configurar.

Passos

- Se você selecionou **Criar chave de acesso S3 do usuário raiz automaticamente**, faça um ou ambos os seguintes procedimentos:
 - Selecione **Baixar chaves de acesso** para baixar um arquivo `.csv` contendo o nome da conta do locatário, o ID da chave de acesso e a chave de acesso secreta.
 - Selecione o ícone de copiar () para copiar o ID da chave de acesso e a chave de acesso secreta para a área de transferência.
- Selecione **Baixar valores de configuração** para baixar um arquivo `.txt` contendo as configurações do endpoint do balanceador de carga, tenant, bucket e do usuário raiz.
- Guarde essas informações em um local seguro.



Não feche esta página até ter copiado ambas as chaves de acesso. As chaves não estarão disponíveis após você fechar esta página. Certifique-se de salvar essas informações em um local seguro, pois elas podem ser usadas para obter dados do seu sistema StorageGRID.

4. Caso seja solicitado, selecione a caixa de seleção para confirmar que você baixou ou copiou as chaves.
5. Selecione **Continuar** para ir para a etapa de regra e política do ILM.

Etapa 5 de 6: Revisar a regra ILM e a política ILM para S3

As regras de gerenciamento de ciclo de vida da informação (ILM) controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos no seu sistema StorageGRID. A política de ILM incluída com o StorageGRID cria duas cópias replicadas de todos os objetos. Essa política permanece em vigor até que você ative pelo menos uma nova política.

Passos

1. Analise as informações fornecidas na página.
2. Se você deseja adicionar instruções específicas para os objetos pertencentes ao novo locatário ou bucket, crie uma nova regra e uma nova política. Consulte ["Criar regra ILM"](#) e ["Use políticas ILM"](#).
3. Selecione **Eu revisei essas etapas e entendi o que preciso fazer**.
4. Selecione a caixa de seleção para indicar que você entende o que fazer a seguir.
5. Selecione **Continuar** para ir para **Resumo**.

Etapa 6 de 6: revisar o resumo

Passos

1. Analise o resumo.
2. Preste atenção aos detalhes nas próximas etapas, que descrevem a configuração adicional que pode ser necessária antes de você se conectar ao cliente S3. Por exemplo, selecionar **Entrar como root** leva você ao Tenant Manager, onde você pode adicionar usuários do tenant, criar buckets adicionais e atualizar as configurações do bucket.
3. Selecione **Concluir**.
4. Configure o aplicativo usando o arquivo que você baixou do StorageGRID ou os valores que você obteve manualmente.

Gerenciar grupos de alta disponibilidade

Saiba mais sobre os grupos de alta disponibilidade do StorageGRID

Os grupos de alta disponibilidade (HA) fornecem conexões de dados altamente disponíveis para clientes S3 e conexões altamente disponíveis para o Grid Manager e o Tenant Manager.

Você pode agrupar as interfaces de rede de vários nós de administração 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.

Cada grupo HA fornece acesso aos serviços compartilhados nos nós selecionados.

- Grupos de HA que incluem Gateway Nodes, Admin Nodes ou ambos fornecem conexões de dados altamente disponíveis para clientes S3.
- Grupos de HA que incluem apenas Admin Nodes fornecem conexões altamente disponíveis para o Grid Manager e o Tenant Manager.

- Um grupo de alta disponibilidade (HA) que inclua apenas appliances de serviços e nós de software baseados em VMware pode fornecer conexões de alta disponibilidade para "[Locatários S3 que usam o S3 Select](#)". Os grupos de HA são recomendados ao usar S3 Select, mas não são obrigatórios.

Como você cria um grupo de alta disponibilidade?

1. Você seleciona uma interface de rede para um ou mais Admin Nodes ou Gateway Nodes. Você pode usar uma interface Grid Network (eth0), interface Client Network (eth2), interface VLAN ou uma interface de acesso que você adicionou ao nó.



Você não pode adicionar uma interface a um grupo HA se ela tiver um endereço IP atribuído por DHCP.

2. Você especifica uma interface para ser a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.
3. Você define a ordem de prioridade para quaisquer interfaces de backup.
4. Você atribui de um a 10 endereços IP virtuais (VIP) ao grupo. Os aplicativos cliente podem usar qualquer um desses endereços IP virtuais (VIP) para se conectar ao StorageGRID.

Para obter instruções, consulte "[Configurar grupos de alta disponibilidade](#)".

Qual é a interface ativa?

Durante a operação normal, todos os endereços VIP do grupo HA são adicionados à interface Primária, que é a primeira interface na ordem de prioridade. Enquanto a interface Primária permanecer disponível, ela será usada quando os clientes se conectarem a qualquer endereço VIP do grupo. Ou seja, durante a operação normal, a interface Primária é a "ativa" para o grupo.

Da mesma forma, durante a operação normal, quaisquer interfaces de prioridade mais baixa para o grupo HA atuam como interfaces de "backup". Essas interfaces de backup não são usadas a menos que a interface Primária (atualmente ativa) fique indisponível.

Visualize o status atual do grupo HA de um nó

Para verificar se um nó está atribuído a um grupo HA e determinar seu status atual, selecione **Nós > nó**.

Se a aba **Visão geral** incluir uma entrada para **HA groups**, o nó será atribuído aos HA groups listados. O valor após o nome do grupo representa o status atual do nó no HA group:

- **Ativo:** O grupo HA está atualmente hospedado neste nó.
- **Backup:** O grupo HA não está usando este nó no momento; esta é uma interface de backup.
- **Parado:** 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 motivos:
 - O serviço Load Balancer (nginx-gw) não está em execução 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 de administração e uma interface de backup para o grupo de clientes

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:	Admin clients (Active) FabricPool clients (Backup)
IP addresses:	172.16.1.225 - eth0 (Grid Network) 10.224.1.225 - eth1 (Admin Network) 47.47.0.2, 47.47.1.225 - eth2 (Client Network) Show additional IP addresses ▼

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 transferidos para a primeira interface de backup disponível, seguindo a ordem de prioridade. Se essa interface falhar, os endereços VIP serão transferidos 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 fica inativo.
- O nó no qual a interface está configurada perde a conectividade com todos os outros nós por pelo menos 2 minutos.
- A interface ativa fica inativa.
- O serviço Load Balancer é interrompido.
- O serviço de Alta Disponibilidade é interrompido.



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 pelos serviços do Grid Manager ou do Tenant Manager.

O processo de failover geralmente leva apenas alguns segundos e é rápido o suficiente para que os aplicativos cliente sofram pouco impacto e possam contar com os comportamentos normais de repetição para continuar operando.

Quando a falha é resolvida e uma interface de prioridade mais alta volta a ficar disponível, os endereços VIP

são automaticamente movidos para a interface de maior prioridade que estiver disponível.

Como os grupos de alta disponibilidade do StorageGRID proporcionam alta disponibilidade

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 HA pode fornecer conexões administrativas altamente disponíveis ao Grid Manager ou ao Tenant Manager.
- Um grupo HA pode fornecer conexões de dados altamente disponíveis para clientes S3.
- Um grupo HA que contém apenas uma interface permite que você forneça vários endereços VIP e defina explicitamente endereços IPv6.

Um grupo de alta disponibilidade (HA) só pode fornecer alta disponibilidade se todos os nós incluídos no grupo fornecerem os mesmos serviços. Ao criar um grupo de HA, adicione interfaces dos tipos de nós que fornecem os serviços que você precisa.

- **Nós de administração:** Inclua o serviço Load Balancer e habilite o acesso ao Grid Manager ou ao Tenant Manager.
- **Nós de Gateway:** Incluem o serviço Load Balancer.

Objetivo do grupo HA	Adicione nós deste tipo ao grupo HA
Acesso ao Grid Manager	• Nó de administração principal (Primary) • Nós Admin não primários Nota: O nó de administração principal deve ser a interface principal. Alguns procedimentos de manutenção só podem ser realizados a partir do nó de administração principal.
Acesso somente ao Tenant Manager	• Nós de administração primários ou não primários
Acesso do cliente S3—serviço de balanceador de carga	• Nós de administração • Nós de gateway
Acesso do cliente S3 para "S3 Select"	• Appliances de serviços • Nós de software baseados em VMware Nota: Grupos de alta disponibilidade (HA) são recomendados ao usar o S3 Select, mas não são obrigatórios.

Limitações do uso de grupos de alta disponibilidade com o Grid Manager ou o 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 Grid Manager ou ao Tenant Manager quando ocorrer uma falha, você será desconectado e precisará entrar novamente para retomar sua tarefa.

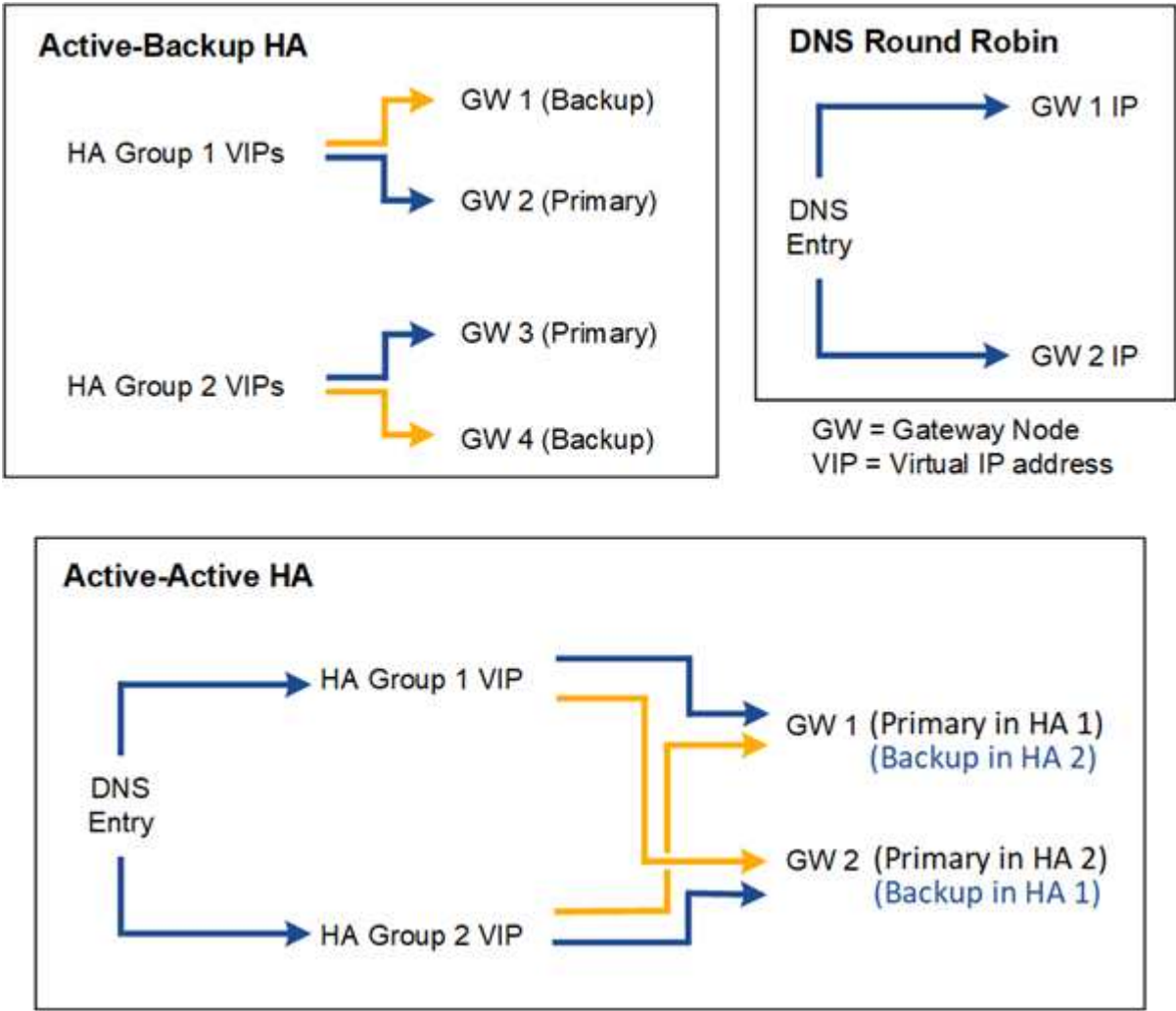
Alguns procedimentos de manutenção não podem ser executados quando o nó de administração primário

está indisponível. Durante o failover, você pode usar o Grid Manager para monitorar seu sistema StorageGRID.

Opções de configuração para grupos de alta disponibilidade do StorageGRID

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

Nos diagramas, azul indica a interface primária no grupo HA e amarelo indica a interface de backup no grupo HA.



A tabela resume os benefícios de cada configuração de alta disponibilidade (HA) mostrada no diagrama.

Configuração	Vantagens	Desvantagens
HA Active-Backup	- Gerenciado pelo StorageGRID sem dependências externas. - Failover rápido.	Apenas um nó em um grupo HA está ativo. Pelo menos um nó por grupo HA ficará ocioso.

Configuração	Vantagens	Desvantagens
DNS Round Robin	• Aumento da taxa de transferência agregada. • Não há hosts ociosos.	• Failover lento, que pode depender do comportamento do cliente. • Requer configuração de hardware fora do StorageGRID. • Necessita de uma verificação de integridade implementada pelo cliente.
HA ativo-ativo	• O tráfego é distribuído por vários grupos de HA. • Alto rendimento agregado que escala com o número de grupos HA. • Failover rápido.	• Mais complexo de configurar. • Requer configuração de hardware fora do StorageGRID. • Necessita de uma verificação de integridade implementada pelo cliente.

Configurar grupos de alta disponibilidade no StorageGRID

Você pode configurar grupos de alta disponibilidade (HA) para fornecer acesso altamente disponível aos serviços em Admin Nodes ou Gateway Nodes.



Um sistema StorageGRID pode ter no máximo 255 grupos de HA.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).
- Se você planeja usar uma interface VLAN em um grupo HA, você criou a interface VLAN. Consulte ["Configurar interfaces VLAN"](#).
- Se você planeja usar uma interface de acesso para um nó em um grupo de alta disponibilidade (HA), você criou a interface:
 - **Linux (antes de instalar o nó):** ["Criar arquivos de configuração de nó"](#)
 - **Linux (após instalar o nó):** ["Adicione interfaces de tronco ou de acesso a um nó"](#)
 - **VMware (após a instalação do nó):** ["Adicione interfaces de tronco ou de acesso a um nó"](#)



"Linux" refere-se a uma instalação do RHEL, Ubuntu ou Debian. Para obter uma lista das versões suportadas, consulte o ["NetApp Ferramenta de Matriz de Interoperabilidade \(IMT\)"](#).

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, você atribui um ou mais endereços VIP ao grupo.

Para que uma interface seja incluída em um grupo de alta disponibilidade (HA), ela deve ser de um nó de Gateway ou de um nó de Admin. Um grupo de HA só pode usar uma interface por nó; no entanto, outras interfaces para o mesmo nó podem ser usadas em outros grupos de HA.

Acesse o assistente

Passos

1. Selecione **Configuração > Rede > Grupos de alta disponibilidade**.
2. Selecione **Create**.

Insira os detalhes do grupo HA

Passos

1. Forneça um nome exclusivo para o grupo HA.
2. Opcionalmente, insira uma descrição para o grupo HA.
3. Selecione **Continue**.

Adicionar interfaces ao grupo HA

Passos

1. Selecione uma ou mais interfaces para adicionar a este grupo de HA.

Use os cabeçalhos das colunas 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.



Total interface count: 4

	Node 	Interface  	Site  	IPv4 subnet 	Node type  
☐	DC1-ADM1-104-96	eth0 	DC1	10.96.104.0/22	Primary Admin Node
☐	DC1-ADM1-104-96	eth2 	DC1	—	Primary Admin Node
☐	DC2-ADM1-104-103	eth0 	DC2	10.96.104.0/22	Admin Node
☐	DC2-ADM1-104-103	eth2 	DC2	—	Admin Node

0 interfaces selected

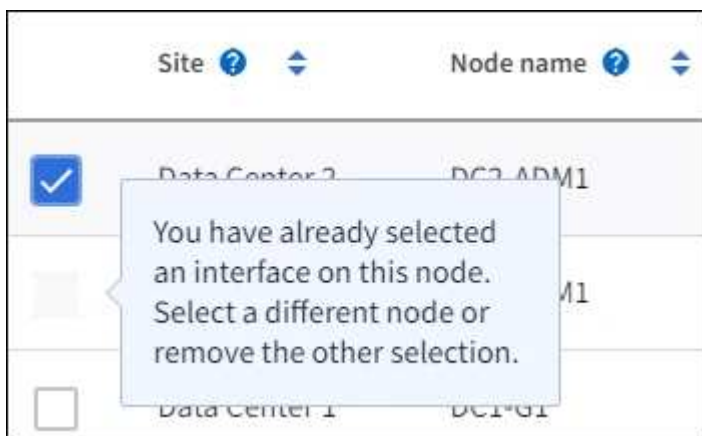


Após criar uma interface VLAN, aguarde até 5 minutos para que a nova interface apareça na tabela.

Diretrizes para seleção de interfaces

- Você deve selecionar pelo menos uma interface.
- Você pode selecionar apenas uma interface para um nó.
- Se o grupo HA for para proteção de alta disponibilidade dos serviços do Admin Node, que incluem o Grid Manager e o Tenant Manager, selecione apenas as interfaces nos Admin Nodes.

- Se o grupo HA for para proteção de alta disponibilidade do tráfego de clientes S3, selecione interfaces em nós de administração, nós de gateway ou em ambos.
- Se você selecionar interfaces em diferentes tipos de nós, uma nota informativa será exibida. Você é lembrado de que, se ocorrer um failover, os serviços fornecidos pelo nó anteriormente ativo podem não estar disponíveis no novo nó ativo. Por exemplo, um nó Gateway de backup não pode fornecer proteção HA dos serviços do nó Admin. Da mesma forma, um nó Admin de backup não pode executar todos os procedimentos de manutenção que o nó Admin primário pode fornecer.
- Se não for possível selecionar uma interface, a caixa de seleção correspondente estará desativada. A dica de ferramenta fornece mais informações.



- Não é possível selecionar uma interface se o valor da sub-rede ou o gateway entrar em conflito com outra interface selecionada.
- Você não pode selecionar uma interface configurada se ela não tiver um endereço IP estático.

2. Selecione **Continue**.

Determine a ordem de prioridade

Se o grupo HA incluir mais de uma interface, você pode determinar qual é a interface Primária e quais são as interfaces de Backup (failover). Se a interface Primária falhar, os endereços VIP são transferidos para a interface disponível de maior prioridade. Se essa interface falhar, os endereços VIP são transferidos para a próxima interface disponível de maior prioridade, e assim por diante.

Passos

1. Arraste as linhas na coluna **Ordem de prioridade** para determinar a interface primária e quaisquer interfaces de backup.

A primeira interface da lista é a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.

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 Grid Manager, você deve selecionar uma interface no Nó de Administração primário para ser a interface primária. Alguns procedimentos de manutenção só podem ser executados a partir do Nó de Administração primário.

2. Selecione **Continue**.

Insira endereços IP

Passos

1. No campo **Subnet CIDR**, especifique a sub-rede VIP na notação CIDR: um endereço IPv4 seguido por 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 servirá 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 administrativo ou locatário S3 acessar esses endereços VIP a partir de uma sub-rede diferente, insira o **endereço IP do gateway**. O endereço do gateway deve estar dentro da sub-rede VIP.

Usuários clientes e administradores usarão este gateway para acessar os endereços IP virtuais.

3. Insira pelo menos um e no máximo dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP e todos estarão ativos ao mesmo tempo na interface ativa.

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

4. Selecione **Criar grupo HA** e selecione **Concluir**.

O grupo HA foi criado e agora você pode usar os endereços IP virtuais configurados.

Próximos passos

Se você for usar este grupo HA para balanceamento de carga, crie um endpoint de balanceador de carga para determinar a porta e o protocolo de rede e para anexar quaisquer certificados necessários. Consulte ["Configurar pontos de extremidade do balanceador de carga"](#).

Editar 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, pode ser necessário editar um grupo de HA se você quiser remover o nó associado a uma interface selecionada em um procedimento de desativação de site ou nó.

Passos

1. Selecione **Configuração > Rede > Grupos de alta disponibilidade**.

A página Grupos de alta disponibilidade mostra todos os grupos de alta disponibilidade existentes.

2. Selecione a caixa de seleção do grupo HA que você deseja editar.
3. Faça uma das seguintes opções, dependendo do 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 para o grupo HA.
 - b. Selecione **Salvar**.
 - c. Selecione **Concluir**.
5. Se você selecionou **Editar grupo HA**:
 - 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 Grid Manager, você deve selecionar uma interface no Nó de Administração primário para ser a interface primária. Alguns procedimentos de manutenção só podem ser executados a partir do Nó de Administração primário.

- c. Opcionalmente, arraste as linhas para alterar a ordem de prioridade da interface primária e de quaisquer interfaces de backup para este grupo de alta disponibilidade.
- d. Opcionalmente, atualize os endereços IP virtuais.
- e. Selecione **Salvar** e depois selecione **Concluir**.

Remover um grupo de alta disponibilidade

Você pode remover um ou mais grupos de alta disponibilidade (HA) de uma só vez.



Não é possível remover um grupo de alta disponibilidade (HA) se ele estiver vinculado a um endpoint do balanceador de carga. Para excluir um grupo de HA, você deve removê-lo de qualquer endpoint do balanceador de carga que o utilize.

Para evitar interrupções nos clientes, atualize todos os aplicativos cliente S3 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 que foi configurado para uma interface durante a instalação.

Passos

1. Selecione **Configuração > Rede > Grupos de alta disponibilidade**.
2. Analise a coluna **Pontos de extremidade do balanceador de carga** para cada grupo de alta disponibilidade que você deseja remover. Se algum ponto de extremidade do balanceador de carga estiver listado:
 - a. Acesse **Configuração > Rede > Pontos de extremidade do balanceador de carga**.
 - b. Selecione a caixa de seleção do endpoint.

- c. Selecione **Actions > Edit endpoint binding mode**.
 - d. Atualize o modo de vinculação para remover o grupo HA.
 - e. Selecione **Save changes**.
3. Se nenhum ponto de extremidade do balanceador de carga estiver listado, selecione a caixa de seleção para cada grupo de HA que você deseja remover.
 4. Selecione **Ações > Remover grupo HA**.
 5. Analise a mensagem e selecione **Excluir grupo HA** para confirmar sua seleção.

Todos os grupos de alta disponibilidade que você selecionou foram removidos. Uma faixa verde de sucesso aparece na página de grupos de alta disponibilidade.

Gerenciar balanceamento de carga

Saiba mais sobre o balanceamento de carga do StorageGRID

Você pode usar o balanceamento de carga para lidar com as cargas de trabalho de ingestão e recuperação de clientes S3.

O que é balanceamento de carga?

Quando um aplicativo cliente salva ou recupera dados de um sistema StorageGRID, StorageGRID utiliza um balanceador de carga para gerenciar a carga de trabalho de ingestão e recuperação. O balanceamento de carga maximiza a velocidade e a capacidade de conexão ao distribuir a carga de trabalho entre vários Storage Nodes.

O serviço StorageGRID Load Balancer está instalado em todos os Nós de Administração e em todos os Nós de Gateway e fornece balanceamento de carga na Camada 7. Ele realiza a terminação TLS das solicitações dos clientes, inspeciona as solicitações e estabelece novas conexões seguras com os Nós de Armazenamento.

O serviço de balanceamento de carga em cada nó opera de forma independente ao encaminhar o tráfego do cliente para os nós de armazenamento. Por meio de um processo de ponderação, o serviço de balanceamento de carga direciona mais solicitações para os nós de armazenamento com maior disponibilidade de CPU.



Embora o serviço StorageGRID Load Balancer seja o mecanismo de balanceamento de carga recomendado, você pode optar por integrar um balanceador de carga de terceiro. Para obter informações, entre em contato com seu representante de contas da NetApp ou consulte "[Use balanceadores de carga de terceiros com StorageGRID](#)".

Quantos nós de balanceamento de carga você precisa?

Como prática recomendada geral, cada site em seu StorageGRID deve incluir dois ou mais nós com o serviço Load Balancer. Por exemplo, um site pode incluir dois Gateway Nodes ou tanto um Admin Node quanto um Gateway Node. Certifique-se de que haja infraestrutura de rede, hardware ou virtualização adequada para cada nó de balanceamento de carga, independentemente de você estar usando appliances de serviços, nós bare metal ou nós baseados em máquina virtual (VM).

O que é um endpoint de balanceador de carga?

Um endpoint de balanceador de carga define a porta e o protocolo de rede (HTTPS ou HTTP) que as solicitações de aplicativos cliente de entrada e saída usarão para acessar os nós que contêm o serviço de Load Balancer. O endpoint também define o tipo de cliente (S3), o modo de vinculação e, opcionalmente, uma lista de tenants permitidos ou bloqueados.

Para criar um endpoint de balanceador de carga, use o Grid Manager ou conclua os assistentes de configuração do S3 e FabricPool:

- ["Configurar pontos de extremidade do balanceador de carga"](#)
- ["Use o assistente de instalação S3"](#)
- ["Utilize o assistente de instalação do FabricPool"](#)

Considerações sobre armazenamento em cache do balanceador de carga

O armazenamento em cache melhora significativamente o desempenho quando uma carga de trabalho opera em um subconjunto de dados e acessa objetos várias vezes. Além disso, o armazenamento em cache fornece acesso remoto ao storage de objetos sem a necessidade de uma implantação completa de grid. O armazenamento em cache do balanceador de carga está disponível apenas para Gateway Nodes.

Ao criar endpoints de balanceamento de carga:

- Habilite armazenamento em cache apenas para cargas de trabalho que são armazenáveis em cache. Cargas de trabalho que acessam dados não armazenados em cache com mais frequência do que dados em cache terão desempenho pior do que se não tivessem sido atendidas pelo cache. Em alguns casos, cargas de trabalho com altas taxas de sobrescrita e remoção também podem exceder a resistência à gravação garantida da unidade.
- Considere adicionar endpoints ou nós adicionais para armazenamento em cache de cargas de trabalho individuais que sejam boas candidatas ao armazenamento em cache.
- Utilize endpoints distintos para cargas de trabalho armazenáveis em cache e não armazenáveis em cache. Essa separação garante que os mecanismos de armazenamento em cache sejam aplicados adequadamente e não interfiram no processamento de dados não armazenáveis em cache.
- Avalie uma carga de trabalho potencialmente armazenável em cache direcionando-a para o endpoint habilitado para cache. Monitore e verifique a taxa de acerto do cache para determinar a adequação da carga de trabalho ao armazenamento em cache. Essa avaliação ajuda a otimizar o desempenho e a garantir o uso eficiente dos recursos de cache.
- ["Analisar registros de auditoria"](#) para determinar se uma carga de trabalho existente seria uma boa candidata para armazenamento em cache. Para um determinado período, determine qual porcentagem de GETs é para objetos únicos. Para ser adequada para armazenamento em cache, esse valor deve ser inferior a 50%.

Exemplos de cargas de trabalho que podem ser boas candidatas ao armazenamento em cache

- Lagos de dados
- Computação de alto desempenho (HPC)
- Treinamento de IA/ML
- Rede de entrega de conteúdo (CDN)
- Gerenciamento de ativos de mídia

- Produção de vídeo



- É possível armazenar em cache várias versões de um objeto.
- Operações de leitura de intervalo são suportadas.

Exemplos de cargas de trabalho que não são boas candidatas para armazenamento em cache

- FabricPool
- Aplicativos de backup
- Tierização de storage



Se algum conteúdo a ser servido pelo cache exigir criptografia em repouso, ["Ativar criptografia de nó ou unidade"](#) no nó de cache.

Tipos de objetos e solicitações que não serão armazenados em cache

- O `response-content-encoding` parâmetro de consulta
- O `partNumber` parâmetro de consulta
- Cabeçalhos condicionais
 - `If-Match`
 - `If-Modified-Since`
 - `If-None-Match`
 - `If-Unmodified-Since`
- Solicitações que foram criptografadas em repouso com qualquer um dos seguintes:
 - SSE (criptografia do lado do servidor com chaves gerenciadas pelo StorageGRID)
 - SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente)
 - Criptografia de objeto armazenado

Qualquer solicitação que não esteja armazenada em cache é encaminhada para um LDR upstream como se o armazenamento em cache não estivesse ativado.

Informações relacionadas

- ["Solucione problemas de armazenamento em cache do balanceador de carga"](#)
- Para obter mais informações sobre armazenamento em cache do balanceador de carga, entre em contato com o suporte técnico.

Considerações para a porta

A porta para um endpoint de balanceador de carga é definida como 10433 por padrão para o primeiro endpoint que você criar, mas você pode especificar qualquer porta externa não utilizada entre 1 e 65535. Se você usar a porta 80 ou 443, o endpoint usará o serviço de Load Balancer apenas nos Gateway Nodes. Essas portas são reservadas nos Admin Nodes. Se você usar a mesma porta para mais de um endpoint, você deve especificar um modo de vinculação diferente para cada endpoint.

Portas utilizadas por outros serviços da rede não são permitidas. Consulte ["Portas internas do StorageGRID"](#).

Considerações sobre o protocolo de rede

Na maioria dos casos, as conexões entre os aplicativos cliente e o StorageGRID devem usar criptografia TLS (Transport Layer Security). Conectar-se ao StorageGRID sem criptografia TLS é suportado, mas não é recomendado, especialmente em ambientes de produção. Ao selecionar o protocolo de rede para o endpoint do balanceador de carga do StorageGRID, você deve selecionar **HTTPS**.

Considerações sobre certificados de endpoint de balanceador de carga

Se você selecionar **HTTPS** como protocolo de rede para o ponto de extremidade do balanceador de carga, deverá fornecer um certificado de segurança. Você pode usar qualquer uma destas três opções ao criar o ponto de extremidade do balanceador de carga:

- **Faça o upload de um certificado assinado (recomendado).** Este certificado pode ser assinado por uma autoridade certificadora (AC) pública ou privada. Usar um certificado de servidor de uma AC pública para proteger a conexão é a melhor prática. Ao contrário dos certificados gerados, os certificados assinados por uma AC podem ser rotacionados sem interrupção, o que pode ajudar a evitar problemas de expiração.

Você precisa obter os seguintes arquivos antes de criar o endpoint do balanceador de carga:

- O arquivo de certificado de servidor personalizado.
- O arquivo de chave privada do certificado de servidor personalizado.
- Opcionalmente, um pacote de certificados das autoridades certificadoras intermediárias.
- **Gerar um certificado autoassinado.**
- **Use o certificado global do StorageGRID S3.** Você precisa carregar ou gerar uma versão personalizada deste certificado antes de poder selecioná-lo para o endpoint do balanceador de carga. Consulte ["Configurar certificados da API S3"](#).

Quais valores você precisa?

Para criar o certificado, você precisa saber todos os nomes de domínio e endereços IP que os aplicativos cliente do S3 usarão para acessar o endpoint.

A entrada **DN do Assunto** (Nome Distinto) para o certificado deve incluir o nome de domínio totalmente qualificado que o aplicativo cliente usará para StorageGRID. Por exemplo:

```
Subject DN:  
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

Conforme necessário, o certificado pode usar curingas para representar os nomes de domínio totalmente qualificados de todos os Nós de Administração e Nós de Gateway que executam o serviço de Balanceador de Carga. Por exemplo, `*.storagegrid.example.com` usa o curinga `*` para representar `adm1.storagegrid.example.com` e `gn1.storagegrid.example.com`.

Se você planeja usar solicitações no estilo de hospedagem virtual do S3, o certificado também deve incluir uma entrada de **Nome Alternativo** para cada ["Nome de domínio do endpoint S3"](#) que você configurou, incluindo quaisquer nomes curinga. Por exemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```




Se você usa curingas para nomes de domínio, revise o ["Diretrizes de reforço para certificados de servidor"](#).

Você também deve definir uma entrada DNS para cada nome no certificado de segurança.

Como faço para gerenciar certificados que estão expirando?



Se o certificado usado para proteger a conexão entre o aplicativo S3 e StorageGRID expirar, o aplicativo poderá perder temporariamente o acesso ao StorageGRID.

Para evitar problemas com a expiração do certificado, siga estas boas práticas:

- Monitore atentamente quaisquer alertas que avisem sobre a proximidade da expiração de certificados, como os alertas **Expiração do certificado do endpoint do balanceador de carga** e **Expiração do certificado global do servidor para S3 API**.
- Mantenha sempre as versões do certificado do StorageGRID e do aplicativo S3 sincronizadas. Se você substituir ou renovar o certificado usado para um endpoint do balanceador de carga, deverá substituir ou renovar o certificado equivalente usado pelo aplicativo S3.
- Use um certificado de uma Autoridade Certificadora (CA) com assinatura pública. Se você usar um certificado assinado por uma CA, você pode substituir certificados prestes a expirar sem interrupções.
- Se você gerou um certificado StorageGRID autoassinado e esse certificado está prestes a expirar, você deve substituí-lo manualmente tanto no StorageGRID quanto no aplicativo S3 antes que o certificado existente expire.

Considerações sobre o modo de binding

O modo de vinculação permite que você controle quais endereços IP podem ser usados para acessar um endpoint do balanceador de carga. Se um endpoint usa o modo de vinculação, os aplicativos cliente só podem acessá-lo se usarem um endereço IP permitido ou seu respectivo domínio totalmente qualificado (FQDN). Aplicativos cliente que usam qualquer outro endereço IP ou FQDN não podem acessar o endpoint.

Você pode especificar qualquer um dos seguintes modos de vinculação:

- **Global (padrão):** Os aplicativos cliente podem acessar o endpoint usando o endereço IP de qualquer Gateway Node ou Admin Node, o endereço VIP de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use esta configuração a menos que você precise restringir a acessibilidade de um endpoint.
- **IPs virtuais de grupos HA.** Os aplicativos cliente devem usar um endereço IP virtual (ou domínio totalmente qualificado correspondente) de um grupo HA.
- **Interfaces de nó.** Os clientes devem usar os endereços IP (ou os FQDNs correspondentes) das interfaces de nó selecionadas.
- **Tipo de nó.** Dependendo do tipo de nó selecionado, os clientes devem usar o endereço IP (ou o FQDN correspondente) de qualquer Nó de Administração ou o endereço IP (ou o FQDN correspondente) de qualquer Nó de Gateway.

Considerações para o acesso do tenant

O acesso de locatários é um recurso de segurança opcional que permite controlar quais contas de locatário do StorageGRID podem usar um endpoint do balanceador de carga para acessar seus buckets. Você pode permitir que todos os locatários acessem um endpoint (padrão) ou especificar uma lista de locatários permitidos ou bloqueados para cada endpoint.

Você pode usar esse recurso para proporcionar um melhor isolamento de segurança entre os locatários e seus endpoints. Por exemplo, você pode usar esse recurso para garantir que materiais ultrassecretos ou altamente confidenciais pertencentes a um locatário permaneçam completamente inacessíveis a outros locatários.



Para fins de controle de acesso, o locatário é determinado pelas chaves de acesso usadas na solicitação do cliente. Se nenhuma chave de acesso for fornecida como parte da solicitação (como no acesso anônimo), o proprietário do bucket é usado para determinar o locatário.

Exemplo de acesso do tenant

Para entender como esse recurso de segurança funciona, considere o seguinte exemplo:

1. Você criou dois pontos de extremidade de balanceamento de carga, conforme descrito a seguir:
 - Endpoint **público**: utiliza a porta 10443 e permite acesso a todos os locatários.
 - Endpoint **ultrassegredo**: utiliza a porta 10444 e permite acesso somente ao tenant **ultrassegredo**. Todos os outros tenants estão bloqueados de acessar este endpoint.
2. O `top-secret.pdf` está em um bucket pertencente ao tenant **Top secret**.

Para acessar o `top-secret.pdf`, um usuário do tenant **Top secret** pode enviar uma requisição GET para `https://w.x.y.z:10444/top-secret.pdf`. Como esse tenant tem permissão para usar o endpoint 10444, o usuário pode acessar o objeto. No entanto, se um usuário de qualquer outro tenant enviar a mesma requisição para a mesma URL, receberá imediatamente uma mensagem de acesso negado. O acesso é negado mesmo que as credenciais e a assinatura sejam válidas.

Disponibilidade da CPU

O serviço Load Balancer em cada Admin Node e Gateway Node opera de forma independente ao encaminhar o tráfego S3 para os Storage Nodes. Por meio de um processo de ponderação, o serviço Load Balancer direciona mais solicitações para Storage Nodes 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 Storage Nodes recebem um valor de peso base mínimo, mesmo que um nó relate 100% de utilização ou não reporte sua utilização.

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

Configurar os endpoints do balanceador de carga do StorageGRID

Os endpoints do balanceador de carga determinam as portas e os protocolos de rede que os clientes S3 podem usar ao se conectar ao balanceador de carga do StorageGRID nos nós de Gateway e de Administração. Você também pode usar endpoints para acessar o Grid Manager, o Tenant Manager ou ambos.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).
- Você revisou o ["Considerações sobre balanceamento de carga"](#).
- Se você já remapeou uma porta que pretende usar para o endpoint do balanceador de carga, você tem ["removeu o remapeamento de porta"](#).

- Você criou todos os grupos de alta disponibilidade (HA) que planeja usar. Os grupos de HA são recomendados, mas não obrigatórios. Consulte ["Gerenciar grupos de alta disponibilidade"](#).
- Se o endpoint do balanceador de carga for usado por ["Locatários S3 para S3 Select"](#), ele não deve usar os endereços IP ou FQDNs de nenhum nó bare-metal. Somente appliances de serviços e nós de software baseados em VMware são permitidos para os endpoints do balanceador de carga usados para S3 Select.
- Você configurou todas as interfaces VLAN que pretende usar. Consulte ["Configurar interfaces VLAN"](#).
- Se você estiver criando um endpoint HTTPS (recomendado), você tem as informações do certificado do servidor.



As alterações em 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 CA bundle.
- Para gerar um certificado, você precisa de todos os nomes de domínio e endereços IP que os clientes S3 usarão para acessar o endpoint. Você também precisa saber o assunto (Distinguished Name).
- Se você deseja usar o certificado da API S3 do StorageGRID (que também pode ser usado para conexões diretas com os Storage Nodes), você já substituiu o certificado padrão por um certificado personalizado assinado por uma autoridade de certificação externa. Consulte ["Configurar certificados da API S3"](#).

Crie um endpoint de balanceador de carga

Cada endpoint do balanceador de carga do cliente S3 especifica uma porta, um tipo de cliente (S3) e um protocolo de rede (HTTP ou HTTPS). Os endpoints do balanceador de carga da interface de gerenciamento especificam uma porta, um tipo de interface e uma Client Network não confiável.

Acesse o assistente

Passos

1. Selecione **Configuração > Rede > Pontos de extremidade do balanceador de carga**.
2. Para criar um endpoint para um cliente S3, selecione a guia **Cliente S3**.
3. Para criar um ponto de extremidade para acesso ao Grid Manager, Tenant Manager ou a ambos, selecione a guia **Interface de gerenciamento**.
4. Selecione **Create**.

Insira os detalhes do endpoint

Passos

1. Selecione as instruções apropriadas para inserir os detalhes do tipo de endpoint que você deseja criar.

Cliente S3

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página de endpoints do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo tem como valor padrão 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada de 1 a 65535. Se você inserir 80 ou 8443, o endpoint será configurado apenas nos nós de gateway, a menos que você tenha liberado a porta 8443. Em seguida, você pode usar a porta 8443 como um endpoint S3, e a porta será configurada tanto nos nós de gateway quanto nos nós de administração.
Tipo de cliente	Deve ser S3 .
Protocolo de rede	O protocolo de rede que os clientes usarão ao se conectar a este endpoint. • Selecione HTTPS para comunicação segura e criptografada por TLS (recomendado). Você precisa anexar um certificado de segurança antes de salvar o endpoint. • Selecione HTTP para comunicação menos segura e não criptografada. Use HTTP somente para uma grid que não seja de produção.
Ativar armazenamento em cache	Ativar ou desativar "armazenamento em cache nos nós de gateway" para este endpoint do balanceador de carga. Se ocorrerem problemas com armazenamento em cache, consulte "Solucione problemas de armazenamento em cache do balanceador de carga".

Interface de gerenciamento

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página de endpoints do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para acessar o Grid Manager, o Tenant Manager ou ambos. • Grid Manager: 8443 • Tenant Manager: 9443 • Tanto o Grid Manager quanto o Tenant Manager: 443 Nota: Você pode usar essas portas predefinidas ou outras portas disponíveis.

Campo	Descrição
Tipo de interface	Selecione o botão de opção para a interface StorageGRID que você acessará usando este endpoint.
Rede de cliente não confiável	Selecione Sim se este endpoint deve ser acessível a redes de clientes não confiáveis. Caso contrário, selecione Não. Ao selecionar Sim, a porta fica aberta em todas as redes de clientes não confiáveis. Nota: Você só pode configurar uma porta para ser aberta ou fechada para redes de clientes não confiáveis ao criar o endpoint do balanceador de carga.

1. Selecione **Continue**.

Selecione um modo de vinculação

Passos

1. Selecione um modo de vinculação para o endpoint para controlar como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

Alguns modos de vinculação estão disponíveis tanto para endpoints de cliente quanto para endpoints de interface de gerenciamento. Todos os modos para ambos os tipos de endpoint estão listados aqui.

Modo	Descrição
Global (padrão para endpoints de cliente)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer Gateway Node ou Admin Node, o endereço IP virtual (VIP) de qualquer grupo HA em qualquer rede ou um FQDN correspondente. Use a configuração Global, a menos que precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este endpoint. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA que você selecionar para os endpoints não se sobreponham.
Interfaces de nó	Os clientes devem usar os endereços IP (ou os FQDNs correspondentes) das interfaces de nó selecionadas para acessar este endpoint.
Tipo de nó (somente endpoints de cliente)	Dependendo do tipo de nó que você selecionar, os clientes devem usar o endereço IP (ou o FQDN correspondente) de qualquer Nó de Administração ou o endereço IP (ou o FQDN correspondente) de qualquer Nó de Gateway para acessar este endpoint.

Modo	Descrição
Todos os nós de administração (padrão para endpoints da interface de gerenciamento)	Os clientes devem usar o endereço IP (ou o FQDN correspondente) de qualquer nó administrativo para acessar este endpoint.

Se mais de um ponto de extremidade usar a mesma porta, StorageGRID usa esta ordem de prioridade para decidir qual ponto de extremidade usar: **IPs virtuais de grupos HA** > **Interfaces de nó** > **Tipo de nó** > **Global**.

Se você estiver criando endpoints de interface de gerenciamento, somente Admin Nodes são permitidos.

2. Se você selecionou **IPs virtuais de grupos HA**, selecione um ou mais grupos HA.

Se você estiver criando endpoints de interface de gerenciamento, selecione apenas os VIPs associados aos Admin Nodes.

3. Se você selecionou **Interfaces de nó**, selecione uma ou mais interfaces de nó para cada Nó de Administração ou Nó de Gateway que você deseja associar a este endpoint.
4. Se você selecionou **Tipo de nó**, selecione Nós de administração, que inclui tanto o nó de administração principal quanto quaisquer nós de administração não primários, ou Nós de gateway.

Controlar o acesso do tenant



Um endpoint de interface de gerenciamento só pode controlar o acesso do locatário quando o endpoint tiver a [tipo de interface do Tenant Manager](#).

Passos

1. Na etapa **Acesso do locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de locatário podem usar este endpoint para acessar seus buckets. Você deve selecionar esta opção se ainda não tiver criado nenhuma conta de locatário. Depois de adicionar contas de locatário, você pode editar o endpoint do balanceador de carga para permitir ou bloquear contas específicas.
Permitir locatários selecionados	Somente as contas de locatário selecionadas podem usar este endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar este endpoint para acessar seus buckets. Todos os outros locatários podem usar este endpoint.

2. Se você estiver criando um endpoint **HTTP**, não precisa anexar um certificado. Selecione **Criar** para adicionar o novo endpoint do balanceador de carga. Em seguida, acesse [Depois que você terminar](#). Caso

contrário, selecione **Continuar** para anexar o certificado.

Anexar certificado

Passos

1. Se você estiver criando um endpoint **HTTPS**, selecione o tipo de certificado de segurança que deseja associar ao endpoint.

O certificado protege as conexões entre os clientes S3 e o serviço Load Balancer no Admin Node ou nos Gateway Nodes.

- **Carregar certificado.** Selecione esta opção se você tiver certificados personalizados para carregar.
- **Gerar certificado.** Selecione esta opção se você tiver os valores necessários para gerar um certificado personalizado.
- **Usar certificado StorageGRID S3.** Selecione esta opção se você quiser usar o certificado global da API S3, que também pode ser usado para conexões diretas com os Storage Nodes.

Você não pode selecionar esta opção a menos que tenha substituído o certificado padrão da API S3, que é assinado pela CA do grid, por um certificado personalizado assinado por uma autoridade de certificação externa. Consulte "[Configurar certificados da API S3](#)".

- **Usar certificado da interface de gerenciamento.** Selecione esta opção se você quiser usar o certificado global da interface de gerenciamento, que também pode ser usado para conexões diretas com os Admin Nodes.
2. Se você não estiver usando o certificado StorageGRID S3, faça o upload ou gere o certificado.

Carregar certificado

a. Selecione **Carregar certificado**.

b. Faça o upload dos arquivos de certificado de servidor necessários:

- **Certificado do servidor:** o arquivo de certificado personalizado do servidor em codificação PEM.
- **Chave privada do certificado:** O arquivo de chave privada do certificado personalizado do servidor (.key).



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

- **Pacote de CA:** Um único arquivo opcional contendo os certificados de cada autoridade certificadora (CA) intermediária. O arquivo deve conter cada um dos arquivos de certificado da CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Expanda **Detalhes do certificado** para ver os metadados de cada certificado que você carregou. Se você carregou um pacote de CA opcional, cada certificado é 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 certificados.

Especifique o nome do arquivo do 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 CA PEM** para copiar o conteúdo do certificado para colar em outro lugar.

d. Selecione **Criar**. + O endpoint do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre os clientes S3 ou a interface de gerenciamento e o endpoint.

Gerar certificado

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados para incluir no certificado. Use um * como caractere curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP para incluir no certificado.
Assunto (opcional)	Nome diferenciado (DN) ou subject X.509 do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usa o primeiro nome de domínio ou endereço IP como nome comum do sujeito (CN).

Campo	Descrição
Dias válidos	Número de dias após a criação em que o certificado expira.
Adicionar extensões de uso de chave	Se selecionado (padrão e recomendado), as extensões de uso de chave e uso de chave estendido são adicionadas ao certificado gerado. Essas extensões definem a finalidade da chave contida no certificado. Nota: Deixe esta caixa de seleção marcada, a menos que você tenha problemas de conexão com clientes mais antigos quando os certificados incluem essas extensões.

c. Selecione **Gerar**.

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

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

Por exemplo: `storagegrid_certificate.pem`

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

e. Selecione **Create**.

O endpoint do balanceador de carga foi criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre os clientes S3 ou a interface de gerenciamento e esse endpoint.

Depois que você terminar

Passos

1. Se você utiliza um DNS, certifique-se de que o DNS inclua um registro para associar o domínio totalmente qualificado (FQDN) do StorageGRID a cada endereço IP que os clientes usarão para se conectar.

O endereço IP que você insere no registro DNS depende de você estar usando um grupo HA de nós de balanceamento de carga:

- Se você configurou um grupo HA, os clientes se conectarão aos endereços IP virtuais desse grupo HA.
- Se você não estiver usando um grupo de alta disponibilidade (HA), os clientes se conectarão ao serviço StorageGRID Load Balancer usando o endereço IP de um Gateway Node ou Admin Node.

Você também deve garantir que o registro DNS faça referência a todos os nomes de domínio de endpoint necessários, incluindo quaisquer nomes curinga.

2. Forneça aos clientes S3 as informações necessárias para se conectar ao endpoint:

- Número da porta
- Domínio totalmente qualificado ou endereço IP
- Quaisquer detalhes de certificado necessários

Visualizar e editar endpoints do balanceador de carga

Você pode visualizar detalhes dos endpoints de balanceamento de carga existentes, incluindo os metadados do certificado para um endpoint seguro. Você pode alterar determinadas configurações de um endpoint.

- Para visualizar informações básicas sobre todos os pontos de extremidade do balanceador de carga, consulte as tabelas na página Pontos de extremidade do balanceador de carga.
- Para visualizar todos os detalhes sobre um endpoint específico, incluindo metadados do certificado, selecione o nome do endpoint na tabela. As informações exibidas variam dependendo do tipo de endpoint e de como ele está configurado.

S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb

Remove

Binding mode

Certificate

Tenant access (2 allowed)

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 de endpoints do load balancer.



Se você perder o acesso ao Grid Manager enquanto estiver editando a porta de um endpoint da interface de gerenciamento, atualize a URL e a porta para recuperar o acesso.



Após editar um endpoint, pode ser necessário aguardar até 15 minutos para que suas alterações sejam aplicadas a todos os nós.

Tarefa	Menu de ações	Página de detalhes
Editar nome do endpoint	a. Selecione a caixa de seleção do endpoint. b. Selecione Ações > Editar nome do endpoint. c. Digite o novo nome. d. Selecione Salvar.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione o ícone de edição . c. Digite o novo nome. d. Selecione Salvar.
Editar porta do endpoint	a. Selecione a caixa de seleção do endpoint. b. Selecione Ações > Editar porta do endpoint. c. Insira um número de porta válido. d. Selecione Salvar.	n/a
Editar modo de vinculação de endpoint	a. Selecione a caixa de seleção do endpoint. b. Selecione Actions > Edit endpoint binding mode. c. Atualize o modo de vinculação conforme necessário. d. Selecione Save changes.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione Editar modo de vinculação. c. Atualize o modo de vinculação conforme necessário. d. Selecione Save changes.
Editar certificado de endpoint	a. Selecione a caixa de seleção do endpoint. b. Selecione Ações > Editar certificado do endpoint. c. Faça o upload ou gere um novo certificado personalizado ou comece a usar o certificado global S3, conforme necessário. d. Selecione Save changes.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia Certificate. c. Selecione Editar certificado. d. Faça o upload ou gere um novo certificado personalizado ou comece a usar o certificado global S3, conforme necessário. e. Selecione Save changes.
Editar acesso do locatário	a. Selecione a caixa de seleção do endpoint. b. Selecione Ações > Editar acesso do tenant. c. Escolha uma opção de acesso diferente, selecione ou remova inquilinos da lista ou faça ambos. d. Selecione Save changes.	a. Selecione o nome do endpoint para exibir os detalhes. b. Selecione a guia Acesso do locatário. c. Selecione Editar acesso do tenant. d. Escolha uma opção de acesso diferente, selecione ou remova inquilinos da lista ou faça ambos. e. Selecione Save changes.

Remover endpoints do balanceador de carga

Você pode remover um ou mais endpoints usando o menu **Ações** ou pode remover um único endpoint na página de detalhes.



Para evitar interrupções nos clientes, atualize todos os aplicativos cliente S3 afetados antes de remover um endpoint do balanceador de carga. Atualize cada cliente para se conectar usando uma porta atribuída a outro endpoint do balanceador de carga. Certifique-se também de atualizar todas as informações de certificado necessárias.



Se você perder o acesso ao Grid Manager ao remover um endpoint da interface de gerenciamento, atualize a URL.

- Para remover um ou mais endpoints:
 - a. Na página do balanceador de carga, selecione a caixa de seleção para cada endpoint que você deseja remover.
 - b. Selecione **Ações > Remover**.
 - c. Selecione **OK**.
- Para remover um endpoint da página de detalhes:
 - a. Na página do balanceador de carga, selecione o nome do endpoint.
 - b. Selecione **Remover** na página de detalhes.
 - c. Selecione **OK**.

Configurar os nomes de domínio dos endpoints do S3 no StorageGRID

Para dar suporte a solicitações no estilo de hospedagem virtual do S3, você deve usar o Grid Manager para configurar a lista de nomes de domínio de endpoint do S3 aos quais os clientes S3 se conectam.



O uso de um endereço IP como nome de domínio de endpoint não é suportado. Versões futuras impedirão essa configuração.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Você confirmou que uma atualização do grid não está em andamento.



Não faça nenhuma alteração na configuração do nome de domínio enquanto uma atualização da grid estiver em andamento.

Sobre esta tarefa

Para permitir que os clientes usem nomes de domínio de endpoints do S3, você deve fazer todas as seguintes ações:

- Utilize o Grid Manager para adicionar os nomes de domínio dos endpoints S3 ao sistema StorageGRID.
- Certifique-se de que o ["certificado que o cliente usa para conexões HTTPS com o StorageGRID"](#) esteja

assinado para todos os nomes de domínio que o cliente necessita.

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 wildcard Subject Alternative Name (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 se conectar e certifique-se de que os registros façam referência a todos os nomes de domínio de endpoint S3 necessários, incluindo quaisquer nomes curinga.



Os clientes podem se conectar ao StorageGRID usando o endereço IP de um Gateway Node, um Admin Node ou um Storage Node, ou conectando-se ao endereço IP virtual de um grupo de alta disponibilidade. Você deve entender como os aplicativos cliente se conectam à grid para incluir os endereços IP corretos nos registros DNS.

Os clientes que utilizam conexões HTTPS (recomendado) com a grid podem usar qualquer um destes certificados:

- Os clientes que se conectam a um endpoint do balanceador de carga podem usar um certificado personalizado para esse endpoint. Cada endpoint do balanceador de carga pode ser configurado para reconhecer diferentes nomes de domínio de endpoint S3.
- Os clientes que se conectam a um endpoint de balanceador de carga ou diretamente a um Storage Node podem personalizar o certificado global da API S3 para incluir todos os nomes de domínio de endpoint S3 necessários.



Se você não adicionar nomes de domínio de endpoint S3 e a lista estiver vazia, o suporte para solicitações no estilo virtual-hosted do S3 será desativado.

Adicionar um nome de domínio de endpoint S3

Passos

1. Selecione **Configuração > Rede > Nomes de domínio de endpoint S3**.
2. Insira o nome de domínio no campo **Nome de domínio 1**. Selecione **Adicionar outro nome de domínio** para adicionar mais nomes de domínio.
3. Selecione **Salvar**.
4. Certifique-se de que os certificados de servidor que os clientes usam correspondam aos nomes de domínio dos endpoints S3 necessários.
 - Se os clientes se conectarem a um endpoint de balanceador de carga que usa seu próprio certificado, "[Atualize o certificado associado ao endpoint](#)".
 - Se os clientes se conectarem a um endpoint de balanceador de carga que usa o certificado da API global do S3 ou diretamente aos nós de armazenamento, "[Atualize o certificado global da API S3](#)".
5. Adicione os registros DNS necessários para garantir que as solicitações de nome de domínio dos endpoints 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 conforme o esperado.

Renomear um nome de domínio de endpoint S3

Se você alterar um nome usado por aplicativos S3, as solicitações no estilo virtual-hosted falharão.

Passos

1. Selecione **Configuração > Rede > Nomes de domínio de endpoint S3**.
2. Selecione o campo do nome de domínio que você deseja editar e faça as alterações necessárias.
3. Selecione **Salvar**.
4. Selecione **Sim** para confirmar sua alteração.

Excluir um nome de domínio de endpoint S3

Se você remover um nome usado por aplicativos S3, as solicitações no estilo virtual-hosted falharão.

Passos

1. Selecione **Configuração > Rede > Nomes de domínio de endpoint S3**.
2. Selecione o ícone de exclusão  ao lado do nome de domínio.
3. Selecione **Sim** para confirmar a exclusão.

Informações relacionadas

- ["Utilize a API REST S3"](#)
- ["Ver endereços IP"](#)
- ["Configurar grupos de alta disponibilidade"](#)

Endereços IP e portas para conexões de clientes StorageGRID

Para armazenar ou recuperar objetos, os aplicativos cliente do S3 se conectam ao serviço Load Balancer, que está incluído em todos os Admin Nodes e Gateway Nodes, ou ao serviço Local Distribution Router (LDR), que está incluído em todos os Storage Nodes.

Os aplicativos cliente podem se conectar ao StorageGRID usando o endereço IP de um nó da grade e o número da porta do serviço nesse nó. Opcionalmente, você pode criar grupos de alta disponibilidade (HA) de nós de balanceamento de carga para fornecer conexões altamente disponíveis que usam endereços IP virtuais (VIP). Se você quiser se conectar ao StorageGRID usando um domínio totalmente qualificado (FQDN) em vez de um endereço IP ou VIP, você pode configurar entradas de DNS.

Esta tabela resume as diferentes maneiras pelas quais os clientes podem se conectar ao StorageGRID e os endereços IP e portas usados para cada tipo de conexão. Se você já criou endpoints de balanceamento de carga e grupos de alta disponibilidade (HA), consulte [Onde encontrar endereços IP](#) para localizar esses valores no Gerenciador de Grid.

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	Porta atribuída ao endpoint do balanceador de carga

Onde a conexão é feita	Serviço ao qual o cliente se conecta	Endereço IP	Porta
Nó de administração	Balanceador de carga	Endereço IP do nó de administração	Porta atribuída ao endpoint do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	Porta atribuída ao endpoint do balanceador de carga
Nó de armazenamento	LDR	Endereço IP do Storage Node	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084

URLs de exemplo

Para conectar um aplicativo cliente ao endpoint do balanceador de carga de um grupo HA de nós de gateway, use uma URL estruturada conforme 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 do endpoint do balanceador de carga for 10443, um aplicativo pode usar a seguinte URL para se conectar ao StorageGRID:

`https://192.0.2.5:10443`

Onde encontrar endereços IP

1. Faça login no Gerenciador de Grade usando um ["navegador web compatível"](#).
2. Para encontrar o endereço IP de um nó da grid:
 - a. Selecione **Nós**.
 - b. Selecione o nó de administração, o nó de gateway ou o nó de armazenamento ao qual você deseja se conectar.
 - c. Selecione a guia **Visão geral**.
 - d. Na seção Informações do Nó, anote os endereços IP do nó.
 - e. Selecione **Mostrar mais** para visualizar os endereços IPv6 e os mapeamentos de interface.

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

- **eth0**: Rede Grid
- **eth1**: Rede Administrativa (opcional)
- **eth2**: Rede do cliente (opcional)



Se você estiver visualizando um Nó de Administração ou um Nó de Gateway e ele for o nó ativo em um grupo de alta disponibilidade, o endereço IP virtual do grupo de alta disponibilidade será exibido em eth2.

3. Para encontrar o endereço IP virtual de um grupo de alta disponibilidade:
 - a. Selecione **Configuração > Rede > Grupos de alta disponibilidade**.
 - b. Na tabela, observe o endereço IP virtual do grupo HA.
4. Para encontrar o número da porta de um endpoint do Load Balancer:
 - a. Selecione **Configuração > Rede > Pontos de extremidade do balanceador de carga**.
 - b. Anote o número da porta do endpoint que você deseja usar.



Se o número da porta for 80 ou 443, o endpoint é configurado apenas nos Nós de Gateway, porque essas portas estão reservadas nos Nós de Administração. Todas as outras portas são configuradas tanto nos Nós de Gateway quanto nos Nós de Administração.

- c. Selecione o nome do endpoint na tabela.
- d. Confirme se o **Tipo de cliente** (S3) corresponde ao aplicativo cliente que irá utilizar o endpoint.

Gerenciar redes e conexões

Configurar as configurações de rede do StorageGRID

Você pode configurar diversas opções de rede no Grid Manager para otimizar o funcionamento do seu sistema StorageGRID.

Configurar interfaces VLAN

Você pode "[criar interfaces de LAN virtual \(VLAN\)](#)" isolar e particionar o tráfego para segurança, flexibilidade e desempenho. Cada interface VLAN está associada a uma ou mais interfaces pai em Admin Nodes e Gateway Nodes. Você pode usar interfaces VLAN em grupos de HA e em endpoints de balanceador de carga para segregar o tráfego de clientes ou de administração por aplicativo ou locatário.

Políticas de classificação de tráfego

Você pode usar "[políticas de classificação de tráfego](#)" para identificar e gerenciar diferentes tipos de tráfego de rede, incluindo tráfego relacionado a buckets, tenants, sub-redes de clientes ou endpoints de balanceadores de carga. Essas políticas podem auxiliar na limitação e no monitoramento do tráfego.

Diretrizes para redes StorageGRID

Você pode usar o Grid Manager para configurar e gerenciar redes e conexões do StorageGRID.

Veja "[Configurar conexões do cliente S3](#)" para saber como conectar clientes S3.

Redes padrão do StorageGRID

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

Para obter mais informações sobre topologia de rede, consulte "[Diretrizes de networking](#)".

Rede de grid

Obrigatório. A Rede Grid é usada para todo o tráfego interno do StorageGRID. Ela fornece conectividade entre todos os nós da grid, em todos os sites e sub-redes.

Rede de administração

Opcional. A Rede Administrativa é normalmente usada para administração e manutenção do sistema. Também pode ser usada para acesso a protocolo do cliente. A Rede Administrativa é normalmente uma rede privada e não precisa ser roteável entre sites.

Rede de cliente

Opcional. A Client Network é uma rede aberta, normalmente usada para fornecer acesso a aplicativos cliente S3, permitindo que a Grid Network seja isolada e protegida. A Client Network pode se comunicar com qualquer sub-rede acessível por meio do gateway local.

Diretrizes

- Cada nó 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 grid não pode ter mais de uma interface em uma rede.
- É suportado um único gateway por rede, por nó de grid, e ele deve estar na mesma sub-rede que o nó. Você pode implementar roteamento mais complexo no gateway, se necessário.
- Em cada nó, cada rede é mapeada para uma interface de rede específica.

Rede	Nome da interface
Grid	eth0
Administrador (opcional)	eth1
Cliente (opcional)	eth2

- Se o nó estiver conectado a um appliance StorageGRID, portas específicas serão usadas para cada rede. Para obter detalhes, consulte as instruções de instalação do seu appliance.
- A rota padrão é gerada automaticamente para cada nó. Se eth2 estiver habilitada, então 0.0.0.0/0 usa a Rede do Cliente em eth2. Se eth2 não estiver habilitada, então 0.0.0.0/0 usa a Rede Grid em eth0.
- A rede de clientes só se torna operacional depois que o nó da grade se junta à grade
- A Rede Administrativa pode ser configurada durante a implantação do nó da grade para permitir o acesso à interface de 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 trunk a um nó Admin ou Gateway, para poder usar ["Interfaces VLAN"](#) para segregar o tráfego pertencente a diferentes aplicativos ou locatários. Ou, você pode querer adicionar uma interface de acesso para usar em um ["grupo de alta disponibilidade \(HA\)"](#).

Para adicionar interfaces de tronco ou de acesso, consulte o seguinte:

- **VMware (após a instalação do nó):** ["VMware: adicionar interfaces de tronco ou de acesso a um nó"](#)
 - **Linux (antes de instalar o nó):** ["Criar arquivos de configuração de nó"](#)
 - **Linux (após instalar o nó):** ["Adicione interfaces de tronco ou de acesso a um nó"](#)



"Linux" refere-se a uma instalação do RHEL, Ubuntu ou Debian. Para obter uma lista das versões suportadas, consulte o ["NetApp Ferramenta de Matriz de Interoperabilidade \(IMT\)"](#).

Visualizar endereços IP no StorageGRID

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

Antes de começar

Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).

Sobre esta tarefa

Para obter informações sobre como alterar endereços IP, consulte ["Configurar endereços IP"](#).

Passos

1. Selecione **Nodes > *grid node* > Overview**.
2. Selecione **Mostrar mais** à direita do título IP Addresses.

Os endereços IP para esse nó da grid estão listados em uma tabela.

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  Connected

Storage used:

Object data		7%	?
Object metadata		5%	?

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 🔗	 Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

Configurar interfaces VLAN no StorageGRID

Crie interfaces de VLAN (Rede Local Virtual) nos Nós de Administração e Nós de Gateway e use-as em grupos de HA e endpoints de balanceador de carga para isolar e particionar o tráfego para segurança, flexibilidade e desempenho. Os nós selecionados no grupo de HA podem usar as interfaces de VLAN para compartilhar até 10 endereços IP virtuais, assim, se um nó falhar, outro nó assume o tráfego de e para os endereços IP virtuais.

Considerações sobre interfaces VLAN

- Você cria uma interface VLAN inserindo um ID de VLAN e escolhendo uma interface principal em um ou mais nós.

- Uma interface principal deve ser configurada como uma interface trunk no switch.
- Uma interface principal pode ser a Grid Network (eth0), a Client Network (eth2) ou uma interface trunk adicional para a VM ou host bare-metal (por exemplo, ens256).
- Para cada interface VLAN, você pode selecionar apenas uma interface principal para um determinado nó. Por exemplo, você não pode usar tanto a interface Grid Network quanto a interface Client Network no mesmo Gateway Node como interface principal para a mesma VLAN.
- Se a interface VLAN for para tráfego do Nó Administrativo, que inclui tráfego relacionado ao Grid Manager e ao Tenant Manager, selecione interfaces apenas nos Nós Administrativos.
- Se a interface VLAN for para tráfego de cliente S3, selecione interfaces em Admin Nodes ou Gateway Nodes.
- Se você precisar adicionar interfaces de tronco, consulte os detalhes a seguir:
 - **VMware (após a instalação do nó):** ["VMware: adicionar interfaces de tronco ou de acesso a um nó"](#)
 - **Linux (antes de instalar o nó):** ["Criar arquivos de configuração de nó"](#)
 - **Linux (após instalar o nó):** ["Adicione interfaces de tronco ou de acesso a um nó"](#)



"Linux" refere-se a uma instalação do RHEL, Ubuntu ou Debian. Para obter uma lista das versões suportadas, consulte o ["NetApp Ferramenta de Matriz de Interoperabilidade \(IMT\)"](#).

Criar uma interface VLAN

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).
- Uma interface trunk foi configurada na rede e conectada à máquina virtual ou ao nó Linux. Você sabe o nome da interface trunk.
- Você conhece o ID da VLAN que está configurando.

Sobre esta tarefa

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

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

Acesse o assistente

Passos

1. Selecione **Configuração > Rede > Interfaces VLAN**.
2. Selecione **Create**.

Insira os detalhes das interfaces VLAN

Passos

1. Especifique o ID da VLAN em sua rede. Você pode inserir qualquer valor entre 1 e 4094.

Os IDs de VLAN não precisam ser únicos. Por exemplo, você pode usar o ID de VLAN 200 para tráfego administrativo em um site e o mesmo ID de VLAN para tráfego de cliente em outro site. Você pode criar interfaces de VLAN separadas com diferentes conjuntos de interfaces pai em cada site. No entanto, duas interfaces de VLAN com o mesmo ID não podem compartilhar a mesma interface em um nó. Se você especificar um ID que já foi usado, uma mensagem aparece.

2. Opcionalmente, insira uma breve descrição para a interface VLAN.
3. Selecione **Continue**.

Escolha as interfaces principais

A tabela lista as interfaces disponíveis para todos os Nós de Administração e Nós de Gateway em cada site da sua grid. As interfaces da Admin Network (eth1) não podem ser usadas como interfaces pai e não são exibidas.

Passos

1. Selecione uma ou mais interfaces principais às quais deseja conectar esta VLAN.

Por exemplo, você pode querer associar uma VLAN à interface Client Network (eth2) para um Gateway Node e um Admin Node.

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.

	Site ?	Node name ?	Interface ?	Description ?	Node type ?	Attached VLANs ?
☐	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
☒	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
☐	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
☒	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
☐	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

[Previous](#)[Continue](#)

2. Selecione **Continue**.

Confirme as configurações

Passos

1. Revise a configuração e faça as alterações necessárias.
 - Se você precisar alterar o ID ou a descrição da VLAN, selecione **Inserir detalhes da VLAN** na parte superior da página.

- Se você precisar alterar uma interface principal, selecione **Escolher interfaces principais** na parte superior da página ou selecione **Anterior**.
- Se você precisar remover uma interface principal, selecione a lixeira .

2. Selecione **Salvar**.

3. Aguarde até 5 minutos para que a nova interface apareça como uma opção na página Grupos de alta disponibilidade e seja listada na tabela **Interfaces de rede** para o nó (**Nós > nó interface pai > Rede**).

Editar uma interface VLAN

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

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

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

Observe o seguinte:

- Não é possível alterar o ID de uma VLAN se a interface VLAN estiver sendo usada em um grupo HA.
- Não é possível remover uma interface principal se essa interface principal estiver sendo usada em um grupo de alta disponibilidade (HA).

Por exemplo, suponha que a VLAN 200 esteja associada às interfaces pai nos nós A e B. Se um grupo HA usar a interface VLAN 200 para o nó A e a interface eth2 para o nó B, você pode remover a interface pai não utilizada do nó B, mas não pode remover a interface pai utilizada do nó A.

Passos

1. Selecione **Configuração > Rede > Interfaces VLAN**.
2. Selecione a caixa de seleção da interface VLAN que você deseja editar. Em seguida, selecione **Ações > Editar**.
3. Opcionalmente, atualize o ID da VLAN ou a descrição. Em seguida, selecione **Continuar**.

Você não pode atualizar um ID de VLAN se a VLAN estiver sendo usada em um grupo de 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 as alterações necessárias.
6. Selecione **Salvar**.

Remover uma interface VLAN

Você pode remover uma ou mais interfaces VLAN.

Não é possível remover uma interface VLAN se ela estiver sendo usada em um grupo HA. Você precisa remover a interface VLAN do grupo HA antes de poder removê-la.

Para evitar interrupções no tráfego de clientes, considere uma das seguintes opções:

- Adicione uma nova interface VLAN ao grupo HA antes de remover esta interface VLAN.

- Crie um novo grupo HA que não utilize esta 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 o final da lista de prioridades. Aguarde até que a comunicação seja estabelecida na nova interface primária e, em seguida, remova a interface antiga do grupo HA. Por fim, exclua a interface VLAN nesse nó.

Passos

1. Selecione **Configuração > Rede > Interfaces VLAN**.
2. Selecione a caixa de seleção para cada interface VLAN que você deseja remover. Em seguida, selecione **Ações > Excluir**.
3. Selecione **Sim** para confirmar sua seleção.

Todas as interfaces VLAN que você selecionou foram removidas. Uma faixa verde de sucesso aparece na página de interfaces VLAN.

Habilite o CORS do StorageGRID para uma interface de gerenciamento

Como administrador de grid, você pode habilitar o compartilhamento de recursos entre origens (CORS) para solicitações de API de gerenciamento ao StorageGRID, caso deseje que os dados no StorageGRID sejam acessíveis por meio de APIs de gerenciamento em outro domínio.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- O ["Permissão de acesso root"](#) fornece acesso a todas as solicitações de configuração CORS.

Sobre esta tarefa

CORS é um mecanismo de segurança que permite que aplicativos web cliente em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você queira criar um painel de monitoramento para StorageGRID no domínio `http://www.example.com`. Ao habilitar o CORS no StorageGRID para `http://www.example.com` e "Grid Manager", o domínio StorageGRID responde às solicitações da API de gerenciamento de grid de `http://www.example.com`.

As solicitações da Management API (mgmt-api) com `application/json` ou `multipart/formdata` solicitações para `Content-Type` são compatíveis com CORS.

Passos

1. No Grid Manager, vá para **CONFIGURAÇÃO > Rede > Configurações CORS da interface de gerenciamento**.
2. Selecione **Grid Manager**, **Tenant Manager** ou ambas as opções.
 - **Gerenciador de Grid:** Habilita CORS para solicitações de API de gerenciamento de Grid entre domínios diferentes.
 - **Gerenciador de Locatários:** Habilita o CORS para solicitações de API de gerenciamento de locatários entre domínios.
3. Insira a URL do outro domínio no campo **Domínios**.

Selecione **Adicionar outro domínio** se você quiser ativar o CORS no StorageGRID para mais de um domínio.

4. Selecione **Salvar**.

Informações relacionadas

["Configurar o CORS do StorageGRID para buckets e objetos"](#)

Gerenciar políticas de classificação de tráfego

Políticas de classificação de tráfego no StorageGRID

As políticas de classificação de tráfego permitem que você identifique e monitore diferentes tipos de tráfego de rede. Essas políticas podem ajudar na limitação e no monitoramento do tráfego para aprimorar suas ofertas de qualidade de serviço (QoS).

As políticas de classificação de tráfego são aplicadas aos endpoints no serviço StorageGRID Load Balancer para Gateway Nodes e Admin Nodes. Para criar políticas de classificação de tráfego, você deve já ter criado endpoints de balanceador de carga.

Regras de correspondência

Cada política de classificação de tráfego contém uma ou mais regras de correspondência para identificar o tráfego de rede relacionado a uma ou mais das seguintes entidades:

- Buckets
- Sub-rede
- Locatário
- Pontos de extremidade do balanceador de carga

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 a uma entidade específica.

Limitação de tráfego

Opcionalmente, você pode adicionar os seguintes tipos de limite a uma política:

- Largura de banda de agregado
- Largura de banda por solicitação
- Solicitações simultâneas
- Taxa de solicitação

Os valores limite são aplicados individualmente a cada balanceador de carga. Se o tráfego for distribuído simultaneamente entre vários balanceadores de carga, as taxas máximas totais serão um múltiplo dos limites de taxa que você especificar.



Você pode criar políticas para limitar a largura de banda de agregado ou para limitar a largura de banda por solicitação. No entanto, StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Os limites de largura de banda de agregado podem impor um pequeno impacto adicional no desempenho do tráfego não limitado.

Para limites de largura de banda de agregado ou por solicitação, as solicitações fluem de entrada ou saída na

taxa que você definir. StorageGRID só pode impor uma velocidade, então a correspondência de política mais específica, por tipo de correspondência, é a que será aplicada. A largura de banda consumida pela solicitação não é contabilizada em outras políticas de correspondência menos específicas que contenham políticas de limite de largura de banda de agregado. Para todos os outros tipos de limite, as solicitações do cliente são atrasadas em 250 milissegundos e recebem uma resposta 503 Slow Down para solicitações que excedam qualquer limite de política correspondente.

No Grid Manager, você pode visualizar gráficos de tráfego e verificar se as políticas estão aplicando os limites de tráfego que você espera.

Utilize 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 impor acordos de nível de serviço (SLAs) que fornecem especificações para capacidade, proteção de dados e desempenho.

O exemplo a seguir mostra três níveis de um SLA. Você pode criar políticas de classificação de tráfego para atingir os objetivos de desempenho de cada nível do SLA.

Nível de serviço	Capacidade	Proteção de dados	Desempenho máximo permitido	Custo
Gold	1 PB de armazenamento permitido	Regra de 3 cópias ILM	25 mil solicitações/segundo 5 GB/s (40 Gbps) largura de banda	\$\$\$ por mês
Prata	250 TB de armazenamento permitido	Regra de 2 cópias ILM	10 mil solicitações/segundo 1,25 GB/s (10 Gbps) largura de banda	\$\$ por mês
Bronze	100 TB de armazenamento permitido	Regra de 2 cópias ILM	5 mil solicitações/segundo 1 GB/s (8 Gbps) largura de banda	\$ por mês

Criar políticas de classificação de tráfego do StorageGRID

Você pode criar políticas de classificação de tráfego se quiser monitorar e, opcionalmente, limitar o tráfego de rede por bucket, expressão regular de bucket, CIDR, endpoint do balanceador de carga ou tenant. Opcionalmente, você pode definir limites para uma política com base na largura de banda, no número de solicitações simultâneas ou na taxa de solicitações.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).
- Você criou todos os endpoints de balanceamento de carga que deseja corresponder.
- Você criou todos os tenants que deseja corresponder.

Passos

1. Selecione **Configuração > Rede > Classificação de tráfego**.
2. Selecione **Create**.
3. Insira um nome e uma descrição (opcional) para a política e selecione **Continuar**.

Por exemplo, descreva a que se aplica esta política de classificação de tráfego e o que ela vai limitar.

4. Selecione **Adicionar regra** e especifique os seguintes detalhes para criar uma ou mais regras correspondentes para a política. Qualquer política que você criar deve ter pelo menos uma regra correspondente. Selecione **Continuar**.

Campo	Descrição
Tipo	Selecione os tipos de tráfego aos quais a regra de correspondência se aplica. Os tipos de tráfego são bucket, expressão regular de bucket, CIDR, endpoint de balanceador de carga e tenant.
Valor correspondente	Insira o valor que corresponde ao tipo selecionado. • Bucket: insira um ou mais nomes de bucket. • Expressão regular para buckets: insira uma ou mais expressões regulares usadas para corresponder a um conjunto de nomes de buckets. A expressão regular não possui âncora. Use a âncora ^ para corresponder ao início do nome do bucket e a âncora \$ para corresponder ao final do nome. A correspondência por expressão regular suporta um subconjunto da sintaxe PCRE (expressão regular compatível com Perl). • CIDR: insira uma ou mais sub-redes IPv4, na notação CIDR, que correspondam à sub-rede desejada. • Ponto de extremidade do balanceador de carga: selecione um nome para o ponto de extremidade. Estes são os pontos de extremidade do balanceador de carga que você definiu no "Configurar pontos de extremidade do balanceador de carga". • Tenant: A correspondência de tenant utiliza o ID da chave de acesso. Se a solicitação não contiver um ID de chave de acesso (por exemplo, acesso anônimo), a propriedade do bucket acessado será usada para determinar o tenant.

Campo	Descrição
Correspondência inversa	Se você deseja corresponder todo o tráfego de rede, <i>exceto</i> o tráfego consistente com o Tipo e o Valor de Correspondência que você acabou de definir, selecione a caixa de seleção Correspondência inversa. Caso contrário, deixe a caixa de seleção desmarcada. Por exemplo, se você quiser que essa política se aplique a todos os endpoints do balanceador de carga, <i>exceto</i> um, especifique o endpoint do balanceador de carga a ser excluído e selecione Correspondência inversa. Para uma política que contenha vários correspondentes, onde pelo menos um seja um correspondente inverso, tome cuidado para não criar uma política que corresponda a todas as solicitações.

5. Opcionalmente, selecione **Adicionar um limite** e selecione os detalhes a seguir para adicionar um ou mais limites para controlar o tráfego de rede correspondente a uma regra.



StorageGRID coleta métricas mesmo que você não adicione nenhum limite, assim você pode entender as tendências de tráfego.

Campo	Descrição
Tipo	O tipo de limite que você deseja aplicar ao tráfego de rede correspondente à regra. Por exemplo, você pode limitar largura de banda ou taxa de requisições. Nota: Você pode criar políticas para limitar a largura de banda de agregado ou para limitar a largura de banda por solicitação. No entanto, StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Quando a largura de banda de agregado está em uso, a largura de banda por solicitação fica indisponível. Da mesma forma, quando a largura de banda por solicitação está em uso, a largura de banda de agregado fica indisponível. Os limites de largura de banda de agregado podem impor um pequeno impacto adicional no desempenho do 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 tiver uma política que limita o tráfego em apenas uma direção, o tráfego na direção oposta será ilimitado, mesmo que haja tráfego que corresponda a políticas adicionais com limites de largura de banda. O StorageGRID implementa as "melhores" correspondências para limites de largura de banda na seguinte ordem: • Endereço IP (máscara /32) • Nome exato do bucket • Expressão regular de bucket • Locatário • Endpoint • Correspondências CIDR não exatas (não /32) • Correspondências inversas

Campo	Descrição
Aplica-se a	Se este limite se aplica a solicitações de leitura do cliente (GET ou HEAD) ou a solicitações de escrita (PUT, POST ou DELETE).
Valor	O valor ao qual o tráfego de rede será limitado, com base na unidade que você selecionar. Por exemplo, insira 10 e selecione MiB/s para impedir que o tráfego de rede correspondente a esta regra exceda 10 MiB/s. Nota: Dependendo da configuração de unidades, as unidades disponíveis serão binárias (por exemplo, GiB) ou decimais (por exemplo, GB). Para alterar a configuração de unidades, selecione o menu suspenso do usuário no canto superior direito do Grid Manager e, em seguida, selecione User Preferences.
Unidade	A unidade que descreve o valor que você inseriu.

Por exemplo, se você quiser criar um limite de largura de banda de 4 GB/s para um nível de SLA, crie dois limites de largura de banda de agregado: GET/HEAD em 4 GB/s e PUT/POST/DELETE em 4 GB/s.

6. Selecione **Continue**.

7. Leia e revise a política de classificação de tráfego. Use o botão **Anterior** para voltar e fazer as alterações necessárias. Quando você estiver satisfeito com a política, selecione **Salvar e continuar**.

O tráfego de cliente S3 agora é tratado de acordo com a política de classificação de tráfego.

Depois que você terminar

["Visualizar métricas de tráfego de rede"](#) para verificar se as políticas estão aplicando os limites de tráfego que você espera.

Editar uma política de classificação de tráfego do StorageGRID

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.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).

Passos

1. Selecione **Configuração > Rede > Classificação de tráfego**.

A página de políticas de classificação de tráfego aparece e as políticas existentes são listadas em uma tabela.

2. Edite a política usando o menu Ações ou a página de detalhes. Veja ["criar políticas de classificação de tráfego"](#) o que inserir.

Menu de ações

- a. Selecione a caixa de seleção da política.
- b. Selecione **Ações > Editar**.

Página de detalhes

- a. Selecione o nome da política.
- b. Selecione o botão **Editar** ao lado do nome da policy.

3. Na etapa "Inserir nome da política", você pode opcionalmente editar o nome ou a descrição da política e selecionar "Continuar".
4. Na etapa Adicionar regras de correspondência, opcionalmente adicione uma regra ou edite o **Tipo** e o **Valor de correspondência** da regra existente e selecione **Continuar**.
5. Na etapa Definir limites, opcionalmente, adicione, edite ou exclua um limite e selecione **Continuar**.
6. Analise a política atualizada e selecione **Salvar e continuar**.

As alterações feitas na política foram salvas e o tráfego de rede agora é gerenciado 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 que você espera.

Excluir uma política de classificação de tráfego do StorageGRID

Você pode excluir uma política de classificação de tráfego se não precisar mais dela. Certifique-se de excluir a política correta, pois uma política não pode ser recuperada quando excluída.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).

Passos

1. Selecione **Configuração > Rede > Classificação de tráfego**.

A página de políticas de classificação de tráfego aparece com as políticas existentes listadas em uma tabela.

2. Exclua a política usando o menu Ações ou a página de detalhes.

Menu de ações

- a. Selecione a caixa de seleção da política.
- b. Selecione **Ações > Remover**.

Página de detalhes da política

- a. Selecione o nome da política.
- b. Selecione o botão **Remover** ao lado do nome da política.

3. Selecione **Sim** para confirmar que você deseja excluir a política.

A política foi excluída.

Visualize métricas de tráfego de rede no StorageGRID

Você pode monitorar o tráfego de rede visualizando os gráficos disponíveis na página de políticas de classificação de tráfego.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Acesso à raiz ou permissão para contas de locatário"](#).

Sobre esta tarefa

Para qualquer política de classificação de tráfego existente, você pode visualizar métricas do serviço de balanceador de carga para determinar se a política está limitando o tráfego na rede com sucesso. Os dados nos gráficos podem ajudar você a determinar se é necessário ajustar a política.

Mesmo que não sejam definidos limites para uma política de classificação de tráfego, métricas são coletadas e os gráficos fornecem informações úteis para a compreensão das tendências de tráfego.

Passos

1. Selecione **Configuração > Rede > Classificação de tráfego**.

A página de políticas de classificação de tráfego é exibida e as políticas existentes são listadas na tabela.

2. Selecione o nome da política de classificação de tráfego para a qual você deseja visualizar métricas.
3. Selecione a guia **Métricas**.

Os gráficos da política de classificação de tráfego são exibidos. Os gráficos mostram métricas apenas para o tráfego que corresponde à política selecionada.

Os seguintes gráficos estão incluídos na página.

- Taxa de requisições: Este gráfico mostra a quantidade de largura de banda correspondente a esta política, gerenciada por todos os balanceadores de carga. Os dados recebidos incluem os cabeçalhos de todas as requisições e o tamanho dos dados do corpo para as respostas que têm dados no corpo. Os dados enviados incluem os cabeçalhos de resposta de todas as requisições e o tamanho dos dados do corpo de resposta para as requisições que incluem dados no corpo da resposta.



Quando as solicitações são concluídas, este gráfico mostra apenas a utilização de largura de banda. Para solicitações de objetos lentos ou grandes, a largura de banda instantânea real pode ser diferente dos valores apresentados neste gráfico.

- Taxa de resposta de erro: Este gráfico fornece uma taxa aproximada na qual as solicitações que correspondem a esta política estão retornando erros (código de status HTTP ≥ 400) aos clientes.
- Duração média das solicitações (sem erros): este gráfico fornece a duração média das solicitações bem-sucedidas que correspondem a esta política.
- Utilização de largura de banda da política: Este gráfico mostra a quantidade de largura de banda correspondente a esta política, gerenciada por todos os balanceadores de carga. Os dados recebidos incluem os cabeçalhos de todas as requisições e o tamanho do corpo das respostas que contêm

dados no corpo. Os dados enviados incluem os cabeçalhos de todas as requisições e o tamanho do corpo das respostas que contêm dados no corpo.

4. Posicione o cursor sobre um gráfico de linhas para ver um pop-up com os valores de uma parte específica do gráfico.
5. Selecione **Grafana dashboard** logo abaixo do título Métricas para visualizar todos os gráficos de uma política. Além dos quatro gráficos da guia **Métricas**, você pode visualizar mais dois gráficos:
 - Taxa de requisições de escrita por tamanho do objeto: a taxa para requisições PUT/POST/DELETE que correspondem a esta política. O posicionamento em uma célula individual mostra as taxas por segundo. As taxas exibidas na visualização ao passar o mouse são truncadas para contagens inteiras e podem mostrar 0 quando houver requisições diferentes de zero no bucket.
 - Taxa de requisições de leitura por tamanho do objeto: a taxa para requisições GET/HEAD que correspondem a esta política. O posicionamento em uma célula individual mostra as taxas por segundo. As taxas exibidas na visualização ao passar o mouse são truncadas para contagens inteiras e podem mostrar 0 quando houver requisições diferentes de zero no bucket.
6. Alternativamente, acesse os gráficos no menu **Suporte**.
 - a. Selecione **Suporte > Ferramentas > Métricas**.
 - b. Selecione **Política de Classificação de Tráfego** na seção **Grafana**.
 - c. Selecione a política no menu no canto superior esquerdo da página.
 - d. Posicione o cursor sobre um gráfico para ver uma janela pop-up que mostra a data e a hora da amostra, os tamanhos dos objetos que são agregados na contagem e o número de solicitações por segundo durante esse período.

As políticas de classificação de tráfego são identificadas por seus IDs. Os IDs das políticas estão listados na página de políticas de classificação de tráfego.
7. Analise os gráficos para determinar com que frequência a política está limitando o tráfego e se você precisa ajustar a política.

Cifras suportadas para conexões TLS de saída no StorageGRID

O sistema StorageGRID suporta um conjunto limitado de suítes de cifras para conexões Transport Layer Security (TLS) com os sistemas externos usados para federação de identidades e Cloud Storage Pools.

Versões compatíveis do TLS

StorageGRID oferece suporte a TLS 1.2 e TLS 1.3 para conexões com sistemas externos usados para federação de identidades e Cloud Storage Pools.

Os algoritmos de criptografia TLS suportados para uso com sistemas externos foram selecionados para garantir a compatibilidade com uma ampla gama de sistemas externos. A lista é maior do que a lista de algoritmos de criptografia suportados para uso com aplicativos cliente S3. Para configurar os algoritmos de criptografia, acesse **Configuração > Segurança > Configurações de segurança** e selecione **Políticas de TLS e SSH**.



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 seu representante de conta da NetApp se você tiver solicitações específicas sobre essas configurações.

Benefícios das conexões HTTP ativas, ociosas e simultâneas no StorageGRID

A forma como você configura as conexões HTTP pode afetar o desempenho do sistema StorageGRID. As configurações variam dependendo se a conexão HTTP está ativa ou ociosa ou se você tem várias conexões simultâneas.

Você pode identificar os benefícios de desempenho para os seguintes tipos de conexões HTTP:

- Conexões HTTP ociosas
- Conexões HTTP ativas
- Conexões HTTP simultâneas

Benefícios de manter conexões HTTP ociosas abertas

Mantenha as conexões HTTP abertas quando os aplicativos cliente estiverem ociosos para permitir transações posteriores. Mantenha uma conexão HTTP ociosa aberta por no máximo 10 minutos. O StorageGRID pode fechar automaticamente uma conexão HTTP que permanecer aberta e ociosa por mais de 10 minutos.

Conexões HTTP abertas e ociosas oferecem os seguintes benefícios:

- Latência reduzida desde o momento em que o sistema StorageGRID determina que precisa realizar uma transação HTTP até o momento em que o sistema StorageGRID pode realizar a transação

A principal vantagem é a latência reduzida, especialmente considerando o tempo necessário para estabelecer conexões TCP/IP e TLS.

- Aumento da taxa de transferência de dados ao preparar o algoritmo de inicialização lenta do TCP/IP com transferências realizadas anteriormente
- Notificação instantânea de diversas classes de falhas que interrompem a conectividade entre o aplicativo cliente e o sistema StorageGRID

Decida por quanto tempo manter uma conexão ociosa aberta, equilibrando os benefícios do slow start e a alocação de recursos.

Benefícios das conexões HTTP ativas

Para conexões diretas com Storage Nodes, você deve limitar a duração de uma conexão HTTP ativa a um máximo de 10 minutos, mesmo que a conexão HTTP execute transações continuamente.

Determinar a duração máxima em que uma conexão deve permanecer aberta é um equilíbrio entre os benefícios da persistência da conexão e a alocação ideal da conexão aos recursos internos do sistema.

Para conexões de clientes com Storage Nodes, limitar as conexões HTTP ativas oferece os seguintes benefícios:

- Permite o balanceamento de carga ideal em todo o sistema StorageGRID.

Com o tempo, uma conexão HTTP pode deixar de ser a ideal à medida que os requisitos de balanceamento de carga mudam. O sistema apresenta o melhor desempenho em balanceamento de carga quando os aplicativos cliente estabelecem uma conexão HTTP separada para cada transação, mas esse método anula os valiosos ganhos associados às conexões persistentes.

- Permite que aplicativos cliente direcionem transações HTTP para serviços LDR que tenham espaço disponível.
- Permite o início dos procedimentos de manutenção.

Alguns procedimentos de manutenção só começam depois que todas as conexões HTTP em andamento forem concluídas.

Para conexões de cliente com o serviço de Load Balancer, limitar a duração das conexões abertas pode ser útil para permitir que alguns procedimentos de manutenção comecem prontamente. Se a duração das conexões de cliente não for limitada, pode levar vários minutos para que as conexões ativas sejam encerradas automaticamente.

Benefícios das conexões HTTP simultâneas

Você deve manter várias conexões TCP/IP abertas com o sistema StorageGRID para permitir o paralelismo, o que aumenta o desempenho. O número ideal de conexões paralelas depende de diversos fatores.

As conexões HTTP simultâneas oferecem os seguintes benefícios:

- Latência reduzida

As transações podem começar imediatamente em vez de esperar que outras transações sejam concluídas.

- Aumento da taxa de transferência

O sistema StorageGRID pode executar transações paralelas e aumentar a capacidade de processamento agregada de transações.

Os aplicativos cliente devem estabelecer múltiplas conexões HTTP. Quando um aplicativo cliente precisa realizar uma transação, ele pode selecionar e usar imediatamente qualquer conexão estabelecida que não esteja processando uma transação no momento.

A topologia de cada sistema StorageGRID apresenta uma taxa de transferência máxima diferente para transações e conexões simultâneas. A taxa de transferência máxima depende de computação, rede, recursos de storage, links WAN e do número de servidores, serviços e aplicativos que o sistema StorageGRID suporta.

Os sistemas StorageGRID geralmente suportam vários aplicativos cliente. Leve isso em consideração ao determinar o número máximo de conexões simultâneas. Se o aplicativo cliente consistir em várias entidades de software que estabelecem conexões com o sistema StorageGRID, some todas as conexões entre as entidades. Talvez seja necessário ajustar o número máximo de conexões simultâneas nas seguintes situações:

- A topologia do StorageGRID afeta o número máximo de transações e conexões simultâneas que o sistema pode suportar.
- Aplicações cliente que interagem com o sistema StorageGRID através de uma rede com largura de banda limitada podem ter que reduzir o grau de concorrência para garantir que as transações individuais sejam concluídas em um tempo razoável.
- Quando muitos aplicativos cliente compartilham o sistema StorageGRID, pode ser necessário reduzir o grau de concorrência para evitar exceder os limites do sistema.

Separação de pools de conexões HTTP para operações de leitura e gravação

Você pode usar pools separados de conexões HTTP para operações de leitura e gravação e controlar quanto do pool usar para cada uma. Pools separados de conexões HTTP permitem que você controle melhor as transações e equilibre as cargas.

Os aplicativos cliente podem gerar cargas de trabalho com predominância de recuperação (leitura) ou de armazenamento (gravação). Com pools separados de conexões HTTP para transações de leitura e gravação, você pode ajustar a quantidade de cada pool dedicada a transações de leitura ou gravação.

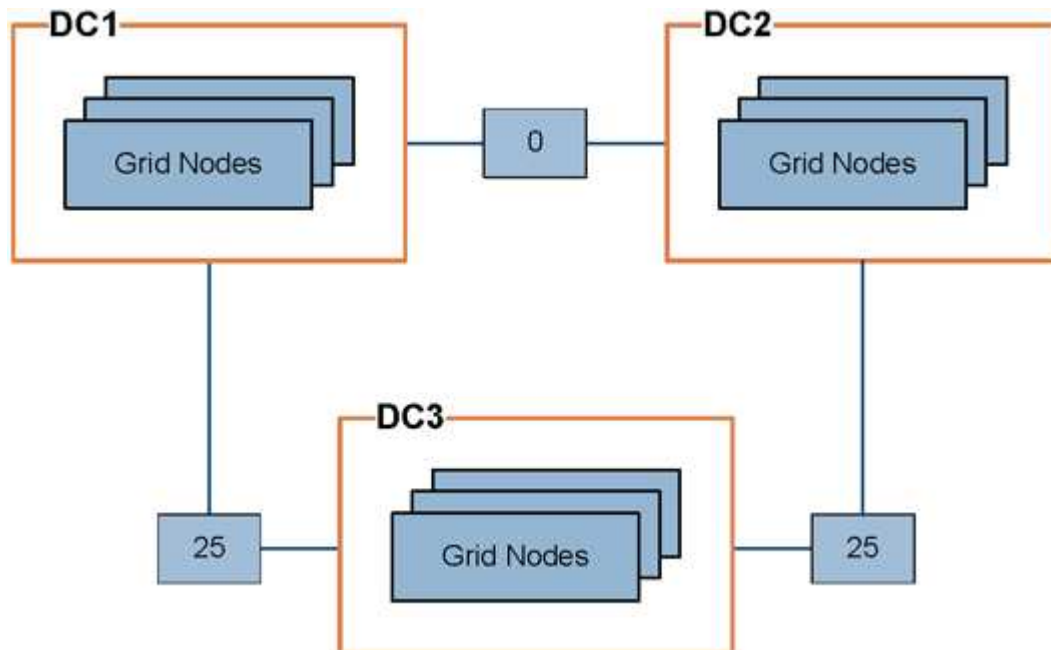
Gerencie os custos de link no StorageGRID

Os custos de enlace permitem que você priorize qual site de data center fornece um serviço solicitado quando existem dois ou mais sites de data center. Você pode ajustar os custos de enlace para refletir a latência entre os sites.

O que são custos de enlace?

- Os custos de enlace são usados para priorizar qual cópia do objeto é usada para realizar a recuperação do objeto.
- Os custos de conexão são usados pela API de Gerenciamento de Grid e pela API de Gerenciamento de Inquilinos para determinar quais serviços internos do StorageGRID devem ser usados.
- Os custos de link são usados pelo serviço Load Balancer nos nós de administração e nos nós de gateway para direcionar as conexões dos clientes. Consulte "[Considerações sobre balanceamento de carga](#)".

O diagrama mostra uma grade de três sites com custos de enlace configurados entre os sites:



- O serviço Load Balancer nos nós de administração e nos nós de gateway distribui igualmente as conexões dos clientes para todos os nós de armazenamento no mesmo site do data center e para quaisquer sites de data center com um custo de link de 0.

No exemplo, um nó de gateway no data center site 1 (DC1) distribui igualmente as conexões de clientes para os nós de armazenamento no DC1 e para os nós de armazenamento no DC2. Um nó de gateway no

DC3 envia conexões de clientes apenas para os nós de armazenamento no DC3.

- Ao recuperar um objeto que existe em múltiplas cópias replicadas, StorageGRID recupera a cópia no data center que possui o menor custo de link.

No exemplo, se um aplicativo cliente no DC2 recuperar um objeto que está armazenado tanto no DC1 quanto no DC3, o objeto será recuperado do DC1, porque o custo do link do DC1 para o DC2 é 0, que é menor que o custo do link do DC3 para o DC2 (25).

Os custos de enlace são números relativos arbitrários, sem uma unidade de medida específica. Por exemplo, um custo de enlace de 50 é usado menos preferencialmente do que um custo de enlace de 25. A tabela mostra os custos de enlace mais comuns.

Link	Custo do link	Notas
Entre sites físicos de data center	25 (padrão)	Data centers conectados por um link WAN.
Entre sites de data center lógicos na mesma localização física	0	Centros de dados lógicos no mesmo edifício físico ou campus conectados por uma LAN.

Atualizar custos do link

Você pode atualizar os custos de conexão entre sites do data center para refletir a latência entre eles.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Outra permissão de configuração da grid"](#).

Passos

1. Selecione **Support > Other > Link cost**.



Link Cost

Updated: 2023-02-15 18:09:28 MST

Site Names (1 - 3 of 3)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	
30	Data Center 3	

Show Records Per Page

Previous
« 1 » Next

Link Costs

Link Source	Link Destination			Actions
	10	20	30	
Data Center 1	0	25	25	

2. Selecione um site em **Origem do link** e insira um valor de custo entre 0 e 100 em **Destino do link**.

Não é possível alterar o custo do link se a origem for a mesma que o destino.

Para cancelar as alterações, selecione **Reverter**.

3. Selecione **Aplicar alterações**.

Use o AutoSupport

Saiba mais sobre AutoSupport no StorageGRID

O recurso AutoSupport permite que o StorageGRID envie pacotes de integridade e status para o suporte técnico da NetApp.

Usar o AutoSupport ajuda a resolver problemas mais rapidamente. O suporte técnico pode monitorar as necessidades de storage do seu sistema e ajudar a determinar se você precisa adicionar novos nós ou sites. Opcionalmente, o AutoSupport pode enviar pacotes para um destino adicional.

StorageGRID possui dois tipos de AutoSupport:

- **StorageGRID AutoSupport** relata problemas de software do StorageGRID. Ativado por padrão quando você instala o StorageGRID pela primeira vez. Você pode ["alterar a configuração padrão do AutoSupport"](#) se necessário.



Se StorageGRID AutoSupport não estiver ativado, uma mensagem será exibida no painel do Gerenciador de Grade. A mensagem inclui um link para a página de configuração do AutoSupport. Se você fechar a mensagem, ela não aparecerá novamente até que o cache do seu navegador seja limpo, mesmo que o AutoSupport permaneça desativado.

- O hardware do appliance **AutoSupport** relata problemas no appliance StorageGRID. Você deve ["configurar hardware AutoSupport em cada appliance"](#).

O que é Active IQ?

Active IQ é um consultor digital baseado na nuvem que aproveita a análise preditiva e o conhecimento da comunidade da base instalada da NetApp. Suas avaliações contínuas de risco, alertas preditivos, orientações prescritivas e ações automatizadas ajudam você a prevenir problemas antes que eles ocorram, resultando em melhor saúde do sistema e maior disponibilidade do sistema.

Se você deseja usar os painéis e funcionalidades do Active IQ no site de suporte da NetApp, você deve habilitar o AutoSupport.

["Documentação do Active IQ Digital Advisor"](#)

Informações incluídas no pacote AutoSupport

Um pacote AutoSupport contém os seguintes arquivos e detalhes.

Nome do arquivo	Campos	Descrição
AUTOSUPPORT-HISTORY.XML	AutoSupport Número de sequência + Destino para este AutoSupport + Status da entrega + Tentativas de entrega + AutoSupport Assunto + URI da entrega + Último erro + AutoSupport Nome do arquivo PUT + Hora de geração + Tamanho compactado do Autosupport + Tamanho descompactado do Autosupport + Tempo total de coleta (ms)	AutoSupport arquivo de histórico.
AUTOSUPPORT.XML	Nó + Protocolo para contatar o suporte + URL de suporte para HTTP/HTTPS + Endereço de suporte + AutoSupport OnDemand State + AutoSupport OnDemand Server URL + AutoSupport OnDemand Polling Interval	Arquivo de status do AutoSupport. Fornece detalhes do protocolo usado, URL e endereço do suporte técnico, intervalo de sondagem e se o OnDemand AutoSupport está ativado ou desativado.

Nome do arquivo	Campos	Descrição
BUCKETS.XML	ID do bucket + ID da conta + versão da build + configuração de restrição de localização + conformidade ativada + configuração de conformidade + S3 Object Lock ativado + configuração de S3 Object Lock + configuração de consistência + CORS ativado + configuração de CORS + último horário de acesso ativado + política ativada + configuração de política + notificações ativadas + configuração de notificações + Cloud Mirror ativado + configuração de Cloud Mirror + busca ativada + configuração de busca + marcação de bucket ativada + configuração de marcação de bucket + configuração de versionamento	Fornece detalhes de configuração e estatísticas no nível do bucket. Exemplos de configurações de bucket incluem serviços de plataforma, conformidade e consistência do bucket.
GRID-CONFIGURATIONS.XML	ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de informações de configuração de toda a grid. Contém informações sobre certificados da grid, espaço reservado de metadados, configurações de toda a grid (conformidade, S3 Object Lock, compactação de objetos, alertas, syslog e configuração ILM), detalhes do perfil de codificação de apagamento, nome DNS e " Nome da NMS ".
GRID-SPEC.XML	Especificações do grid, XML bruto	Utilizado para configurar e implementar StorageGRID. Contém especificações da grid, endereço IP do servidor NTP, endereço IP do servidor DNS, topologia de rede e perfis de hardware dos nós.
GRID-TASKS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de status das tarefas da grade (procedimentos de manutenção). Fornece detalhes das tarefas ativas, finalizadas, concluídas, com falha e pendentes da grade.
GRID.JSON	Grid + Revisão + Versão do Software + Descrição + Licença + Senhas + DNS + NTP + Sites + Nós	Informações do grid.

Nome do arquivo	Campos	Descrição
ILM-CONFIGURATION.XML	ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Lista de atributos para configurações ILM.
ILM-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de informações de métricas do ILM. Contém as taxas de avaliação do ILM para cada nó e métricas em toda a grid.
ILM.XML	XML bruto do ILM	Arquivo de política ativa do ILM. Contém detalhes sobre as políticas ativas do ILM, como ID do pool de storage, comportamento de ingestão, filtros, regras e descrição.
LOG.TGZ	<i>n/a</i>	Arquivo de log para download. Contém <code>broadcast-err.log</code> e <code>servermanager.log</code> de cada nó.
MANIFEST.XML	Ordem de coleta + AutoSupport content filename para esses dados + descrição deste item de dados + número de bytes coletados + tempo gasto na coleta + status deste item de dados + descrição do erro + AutoSupport tipo de conteúdo para esses dados +	Contém metadados do AutoSupport e breves descrições de todos os arquivos AutoSupport.
NMS-ENTITIES.XML	Índice de atributo + OID da entidade + ID do nó + ID do modelo do dispositivo + Versão do modelo do dispositivo + Nome da entidade	Agrupar entidades e serviços no " Árvore NMS ". Fornece detalhes da topologia da grade. O nó pode ser determinado com base nos serviços em execução no nó.
OBJECTS-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Estado do objeto, incluindo o estado da verificação em segundo plano, transferência ativa, taxa de transferência, total de transferências, taxa de exclusão, fragmentos corrompidos, objetos perdidos, objetos ausentes, tentativa de reparo, taxa de verificação, período estimado de verificação e estado de conclusão do reparo.

Nome do arquivo	Campos	Descrição
SERVER-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Configurações do servidor. Contém estes detalhes para cada nó: tipo de plataforma, sistema operacional, memória instalada, memória disponível, conectividade de storage, número de série do chassi do dispositivo de storage, quantidade de unidades com falha no controlador de storage, temperatura do chassi do controlador de computação, hardware de computação, número de série do controlador de computação, fonte de alimentação, tamanho da unidade e tipo de unidade.
SERVICE-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de informações do nó de serviço. Contém detalhes como espaço de tabela alocado, espaço de tabela livre, métricas Reaper do banco de dados, duração do reparo do segmento, duração da tarefa de reparo, reinicializações automáticas de tarefas e encerramento automático de tarefas.
STORAGE-GRADES.XML	ID da classe de armazenamento + Nome da classe de armazenamento + ID do nó de armazenamento + Caminho do nó de armazenamento	Arquivo de definições de storage grade para cada Storage Node.
SUMMARY-ATTRIBUTES.XML	OID do grupo + Caminho do grupo + ID do atributo de resumo + Nome do atributo de resumo + Valor + Índice + ID da tabela + Nome da tabela	Dados de status de alto nível do sistema que resumem as informações de uso do StorageGRID. Fornece detalhes como nome da grid, nomes dos sites, número de Storage Nodes por grid e por site, tipo de licença, capacidade e uso da licença, termos de suporte do software e detalhes das operações S3.
SYSTEM-ALERTS.XML	Nome + Gravidade + Nome do nó + Status do alerta + Nome do site + Hora de disparo do alerta + Hora de resolução do alerta + ID da regra + ID do nó + ID do site + Silenciado + Outras anotações + Outros rótulos	Alertas atuais do sistema que indicam possíveis problemas no sistema StorageGRID.

Nome do arquivo	Campos	Descrição
USERAGENTS.XML	Agente do usuário + Número de dias + Total de requisições HTTP + Total de bytes ingeridos + Total de bytes recuperados + Requisições PUT + Requisições GET + Requisições DELETE + Requisições HEAD + Requisições POST + Requisições OPTIONS + Tempo médio de requisição (ms) + Tempo médio de requisição PUT (ms) + Tempo médio de requisição GET (ms) + Tempo médio de requisição DELETE (ms) + Tempo médio de requisição HEAD (ms) + Tempo médio de requisição POST (ms) + Tempo médio de requisição OPTIONS (ms)	Estatísticas baseadas nos agentes de usuário do aplicativo. Por exemplo, o número de operações PUT/GET/DELETE/HEAD por agente de usuário e o tamanho total em bytes de cada operação.
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name +	AutoSupport dados do cabeçalho.

Configurar AutoSupport em StorageGRID

Por padrão, o recurso AutoSupport do StorageGRID é ativado quando você instala o StorageGRID pela primeira vez. No entanto, você deve configurar o hardware AutoSupport em cada appliance. Se necessário, você pode alterar a configuração do AutoSupport.

Se você deseja alterar a configuração do StorageGRID AutoSupport, faça as alterações somente no nó de administração primário. Você deve [configurar hardware AutoSupport](#) em cada appliance.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).
- Se você for usar HTTPS para enviar AutoSupport pacotes, você terá fornecido acesso de saída à internet para o nó de administração principal, seja diretamente ou ["usando um servidor proxy"](#) (conexões de entrada não são necessárias).
- Se o HTTP for selecionado na página do AutoSupport do StorageGRID, você tem ["configurou um servidor proxy"](#) para encaminhar pacotes do AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitarão pacotes enviados usando HTTP.

- Se você for usar SMTP como protocolo para pacotes do AutoSupport, você configurou um servidor de e-mail SMTP.

Sobre esta tarefa

Você pode usar qualquer combinação das seguintes opções para enviar pacotes AutoSupport para o suporte técnico:

- **Semanal:** Enviar pacotes AutoSupport automaticamente uma vez por semana. Configuração padrão: Ativado.
- **Acionado por evento:** Enviar automaticamente pacotes AutoSupport a cada hora ou quando ocorrerem eventos significativos do sistema. Configuração padrão: Ativado.
- **Sob Demanda:** Permite que o suporte técnico solicite que seu sistema StorageGRID envie pacotes AutoSupport automaticamente, o que é útil quando eles estão trabalhando ativamente em um problema (requer o protocolo de transmissão AutoSupport HTTPS). Configuração padrão: Desativado.
- **Acionado pelo usuário:** Envie pacotes AutoSupport manualmente a qualquer momento.
- **Coleta de logs:** ["coletar manualmente arquivos de log e dados do sistema e enviar um pacote AutoSupport"](#).

Especifique o protocolo para pacotes AutoSupport

Você pode usar qualquer um dos seguintes protocolos para enviar pacotes AutoSupport:

- **HTTPS:** Esta é a configuração padrão e recomendada para novas instalações. Este protocolo utiliza a porta 443. Se você quiser [Ative o recurso AutoSupport on Demand](#), deve usar HTTPS.
- **HTTP:** se você selecionar HTTP, deverá configurar um servidor proxy para encaminhar pacotes AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitam pacotes enviados usando HTTP. Este protocolo usa a porta 80.
- **SMTP:** Use esta opção se você quiser que os pacotes AutoSupport sejam enviados por e-mail.

O protocolo que você definir será usado para o envio de todos os tipos de pacotes AutoSupport.

Passos

1. Selecione **Suporte > Ferramentas > AutoSupport > Configurações**.
2. Selecione o protocolo que você deseja usar para enviar pacotes AutoSupport.
3. Se você selecionou **HTTPS**, escolha se deseja usar um certificado de suporte NetApp (certificado TLS) para proteger a conexão com o servidor de suporte técnico.
 - **Verificar certificado** (padrão): Garante que a transmissão de pacotes AutoSupport seja segura. O certificado de suporte NetApp já está instalado com o software StorageGRID.
 - **Não verificar certificado:** selecione esta opção somente quando tiver um bom motivo para não usar a validação de certificado, como quando houver um problema temporário com um certificado.
4. Selecione **Salvar**. Todos os pacotes semanais, acionados pelo usuário e acionados por eventos são enviados usando o protocolo selecionado.

Desativar AutoSupport semanal

Por padrão, o sistema StorageGRID está configurado para enviar um pacote AutoSupport para o suporte técnico uma vez por semana.

Para determinar quando o pacote semanal do AutoSupport será enviado, vá até a guia **AutoSupport >**

Resultados. Na seção **Semanal AutoSupport**, verifique o valor de **Próximo horário agendado**.

Você pode desativar o envio automático de pacotes semanais do AutoSupport a qualquer momento.

Passos

1. Selecione **Suporte > Ferramentas > AutoSupport > Configurações**.
2. Desmarque a caixa de seleção **Ativar semanalmente AutoSupport**.
3. Selecione **Salvar**.

Desativar AutoSupport acionado por evento

Por padrão, o sistema StorageGRID está configurado para enviar um pacote AutoSupport para o suporte técnico a cada hora.

Você pode desativar o acionamento por eventos AutoSupport a qualquer momento.

Passos

1. Selecione **Suporte > Ferramentas > AutoSupport > Configurações**.
2. Desmarque a caixa de seleção **Ativar acionamento por evento AutoSupport**.
3. Selecione **Salvar**.

Ativar AutoSupport sob demanda

AutoSupport on Demand pode ajudar a resolver problemas nos quais o suporte técnico está trabalhando ativamente.

Por padrão, o AutoSupport Sob Demanda está desativado. Habilitar esse recurso permite que o suporte técnico solicite que seu sistema StorageGRID envie pacotes AutoSupport automaticamente. O suporte técnico também pode definir o intervalo de tempo de sondagem para consultas AutoSupport Sob Demanda.

O suporte técnico não pode ativar ou desativar AutoSupport on Demand.

Passos

1. Selecione **Suporte > Ferramentas > AutoSupport > Configurações**.
2. Selecione **HTTPS** para o protocolo.
3. Selecione a caixa de seleção **Ativar semanalmente AutoSupport**.
4. Selecione a caixa de seleção **Ativar AutoSupport sob demanda**.
5. Selecione **Salvar**.

AutoSupport On Demand está ativado e o suporte técnico pode enviar solicitações AutoSupport On Demand para o StorageGRID.

Desative as verificações de atualizações de software

Por padrão, StorageGRID entra em contato com a NetApp para verificar se há atualizações de software disponíveis para o seu sistema. Se uma hotfix do StorageGRID ou uma nova versão estiver disponível, a nova versão será exibida na página de upgrade do StorageGRID.

Se necessário, você pode opcionalmente desativar a verificação de atualizações de software. Por exemplo, se seu sistema não tiver acesso à WAN, você deve desativar a verificação para evitar erros de download.

Passos

1. Selecione **Suporte > Ferramentas > AutoSupport > Configurações**.
2. Desmarque a caixa de seleção **Verificar atualizações de software**.
3. Selecione **Salvar**.

Adicionar um destino adicional do AutoSupport

Quando você ativa o AutoSupport, os pacotes de integridade e status são enviados para o suporte técnico. Você pode especificar um destino adicional para todos os pacotes do AutoSupport.

Para verificar ou alterar o protocolo usado para enviar pacotes AutoSupport, consulte as instruções para [especifique o protocolo para pacotes AutoSupport](#).



Não é possível usar o protocolo SMTP para enviar pacotes AutoSupport para um destino adicional.

Passos

1. Selecione **Suporte > Ferramentas > AutoSupport > Configurações**.
2. Selecione **Ativar destino adicional do AutoSupport**.
3. Especifique o seguinte:

Nome do host

O nome do host ou endereço IP de um servidor de destino AutoSupport adicional.



Você pode inserir apenas um destino adicional.

Porta

A porta usada para conectar a um servidor de destino AutoSupport adicional. O padrão é a porta 80 para HTTP ou a porta 443 para HTTPS.

Validação de certificado

Indica se um certificado TLS é usado para proteger a conexão com o destino adicional.

- Selecione **Verificar certificado** para usar a validação de certificado.
- Selecione **Não verificar certificado** para enviar seus AutoSupport pacotes sem validação de certificado.

Selecione esta opção somente quando tiver um bom motivo para não usar a validação de certificado, como quando houver um problema temporário com um certificado.

4. Se você selecionou **Verificar certificado**, faça o seguinte:
 - a. Navegue até a localização do certificado da CA.
 - b. Faça o upload do arquivo de certificado da CA.

Os metadados do certificado CA são exibidos.

5. Selecione **Salvar**.

Todos os futuros pacotes semanais, acionados por eventos e acionados pelo usuário de AutoSupport

serão enviados para o destino adicional.

Configurar AutoSupport para dispositivos de storage

AutoSupport para dispositivos reporta problemas de hardware do StorageGRID, e StorageGRID AutoSupport reporta problemas de software do StorageGRID, com uma exceção: para o SGF6112, StorageGRID AutoSupport reporta problemas tanto de hardware quanto de software. Você deve configurar AutoSupport em cada dispositivo, exceto o SGF6112, que não requer configuração adicional. AutoSupport é implementado de forma diferente para dispositivos de serviço e dispositivos de storage.

Você utiliza SANtricity para habilitar o AutoSupport para cada dispositivo de storage. Você pode configurar o SANtricity AutoSupport durante a configuração inicial do dispositivo ou após a instalação do dispositivo:

- Para os dispositivos SG6000 e SG5700, ["configurar AutoSupport no SANtricity System Manager"](#)

AutoSupport pacotes de dispositivos E-Series podem ser incluídos no StorageGRID AutoSupport se você configurar a entrega do AutoSupport por proxy em ["SANtricity System Manager"](#).

StorageGRID AutoSupport não reporta problemas de hardware, como falhas em módulos DIMM ou placas de interface de host (HIC). No entanto, algumas falhas de componentes podem gerar ["alertas de hardware"](#). Para dispositivos de storage StorageGRID com um controlador de gerenciamento de placa-mãe (BMC), você pode configurar e-mail e traps SNMP para reportar falhas de hardware:

- ["Configure notificações por e-mail para alertas do BMC"](#)
- ["Configurar as definições de SNMP para BMC"](#)

Informações relacionadas

["Suporte da NetApp"](#)

Acionar manualmente um pacote AutoSupport no StorageGRID

Para ajudar o suporte técnico a solucionar problemas com seu sistema StorageGRID, você pode acionar manualmente o envio de um pacote AutoSupport.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você possui acesso de root ou permissão de configuração de outra grid.

Passos

1. Selecione **Suporte > Ferramentas > AutoSupport**.
2. Na aba **Ações**, selecione **Enviar AutoSupport acionado pelo usuário**.

StorageGRID tenta enviar um pacote AutoSupport para o site de suporte da NetApp. Se a tentativa for bem-sucedida, os valores **Resultado Mais Recente** e **Última Vez Bem-Sucedida** na aba **Resultados** são atualizados. Se houver um problema, o valor **Resultado Mais Recente** é atualizado para "Falha" e o StorageGRID não tenta enviar o pacote AutoSupport novamente.

3. Após 1 minuto, atualize a página AutoSupport no seu navegador para acessar os resultados mais recentes.



Além disso, você pode ["coletar arquivos de log e dados do sistema mais extensos"](#) e enviá-los para o site de suporte da NetApp.

Solucionar problemas dos pacotes AutoSupport do StorageGRID

Se uma tentativa de envio de um pacote AutoSupport falhar, o sistema StorageGRID tomará ações diferentes dependendo do tipo de pacote AutoSupport. Você pode verificar o status dos pacotes AutoSupport selecionando **Suporte > Ferramentas > AutoSupport > Resultados**.

Quando o pacote AutoSupport falha ao ser enviado, "Falha" aparece na guia **Resultados** da página **AutoSupport**.



Se você configurou um servidor proxy para encaminhar pacotes AutoSupport para NetApp, você deve "[Verifique se as configurações do servidor proxy estão corretas.](#)".

Falha semanal no pacote AutoSupport

Se um pacote semanal do AutoSupport falhar ao ser enviado, o sistema StorageGRID executa as seguintes ações:

1. Atualiza o atributo Resultado Mais Recente para Tentando Novamente.
2. O sistema tenta reenviar o pacote AutoSupport 15 vezes a cada quatro minutos durante uma hora.
3. Após uma hora de falhas no envio, atualiza o atributo "Resultado Mais Recente" para "Falha".
4. Tenta enviar novamente um pacote AutoSupport no próximo horário agendado.
5. Mantém a programação regular do AutoSupport caso o pacote falhe devido à indisponibilidade do serviço NMS e se um pacote for enviado antes de sete dias.
6. Quando o serviço NMS estiver disponível novamente, envia um pacote AutoSupport imediatamente se nenhum pacote tiver sido enviado por sete dias ou mais.

Falha de pacote AutoSupport acionada pelo usuário ou por evento

Se um pacote AutoSupport acionado pelo usuário ou por um evento não for enviado, o sistema StorageGRID executa 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 de e-mail corretas, o seguinte erro será exibido: AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.
2. Não tenta enviar o pacote novamente.
3. Registra o erro em `nms.log`.

Se ocorrer uma falha e o protocolo selecionado for SMTP, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se o seu servidor de e-mail está em execução (**Suporte > Alarmes (legado) > Configuração de e-mail legado**). A seguinte mensagem de erro pode aparecer na página AutoSupport: AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.

Saiba como "[configurar as configurações do servidor de e-mail](#)".

Corrigir uma falha no pacote AutoSupport

Se ocorrer uma falha e o protocolo selecionado for SMTP, verifique se o servidor de e-mail do sistema

StorageGRID está configurado corretamente e se o seu servidor de e-mail está em execução. A seguinte mensagem de erro pode aparecer na página AutoSupport: AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.

Envie pacotes E-Series AutoSupport através do StorageGRID

Você pode enviar pacotes AutoSupport do E-Series SANtricity System Manager para o suporte técnico por meio de um nó Admin do StorageGRID, em vez da porta de gerenciamento do dispositivo de storage.

Consulte "[Hardware E-Series AutoSupport](#)" para obter mais informações sobre o uso do AutoSupport com dispositivos de storage E-Series.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador web compatível](#)".
- Você tem o "[Permissão de administrador do dispositivo de storage ou acesso root](#)".
- Você configurou SANtricity AutoSupport:
 - Para os dispositivos SG6000 e SG5700, "[configurar AutoSupport no SANtricity System Manager](#)"



Você precisa ter firmware SANtricity 8.70 ou superior para acessar o SANtricity System Manager usando o Grid Manager.

Sobre esta tarefa

Os pacotes E-Series AutoSupport contêm detalhes do hardware de storage e são mais específicos do que outros pacotes AutoSupport enviados pelo sistema StorageGRID.

Você pode configurar um endereço de servidor proxy especial no SANtricity System Manager para transmitir pacotes AutoSupport através de um StorageGRID Admin Node sem usar a porta de gerenciamento do appliance. Pacotes AutoSupport transmitidos dessa forma são enviados pelo "[Nó de administração remetente preferencial](#)" e utilizam qualquer "[configurações de proxy do admin](#)" que tenha sido configurado no Grid Manager.

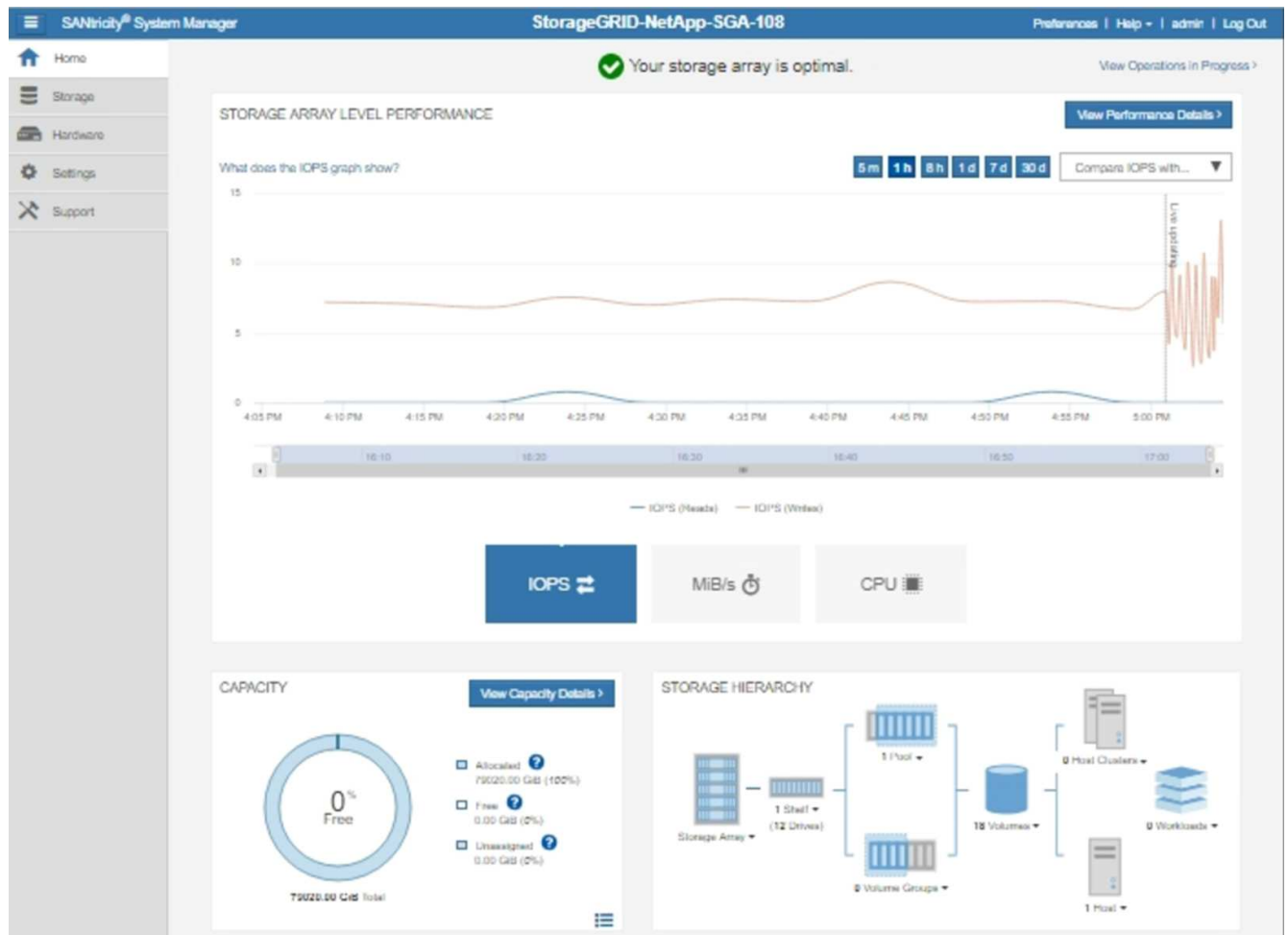


Este procedimento é apenas para configurar um servidor proxy StorageGRID para pacotes AutoSupport do E-Series. Para obter detalhes adicionais sobre a configuração do E-Series AutoSupport, consulte o "[NetApp E-Series e documentação do SANtricity](#)".

Passos

1. No Gerenciador de Grade, selecione **Nós**.
2. Na lista de nós à esquerda, selecione o dispositivo de storage que você deseja configurar.
3. Selecione **SANtricity System Manager**.

A página inicial do SANtricity System Manager é exibida.



4. Selecione **Suporte** > **Central de suporte** > **AutoSupport**.

A página de operações do AutoSupport é exibida.

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 AutoSupport Delivery Method**.

A página Configurar AutoSupport Método de Entrega é exibida.

Configure AutoSupport Delivery Method

Select AutoSupport dispatch delivery method...

☒ HTTPS
☐ HTTP
☐ Email

HTTPS delivery settings [Show destination address](#)

Connect to support team...

☐ Directly ?
☒ via Proxy server ?
☐ via Proxy auto-configuration script (PAC) ?

Host address ?
tunnel-host

Port number ?
10225

☐ My proxy server requires authentication

Save Test Configuration Cancel

6. Selecione **HTTPS** como método de entrega.



O certificado que habilita o HTTPS já está pré-instalado.

7. Selecione **via servidor proxy**.

8. Insira `tunnel-host` para o **Endereço do host**.

`tunnel-host` é o endereço especial para usar um Nó de Administração para enviar pacotes E-Series AutoSupport.

9. Digite 10225 para o **número da porta**.

10225 é o número da porta no servidor proxy do StorageGRID que recebe pacotes AutoSupport do controlador E-Series no dispositivo.

10. Selecione **Testar Configuração** para testar o roteamento e a configuração do seu servidor proxy AutoSupport.

Se estiver correta, uma mensagem em uma faixa verde aparecerá: "Sua configuração do AutoSupport foi verificada."

Se o teste falhar, uma mensagem de erro aparecerá em uma faixa vermelha. Verifique suas configurações de DNS do StorageGRID e de rede, certifique-se de que ["Nó de administração remetente preferencial"](#) pode se conectar ao site de suporte da NetApp e tente o teste novamente.

11. Selecione **Salvar**.

A configuração é salva e uma mensagem de confirmação aparece: "AutoSupport delivery method foi configurado."

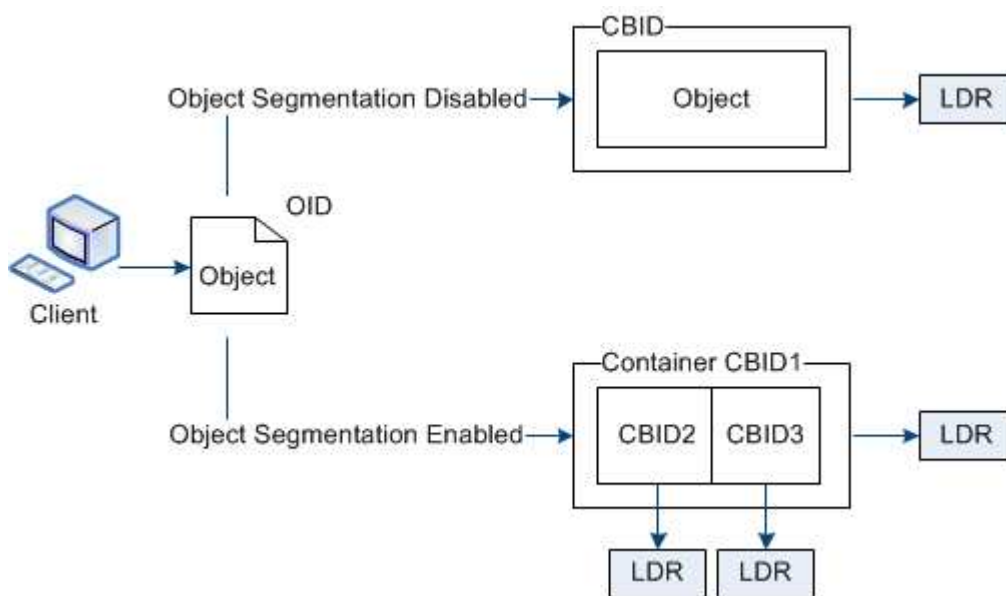
Gerenciar nós de armazenamento

Use as opções de armazenamento

Saiba mais sobre segmentação de objetos no StorageGRID

A segmentação de objetos é o processo de dividir um objeto em uma coleção de objetos menores de tamanho fixo para otimizar o armazenamento e o uso de recursos para objetos grandes. O upload multipartes do S3 também cria objetos segmentados, com um objeto representando cada parte.

Quando um objeto é inserido no sistema StorageGRID, o serviço LDR divide o objeto em segmentos e cria um contêiner de segmentos que lista as informações de cabeçalho de todos os segmentos como conteúdo.



Ao recuperar um contêiner de segmento, o serviço LDR monta o objeto original a partir de seus segmentos e retorna o objeto ao cliente.

O contêiner e os segmentos não precisam estar armazenados no mesmo Storage Node. O contêiner e os segmentos podem estar armazenados em qualquer Storage Node dentro do pool de storage especificado na regra ILM.

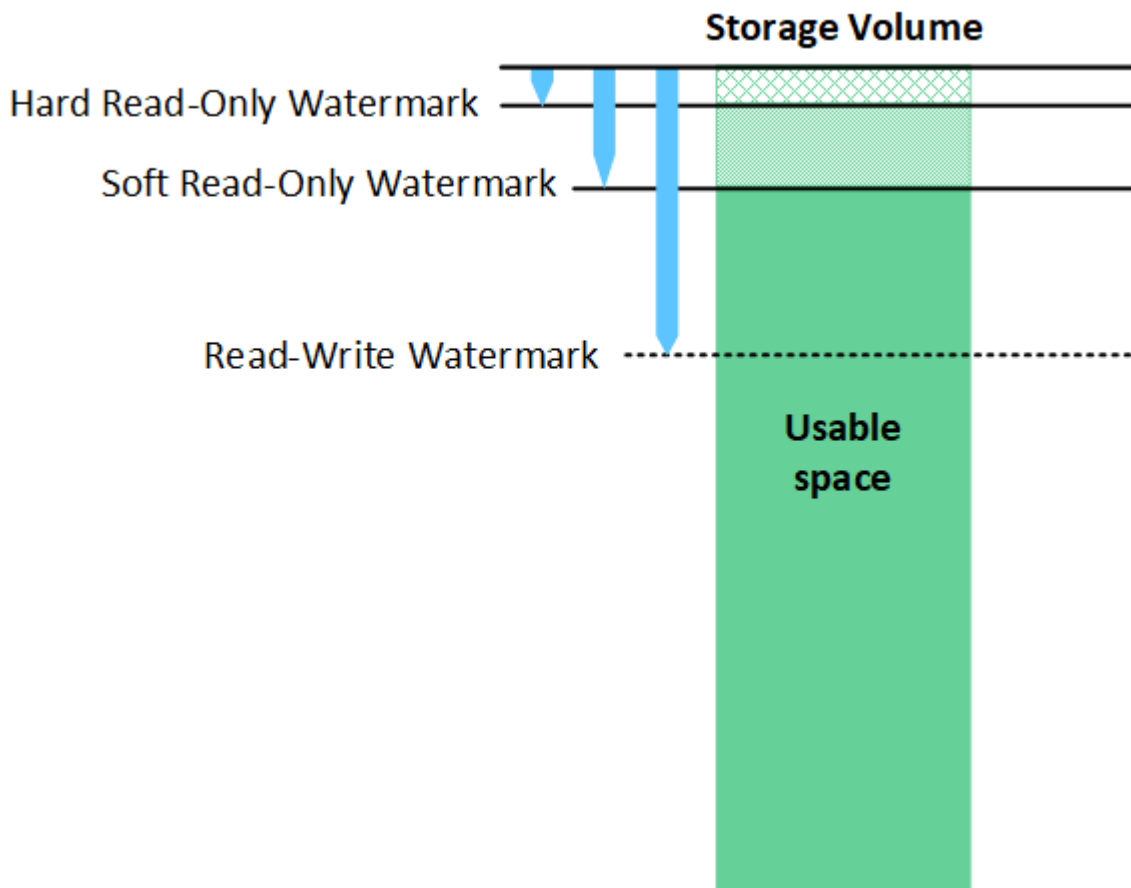
Cada segmento é tratado pelo sistema StorageGRID de forma independente e contribui para a contagem de atributos como Objetos Gerenciados e Objetos Armazenados. Por exemplo, se um objeto armazenado no

sistema StorageGRID for dividido em dois segmentos, o valor de Objetos Gerenciados aumentará em três após a conclusão da ingestão, conforme a seguir:

segment container + segment 1 + segment 2 = three stored objects

Saiba mais sobre marcas d'água de volume de armazenamento no StorageGRID

StorageGRID utiliza três marcas d'água de volume de armazenamento para garantir que os nós de armazenamento sejam transferidos com segurança para um estado somente leitura antes que fiquem criticamente sem espaço e para permitir que os nós de armazenamento que foram transferidos para um estado somente leitura voltem a ser de leitura e gravação.



As marcas d'água de volume de armazenamento aplicam-se apenas ao espaço usado para dados de objetos replicados e codificados por apagamento. Para saber mais sobre o espaço reservado para metadados de objetos no volume 0, acesse ["Gerencie o armazenamento de metadados de objetos"](#).

O que é a marca d'água "somente leitura" suave?

A **marca d'água somente leitura flexível do volume de storage** é a primeira marca d'água a indicar que o espaço utilizável de um Storage Node para dados de objetos está ficando cheio.

Se cada volume em um Nó de Armazenamento tiver menos espaço livre do que a marca d'água de leitura flexível desse volume, o Nó de Armazenamento entra no modo somente leitura. O modo somente leitura

significa que o Nó de Armazenamento anuncia serviços somente leitura para o restante do sistema StorageGRID, mas atende a todas as solicitações de gravação pendentes.

Por exemplo, suponha que cada volume em um Storage Node tenha uma marca d'água de leitura flexível de 10 GB. Assim que cada volume tiver menos de 10 GB de espaço livre, o Storage Node entra no modo de leitura flexível.

O que é o watermark rígido de somente leitura?

A **marca d'água rígida de somente leitura do volume de storage** é a próxima marca d'água a indicar que o espaço utilizável de um nó para dados de objetos está ficando cheio.

Se o espaço livre em um volume for menor que a marca d'água de leitura obrigatória desse volume, as gravações nesse volume falharão. No entanto, as gravações em outros volumes podem continuar até que o espaço livre nesses volumes seja menor que suas respectivas marcas d'água de leitura obrigatória.

Por exemplo, suponha que cada volume em um Storage Node tenha uma marca d'água rígida de somente leitura de 5 GB. Assim que cada volume tiver menos de 5 GB de espaço livre, o Storage Node não aceitará mais solicitações de gravação.

A marca d'água rígida de somente leitura é sempre menor que a marca d'água flexível de somente leitura.

O que é a marca d'água de leitura/gravação?

A **marca d'água de leitura/gravação do volume de storage** aplica-se somente aos Storage Nodes que passaram para o modo somente leitura. Ela determina quando o nó pode voltar a ser leitura/gravação. Quando o espaço livre em qualquer volume de storage em um Storage Node for maior que a marca d'água de leitura/gravação desse volume, o nó retorna automaticamente ao estado de leitura/gravação.

Por exemplo, suponha que o Storage Node tenha entrado em modo somente leitura. Suponha também que cada volume tenha uma marca d'água de leitura/gravação de 30 GB. Assim que o espaço livre em qualquer volume aumentar para 30 GB, o nó volta a ser leitura/gravação.

A marca d'água de leitura/gravação é sempre maior do que tanto a marca d'água de leitura flexível quanto a marca d'água de leitura rígida.

Exibir marcas d'água de volume de armazenamento

Você pode visualizar as configurações atuais da marca d'água e os valores otimizados pelo sistema. Caso as marcas d'água otimizadas não estejam sendo utilizadas, você pode determinar se é possível ou recomendável ajustar as configurações.

Antes de começar

- Você concluiu a atualização para StorageGRID 11.6 ou superior.
- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).

Ver as configurações atuais da marca d'água

Você pode visualizar as configurações atuais da marca d'água de storage no Grid Manager.

Passos

1. Selecione **Support > Other > Storage watermarks**.

2. Na página de marcas d'água de storage, verifique a caixa de seleção "Usar valores otimizados".
 - Se a caixa de seleção estiver marcada, todas as três marcas d'água serão otimizadas para cada volume de storage em cada Storage Node, com base no tamanho do Storage Node e na capacidade relativa do volume.

Esta é a configuração padrão e recomendada. Não altere esses valores. Opcionalmente, você pode [Visualizar marcas d'água de storage otimizadas](#).

- Se a caixa de seleção "Usar valores otimizados" estiver desmarcada, marcas d'água personalizadas (não otimizadas) estão sendo usadas. Não é recomendável usar configurações de marca d'água personalizadas. Use as instruções para ["Solução de problemas de alertas de sobreposição de marca d'água somente leitura baixa"](#) determinar se você pode ou deve ajustar as configurações.

Ao especificar configurações de marca d'água personalizadas, você deve inserir valores maiores que 0.

Visualizar marcas d'água de storage otimizadas

StorageGRID usa duas métricas do Prometheus para mostrar os valores otimizados que calculou para a marca d'água de leitura somente leitura suave do volume de storage. Você pode visualizar os valores otimizados mínimo e máximo para cada Storage Node em sua grid.

1. Selecione **Suporte > Ferramentas > Métricas**.
2. Na seção Prometheus, selecione o link para acessar a interface de usuário do Prometheus.
3. Para visualizar a marca d'água mínima recomendada para leitura somente leitura, insira a seguinte métrica do Prometheus e selecione **Executar**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

A última coluna mostra o valor mínimo otimizado da marca d'água de leitura somente leitura flexível para todos os volumes de armazenamento em cada Storage Node. Se esse valor for maior que a configuração personalizada para a marca d'água de leitura somente leitura flexível do volume de armazenamento, o alerta **Low read-only watermark override** será acionado para o Storage Node.

4. Para visualizar a marca d'água máxima recomendada para leitura somente leitura, insira a seguinte métrica do Prometheus e selecione **Executar**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

A última coluna mostra o valor máximo otimizado da marca d'água de leitura somente leitura flexível para todos os volumes de armazenamento em cada Storage Node.

Gerencie o armazenamento de metadados de objetos no StorageGRID

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 suficiente para armazenar novos objetos, você precisa entender onde e como o StorageGRID armazena os metadados dos objetos.

O que são metadados de objeto?

Metadados de objeto são quaisquer informações que descrevem um objeto. StorageGRID usa metadados de objeto para rastrear as localizações de todos os objetos na grid e para gerenciar o ciclo de vida de cada objeto ao longo do tempo.

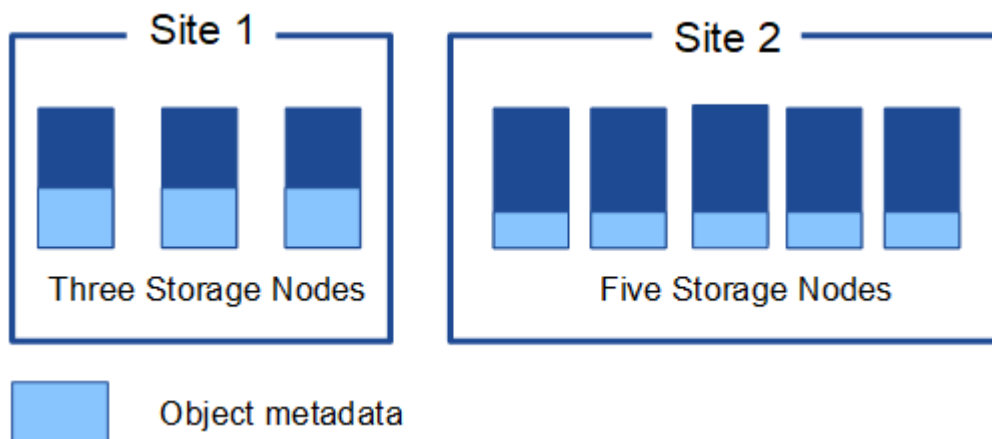
Para um objeto no StorageGRID, os metadados do objeto incluem os seguintes tipos de informações:

- Metadados do sistema, incluindo um ID exclusivo para cada objeto (UUID), o nome do objeto, o nome do bucket S3, o nome ou ID da conta do tenant, 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 chave-valor de metadados de usuário personalizados associados ao objeto.
- Para objetos S3, quaisquer pares de chave-valor de tag de objeto associados ao objeto.
- Para cópias de objetos replicadas, o local de armazenamento atual de cada cópia.
- Para cópias de objetos com código de apagamento, o local de armazenamento atual de cada fragmento.
- Para cópias de objetos em um Cloud Storage Pool, a localização 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 objeto são armazenados?

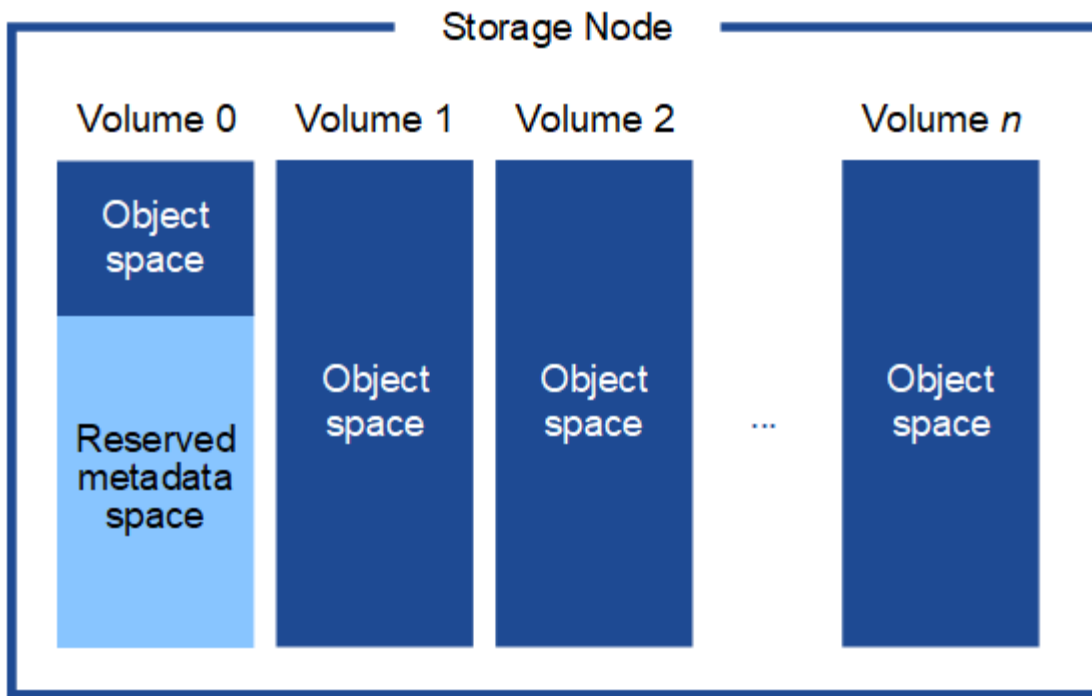
StorageGRID mantém os metadados dos objetos em um banco de dados Cassandra, que é armazenado independentemente dos dados dos objetos. Para garantir a redundância e proteger os metadados dos objetos contra perda, StorageGRID armazena três cópias dos metadados para todos os objetos do sistema em cada site.

Esta figura representa os nós de armazenamento em dois locais. Cada local possui a mesma quantidade de metadados de objetos, e os metadados de cada local são subdivididos entre todos os nós de armazenamento desse local.



Onde os metadados do objeto são armazenados?

Esta figura representa os volumes de armazenamento para um único Storage Node.



Conforme ilustrado na figura, StorageGRID reserva espaço para metadados de objetos no volume de armazenamento 0 de cada Nó de Armazenamento. Ele utiliza o espaço reservado para armazenar metadados de objetos e para executar operações essenciais do banco de dados. Qualquer espaço restante no volume de armazenamento 0 e em todos os outros volumes de armazenamento do Nó de Armazenamento é utilizado exclusivamente para dados de objetos (cópias replicadas e fragmentos codificados por eliminação).

A quantidade de espaço reservada para metadados de objetos em um determinado Nó de Armazenamento depende de vários fatores, que são descritos abaixo.

Configuração de espaço reservado para metadados

O *Espaço reservado para metadados* é uma configuração de todo o sistema que representa a quantidade de espaço que será reservada para metadados no volume 0 de cada Storage Node. Conforme mostrado na tabela, o valor padrão dessa configuração é baseado em:

- A versão do software que você estava usando quando instalou StorageGRID.
- A quantidade de RAM em cada Storage Node.

Versão usada para a instalação inicial do StorageGRID	Quantidade de RAM nos nós de armazenamento	Configuração padrão de espaço reservado para metadados
11,5 a 12,0	128 GB ou mais em cada nó de armazenamento na grade	8 TB (8.000 GB)
	Menos de 128 GB em qualquer nó de armazenamento na grade	3 TB (3.000 GB)
11.1 a 11.4	128 GB ou mais em cada nó de armazenamento em qualquer local	4 TB (4.000 GB)

Versão usada para a instalação inicial do StorageGRID	Quantidade de RAM nos nós de armazenamento	Configuração padrão de espaço reservado para metadados
	Menos de 128 GB em qualquer nó de armazenamento em cada local	3 TB (3.000 GB)
11.0 ou anterior	Qualquer quantidade	2 TB (2.000 GB)

Visualizar configuração de espaço reservado de metadados

Siga estas etapas para visualizar a configuração de espaço reservado para metadados do seu sistema StorageGRID.

Passos

1. Selecione **Configuração > Sistema > Configurações de armazenamento**.
2. Na página Configurações de armazenamento, expanda a seção **Espaço reservado para metadados**.

Para StorageGRID 11.8 ou superior, o valor do espaço reservado para metadados deve ser de pelo menos 100 GB e no máximo 1 PB.

A configuração padrão para uma nova instalação do StorageGRID 11.6 ou superior, na qual cada nó de armazenamento possui 128 GB ou mais de RAM, é de 8.000 GB (8 TB).

Espaço reservado real para metadados

Em contraste com a configuração de espaço reservado para metadados em todo o sistema, o espaço reservado real para metadados de objetos é determinado para cada Storage Node. Para qualquer Storage Node, o espaço reservado real para metadados depende do tamanho do volume 0 do nó e da configuração de espaço reservado para metadados em todo o sistema.

Tamanho do volume 0 para o nó	Espaço reservado real para metadados
Menos de 500 GB (uso não produtivo)	10% do volume 0
500 GB ou mais + ou + Nós de armazenamento somente de metadados	O menor desses valores: • Volume 0 • Configuração de espaço reservado para metadados Nota: Apenas um rangedb é necessário para nós de armazenamento somente de metadados.

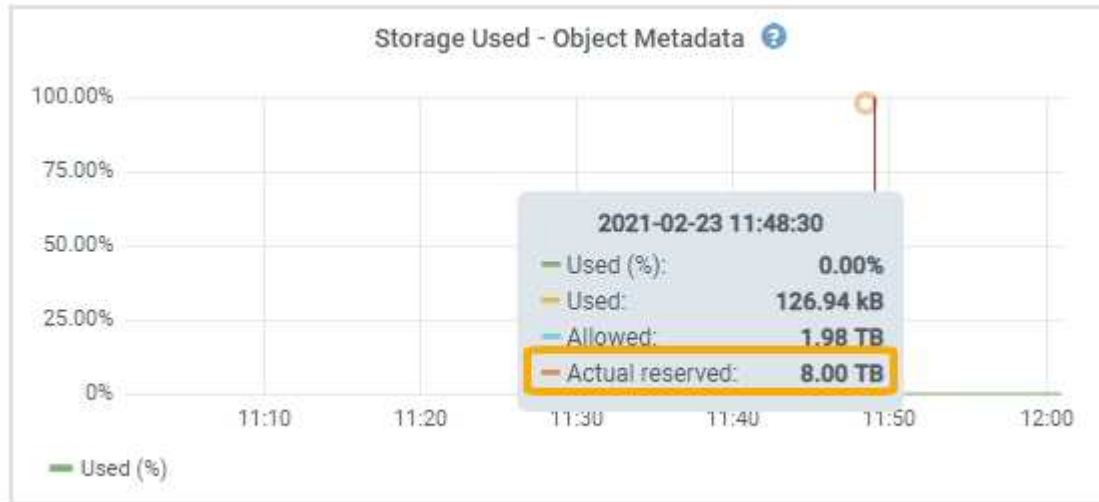
Veja o espaço reservado real para metadados

Siga estes passos para visualizar o espaço reservado para metadados em um determinado Storage Node.

Passos

1. No Gerenciador de Grade, selecione **Nós > Nó de Armazenamento**.
2. Selecione a guia **Storage**.

3. Posicione o cursor sobre o gráfico "Armazenamento Utilizado - Metadados do Objeto" e localize o valor **"Reservado de fato"**.



Na captura de tela, o valor **Reservado real** é 8 TB. Esta captura de tela é de um Storage Node grande em uma nova instalação do StorageGRID 11.6. Como a configuração de espaço reservado para metadados em todo o sistema é menor que o volume 0 para este Storage Node, o espaço reservado real para este nó é igual à configuração de espaço reservado para metadados.

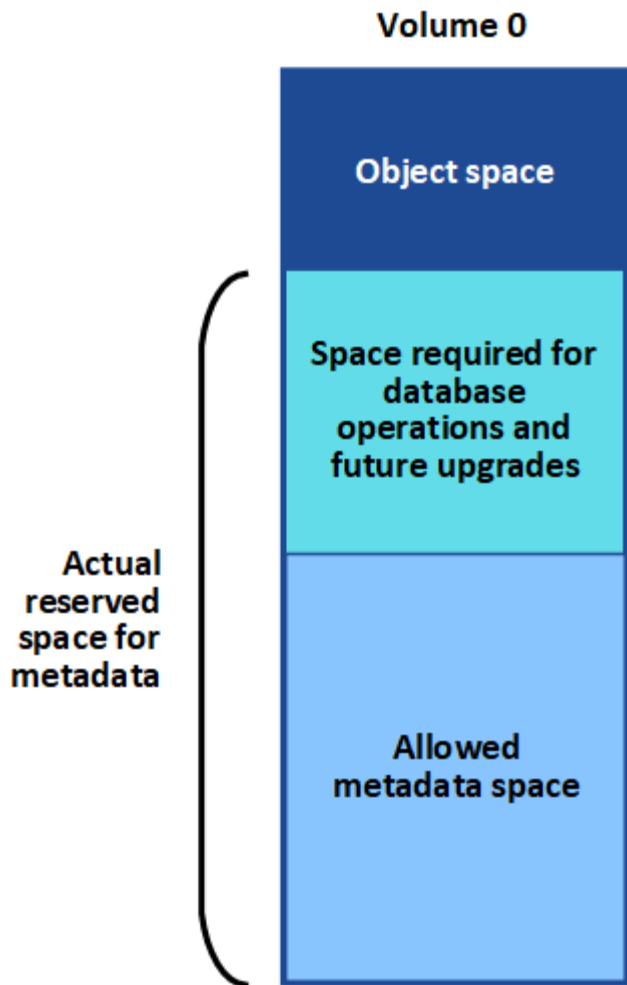
Exemplo de espaço reservado real de metadados

Suponha que você instale um novo sistema StorageGRID usando a versão 11.7 ou posterior. Para este exemplo, suponha que cada Storage Node tenha mais de 128 GB de RAM e que o volume 0 do Storage Node 1 (SN1) tenha 6 TB. Com base nesses valores:

- O **espaço reservado de metadados** em todo o sistema está definido como 8 TB. (Este é o valor padrão para uma nova instalação do StorageGRID 11.6 ou superior se cada Storage Node tiver mais de 128 GB de RAM.)
- O espaço reservado real para metadados no SN1 é de 6 TB. (Todo o volume está reservado porque o volume 0 é menor que a configuração **Espaço reservado para metadados**.)

Espaço de metadados permitido

O espaço reservado real de cada Storage Node para metadados é subdividido no espaço disponível para metadados de objeto (o *espaço de metadados permitido*) e no espaço necessário para operações essenciais do banco de dados (como compactação e reparo) e upgrades futuros de hardware e software. O espaço de metadados permitido controla a capacidade geral de objetos.



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 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

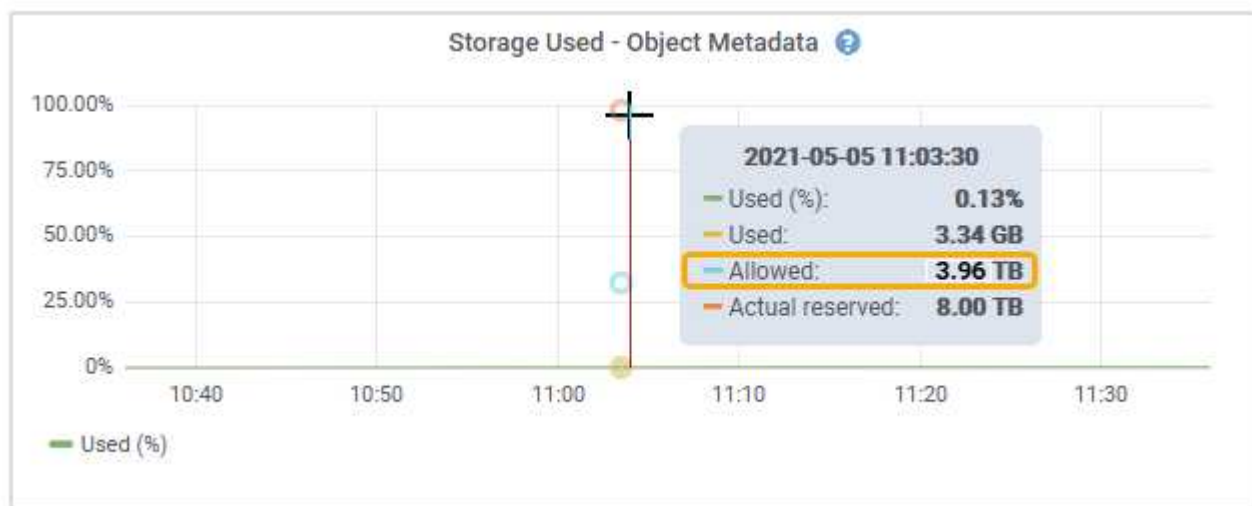
Exibir espaço de metadados permitido

Siga estas etapas para visualizar o espaço de metadados permitido para um Storage Node.

Passos

1. No Gerenciador de Grade, selecione **Nós**.

2. Selecione o nó de armazenamento.
3. Selecione a guia **Storage**.
4. Posicione o cursor sobre o gráfico "Storage used - object metadata" e localize o valor **Allowed**.



Na captura de tela, o valor **Permitido** é 3,96 TB, que é o valor máximo para um Storage Node cujo espaço reservado para metadados é superior a 4 TB.

O valor **Permitido** corresponde a esta métrica do Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemplo de espaço de metadados permitido

Suponha que você instale um StorageGRID usando a versão 11.6. Para este exemplo, considere que cada Storage Node possui mais de 128 GB de RAM e que o volume 0 do Storage Node 1 (SN1) tem 6 TB. Com base nesses valores:

- O **espaço reservado de metadados** em todo o sistema está definido para 8 TB. (Este é o valor padrão para o StorageGRID 11.6 ou superior quando cada Storage Node tem mais de 128 GB de RAM.)
- O espaço reservado real para metadados no SN1 é de 6 TB. (Todo o volume está reservado porque o volume 0 é menor que a configuração **Espaço reservado para metadados**.)
- O espaço permitido para metadados no SN1 é de 3 TB, com base no cálculo mostrado na [tabela de espaço permitido para metadados](#): (espaço reservado para metadados – 1 TB) × 60%, até um máximo de 3,96 TB.

Como os nós de armazenamento de diferentes tamanhos afetam a capacidade de objetos

Conforme descrito acima, StorageGRID distribui uniformemente os metadados de objetos entre os Storage Nodes em cada site. Por esse motivo, se um site contiver Storage Nodes de tamanhos diferentes, o menor node do site determinará a capacidade de metadados do site.

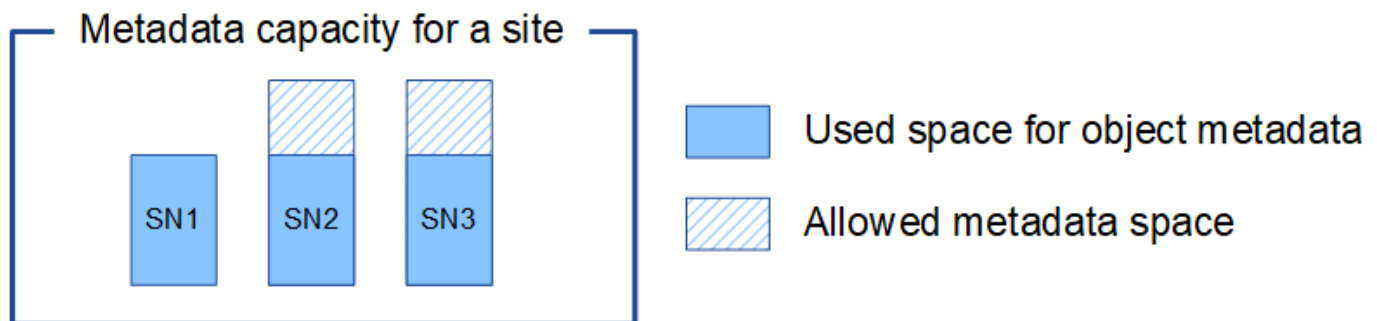
Considere o seguinte exemplo:

- Você possui uma grid de site único contendo três Storage Nodes de tamanhos diferentes.
- A configuração **Espaço reservado para metadados** é de 4 TB.

- Os nós de armazenamento possuem os seguintes valores para o espaço de metadados reservado real e o espaço de metadados permitido.

Nó de armazenamento	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 entre os Storage Nodes em um site, cada nó neste exemplo pode armazenar apenas 1,32 TB de metadados. Os 0,66 TB adicionais de espaço de metadados permitido para SN2 e SN3 não podem ser usados.



Da mesma forma, como o StorageGRID mantém todos os metadados de objetos de um sistema StorageGRID em cada site, a capacidade geral de metadados de um sistema StorageGRID é determinada pela capacidade de metadados de objetos do menor site.

E como a capacidade de metadados do objeto controla a quantidade máxima de objetos, quando um nó fica sem capacidade de metadados, a grid fica efetivamente cheia.

Informações relacionadas

- Para aprender como monitorar a capacidade de metadados de objetos para cada Storage Node, consulte as instruções para ["Monitorando o StorageGRID"](#).
- Para aumentar a capacidade de metadados de objetos do seu sistema, ["expandir uma grid"](#) adicione novos Storage Nodes.

Aumente a configuração de Espaço Reservado para Metadados no StorageGRID

Você poderá aumentar a configuração de Espaço Reservado para Metadados se seus nós de armazenamento atenderem a requisitos específicos de RAM e espaço disponível.

O que você vai precisar

- Você está conectado ao Grid Manager usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root ou permissão de outra configuração da grid"](#).

Sobre esta tarefa

Você pode aumentar manualmente a configuração de Espaço Reservado para Metadados em todo o sistema

para até 8 TB.

Você só pode aumentar o valor da configuração de Espaço Reservado para Metadados em todo o sistema se ambas as afirmações a seguir forem verdadeiras:

- Os nós de armazenamento em qualquer site do seu sistema possuem 128 GB ou mais de RAM.
- Os nós de armazenamento em qualquer site do seu sistema têm espaço disponível suficiente no volume de armazenamento 0.

Tenha em mente que, ao aumentar essa configuração, você reduzirá simultaneamente o espaço disponível para storage de objetos no volume de armazenamento 0 de todos os Storage Nodes. Por esse motivo, talvez seja melhor definir o Espaço Reservado para Metadados para um valor inferior a 8 TB, com base nos seus requisitos esperados de metadados de objetos.



Em geral, é melhor usar um valor mais alto do que um valor mais baixo. Se a configuração de Espaço Reservado para Metadados for muito grande, você pode diminuí-la depois. Por outro lado, se você aumentar o valor depois, o sistema pode precisar mover dados de objetos para liberar espaço.

Para uma explicação detalhada de como a configuração Espaço Reservado para Metadados afeta o espaço permitido para armazenamento de metadados de objetos em um determinado Storage Node, consulte ["Gerencie o armazenamento de metadados de objetos"](#).

Passos

1. Determine a configuração atual de Espaço Reservado para Metadados.
 - a. Selecione **Configuração > Sistema > Configurações de armazenamento**.
 - b. Observe o valor de **Espaço Reservado para Metadados**.
2. Certifique-se de que você tem espaço disponível suficiente no volume de armazenamento 0 de cada Storage Node para aumentar esse valor.
 - a. Selecione **Nós**.
 - b. Selecione o primeiro nó de armazenamento na grid.
 - c. Selecione a guia Armazenamento.
 - d. Na seção Volumes, localize a entrada **/var/local/rangedb/0**.
 - e. Confirme que o valor Disponível é igual ou maior que a diferença entre o novo valor que você deseja usar e o valor atual do Espaço Reservado para Metadados.

Por exemplo, se a configuração de Espaço Reservado para Metadados estiver atualmente em 4 TB e você quiser aumentá-la para 6 TB, o valor Disponível deve ser de 2 TB ou superior.

- f. Repita estas etapas para todos os Storage Nodes.
 - Se um ou mais nós de armazenamento não tiverem espaço disponível suficiente, o valor de Espaço Reservado para Metadados não poderá ser aumentado. Não prossiga com este procedimento.
 - Se cada nó de armazenamento tiver espaço disponível suficiente no volume 0, passe para a próxima etapa.
3. Certifique-se de ter pelo menos 128 GB de RAM em cada Storage Node.
 - a. Selecione **Nós**.

- b. Selecione o primeiro nó de armazenamento na grid.
 - c. Selecione a guia **Hardware**.
 - d. Posicione o cursor sobre o gráfico de Uso de Memória. Certifique-se de que a **Memória Total** seja de pelo menos 128 GB.
 - e. Repita estas etapas para todos os Storage Nodes.
 - Se um ou mais nós de armazenamento não tiverem memória total disponível suficiente, o valor do Espaço Reservado para Metadados não poderá ser aumentado. Não prossiga com este procedimento.
 - Se cada nó de armazenamento tiver pelo menos 128 GB de memória total, vá para a próxima etapa.
4. Atualize a configuração de Espaço Reservado para Metadados.
- a. Selecione **Configuração > Sistema > Configurações de armazenamento**.
 - b. Selecione **Espaço Reservado para Metadados**.
 - c. Insira o novo valor.
- Por exemplo, para inserir 8 TB, que é o valor máximo suportado, digite **8000000000000** (8, seguido de 12 zeros)
- d. Selecione **Salvar**.

Compactar objetos armazenados no StorageGRID

Você pode habilitar a compactação de objetos para reduzir o tamanho dos objetos armazenados no StorageGRID, para que os objetos consumam menos armazenamento.

Antes de começar

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

Sobre esta tarefa

Por padrão, a compressão de objetos está desativada. Se você ativar a compressão, StorageGRID tenta comprimir cada objeto ao salvá-lo, usando compressão sem perdas.



Se você alterar essa configuração, levará cerca de um minuto para que a nova configuração seja aplicada. O valor configurado é armazenado em cache para desempenho e escalabilidade.

Antes de ativar a compactação de objetos, esteja ciente do seguinte:

- Você não deve selecionar **Comprimir objetos armazenados** a menos que saiba que os dados armazenados são compressíveis.
- Aplicações que salvam objetos no StorageGRID podem compactar os objetos antes de salvá-los. Se um aplicativo cliente já tiver compactado um objeto antes de salvá-lo no StorageGRID, selecionar esta opção não reduzirá ainda mais o tamanho do objeto.
- Não selecione **Comprimir objetos armazenados** se você estiver usando NetApp FabricPool com StorageGRID.
- Se a opção **Comprimir objetos armazenados** estiver selecionada, os aplicativos cliente do S3 devem evitar realizar operações GetObject que especifiquem um intervalo de bytes a ser retornado. Essas

operações de "leitura de intervalo" são ineficientes porque o StorageGRID precisa descompactar os objetos para acessar os bytes solicitados. Operações GetObject 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 de um objeto compactado de 50 GB.

Se intervalos forem lidos 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 do aplicativo.

Passos

1. Selecione **Configuração > Sistema > Configurações de armazenamento > Compressão de objetos**.
2. Selecione a caixa de seleção **Comprimir objetos armazenados**.
3. Selecione **Salvar**.

Gerencie nós de armazenamento completos no StorageGRID

À medida que os nós de armazenamento atingem a capacidade, você deve expandir o sistema StorageGRID por meio da adição de novo storage. Existem três opções disponíveis: adicionar volumes de storage, adicionar prateleiras de expansão de storage e adicionar nós de armazenamento.

Adicionar volumes de storage

Cada Storage Node suporta um número máximo de volumes de storage. O máximo definido varia de acordo com a plataforma. Se um Storage Node contiver menos do que o número máximo de volumes de storage, você pode adicionar volumes para aumentar sua capacidade. Veja as instruções para ["Expandindo um sistema StorageGRID"](#).

Adicionar prateleiras de expansão de storage

Alguns StorageGRID appliance Storage Nodes, como o SG6060 ou o SG6160, podem suportar prateleiras de armazenamento adicionais. Se você tiver StorageGRID appliances com capacidade de expansão que ainda não foram expandidos ao máximo, pode adicionar prateleiras de armazenamento para aumentar a capacidade. Consulte as instruções para ["Expandindo um sistema StorageGRID"](#).

Adicionar nós de armazenamento

Você pode aumentar a capacidade de storage adicionando Storage Nodes. Ao adicionar storage, é necessário considerar cuidadosamente as regras ILM ativas e os requisitos de capacidade. Consulte as instruções para ["Expandindo um sistema StorageGRID"](#).

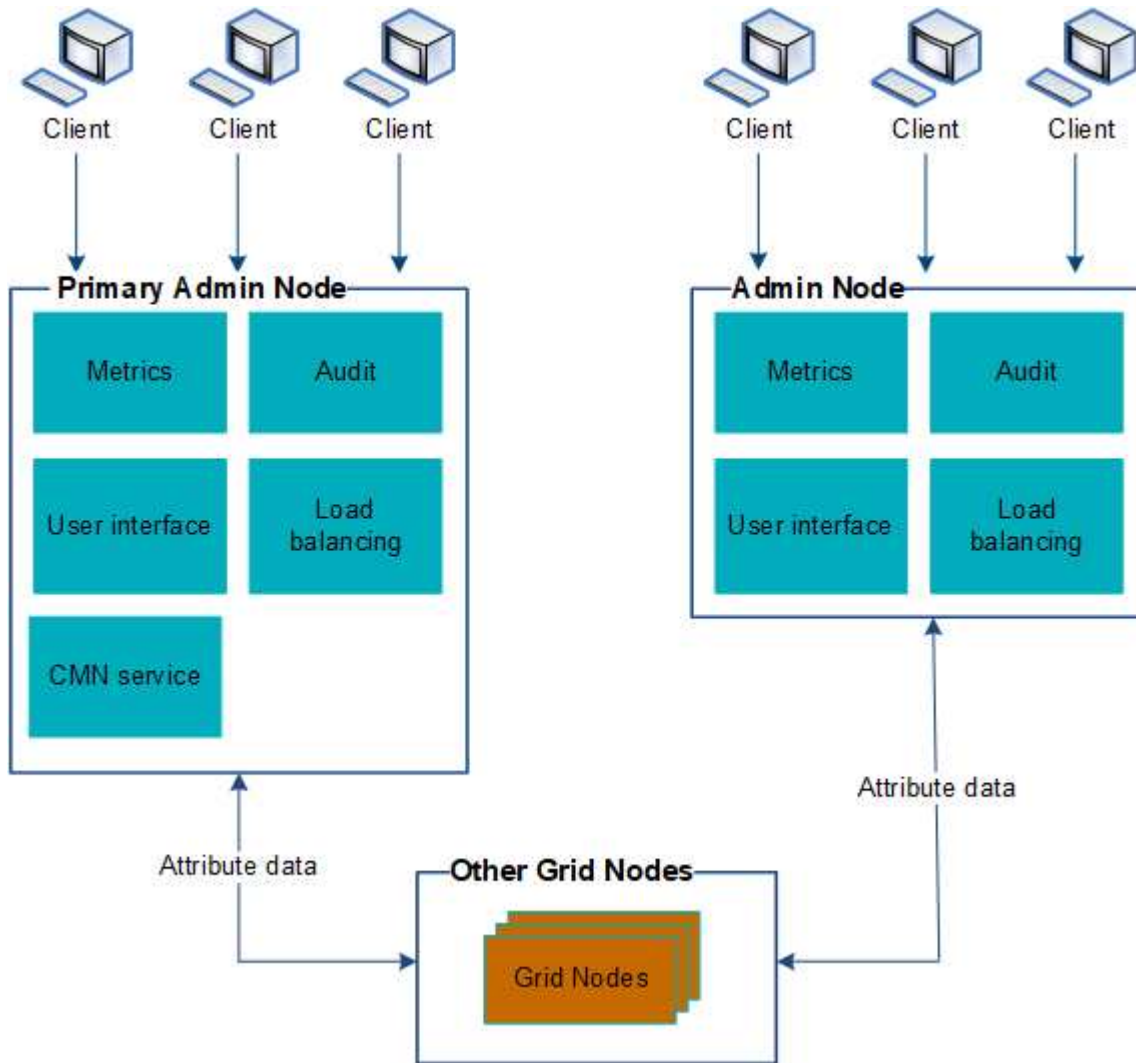
Gerenciar nós de administração

Use vários nós de administração no StorageGRID

Um sistema StorageGRID pode incluir vários nós de administração para que você possa monitorar e configurar seu sistema StorageGRID continuamente, mesmo que um nó de administração falhe.

Se um nó administrativo ficar indisponível, o processamento de atributos continua, os alertas ainda são

acionados e as notificações por e-mail e os pacotes AutoSupport ainda são enviados. No entanto, ter vários nós administrativos não oferece proteção contra falhas, exceto para notificações e pacotes AutoSupport.



Existem duas opções para continuar a visualizar e configurar o sistema StorageGRID caso um nó de administração falhe:

- Os clientes web podem se reconectar a qualquer outro Admin Node disponível.
- Se um administrador do sistema tiver configurado um grupo de alta disponibilidade de Nós de Administração, os clientes web podem continuar a acessar o Grid Manager ou o Tenant Manager usando o endereço IP virtual do grupo de alta disponibilidade. Consulte ["Gerenciar grupos de alta disponibilidade"](#).



Ao usar um grupo de alta disponibilidade (HA), o acesso é interrompido se o nó de administração ativo falhar. Os usuários precisam fazer login novamente depois que o endereço IP virtual do grupo HA for transferido para outro nó de administração do grupo.

Algumas tarefas de manutenção só podem ser realizadas usando o nó de administração primário. Se o nó de administração primário falhar, ele deverá ser recuperado antes que o sistema StorageGRID volte a funcionar plenamente.

Identifique o nó de administração principal no StorageGRID

O nó de administração principal oferece mais funcionalidades do que os nós de administração não principais. Por exemplo, alguns procedimentos de manutenção devem ser realizados usando o nó de administração principal.

Para obter mais informações sobre nós de administração, consulte ["O que é um nó de administração"](#).

Antes de começar

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

Passos

1. Selecione **Nós**.
2. Digite **principal** na caixa de pesquisa.

Nos resultados da pesquisa, identifique o nó com "Primary Admin Node" exibido na coluna Tipo. Um Primary Admin Node deve ser listado.

Gerencie objetos com ILM

Gerencie objetos com ILM no StorageGRID

As regras de gerenciamento do ciclo de vida das informações (ILM) em uma política de ILM instruem o StorageGRID sobre como criar e distribuir cópias dos dados de objetos e como gerenciar essas cópias ao longo do tempo.

Sobre estas instruções

Projetar e implementar regras e políticas de ILM exige um planejamento cuidadoso. Você deve compreender seus requisitos operacionais, a topologia do seu sistema StorageGRID, suas necessidades de proteção de objetos e os tipos de storage disponíveis. Depois, você deve determinar como deseja que diferentes tipos de objetos sejam copiados, distribuídos e armazenados.

Use estas instruções para:

- Saiba mais sobre StorageGRID ILM, incluindo ["Como o ILM opera ao longo da vida útil de um objeto"](#).
- Aprenda como configurar ["pools de storage"](#), ["Pools de storage em nuvem"](#) e ["Regras do ILM"](#).
- Aprenda como ["criar, simular e ativar uma política ILM"](#) proteger os dados de objetos em um ou mais sites.
- Aprenda como ["Gerencie objetos com S3 Object Lock"](#), o que ajuda a garantir que objetos em buckets específicos do S3 não sejam excluídos ou sobrescritos por um período de tempo determinado.

Saiba mais

Para saber mais, confira estes vídeos:

[Visão geral das regras do ILM](#)

[Visão geral das políticas do ILM](#)

ILM e ciclo de vida de objetos

Como o ILM opera ao longo do ciclo de vida de um objeto no StorageGRID

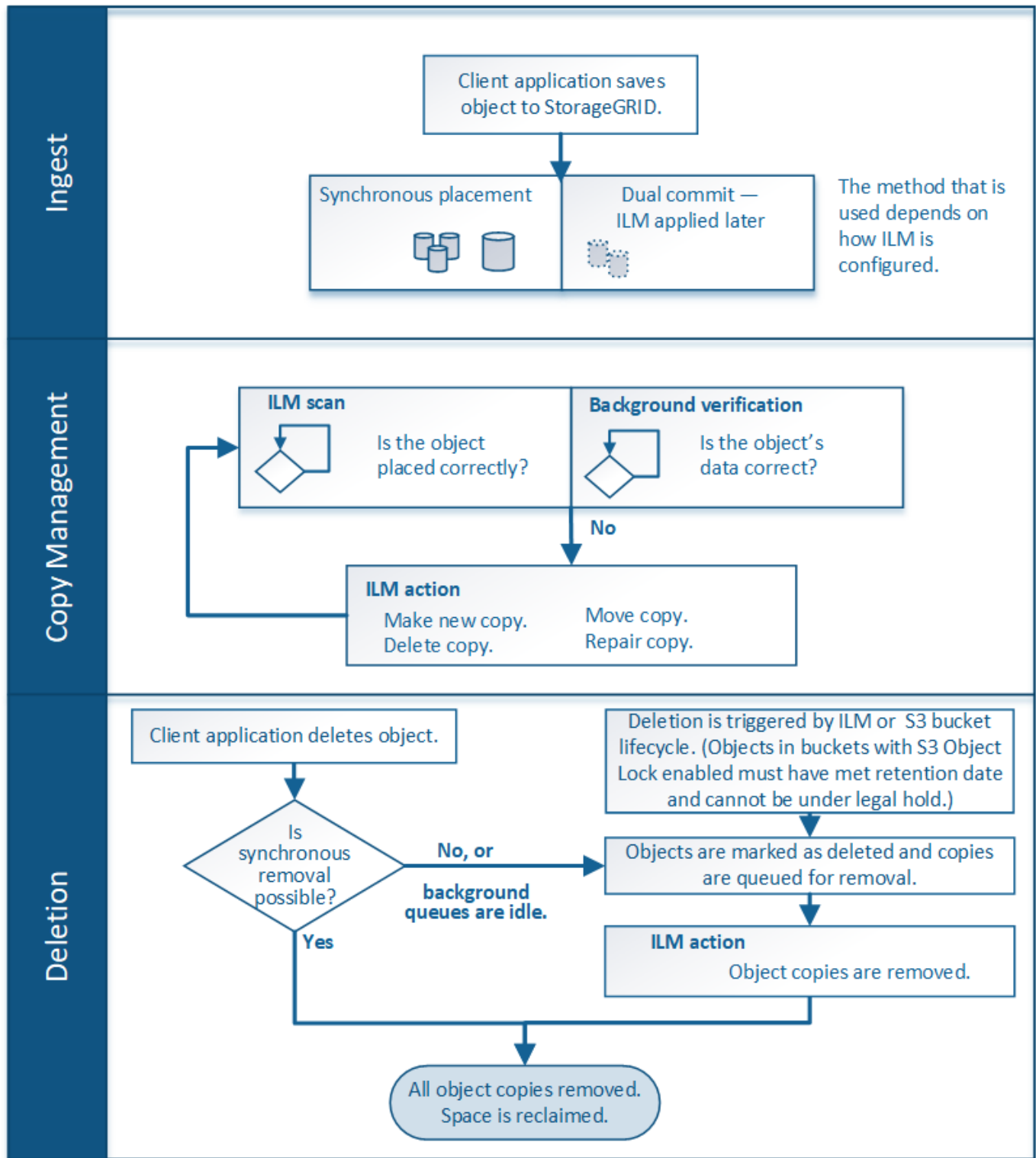
Compreender como StorageGRID usa o ILM para gerenciar objetos em cada etapa do seu ciclo de vida pode ajudar você a criar uma política mais eficaz.

- **Ingestão:** A ingestão começa quando um aplicativo cliente S3 estabelece uma conexão para salvar um objeto no sistema StorageGRID e é concluída quando o StorageGRID retorna uma mensagem de "ingestão bem-sucedida" para o cliente. Os dados do objeto são protegidos durante a ingestão, seja aplicando instruções de ILM imediatamente (posicionamento síncrono) ou criando cópias intermediárias e aplicando o ILM posteriormente (confirmação dupla), dependendo de como os requisitos de ILM foram especificados.
- **Gerenciamento de cópias:** Após criar o número e o tipo de cópias de objetos especificados nas instruções de posicionamento do ILM, StorageGRID gerencia os locais dos objetos e os protege contra perda.
 - **Verificação e avaliação do ILM:** StorageGRID verifica continuamente a lista de objetos armazenados na grid e verifica se as cópias atuais atendem aos requisitos do ILM. Quando são necessários diferentes tipos, números ou locais de cópias de objetos, StorageGRID cria, exclui ou move cópias conforme necessário.
 - **Verificação em segundo plano:** StorageGRID realiza verificações contínuas em segundo plano para verificar a integridade dos dados do objeto. Se um problema for encontrado, StorageGRID cria automaticamente uma nova cópia do objeto ou um fragmento de objeto com codificação de apagamento em um local que atenda aos requisitos atuais do ILM. Consulte ["Verificar integridade do objeto"](#).
- **Exclusão de objeto:** O gerenciamento de um objeto termina quando todas as cópias são removidas do sistema StorageGRID. Os objetos podem ser removidos como resultado de uma solicitação de exclusão feita por um cliente, ou como resultado da exclusão pelo ILM ou da exclusão causada pela expiração do ciclo de vida do bucket S3.



Os objetos em um bucket com o S3 Object Lock ativado não podem ser excluídos se estiverem sob guarda legal ou se uma data de retenção tiver sido especificada, mas ainda não tiver sido atingida.

O diagrama resume como o ILM opera ao longo do ciclo de vida de um objeto.



Como os objetos são ingeridos

Opções de ingestão de ILM no StorageGRID

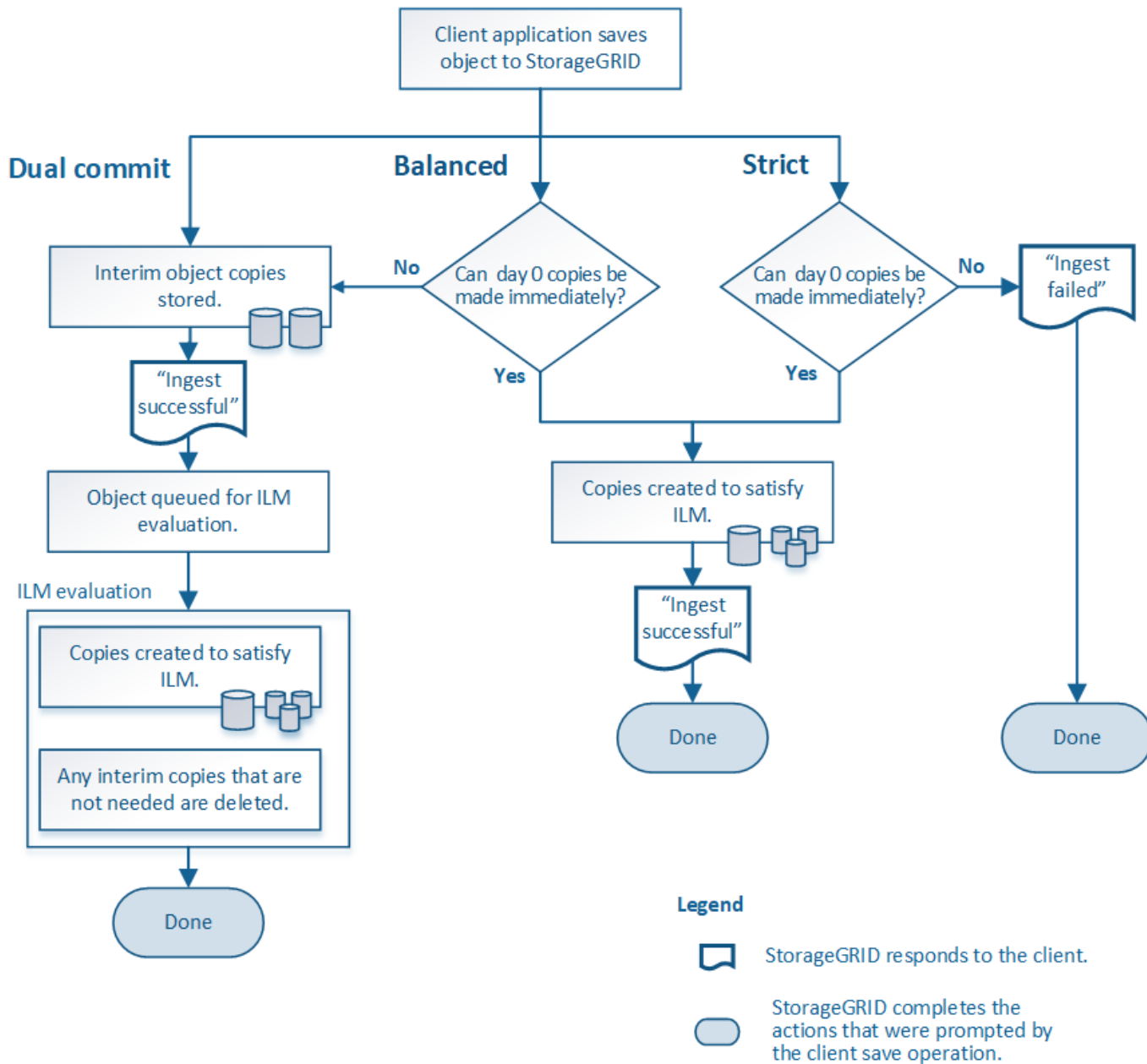
Ao criar uma regra ILM, você especifica uma das três opções para proteger objetos na ingestão: dual commit, strict ou balanced.

Dependendo da sua escolha, StorageGRID cria cópias provisórias e enfileira os objetos para avaliação do ILM

posteriormente, ou utiliza o posicionamento síncrono e cria cópias imediatamente para atender aos requisitos do ILM.

Fluxograma das opções de ingestão

O fluxograma mostra o que acontece quando os objetos são correspondidos por uma regra ILM que usa cada uma das três opções de ingest.



Commit duplo

Ao selecionar a opção Dual commit, StorageGRID cria imediatamente cópias provisórias do objeto em dois nós de armazenamento diferentes e retorna uma mensagem de "ingest successful" para o cliente. O objeto é enfileirado para avaliação do ILM e as cópias que atendem às instruções de posicionamento da regra são criadas posteriormente. Se a política do ILM não puder ser processada imediatamente após o dual commit, a proteção contra perda de site pode levar algum tempo para ser alcançada.

Utilize a opção de confirmação dupla em qualquer um destes casos:

- Você está usando regras ILM em vários sites e a latência de ingestão do cliente é sua principal consideração. Ao usar o Dual commit, você deve garantir que seu grid possa executar o trabalho adicional de criar e remover as cópias de dual commit caso elas não atendam ao ILM. Especificamente:
 - A carga na grid deve ser suficientemente baixa para evitar um backlog de ILM.
 - A rede deve ter recursos de hardware excedentes (IOPS, CPU, memória, largura de banda, e assim por diante).
- Você está usando regras ILM em vários sites e a conexão WAN entre os sites geralmente apresenta alta latência ou largura de banda limitada. Nesse cenário, usar a opção Dual commit pode ajudar a evitar timeouts do cliente. Antes de escolher a opção Dual commit, você deve testar o aplicativo cliente com cargas de trabalho realistas.

Equilibrado (padrão)

Ao selecionar a opção Balanceada, StorageGRID também usa o posicionamento síncrono na ingestão e cria imediatamente todas as cópias especificadas nas instruções de posicionamento da regra. Em contraste com a opção Estrita, se StorageGRID não puder criar imediatamente todas as cópias, ele usa o Dual commit. Se a política ILM usar posicionamentos em vários sites e a proteção imediata contra perda de site não puder ser alcançada, o alerta **ILM placement unachievable** será acionado.

Use a opção Balanced para obter a melhor combinação de proteção de dados, desempenho do grid e sucesso na ingestão. Balanced é a opção padrão no assistente Criar regra ILM.

Estrito

Ao selecionar a opção Estrita, StorageGRID usa o posicionamento síncrono na ingestão e cria imediatamente todas as cópias de objetos especificadas nas instruções de posicionamento da regra. A ingestão falha se StorageGRID não conseguir criar todas as cópias, por exemplo, porque um local de storage necessário está temporariamente indisponível. O cliente deve tentar a operação novamente.

Use a opção Estrita se você tiver um requisito operacional ou regulamentar para armazenar objetos imediatamente apenas nos locais definidos na regra ILM. Por exemplo, para atender a um requisito regulamentar, você pode precisar usar a opção Estrita e um filtro avançado de Restrição de Localização para garantir que os objetos nunca sejam armazenados em determinados data centers.

Consulte ["Exemplo 5: regras e política do ILM para comportamento de ingestão estrito"](#).

Vantagens, desvantagens e limitações das opções de ingest de ILM no StorageGRID

Compreender as vantagens e desvantagens de cada uma das três opções para proteger os dados na ingestão (Balanced, Strict ou Dual commit) pode ajudar você a decidir qual selecionar para uma regra ILM.

Para uma visão geral das opções de ingestão, consulte ["Opções de ingestão"](#).

Vantagens das opções Equilibrada e Rigorosa

Em comparação com o Dual commit, que cria cópias provisórias durante a ingestão, as duas opções de posicionamento síncrono podem oferecer as seguintes vantagens:

- **Maior segurança de dados:** Os dados do objeto são protegidos imediatamente, conforme especificado nas instruções de posicionamento da regra ILM, que podem ser configuradas para proteger contra uma ampla variedade de condições de falha, incluindo a falha de mais de um local de storage. O commit duplo só pode proteger contra a perda de uma única cópia local.

- **Operação de grid mais eficiente:** Cada objeto é processado apenas uma vez, no momento da ingestão. Como o sistema StorageGRID não precisa rastrear ou excluir cópias intermediárias, há menos carga de processamento e menos espaço de banco de dados consumido.
- **(Balanced) Recomendado:** A opção Balanced oferece eficiência ideal do ILM. Recomenda-se o uso da opção Balanced, a menos que seja necessário um comportamento de ingest estrito ou que o grid atenda a todos os critérios para usar o Dual commit.
- **Certeza (estrita) sobre a localização dos objetos:** A opção Strict garante que os objetos sejam armazenados imediatamente de acordo com as instruções de posicionamento na regra ILM.

Desvantagens das opções Equilibrada e Rigorosa

Em comparação com o Dual commit, as opções Balanced e Strict apresentam algumas desvantagens:

- **Ingestão mais demorada por parte do cliente:** A latência de ingestão por parte do cliente pode ser maior. Ao usar as opções Balanced ou Strict, uma mensagem de "ingestão bem-sucedida" não é retornada ao cliente até que todos os fragmentos de codificação de apagamento ou cópias replicadas sejam criados e armazenados. No entanto, os dados do objeto provavelmente chegarão ao seu destino final muito mais rapidamente.
- **(Estrito) Taxas mais altas de falha na ingestão:** Com a opção Estrito, a ingestão falha sempre que StorageGRID não consegue fazer imediatamente todas as cópias especificadas na regra ILM. Você pode observar altas taxas de falha na ingestão se um local de storage necessário estiver temporariamente offline ou se problemas de rede causarem atrasos na cópia de objetos entre sites.
- **(Estrito) Em algumas circunstâncias, o posicionamento dos uploads multipartes no S3 pode não ser o esperado:** Com o modo Estrito, você espera que os objetos sejam posicionados conforme descrito pela regra ILM ou que a ingestão falhe. No entanto, em um upload multipartes no S3, o ILM é avaliado para cada parte do objeto à medida que é ingerida e para o objeto como um todo quando o upload multipartes é concluído. Nas seguintes circunstâncias, isso pode resultar em posicionamentos diferentes do que você espera:
 - **Se o ILM for alterado durante um upload multipart do S3:** Como cada parte é posicionada de acordo com a regra ativa no momento da ingestão, algumas partes do objeto podem não atender aos requisitos atuais do ILM quando o upload multipart for concluído. Nesses casos, a ingestão do objeto não falha. Em vez disso, qualquer parte que não esteja posicionada corretamente é enfileirada para reavaliação do ILM e movida para o local correto posteriormente.
 - **Quando as regras do ILM filtram por tamanho:** Ao avaliar o ILM para uma parte, StorageGRID filtra pelo tamanho da parte, não pelo tamanho do objeto. Isso significa que partes de um objeto podem ser armazenadas em locais que não atendem aos requisitos do ILM para o objeto como um todo. Por exemplo, se uma regra especificar que todos os objetos com 10 GB ou mais sejam armazenados no DC1, enquanto todos os objetos menores sejam armazenados no DC2, na ingestão cada parte de 1 GB de um upload multipart de 10 partes é armazenada no DC2. Quando o ILM é avaliado para o objeto, todas as partes do objeto são movidas para o DC1.
- **(Estrito) A ingestão não falha quando as tags ou metadados são atualizados e os novos posicionamentos necessários não podem ser feitos:** Com o modo Estrito, você espera que os objetos sejam posicionados conforme descrito pela regra ILM ou que a ingestão falhe. No entanto, ao atualizar metadados ou tags de um objeto já armazenado na grid, o objeto não é reingerido. Isso significa que quaisquer alterações no posicionamento do objeto acionadas pela atualização não são feitas imediatamente. As alterações de posicionamento são feitas quando o ILM é reavaliado pelos processos normais de ILM em segundo plano. Se as alterações de posicionamento necessárias não puderem ser feitas (por exemplo, porque um novo local necessário não está disponível), o objeto atualizado mantém seu posicionamento atual até que as alterações de posicionamento sejam possíveis.

Limitações no posicionamento de objetos com as opções **Balanced** e **Strict**

As opções **Equilibrado** ou **Rigorous** não podem ser usadas para regras ILM que tenham alguma destas instruções de posicionamento:

- Alocação em um pool de storage em nuvem no dia 0.
- Posicionamentos em um pool de storage em nuvem quando a regra tem um horário de criação definido pelo usuário como horário de referência.

Essas restrições existem porque StorageGRID não consegue fazer cópias síncronas para um Cloud Storage Pool, e um horário de criação definido pelo usuário pode ser resolvido para o presente.

Como as regras do ILM e a consistência interagem para afetar a proteção de dados

Tanto a sua regra ILM quanto a sua escolha de consistência afetam a forma como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, o comportamento de ingestão selecionado para uma regra ILM afeta o posicionamento inicial das cópias de objetos, enquanto a consistência usada quando um objeto é armazenado afeta o posicionamento inicial dos metadados do objeto. Como StorageGRID requer acesso tanto aos dados quanto aos metadados de um objeto para atender às solicitações do cliente, selecionar níveis de proteção correspondentes para a consistência e o comportamento de ingestão pode proporcionar melhor proteção inicial dos dados e respostas mais previsíveis do sistema.

Segue um breve resumo dos valores de consistência disponíveis no StorageGRID:

- **Todos**: Todos os nós recebem metadados de objeto imediatamente ou a solicitação falhará.
- **Strong-global**: Garante a consistência de leitura após gravação para todas as solicitações do cliente em todos os sites. Quando a semântica de Quorum está configurada, os seguintes comportamentos se aplicam:
 - Permite tolerância a falha do local para solicitações de clientes quando as grades têm três ou mais sites. Grades com dois sites não terão tolerância a falha do local.
 - As seguintes operações do S3 não serão bem-sucedidas com um site inativo:
 - DeleteBucketEncryption
 - PutBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Se necessário, você pode ["configurar a semântica de quorum do StorageGRID para consistência global forte"](#).

- **Strong-site**: os metadados do objeto são distribuídos imediatamente para outros nós no site. Garante a consistência de leitura após gravação para todas as solicitações do cliente dentro de um site.
- **Leitura após nova gravação**: Oferece consistência de leitura após gravação para novos objetos e consistência eventual para atualizações de objetos. Oferece alta disponibilidade e garantias de proteção de dados. Recomendado para a maioria dos casos.

- **Disponível:** Oferece consistência eventual tanto para novos objetos quanto para atualizações de objetos. Para buckets do S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que são lidos raramente ou para operações HEAD ou GET em chaves que não existem). Não é compatível com buckets do S3 FabricPool.



Antes de selecionar um valor de consistência, "[Leia a descrição completa de consistência](#)". Você deve entender os benefícios e as limitações antes de alterar o valor padrão.

Exemplo de como as regras de consistência e ILM podem interagir

Suponha que você tenha uma grade de três sites com a seguinte regra ILM e a seguinte consistência:

- **Regra ILM:** Crie três cópias do objeto, uma no local e uma em cada local remoto. Use o comportamento de ingestão estrito.
- **Consistência:** Global forte (os metadados do objeto são distribuídos imediatamente para vários sites).

Quando um cliente armazena um objeto na grid, StorageGRID cria as três cópias do objeto e distribui os metadados para vários sites antes de retornar sucesso ao cliente.

O objeto fica totalmente protegido contra perda no momento em que a mensagem de ingestão bem-sucedida é recebida. Por exemplo, se o local remoto for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existirão nos locais remotos. O objeto poderá ser recuperado integralmente dos outros locais.

Se, em vez disso, você usasse a mesma regra ILM e a consistência forte do site, o cliente poderia receber uma mensagem de sucesso após os dados do objeto serem replicados para os locais remotos, mas antes que os metadados do objeto fossem distribuídos lá. Nesse caso, o nível de proteção dos metadados do objeto não corresponde ao nível de proteção dos dados do objeto. Se o local remoto for perdido logo após a ingestão, os metadados do objeto serão perdidos. O objeto não pode ser recuperado.

A inter-relação entre as regras de consistência e as regras de ILM pode ser complexa. Entre em contato com a NetApp se você precisar de assistência.

Informações relacionadas

["Exemplo 5: regras e política do ILM para comportamento de ingestão estrito"](#)

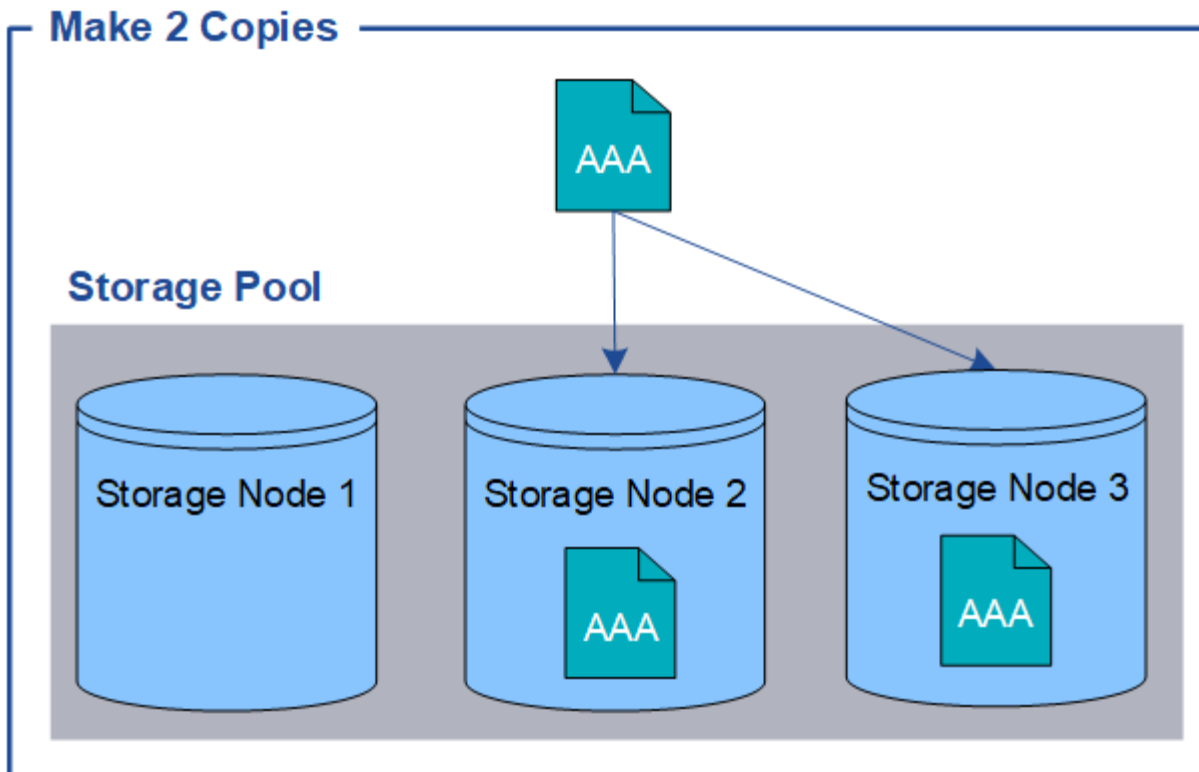
Como os objetos são armazenados (replicação ou codificação de apagamento)

Saiba mais sobre replicação no StorageGRID

A replicação é um dos dois métodos usados pelo StorageGRID para armazenar dados de objetos (codificação de apagamento é o outro método). Quando os objetos correspondem a uma regra ILM que usa replicação, o sistema cria cópias exatas dos dados do objeto e armazena as cópias nos Storage Nodes.

Ao configurar uma regra ILM para criar cópias replicadas, você especifica quantas cópias devem ser criadas, onde essas cópias devem ser colocadas e por quanto tempo as cópias devem ser armazenadas em cada local.

No exemplo a seguir, a regra ILM especifica que duas cópias replicadas de cada objeto sejam colocadas em um pool de storage que contém três Storage Nodes.



Quando StorageGRID encontra objetos que correspondem a esta regra, ele cria duas cópias do objeto, colocando cada cópia em um Storage Node diferente no pool de storage. As duas cópias podem ser colocadas em quaisquer dois dos três Storage Nodes disponíveis. Neste caso, a regra colocou cópias do objeto nos Storage Nodes 2 e 3. Como existem duas cópias, o objeto pode ser recuperado se algum dos nós no pool de storage falhar.



StorageGRID só pode armazenar uma cópia replicada de um objeto em qualquer Storage Node. Se sua grid incluir três Storage Nodes e você criar uma regra ILM de 4 cópias, apenas três cópias serão criadas, uma cópia para cada Storage Node. O alerta **ILM placement unachievable** é acionado para indicar que a regra ILM não pôde ser aplicada completamente.

Informações relacionadas

- ["O que é codificação de apagamento"](#)
- ["O que é um pool de storage"](#)
- ["Habilite a proteção contra perda de site usando replicação e codificação de apagamento"](#)

Riscos da replicação de cópia única no StorageGRID

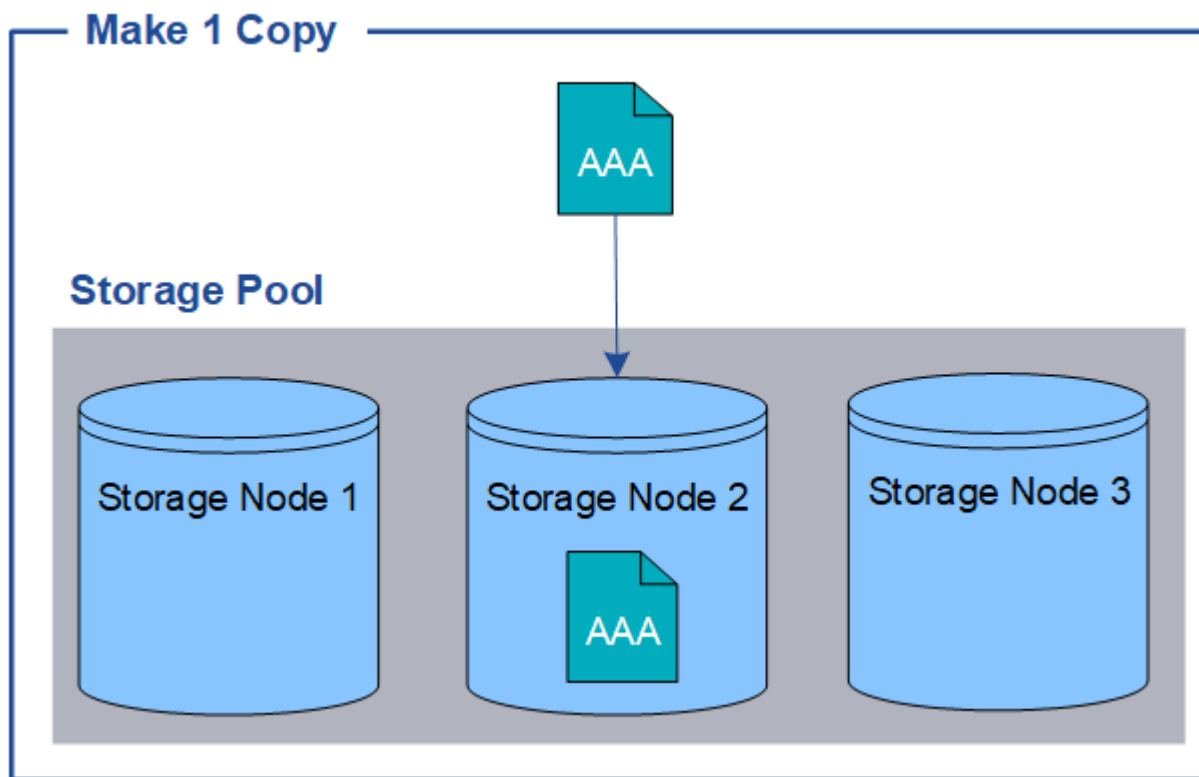
Ao criar uma regra ILM para criar cópias replicadas, você deve sempre especificar pelo menos duas cópias para qualquer período de tempo nas instruções de posicionamento.



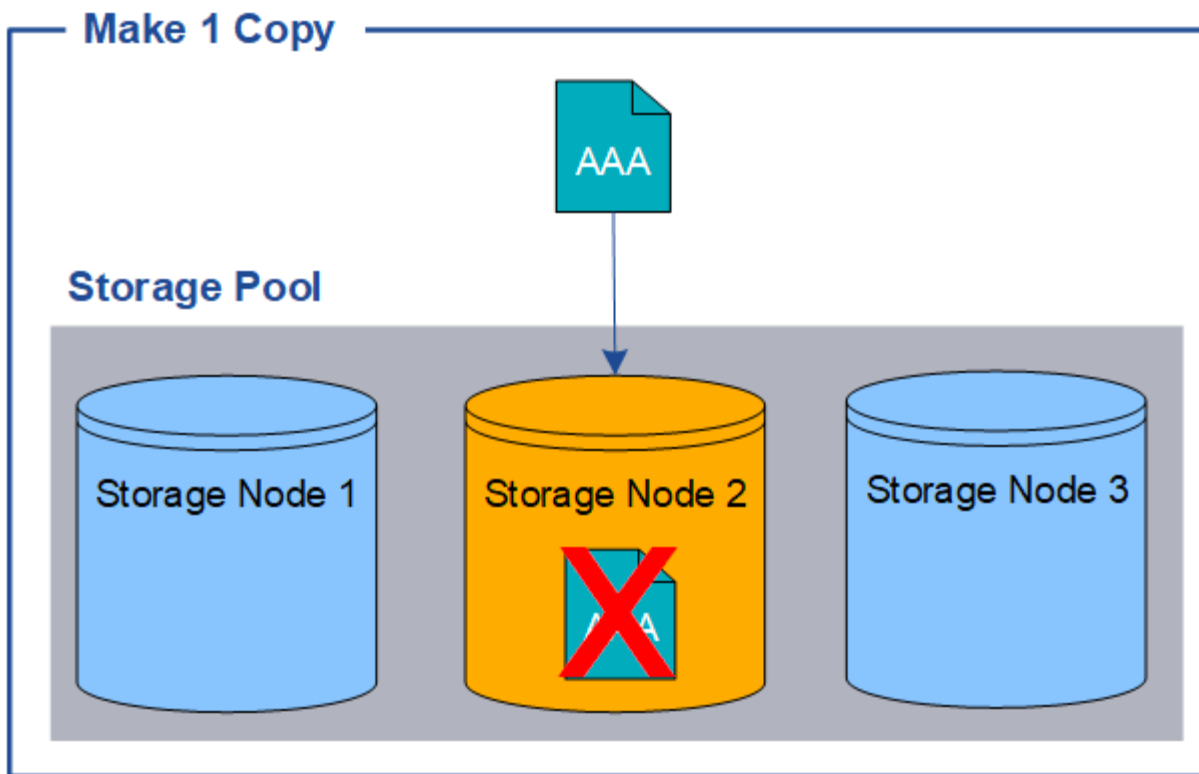
Não utilize uma regra ILM que crie apenas uma cópia replicada para qualquer período de tempo. Se existir apenas uma cópia replicada de um objeto, esse objeto será perdido se um Storage Node falhar ou apresentar um erro significativo. Você também perderá temporariamente o acesso ao objeto durante procedimentos de manutenção, como upgrades.

No exemplo a seguir, a regra ILM "Make 1 Copy" especifica que uma cópia replicada de um objeto seja colocada em um pool de storage que contenha três Storage Nodes. Quando um objeto que corresponde a

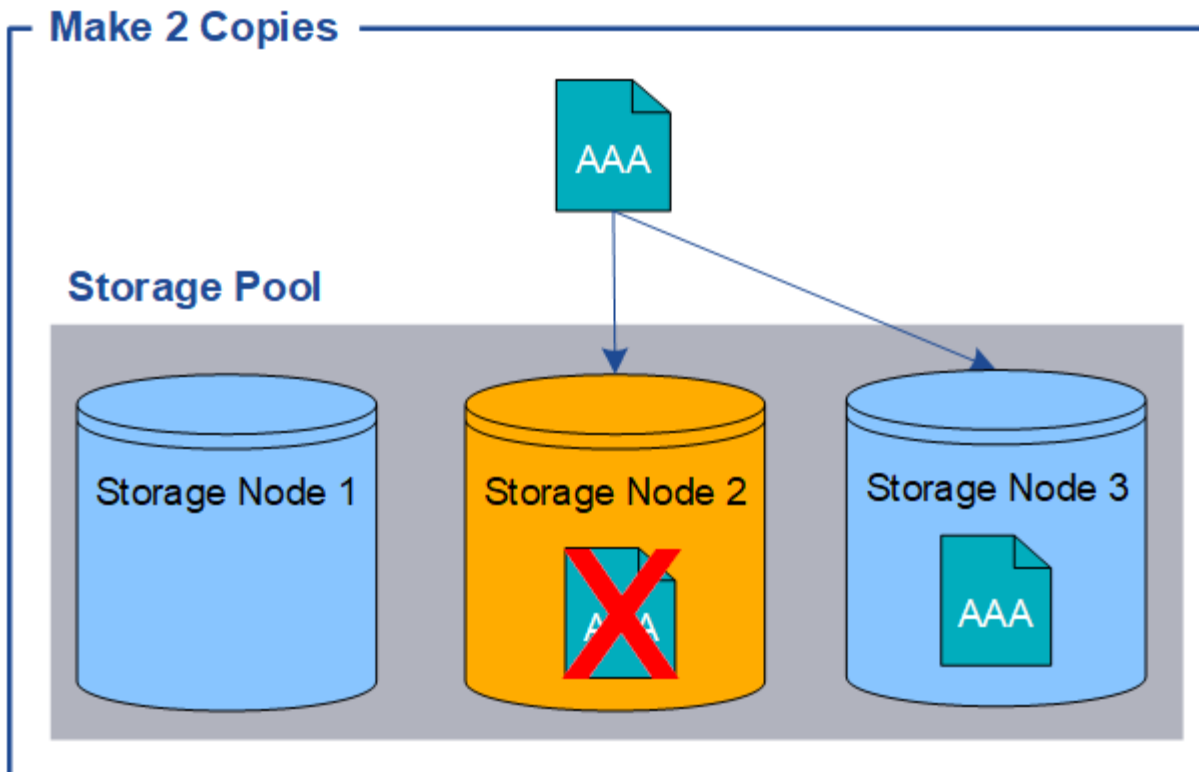
essa regra é ingerido, StorageGRID coloca uma única cópia em apenas um Storage Node.



Quando uma regra ILM cria apenas uma cópia replicada de um objeto, o objeto fica inacessível quando o Storage Node está indisponível. Neste exemplo, você perderá temporariamente o acesso ao objeto AAA sempre que o Storage Node 2 estiver offline, como durante uma atualização ou outro procedimento de manutenção. Você perderá o objeto AAA completamente se o Storage Node 2 falhar.



Para evitar a perda de dados de objetos, você deve sempre criar pelo menos duas cópias de todos os objetos que deseja proteger com replicação. Se existirem duas ou mais cópias, você ainda pode acessar o objeto se um Storage Node falhar ou ficar offline.



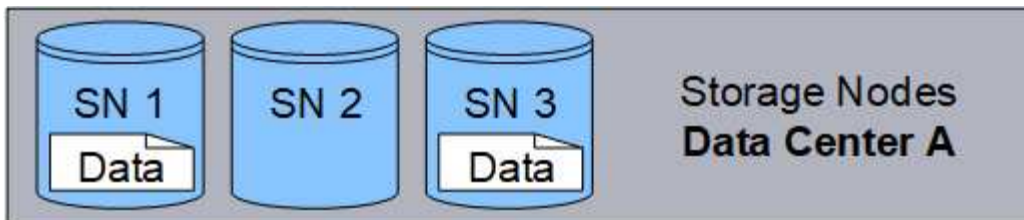
Saiba mais sobre codificação de apagamento no StorageGRID

A codificação de apagamento é um dos dois métodos que o StorageGRID usa para armazenar dados de objetos (a replicação é o outro método). Quando os objetos correspondem a uma regra ILM que usa codificação de apagamento, esses objetos são divididos em fragmentos de dados, fragmentos de paridade adicionais são calculados e cada fragmento é armazenado em um Storage Node diferente.

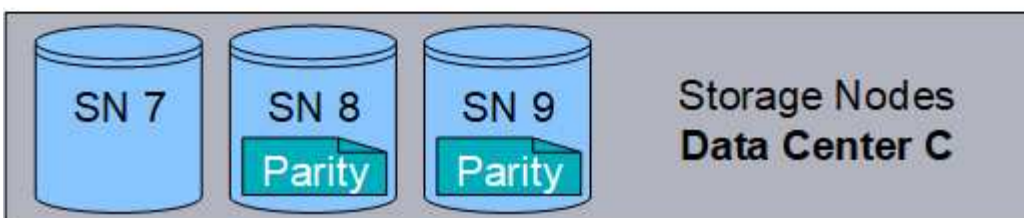
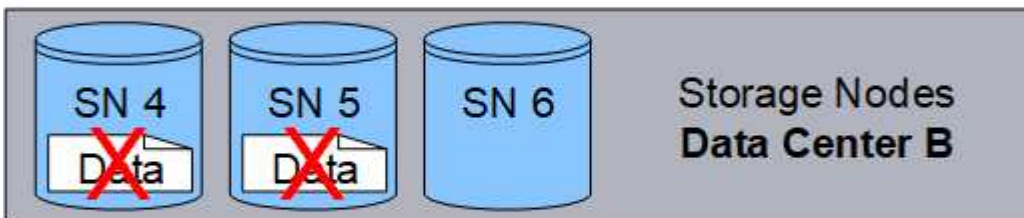
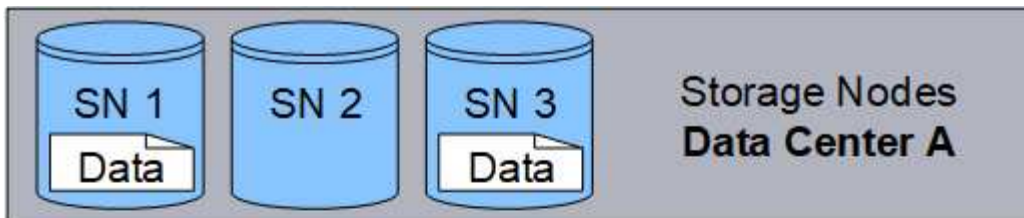
Quando um objeto é acessado, ele é remontado usando os fragmentos armazenados. Se um fragmento de dados ou de paridade for corrompido ou perdido, o algoritmo de codificação de apagamento pode recriar esse fragmento usando um subconjunto dos fragmentos de dados e de paridade restantes.

À medida que você cria regras ILM, StorageGRID cria perfis de codificação de apagamento que dão suporte a essas regras. Você pode visualizar uma lista de perfis de codificação de apagamento, ["renomear um perfil de codificação de apagamento"](#), ou ["desativar um perfil de codificação de apagamento se ele não estiver sendo usado em nenhuma regra do ILM"](#).

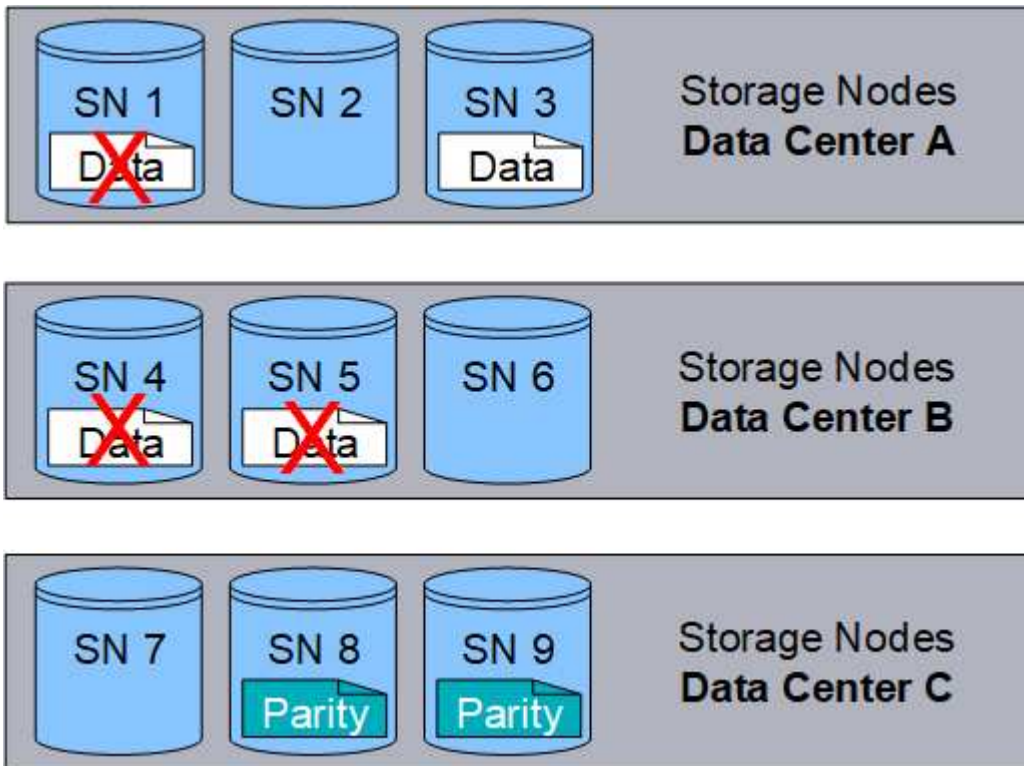
O exemplo a seguir ilustra o uso de um algoritmo de codificação de apagamento nos dados de um objeto. Neste exemplo, a regra ILM utiliza um esquema de codificação de apagamento 4+2. Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são calculados a partir dos dados do objeto. Cada um dos seis fragmentos é armazenado em um nó diferente em três data center para fornecer proteção de dados em caso de falhas de nós ou perda de um dos sites.



O esquema de codificação de apagamento 4+2 pode ser configurado de diversas maneiras. Por exemplo, você pode configurar um pool de storage que contenha seis Storage Nodes. Para "[proteção contra perda de site](#)", você pode usar um pool de storage contendo três sites com três Storage Nodes em cada site. Um objeto pode ser recuperado desde que qualquer quatro dos seis fragmentos (dados ou paridade) permaneçam disponíveis. Até dois fragmentos podem ser perdidos sem perda dos dados do objeto. Se um site inteiro for perdido, o objeto ainda poderá ser recuperado ou reparado, desde que todos os outros fragmentos permaneçam acessíveis.



Se mais de dois nós de armazenamento forem perdidos, o objeto não poderá ser recuperado.



Informações relacionadas

- ["O que é replicação"](#)
- ["O que é um pool de storage"](#)
- ["O que são esquemas de codificação de apagamento"](#)
- ["Renomear um perfil de codificação de apagamento"](#)
- ["Desativar um perfil de codificação de apagamento"](#)

Saiba mais sobre esquemas de codificação de apagamento em StorageGRID

Os esquemas de codificação de apagamento controlam quantos fragmentos de dados e quantos fragmentos de paridade são criados para cada objeto.

Ao criar ou editar uma regra ILM, você seleciona um esquema de codificação de apagamento disponível. StorageGRID cria automaticamente esquemas de codificação de apagamento com base na quantidade de Storage Nodes e sites que compõem o pool de storage que você planeja usar.

Proteção de dados

O sistema StorageGRID utiliza o algoritmo de codificação de apagamento Reed-Solomon. O algoritmo divide um objeto em k fragmentos de dados e calcula m fragmentos de paridade.

Os $k + m = n$ fragmentos são distribuídos entre n Storage Nodes para fornecer proteção de dados da seguinte forma:

- Para recuperar ou reparar um objeto, são necessários k fragmentos.
- Um objeto pode suportar até m fragmentos perdidos ou corrompidos. Quanto maior o valor de m , maior a

tolerância a falhas.

A melhor proteção de dados é fornecida pelo esquema de codificação de apagamento com a maior tolerância a falhas de nós ou volumes dentro de um pool de storage.

Sobrecarga de storage

A sobrecarga de storage de um esquema de codificação de apagamento é calculada dividindo o número de fragmentos de paridade (m) pelo número de fragmentos de dados (k). Você pode usar a sobrecarga de storage para calcular quanto espaço de disco cada objeto codificado por apagamento requer:

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Por exemplo, se você armazenar um objeto de 10 MB usando o esquema 4+2 (que tem 50% de sobrecarga de storage), o objeto consumirá 15 MB de storage em grade. Se você armazenar o mesmo objeto de 10 MB usando o esquema 6+2 (que tem 33% de sobrecarga de storage), o objeto consumirá aproximadamente 13,3 MB.

Selecione o esquema de codificação de apagamento com o menor valor total de $k+m$ que atenda às suas necessidades. Esquemas de codificação de apagamento com um número menor de fragmentos são mais eficientes computacionalmente porque:

- Menos fragmentos são criados e distribuídos (ou recuperados) por objeto
- Eles apresentam melhor desempenho porque o tamanho do fragmento é maior
- Eles podem exigir a adição de menos nós em um ["expansão quando for necessário mais storage"](#)

Diretrizes para pools de storage

Ao selecionar o pool de storage a ser usado para uma regra que criará uma cópia com codificação de apagamento, utilize as seguintes diretrizes para pools de storage:

- O pool de storage deve incluir três ou mais sites, ou exatamente um site.



Não é possível usar codificação de apagamento se o pool de storage incluir dois sites.

- [Esquemas de codificação de apagamento para pools de storage contendo três ou mais sites](#)
- [Esquemas de codificação de apagamento para pools de storage de um único local](#)
- Não utilize um pool de storage que inclua o site All Sites.
- O pool de storage deve incluir pelo menos $k+m + 1$ Storage Nodes que possam armazenar dados de objetos.



Os nós de armazenamento podem ser configurados durante a instalação para conter dados de objetos e metadados ("nó de armazenamento combinado"), apenas metadados de objetos ou apenas dados de objetos. Para obter mais informações, consulte ["Tipos de nós de armazenamento"](#).

O número mínimo de nós de armazenamento necessários é $k+m$. No entanto, ter pelo menos um nó de armazenamento adicional pode ajudar a evitar falhas de ingestão ou acúmulo de ILM caso um nó de armazenamento necessário esteja temporariamente indisponível.

Esquemas de codificação de apagamento para pools de storage contendo três ou mais sites

A tabela a seguir descreve os esquemas de codificação de apagamento atualmente suportados pelo StorageGRID para pool de storage que incluem três ou mais sites. Todos esses esquemas oferecem proteção contra perda de site. Um site pode ser perdido e o objeto ainda estará acessível.

Para esquemas de codificação de apagamento que oferecem proteção contra perda de site, o número recomendado de nós de armazenamento no pool de storage excede $k+m+1$ porque cada site requer um mínimo de três nós de armazenamento.

Esquema de codificação de apagamento ($k+m$)	Número mínimo de sites implantados	Número recomendado de Storage Nodes em cada site	Número total recomendado de Storage Nodes	Proteção contra perda de site?	Sobrecarga de storage
4+2	3	3	9	Sim	50%
6+2	4	3	12	Sim	33%
8+2	5	3	15	Sim	25%
6+3	3	4	12	Sim	50%
9+3	4	4	16	Sim	33%
2+1	3	3	9	Sim	50%
4+1	5	3	15	Sim	25%
6+1	7	3	21	Sim	17%
7+5	3	5	15	Sim	71%



StorageGRID requer um mínimo de três nós de armazenamento por local. Para usar o esquema 7+5, cada local requer um mínimo de quatro nós de armazenamento. Recomenda-se o uso de cinco nós de armazenamento por local.

Ao selecionar um esquema de codificação de apagamento que ofereça proteção ao site, equilibre a importância relativa dos seguintes fatores:

- **Número de fragmentos:** O desempenho e a flexibilidade de expansão são geralmente melhores quando o número total de fragmentos é menor.
- **Tolerância de falhas:** A tolerância de falhas aumenta com mais segmentos de paridade (ou seja, quando m tem um valor mais alto).
- **Tráfego de rede:** Ao recuperar de falhas, usar um esquema com mais fragmentos (ou seja, um total maior para $k+m$) cria mais tráfego de rede.
- **Sobrecarga de storage:** Esquemas com sobrecarga maior exigem mais espaço de storage por objeto.

Por exemplo, ao decidir entre um esquema 4+2 e um esquema 6+3 (ambos com 50% sobrecarga de storage), selecione o esquema 6+3 se for necessária tolerância de falhas adicional. Selecione o esquema 4+2 se recursos de rede estiverem limitados. Se todos os outros fatores forem iguais, selecione o 4+2 porque ele tem um número total menor de fragmentos.



Se você não tiver certeza de qual esquema usar, selecione 4+2 ou 6+3 ou entre em contato com o suporte técnico.

Esquemas de codificação de apagamento para pools de storage de um único local

Um pool de storage de um único site suporta todos os esquemas de codificação de apagamento definidos para três ou mais sites, desde que o site tenha Storage Nodes suficientes.

O número mínimo de Storage Nodes necessários é $k+m$, mas recomenda-se um pool de storage com $k+m + 1$ Storage Nodes. Por exemplo, o esquema de codificação de apagamento 2+1 requer um pool de storage com um mínimo de três Storage Nodes, mas recomenda-se quatro Storage Nodes.

Esquema de codificação de apagamento ($k+m$)	Número mínimo de Storage Nodes	Número recomendado de Storage Nodes	Sobrecarga de storage
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Vantagens, desvantagens e requisitos para codificação de apagamento no StorageGRID

Antes de decidir se deve usar replicação ou codificação de apagamento para proteger os dados de objeto contra perda, você deve entender as vantagens, desvantagens e os requisitos da codificação de apagamento.

Vantagens da codificação de apagamento

Em comparação com a replicação, a codificação de apagamento oferece maior confiabilidade, disponibilidade e eficiência de storage.

- **Confiabilidade:** medida pelo número de falhas simultâneas que podem ser suportadas sem perda de dados.
 - Replicação: múltiplas cópias idênticas de um mesmo objeto são armazenadas em nós diferentes e em vários locais.
 - Codificação de apagamento: um objeto é codificado em fragmentos de dados e paridade e distribuído por vários nós e locais. Essa dispersão oferece proteção contra falhas tanto do local quanto do nó.
- **Disponibilidade:** A capacidade de recuperar objetos caso os Storage Nodes falhem ou se tornem inacessíveis. Em comparação com a replicação, codificação de apagamento oferece maior disponibilidade a custos de storage comparáveis.
- **Eficiência de storage:** Para disponibilidade e confiabilidade semelhantes, objetos com codificação de apagamento usam menos espaço de disco do que objetos replicados. Por exemplo, um objeto de 10 MB replicado em dois sites consome 20 MB de espaço de disco (duas cópias), enquanto um objeto com codificação de apagamento em três sites usando um esquema de codificação de apagamento 6+3 consome apenas 15 MB de espaço de disco.



O espaço em disco para objetos com codificação de apagamento é calculado como o tamanho do objeto mais a sobrecarga de storage. A porcentagem de sobrecarga de storage é o número de fragmentos de paridade dividido pelo número de fragmentos de dados.

Desvantagens da codificação de apagamento

Em comparação com a replicação, a codificação de apagamento apresenta as seguintes desvantagens:

- É recomendável aumentar o número de Storage Nodes e sites, dependendo do esquema de codificação de apagamento. Por outro lado, se você replicar dados de objetos, precisará apenas de um Storage Node para cada cópia. Consulte ["Esquemas de codificação de apagamento para pools de storage contendo três ou mais sites"](#) e ["Esquemas de codificação de apagamento para pools de storage de um único local"](#).
- Aumento do custo e da complexidade das expansões de armazenamento. Para expandir uma implementação que usa replicação, você adiciona capacidade de storage em todos os locais onde as cópias de objetos são feitas. Para expandir uma implementação que usa codificação de apagamento, você deve considerar tanto o esquema de codificação de apagamento em uso quanto o nível de ocupação dos Storage Nodes existentes. Por exemplo, se você esperar até que os nós existentes estejam 100% cheios, precisará adicionar pelo menos $k+m$ Storage Nodes, mas se você expandir quando os nós existentes estiverem 70% cheios, poderá adicionar dois nós por site e ainda maximizar a capacidade de storage. Para obter mais informações, consulte ["Adicionar capacidade de storage para objetos com codificação de apagamento"](#).
- Há um aumento na latência de recuperação quando você utiliza codificação de apagamento em sites geograficamente distribuídos. Os fragmentos de um objeto que é codificado por apagamento e distribuído em sites remotos levam mais tempo para serem recuperados por conexões WAN do que um objeto que é replicado e está disponível localmente (no mesmo site ao qual o cliente se conecta).
- Ao utilizar codificação de apagamento em locais geograficamente distribuídos, há maior uso de tráfego de rede WAN para recuperações e reparos, especialmente para objetos recuperados com frequência ou para reparos de objetos em conexões de rede WAN.
- Ao usar codificação de apagamento entre sites, a taxa de transferência máxima de objetos diminui drasticamente à medida que a latência de rede entre os sites aumenta. Essa diminuição resulta da redução na taxa de transferência da rede TCP, o que afeta a velocidade com que o sistema StorageGRID consegue armazenar e recuperar fragmentos de objetos.
- Maior utilização de recursos computacionais.

Quando usar codificação de apagamento

Utilize codificação de apagamento para os seguintes requisitos:

- Objetos com tamanho superior a 1 MB.



A codificação de apagamento é mais adequada para objetos maiores que 1 MB. Não use codificação de apagamento para objetos menores que 200 KB para evitar a sobrecarga de gerenciar fragmentos codificados por apagamento muito pequenos.

- Armazenamento a longo prazo ou cold storage para conteúdo acessado com pouca frequência.
- Alta disponibilidade de dados e confiabilidade.
- Proteção contra falhas totais de site e nó.
- Eficiência de storage.
- Implantações em um único local que exigem proteção de dados eficiente com apenas uma única cópia com codificação de apagamento, em vez de várias cópias replicadas.
- Implantações em múltiplos locais onde a latência entre sites é inferior a 100 ms.

Como StorageGRID determina a retenção de objetos

StorageGRID oferece opções para que tanto os administradores do grid quanto os usuários individuais especifiquem por quanto tempo os objetos devem ser armazenados. Em geral, quaisquer instruções de retenção fornecidas por um usuário têm precedência sobre as instruções de retenção fornecidas pelo administrador do grid.

Como os usuários locatários controlam a retenção de objetos

Os usuários locatários podem usar esses métodos para controlar por quanto tempo seus objetos são armazenados no StorageGRID:

- Se a configuração global de S3 Object Lock estiver habilitada para o grid, os usuários do tenant S3 podem criar buckets com S3 Object Lock ativado e, em seguida, selecionar um **período de retenção padrão** para cada bucket.
- Se a configuração global de S3 Object Lock estiver habilitada para o grid, os usuários do tenant S3 podem criar buckets com S3 Object Lock ativado e, em seguida, usar a API REST do S3 para especificar retain-until-date e as configurações de legal hold para cada versão de objeto adicionada a esse bucket.
 - Uma versão de objeto que esteja sob guarda legal não pode ser excluída por nenhum método.
 - Antes que a data de retenção de uma versão de objeto seja atingida, essa versão não pode ser excluída por nenhum método.
 - Os objetos em buckets com o S3 Object Lock ativado são retidos pelo ILM "para sempre". No entanto, após a data de retenção ser atingida, uma versão do objeto pode ser excluída por uma solicitação do cliente ou pelo término do ciclo de vida do bucket. Consulte ["Gerencie objetos com S3 Object Lock"](#).
- Os usuários locatários do S3 podem adicionar uma configuração de ciclo de vida aos seus buckets que especifica uma ação de Expiração. Se um ciclo de vida do bucket existir, o StorageGRID armazena um objeto até que a data ou o número de dias especificados na ação de Expiração sejam atingidos, a menos que o cliente exclua o objeto primeiro. Consulte ["Criar configuração de ciclo de vida do S3"](#).
- Um cliente S3 pode emitir uma solicitação de exclusão de objeto. StorageGRID sempre prioriza as solicitações de exclusão do cliente em relação ao ciclo de vida do bucket S3 ou ao ILM ao determinar se

deve excluir ou reter um objeto.

Como os administradores de grids controlam a retenção de objetos

Os administradores da grade podem usar esses métodos para controlar a retenção de objetos:

- Defina um período máximo de retenção do S3 Object Lock para cada locatário. Em seguida, os usuários do locatário podem definir um período de retenção padrão para cada um de seus buckets. O período máximo de retenção também é aplicado a quaisquer objetos recém-ingeridos para esse bucket (retain-until-date do objeto).
- Crie instruções de posicionamento ILM para controlar por quanto tempo os objetos são armazenados. Quando os objetos correspondem a uma regra ILM, StorageGRID armazena esses objetos até que o último período de tempo na regra ILM tenha expirado. Os objetos são retidos indefinidamente se "forever" for especificado para as instruções de posicionamento.
- Independentemente de quem controla por quanto tempo os objetos são retidos, as configurações do ILM controlam quais tipos de cópias de objetos (replicadas ou codificadas de apagamento) são armazenadas e onde as cópias estão localizadas (Storage Nodes ou Cloud Storage Pools).

Como o ciclo de vida do bucket S3 e o ILM interagem

Quando um ciclo de vida de bucket S3 é configurado, as ações de expiração do ciclo de vida substituem a política de ILM para objetos que correspondem ao filtro de ciclo de vida. Como resultado, um objeto pode ser retido no grid mesmo após o vencimento de quaisquer instruções de ILM para alocar o objeto.

Exemplos de retenção de objeto

Para melhor compreender as interações entre S3 Object Lock, as configurações de ciclo de vida do bucket, as solicitações de exclusão do cliente e o ILM, considere os exemplos a seguir.

Exemplo 1: o ciclo de vida do bucket S3 mantém os objetos por mais tempo do que o ILM

ILM

Armazene duas cópias por 1 ano (365 dias)

Ciclo de vida do bucket

Expirar objetos em 2 anos (730 dias)

Resultado

StorageGRID armazena o objeto por 730 dias. StorageGRID usa as configurações de ciclo de vida do bucket para determinar se deve excluir ou reter um objeto.



Se o ciclo de vida do bucket especificar que os objetos devem ser mantidos por mais tempo do que o especificado pelo ILM, StorageGRID continuará usando as instruções de posicionamento do ILM ao determinar o número e o tipo de cópias a serem armazenadas. Neste exemplo, duas cópias do objeto continuarão sendo armazenadas no StorageGRID do dia 366 ao dia 730.

Exemplo 2: ciclo de vida do bucket S3 expira os objetos antes do ILM

ILM

Armazene duas cópias por 2 anos (730 dias)

Ciclo de vida do bucket

Expirar objetos em 1 ano (365 dias)

Resultado

StorageGRID exclui ambas as cópias do objeto após o dia 365.

Exemplo 3: a exclusão pelo cliente substitui o ciclo de vida do bucket e o ILM

ILM

Armazene duas cópias em Storage Nodes "para sempre"

Ciclo de vida do bucket

Expirar objetos em 2 anos (730 dias)

Solicitação de exclusão do cliente

Emitido no dia 400

Resultado

StorageGRID exclui ambas as cópias do objeto no dia 400 em resposta à solicitação de exclusão do cliente.

Exemplo 4: O S3 Object Lock substitui a solicitação de exclusão do cliente

Bloqueio de objeto S3

A data limite de retenção para uma versão do objeto é 31/03/2026. Não há guarda legal em vigor.

Regra ILM compatível

Armazene duas cópias em Storage Nodes "para sempre"

Solicitação de exclusão do cliente

Emitido em 31/03/2024

Resultado

StorageGRID não excluirá a versão do objeto porque a data de retenção ainda está a 2 anos de distância.

Como StorageGRID exclui objetos

StorageGRID pode excluir objetos tanto em resposta direta a uma solicitação do cliente quanto automaticamente, como resultado da expiração do ciclo de vida de um bucket S3 ou dos requisitos da política ILM. Compreender as diferentes maneiras pelas quais os objetos podem ser excluídos e como o StorageGRID lida com as solicitações de exclusão pode ajudar você a gerenciar objetos com mais eficiência.

StorageGRID pode usar um dos dois métodos para excluir objetos:

- **Exclusão síncrona:** Quando StorageGRID recebe uma solicitação de exclusão do cliente, todas as cópias do objeto são removidas imediatamente. O cliente é informado de que a exclusão foi bem-sucedida após a remoção das cópias.
- **Os objetos são enfileirados para exclusão:** quando StorageGRID recebe uma solicitação de exclusão, o objeto é enfileirado para exclusão e o cliente é informado imediatamente de que a exclusão foi bem-sucedida. As cópias dos objetos são removidas posteriormente pelo processamento ILM em segundo

plano.

Ao excluir objetos, StorageGRID utiliza o método que otimiza o desempenho da exclusão, minimiza possíveis atrasos na exclusão e libera espaço mais rapidamente.

A tabela resume quando StorageGRID utiliza cada método.

Método de realização da exclusão	Quando usado
Os objetos são enfileirados para exclusão	Quando qualquer uma das seguintes condições for verdadeira: • A exclusão automática de objetos foi acionada por um dos seguintes eventos: ◦ A data de expiração ou o número de dias na configuração do ciclo de vida de um bucket S3 é alcançado. ◦ O último período de tempo especificado em uma regra ILM expira. Nota: Os objetos em um bucket com o S3 Object Lock ativado não podem ser excluídos se estiverem sob guarda legal ou se uma data de retenção tiver sido especificada, mas ainda não tiver sido atingida. • Um cliente S3 solicita a exclusão e uma ou mais destas condições são verdadeiras: ◦ As cópias não podem ser excluídas em 30 segundos porque, por exemplo, a localização de um objeto está temporariamente indisponível. ◦ As filas de exclusão em segundo plano estão ociosas.
Os objetos são removidos imediatamente (exclusão síncrona)	Quando um cliente S3 faz uma solicitação de exclusão e todas as seguintes condições são atendidas: • Todas as cópias podem ser removidas em 30 segundos. • As filas de exclusão em segundo plano contêm objetos para processar.

Quando os clientes do S3 fazem solicitações de exclusão, StorageGRID começa adicionando objetos à fila de exclusão. Em seguida, passa a realizar a exclusão síncrona. Garantir que a fila de exclusão em segundo plano tenha objetos para processar permite que o StorageGRID processe exclusões com mais eficiência, especialmente para clientes com baixa concorrência, além de ajudar a evitar o acúmulo de exclusões por parte dos clientes.

Tempo necessário para excluir objetos

A forma como o StorageGRID exclui objetos pode afetar como o sistema aparenta funcionar:

- Quando StorageGRID realiza a exclusão síncrona, pode levar até 30 segundos para que StorageGRID retorne um resultado ao cliente. Isso significa que a exclusão pode parecer estar acontecendo mais lentamente, mesmo que as cópias estejam sendo removidas mais rapidamente do que quando StorageGRID coloca objetos em fila para exclusão.
- Se você estiver monitorando atentamente o desempenho de exclusão durante uma exclusão em massa, pode notar que a taxa de exclusão parece diminuir após um certo número de objetos terem sido excluídos. Essa mudança ocorre quando StorageGRID passa de enfileirar objetos para exclusão para realizar a exclusão síncrona. A aparente redução na taxa de exclusão não significa que as cópias dos objetos

estejam sendo removidas mais lentamente. Pelo contrário, indica que, em média, o espaço está sendo liberado mais rapidamente.

Se você estiver excluindo um grande número de objetos e sua prioridade for liberar espaço rapidamente, considere usar uma solicitação do cliente para excluir os objetos em vez de excluí-los usando o ILM ou outros métodos. Em geral, o espaço é liberado mais rapidamente quando a exclusão é realizada pelos clientes, pois o StorageGRID pode usar a exclusão síncrona.

O tempo necessário para liberar espaço após a exclusão de um objeto depende de vários fatores:

- Se as cópias de objetos são removidas de forma síncrona ou se são enfileiradas para remoção posterior (para solicitações de exclusão do cliente).
- Outros fatores, como o número de objetos na grade ou a disponibilidade de recursos da grade quando as cópias dos objetos são enfileiradas para remoção (tanto para exclusões feitas pelo cliente quanto por outros métodos).

Como os objetos versionados do S3 são excluídos

Quando o versionamento está habilitado para um bucket do S3, StorageGRID segue o comportamento do Amazon S3 ao responder a solicitações de exclusão, independentemente de essas solicitações virem de um cliente S3, do vencimento do ciclo de vida de um bucket S3 ou dos requisitos da política de ILM.

Quando os objetos são versionados, as solicitações de exclusão de objetos não excluem a versão atual do objeto e não liberam espaço livre. Em vez disso, uma solicitação de exclusão de objeto cria um marcador de exclusão de zero bytes como a versão atual do objeto, o que torna a versão anterior do objeto "não atual". Um marcador de exclusão de objeto se torna um marcador de exclusão de objeto expirado quando é a versão atual e não há versões não atuais.

Embora o objeto não tenha sido removido, StorageGRID se comporta como se a versão atual do objeto não estivesse mais disponível. Solicitações para esse objeto retornam 404 Not Found. No entanto, como os dados não atuais do objeto não foram removidos, solicitações que especificam uma versão não atual do objeto podem ser bem-sucedidas.

Se um cliente excluir uma versão de objeto com um ID de versão de um ["bucket de branch"](#)bucket de branch, StorageGRID oculta a existência da versão do objeto, mas não cria um marcador de exclusão no bucket de branch. Se um cliente excluir um objeto sem um ID de versão de um bucket de branch, StorageGRID cria um marcador de exclusão no bucket de branch de acordo com o comportamento padrão do S3.

Para liberar espaço ao excluir objetos versionados ou para remover marcadores de exclusão, use um dos seguintes métodos:

- **Solicitação do cliente S3:** Especifique o ID da versão do objeto na solicitação DELETE Object do S3 (DELETE /object?versionId=ID). Lembre-se de que esta solicitação remove apenas as cópias do objeto para a versão especificada (as outras versões ainda ocupam espaço).
- **Bucket lifecycle:** Use a ação `NoncurrentVersionExpiration` na configuração do ciclo de vida do bucket. Quando o número de `NoncurrentDays` especificado for atingido, StorageGRID remove permanentemente todas as cópias de versões de objeto não atuais. Essas versões de objeto não podem ser recuperadas.

A `NewerNoncurrentVersions` ação na configuração do ciclo de vida do bucket especifica o número de versões não atuais retidas em um bucket S3 versionado. Se houver mais versões não atuais do que `NewerNoncurrentVersions` especificado, StorageGRID remove as versões mais antigas quando o valor de `NoncurrentDays` expirar. O `NewerNoncurrentVersions` limite substitui as regras de ciclo de vida fornecidas pelo ILM, o que significa que um objeto não atual com uma versão dentro do

`NewerNoncurrentVersions` limite é retido se o ILM solicitar sua exclusão.

Para remover marcadores de exclusão de objetos expirados, use a `Expiration` ação com uma das seguintes tags: `ExpiredObjectDeleteMarker`, `Days` ou `Date`.

- **ILM: "Clonar uma política ativa"** e adicione duas regras ILM à nova política:
 - Primeira regra: Use "Tempo não atual" como Tempo de referência para corresponder às versões não atuais do objeto. Em "[Etapa 1 \(Inserir detalhes\) do assistente Criar uma regra ILM](#)", selecione **Sim** para a pergunta "Aplicar esta regra somente a versões mais antigas do objeto (em buckets do S3 com versionamento ativado)?"
 - Segunda regra: Use o **Tempo de ingestão** para corresponder à versão atual. A regra "Tempo não atual" deve aparecer na política acima da regra **Tempo de ingestão**.

Para remover marcadores de exclusão de objetos expirados, use uma regra de **Tempo de ingestão** que corresponda aos marcadores de exclusão atuais. Os marcadores de exclusão são removidos somente quando um **Período de tempo de Dias** tiver decorrido e o marcador de exclusão atual tiver expirado (não existem versões não atuais).

- **Excluir objetos no bucket:** Use o gerenciador de locatários para "[Excluir todas as versões do objeto](#)" excluir objetos, incluindo marcadores de exclusão, de um bucket.

Quando um objeto versionado é excluído, StorageGRID cria um marcador de exclusão de zero bytes como a versão atual do objeto. Todos os objetos e marcadores de exclusão devem ser removidos antes que um bucket versionado possa ser excluído.

- Marcadores de exclusão criados no StorageGRID 11.7 ou anterior só podem ser removidos por solicitações do cliente S3; eles não são removidos pelo ILM, pelas regras de ciclo de vida do bucket ou pelas operações de exclusão de objetos no bucket.
- Marcadores de exclusão de um bucket criado no StorageGRID 11.8 ou posterior podem ser removidos pelo gerenciamento do ciclo de vida das informações (ILM), regras de ciclo de vida do bucket, operações de exclusão de objetos no bucket ou por uma exclusão explícita pelo cliente S3.

Informações relacionadas

- "[Utilize a API REST S3](#)"
- "[Exemplo 4: regras e políticas do ILM para objetos versionados do S3](#)"

Crie e atribua níveis de storage no StorageGRID

Os níveis de armazenamento identificam o tipo de armazenamento usado por um Nó de Armazenamento. Você pode criar níveis de armazenamento se desejar que as regras do ILM aloquem determinados objetos em Nós de Armazenamento específicos.

Antes de começar

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

Sobre esta tarefa

Ao instalar StorageGRID, a classificação de storage **Default** é atribuída automaticamente a cada Storage Node do seu sistema. Conforme necessário, você pode definir classificações de storage personalizadas e atribuí-las a diferentes Storage Nodes.

O uso de níveis de armazenamento personalizados permite criar pools de storage ILM que contenham apenas um tipo específico de Storage Node. Por exemplo, você pode querer que determinados objetos sejam armazenados nos seus Storage Nodes mais rápidos, como os appliances de storage all-flash StorageGRID.



Nós de storage somente de metadados não podem ter uma classificação de storage atribuída. Para obter mais informações, consulte ["Tipos de nós de armazenamento"](#).

Se a classificação de armazenamento não for uma preocupação (por exemplo, se todos os Storage Nodes forem idênticos), você pode ignorar este procedimento e usar a opção **inclui todas as classificações de armazenamento** para a classificação de armazenamento quando você ["criar pools de storage"](#). Usar essa opção garante que o pool de storage incluirá todos os Storage Nodes no site, independentemente de sua classificação de armazenamento.



Não crie mais níveis de armazenamento do que o necessário. Por exemplo, não crie um nível de armazenamento para cada Storage Node. Em vez disso, atribua cada nível de armazenamento a dois ou mais nós. Níveis de armazenamento atribuídos a apenas um nó podem causar atrasos no ILM se esse nó ficar indisponível.

Passos

1. Selecione **ILM > Storage grades**.
2. Defina níveis de armazenamento personalizados:
 - a. Para cada nível de armazenamento personalizado que você deseja adicionar, selecione **Inserir**  para adicionar uma linha.
 - b. Insira um rótulo descritivo.



Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

c. Selecione **Aplicar alterações**.

d. Opcionalmente, se precisar modificar um rótulo salvo, selecione **Editar** e selecione **Aplicar alterações**.



Você não pode excluir níveis de armazenamento.

3. Atribua novas categorias de armazenamento aos nós de armazenamento:

a. Localize o nó de armazenamento na lista LDR e selecione o ícone **Editar** .

b. Selecione a classe de armazenamento apropriada na lista.



LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default disk	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes



Atribua um storage grade a um determinado Storage Node apenas uma vez. Um Storage Node recuperado de uma falha mantém o storage grade atribuído anteriormente. Não altere essa atribuição após a ativação da política de ILM. Se a atribuição for alterada, os dados serão armazenados com base no novo storage grade.

- Selecione **Aplicar alterações**.

Utilize pools de storage

Saiba mais sobre pool de storage no StorageGRID

Um pool de storage é um agrupamento lógico de Storage Nodes.

Ao instalar StorageGRID, um pool de storage por site é criado automaticamente. Você pode configurar pools de storage adicionais conforme necessário para atender às suas necessidades de armazenamento.



Os nós de armazenamento podem ser configurados durante a instalação para conter dados de objetos e metadados ("nó de armazenamento combinado"), apenas metadados de objetos ou apenas dados de objetos. Nós de armazenamento somente com metadados não podem ser usados em pool de storage. Para mais informações, consulte "[Tipos de nós de armazenamento](#)".

Os pools de storage possuem dois atributos:

- **Nível de armazenamento:** Para nós de armazenamento, o desempenho relativo do armazenamento de suporte.
- **Local:** O data center onde os objetos serão armazenados.

Os pools de armazenamento são usados nas regras do ILM para determinar onde os dados do objeto são armazenados e o tipo de armazenamento usado. Ao configurar as regras do ILM para replicação, você seleciona um ou mais pools de armazenamento.

Diretrizes de configuração do pool de storage no StorageGRID

Configure e utilize pools de storage para proteger contra perda de dados distribuindo os dados por vários sites. Cópias replicadas e cópias com codificação de apagamento exigem diferentes configurações de pool de storage.

Consulte ["Exemplos de ativação da proteção contra perda de dados usando replicação e codificação de apagamento"](#).

Diretrizes para todos os pools de storage

- Mantenha as configurações do pool de storage o mais simples possível. Não crie mais pools de storage do que o necessário.
- Crie pools de storage com o máximo de nós possível. Cada pool de storage deve conter dois ou mais nós. Um pool de storage com nós insuficientes pode causar atrasos no ILM se um nó ficar indisponível.
- Evite criar ou usar pools de storage que se sobreponham (contenham um ou mais dos mesmos nós). Se pools de storage se sobrepuserem, mais de uma cópia dos dados do objeto pode ser salva no mesmo nó.
- Em geral, não utilize o pool de storage All Storage Nodes (StorageGRID 11.6 e versões anteriores) nem o site All Sites. Esses itens são atualizados automaticamente para incluir quaisquer novos sites que você adicionar em uma expansão, o que pode não ser o comportamento que você deseja.

Diretrizes para pools de storage usados para cópias replicadas

- Para proteção contra perda de site usando ["replicação"](#), especifique um ou mais pools de storage específicos do site no ["Instruções de posicionamento para cada regra ILM"](#).

Um pool de storage é criado automaticamente para cada site durante a instalação do StorageGRID.

Utilizar um pool de storage para cada site garante que as cópias replicadas dos objetos sejam colocadas exatamente onde você espera (por exemplo, uma cópia de cada objeto em cada site para proteção contra perda de site).

- Se você adicionar um site em uma expansão, crie um novo pool de storage que contenha apenas o novo site. Em seguida, ["Atualizar regras do ILM"](#) para controlar quais objetos são armazenados no novo site.
- Se o número de cópias for menor que o número de pools de storage, o sistema distribui as cópias para equilibrar o uso do disco entre os pools.
- Se os pools de armazenamento se sobrepuserem (contiverem os mesmos Storage Nodes), todas as cópias do objeto poderão ser salvas em apenas um site. Você deve garantir que os pools de armazenamento selecionados não contenham os mesmos Storage Nodes.

Diretrizes para pools de storage usados para cópias com codificação de apagamento

- Para proteção contra perda de sites usando ["codificação de apagamento"](#), crie pools de storage que consistam em pelo menos três sites. Se um pool de storage incluir apenas dois sites, você não pode usar esse pool de storage para codificação de apagamento. Nenhum esquema de codificação de apagamento está disponível para um pool de storage que tenha dois sites.
- O número de nós de armazenamento e sites contidos no pool de storage determina quais ["esquemas de codificação de apagamento"](#) estão disponíveis.
- Se possível, um pool de storage deve incluir mais do que o número mínimo de Storage Nodes exigido pelo esquema de codificação de apagamento que você selecionar. Por exemplo, se você usar um esquema de codificação de apagamento 6+3, será necessário ter pelo menos nove Storage Nodes. No entanto,

recomenda-se ter pelo menos um Storage Node adicional por site.

- Distribua os nós de armazenamento entre os locais da forma mais uniforme possível. Por exemplo, para suportar um esquema de codificação de apagamento 6+3, configure um pool de storage que inclua pelo menos três nós de armazenamento em três locais.
- Se você tiver requisitos de taxa de transferência elevados, não é recomendável usar um pool de storage que inclua vários sites se a latência de rede entre os sites for superior a 100 ms. À medida que a latência aumenta, a taxa na qual o StorageGRID pode criar, posicionar e recuperar fragmentos de objetos diminui drasticamente devido à redução na taxa de transferência da rede TCP.

A diminuição da taxa de transferência afeta as taxas máximas alcançáveis de ingestão e recuperação de objetos (quando Balanced ou Strict são selecionados como o comportamento de ingestão) ou pode levar a atrasos na fila do ILM (quando Dual commit é selecionado como o comportamento de ingestão). Consulte ["Comportamento de ingestão da regra ILM"](#).



Se sua grade incluir apenas um site, você ficará impedido de usar o pool de storage All Storage Nodes (StorageGRID 11.6 e versões anteriores) ou o site All Sites em um perfil de codificação de apagamento. Esse comportamento impede que o perfil se torne inválido caso um segundo site seja adicionado.

Proteção contra perda de sites com pools de storage no StorageGRID

Se sua implantação do StorageGRID incluir mais de um site, você pode usar replicação e codificação de apagamento com pools de storage configurados adequadamente para habilitar a proteção contra perda de site.

A replicação e a codificação de apagamento exigem diferentes configurações de pool de storage:

- Para usar a replicação para proteção contra perda de site, use os pools de storage específicos do site que são criados automaticamente durante a instalação do StorageGRID. Em seguida, crie regras ILM com ["instruções de colocação"](#) que especifiquem vários pools de storage, para que uma cópia de cada objeto seja colocada em cada site.
- Para usar codificação de apagamento para proteção contra perda de sites, ["Criar pools de storage que consistem em vários sites"](#). Em seguida, crie regras ILM que usem um pool de storage composto por vários sites e qualquer esquema de codificação de apagamento disponível.



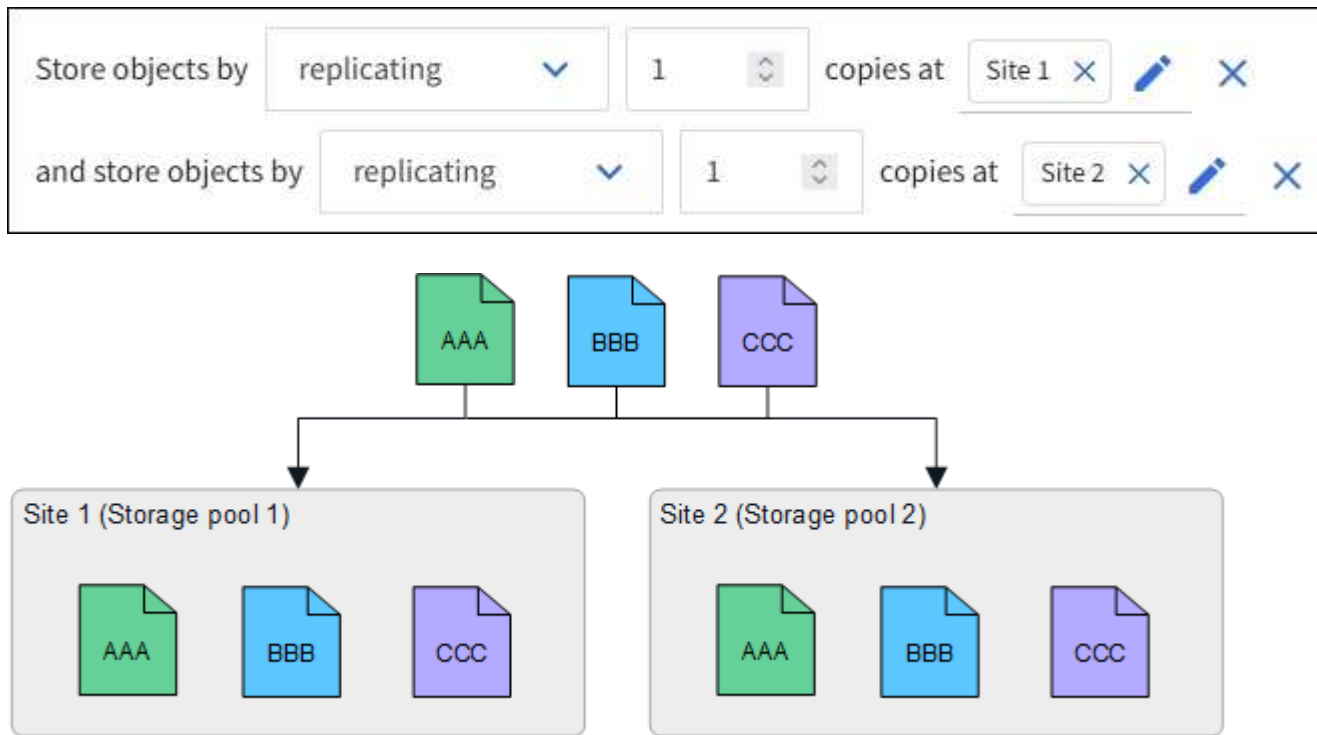
Ao configurar sua implantação do StorageGRID para proteção contra perda de site, você também deve levar em consideração os efeitos de ["opções de ingestão"](#) e ["consistência"](#).

Exemplo de replicação

Por padrão, um pool de storage é criado para cada site durante a instalação do StorageGRID. Ter pools de storage compostos por apenas um site permite que você configure regras ILM que usam replicação para proteção contra perda de site. Neste exemplo:

- O pool de storage 1 contém o Site 1
- O pool de storage 2 contém Site 2
- A regra ILM contém duas colocações:
 - Armazene objetos replicando 1 cópia no Site 1
 - Armazene objetos replicando 1 cópia no Site 2

Posicionamento das regras de ILM:



Caso um dos locais seja perdido, cópias dos objetos estão disponíveis no outro local.

Exemplo de codificação de apagamento

Ter pools de armazenamento compostos por mais de um site por pool de storage permite configurar regras ILM que utilizam codificação de apagamento para proteção contra perda de site. Neste exemplo:

- O pool de storage 1 contém os sites 1 a 3
- A regra ILM contém um posicionamento: armazenar objetos por codificação de apagamento usando um esquema EC 4+2 no pool de storage 1, que contém três sites

Posicionamento das regras de ILM:



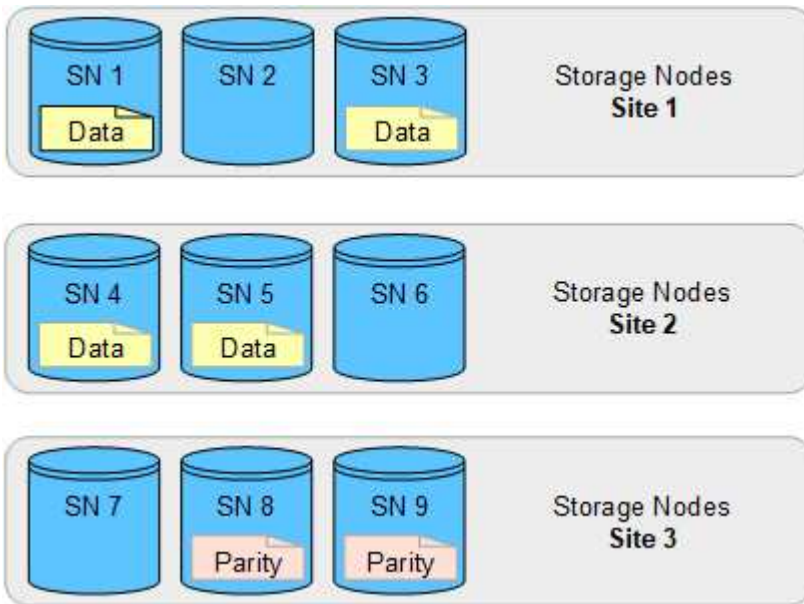
Neste exemplo:

- A regra ILM utiliza um esquema de codificação de apagamento 4+2.
- Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são calculados a partir dos dados do objeto.
- Cada um dos seis fragmentos é armazenado em um nó diferente em três sites de data center para fornecer proteção de dados em caso de falhas de nó ou perda de site.

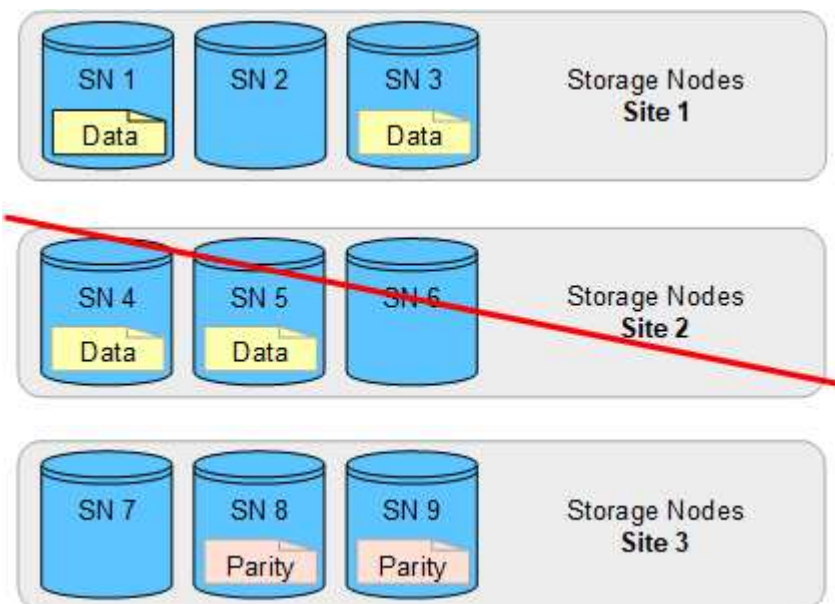


A codificação de apagamento é permitida em pools de storage que contenham qualquer número de sites, *exceto* dois sites.

Regra ILM usando esquema de codificação de apagamento 4+2:



Se um dos sites for perdido, os dados ainda poderão ser recuperados:



Crie um pool de storage no StorageGRID

Você cria pools de storage para determinar onde o StorageGRID armazena os dados dos objetos e o tipo de storage utilizado. Cada pool de storage inclui um ou mais sites e um ou mais storage grades.



Ao instalar StorageGRID 12.0 em uma nova grid, os pools de storage são criados automaticamente para cada site. No entanto, se você instalou inicialmente StorageGRID 11.6 ou uma versão anterior, os pools de storage não são criados automaticamente para cada site.

Se você deseja criar Cloud Storage Pools para armazenar dados de objetos fora do seu sistema StorageGRID, consulte o ["Informações sobre como usar os Cloud Storage Pools"](#).

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Você já analisou as diretrizes para a criação de pools de storage.

Sobre esta tarefa

Os pools de storage determinam onde os dados dos objetos são armazenados. O número de pools de storage que você precisa depende da quantidade de sites em seu grid e dos tipos de cópias que você deseja: replicadas ou com codificação de apagamento.

- Para replicação e codificação de apagamento em um único site, crie um pool de storage para cada site. Por exemplo, se você quiser armazenar cópias replicadas de objetos em três sites, crie três pools de storage.
- Para codificação de apagamento em três ou mais locais, crie um pool de storage que inclua uma entrada para cada local. Por exemplo, se você quiser aplicar codificação de apagamento a objetos em três locais, crie um pool de storage.



Não inclua o site "All Sites" em um pool de storage que será usado em um perfil de codificação de apagamento. Em vez disso, adicione uma entrada separada ao pool de storage para cada site que armazenará dados codificados por apagamento. Veja [esta etapa](#) para um exemplo.

- Se você tiver mais de um tipo de armazenamento, não crie um pool de storage que inclua diferentes tipos de armazenamento em um único local. Consulte o ["Diretrizes para a criação de pools de storage"](#).

Passos

1. Selecione **ILM > pool de storage**.

A aba "Pools de storage" lista todos os pools de storage definidos.



Para novas instalações do StorageGRID 11.6 ou anterior, o pool de storage All Storage Nodes é atualizado automaticamente sempre que você adiciona novos sites de data center. Não utilize este pool em regras ILM.

2. Para criar um novo pool de storage, selecione **Criar**.
3. Insira um nome exclusivo para o pool de storage. Use um nome que seja fácil de identificar ao configurar perfis de codificação de apagamento e regras ILM.
4. Na lista suspensa **Site**, selecione um site para este pool de storage.

Ao selecionar um site, o número de nós de Storage Nodes na tabela é atualizado automaticamente.

Em geral, não utilize o site "All Sites" em nenhum pool de storage. As regras do ILM que utilizam um pool de storage All Sites alocam objetos em qualquer site disponível, reduzindo seu controle sobre a alocação de objetos. Além disso, um pool de storage All Sites utiliza os Storage Nodes em um novo site imediatamente, o que pode não ser o comportamento que você espera.

5. Na lista suspensa **Nível de armazenamento**, selecione o tipo de storage que será usado se uma regra do ILM usar esse pool de storage.

A categoria de armazenamento, *inclui todas as categorias de armazenamento*, engloba todos os Storage Nodes no site selecionado. Se você criou categorias de armazenamento adicionais para os Storage

Nodes em sua grid, elas serão listadas no menu suspenso.

6. Se você quiser usar o pool de storage em um perfil de codificação de apagamento de vários sites, selecione **Adicionar mais nós** para adicionar uma entrada para cada site ao pool de storage.



Você será avisado se adicionar mais de uma entrada com diferentes grades de storage para um site.

Para remover uma entrada, selecione o ícone de excluir .

7. Quando estiver satisfeito com suas seleções, selecione **Salvar**.

O novo pool de storage é adicionado à lista.

Veja os detalhes do pool de storage no StorageGRID

Você pode visualizar os detalhes de um pool de storage para determinar onde o pool de storage é utilizado e para ver quais nós e grades de storage estão incluídos.

Antes de começar

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

Passos

1. Selecione **ILM > pool de storage**.

A tabela de pools de storage inclui as seguintes informações para cada pool de storage que inclui Storage Nodes:

- **Nome:** o nome de exibição exclusivo do pool de storage.
- **Contagem de nós:** o número de nós no pool de storage.
- **Uso de armazenamento:** A porcentagem do espaço total utilizável que foi usada para dados de objetos neste nó. Este valor não inclui metadados de objetos.
- **Capacidade total:** O tamanho do pool de storage, que corresponde à quantidade total de espaço utilizável para dados de objetos em todos os nós do pool de storage.
- **Uso do ILM:** Como o pool de storage está sendo usado atualmente. Um pool de storage pode estar ocioso ou pode estar sendo usado em uma ou mais regras de ILM, perfis de codificação de apagamento ou ambos.

2. Para visualizar os detalhes de um pool de storage específico, selecione o nome dele.

A página de detalhes do pool de storage é exibida.

3. Consulte a aba **Nós** para saber mais sobre os Nós de Armazenamento incluídos no pool de storage.

A tabela inclui as seguintes informações para cada nó:

- Nome do nó
- Nome do site
- Grau de storage

- Utilização do armazenamento: a porcentagem do espaço total utilizável para dados de objetos que foi utilizada pelo Nó de Armazenamento.



O mesmo valor de uso de storage (%) também é exibido no gráfico "Storage Utilizado - Dados do Objeto" para cada Storage Node (selecione **Nodes > Storage Node > Storage**).

4. Consulte a guia **Uso do ILM** para determinar se o pool de storage está sendo usado em alguma regra do ILM ou perfil de codificação de apagamento.
5. Opcionalmente, acesse a **página de regras do ILM** para saber mais e gerenciar quaisquer regras que utilizam o pool de storage.

Consulte o "[Instruções para trabalhar com regras ILM](#)".

Editar um pool de storage no StorageGRID

Você pode editar um pool de storage para alterar seu nome ou atualizar sites e storage grades.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador web compatível](#)".
- Você tem "[permissões de acesso específicas](#)".
- Você revisou o "[diretrizes para a criação de pools de storage](#)".
- Se você planeja editar um pool de storage usado por uma regra na política ILM ativa, você já considerou como suas alterações afetarão o posicionamento dos dados do objeto.

Sobre esta tarefa

Se você estiver adicionando um novo site ou nível de armazenamento a um pool de storage usado na política ILM ativa, esteja ciente de que os Storage Nodes no novo site ou nível de armazenamento não serão usados automaticamente. Para forçar o StorageGRID a usar um novo site ou nível de armazenamento, você deve ativar uma nova política ILM após salvar o pool de storage editado.

Passos

1. Selecione **ILM > pool de storage**.
2. Selecione a caixa de seleção correspondente ao pool de storage que você deseja editar.

Você não pode editar o pool de storage All Storage Nodes (StorageGRID 11.6 e versões anteriores).

3. Selecione **Editar**.
4. Se necessário, altere o nome do pool de storage.
5. Conforme necessário, selecione outros sites e níveis de storage.

Você está impedido de alterar o site ou o nível de armazenamento se o pool de storage for usado em um perfil de codificação de apagamento e a alteração invalidar o esquema de codificação de apagamento. Por exemplo, se um pool de storage usado em um perfil de codificação de apagamento incluir atualmente um nível de armazenamento com apenas um site, você está impedido de usar um nível de armazenamento com dois sites porque a alteração invalidaria o esquema de codificação de apagamento.



Adicionar ou remover sites de um pool de storage existente não moverá nenhum dado já codificado por apagamento. Se você quiser mover os dados existentes do site, será necessário criar um novo pool de storage e um novo perfil de EC para recodificar os dados.

6. Selecione **Salvar**.

Depois que você terminar

Se você adicionou um novo site ou nível de armazenamento a um pool de storage usado na política ILM ativa, ative uma nova política ILM para forçar o StorageGRID a usar o novo site ou nível de armazenamento. Por exemplo, clone sua política ILM existente e depois ative o clone. Consulte ["Trabalhe com regras e políticas do ILM"](#).

Remover um pool de storage no StorageGRID

Você pode remover um pool de storage que não está sendo usado.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["permissões de acesso necessárias"](#).

Passos

1. Selecione **ILM > pool de storage**.
2. Consulte a coluna de uso do ILM na tabela para determinar se você pode remover o pool de storage.

Não é possível remover um pool de storage se ele estiver sendo usado em uma regra ILM ou em um perfil de codificação de apagamento. Se necessário, selecione **storage pool name > ILM usage** para determinar onde o pool de storage está sendo usado.

3. Se o pool de storage que você deseja remover não estiver sendo usado, selecione a caixa de seleção.
4. Selecione **Remove**.
5. Selecione **OK**.

Use Cloud Storage Pools

Saiba mais sobre Cloud Storage Pools no StorageGRID

Um pool de storage em nuvem permite que você use o ILM para mover dados de objetos para fora do seu sistema StorageGRID. Por exemplo, você pode querer mover objetos acessados com pouca frequência para storage de nuvem de menor custo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou a camada de acesso Archive no Microsoft Azure Blob storage. Ou, você pode querer manter um backup em nuvem dos objetos do StorageGRID para aprimorar a recuperação de desastres.

Do ponto de vista do ILM, um pool de storage de nuvem é semelhante a um pool de storage. Para armazenar objetos em qualquer um dos locais, você seleciona o pool ao criar as instruções de posicionamento para uma regra do ILM. No entanto, enquanto os pools de storage consistem em Storage Nodes dentro do sistema StorageGRID, um pool de storage de nuvem consiste em um bucket externo (S3) ou contêiner (Azure Blob storage).

A tabela compara os pools de storage com os Cloud Storage Pools e mostra as semelhanças e diferenças de

alto nível.

	Pool de storage	Pool de storage em nuvem
Como é criado?	Utilizando a opção ILM > Pools de storage no Grid Manager.	Utilizando a opção ILM > Storage pools > Cloud Storage Pools no Grid Manager. Você precisa configurar o bucket ou contêiner externo antes de criar o Cloud Storage Pool.
Quanto pools você pode criar?	Ilimitado.	Até 10.
Onde os objetos são armazenados?	Em um ou mais nós de armazenamento dentro do StorageGRID.	Em um bucket do Amazon S3, um contêiner do Azure Blob storage ou um serviço do Google Cloud que é externo ao sistema StorageGRID. Se o pool de storage de nuvem for um bucket do Amazon S3: • Opcionalmente, você pode configurar um ciclo de vida do bucket para transferir objetos para storage de longo prazo e baixo custo, como Amazon S3 Glacier ou S3 Glacier Deep Archive. O sistema de storage externo deve ser compatível com a classe de storage Glacier e com a API S3 RestoreObject. • Você pode criar Cloud Storage Pools para uso com AWS Commercial Cloud Services (C2S), que são compatíveis com AWS Secret Region. Se o pool de storage de nuvem for um contêiner de Azure Blob storage, StorageGRID faz a transição do objeto para a camada Archive. Observação: Em geral, não configure o gerenciamento de ciclo de vida do Azure Blob storage para o contêiner usado para um Cloud Storage Pool. As operações RestoreObject em objetos no Cloud Storage Pool podem ser afetadas pelo ciclo de vida configurado.
O que controla o posicionamento dos objetos?	Uma regra ILM nas políticas ILM ativas.	Uma regra ILM nas políticas ILM ativas.
Qual método de proteção de dados é usado?	Replicação ou codificação de apagamento.	Replicação.

	Pool de storage	Pool de storage em nuvem
Quantas cópias de cada objeto são permitidas?	Múltiplos.	Uma cópia no Cloud Storage Pool e, opcionalmente, uma ou mais cópias no StorageGRID. Observação: Você não pode armazenar um objeto em mais de um pool de storage de nuvem ao mesmo tempo.
Quais são as vantagens?	Os objetos são rapidamente acessíveis a qualquer momento.	Storage de baixo custo. Observação: os dados do FabricPool não podem ser organizados em camadas nos Cloud Storage Pools.

Ciclo de vida de um objeto de pool de storage em nuvem no StorageGRID

Antes de implementar os Cloud Storage Pools, revise o ciclo de vida dos objetos armazenados em cada tipo de Cloud Storage Pool.

S3: Ciclo de vida de um objeto de pool de storage em nuvem

As etapas descrevem os estágios do ciclo de vida de um objeto armazenado em um pool de storage em nuvem do S3.



"Glacier" refere-se tanto à classe de armazenamento Glacier quanto à classe de armazenamento Glacier Deep Archive, com uma exceção: a classe de armazenamento Glacier Deep Archive não suporta o nível de restauração Expedited. Apenas a recuperação Bulk ou Standard é suportada.



A plataforma Google Cloud (GCP) suporta a recuperação de objetos do storage de longo prazo sem a necessidade de uma operação POST Restore.

1. Objeto armazenado no StorageGRID

Para iniciar o ciclo de vida, um aplicativo cliente armazena um objeto no StorageGRID.

2. Objeto movido para o pool de storage em nuvem S3

- Quando o objeto é correspondido por uma regra ILM que usa um Cloud Storage Pool S3 como local de armazenamento, StorageGRID move o objeto para o bucket S3 externo especificado pelo Cloud Storage Pool.
- Quando o objeto for movido para o S3 Cloud Storage Pool, o aplicativo cliente poderá recuperá-lo usando uma solicitação S3 GetObject do StorageGRID, a menos que o objeto tenha sido migrado para o armazenamento Glacier.

3. Objeto transferido para o Glacier (estado não recuperável)

- Opcionalmente, o objeto pode ser transferido para o storage Glacier. Por exemplo, o bucket S3 externo pode usar a configuração de ciclo de vida para transferir um objeto para o storage Glacier imediatamente ou após um determinado número de dias.



Se você deseja realizar a transição de objetos, precisa criar uma configuração de ciclo de vida para o bucket S3 externo e usar uma solução de storage que implemente a classe de armazenamento Glacier e seja compatível com a API RestoreObject do S3.

- Durante a transição, o aplicativo cliente pode usar uma solicitação S3 HeadObject para monitorar o status do objeto.

4. Objeto restaurado do storage Glacier

Se um objeto tiver sido migrado para o storage Glacier, o aplicativo cliente pode emitir uma solicitação S3 RestoreObject para restaurar uma cópia recuperável para o pool de storage em nuvem do S3. A solicitação especifica por quantos dias a cópia deve estar disponível no pool de storage em nuvem e o nível de acesso a dados a ser usado para a operação de restauração (Expedited, Standard ou Bulk). Quando a data de expiração da cópia recuperável for atingida, a cópia retorna automaticamente a um estado não recuperável.



Se uma ou mais cópias do objeto também existirem em Storage Nodes dentro do StorageGRID, não é necessário restaurar o objeto do Glacier emitindo uma solicitação RestoreObject. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação GetObject.

5. Objeto recuperado

Depois que um objeto for restaurado, o aplicativo cliente pode emitir uma solicitação GetObject para recuperar o objeto restaurado.

Azure: ciclo de vida de um objeto de pool de storage em nuvem

As etapas descrevem os estágios do ciclo de vida de um objeto armazenado em um pool de storage do Azure Cloud Storage.

1. Objeto armazenado no StorageGRID

Para iniciar o ciclo de vida, um aplicativo cliente armazena um objeto no StorageGRID.

2. Objeto movido para o pool de storage em nuvem do Azure

Quando o objeto é correspondido por uma regra de ILM que usa um pool de storage em nuvem do Azure como local de colocação, StorageGRID move o objeto para o container de Azure Blob storage externo especificado pelo Cloud Storage Pool.

3. Objeto transferido para o nível de Archive (estado não recuperável)

Imediatamente após mover o objeto para o pool de storage em nuvem do Azure, StorageGRID automaticamente transfere o objeto para a camada Archive do Azure Blob storage.

4. Objeto restaurado do nível Archive

Se um objeto tiver sido movido para a camada de Archive, o aplicativo cliente pode emitir uma solicitação S3 RestoreObject para restaurar uma cópia recuperável no pool de storage em nuvem do Azure.

Quando StorageGRID recebe o RestoreObject, ele transiciona temporariamente o objeto para a camada Cool do Azure Blob storage. Assim que a data de expiração na solicitação RestoreObject é atingida, StorageGRID transiciona o objeto de volta para a camada Archive.



Se uma ou mais cópias do objeto também existirem em Storage Nodes dentro do StorageGRID, não é necessário restaurar o objeto da camada de acesso Archive emitindo uma solicitação RestoreObject. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação GetObject.

5. Objeto recuperado

Depois que um objeto for restaurado para o pool de storage em nuvem do Azure, o aplicativo cliente pode emitir uma solicitação GetObject para recuperar o objeto restaurado.

Informações relacionadas

["Utilize a API REST S3"](#)

Casos de uso do Cloud Storage Pool no StorageGRID

Usando os Cloud Storage Pools, você pode fazer backup ou armazenar dados em camadas em um local externo. Além disso, você pode fazer backup ou armazenar dados em camadas em mais de uma nuvem.

Faça backup dos dados do StorageGRID em um local externo

Você pode usar um Cloud Storage Pool para fazer backup de objetos do StorageGRID em um local externo.

Se as cópias no StorageGRID estiverem inacessíveis, os dados do objeto no Cloud Storage Pool podem ser usados para atender às solicitações do cliente. No entanto, talvez seja necessário emitir uma solicitação S3 RestoreObject para acessar a cópia de backup do objeto no Cloud Storage Pool.

Os dados de objeto em um Cloud Storage Pool também podem ser usados para recuperar dados perdidos do StorageGRID devido a uma falha de volume de storage ou de Storage Node. Se a única cópia restante de um objeto estiver em um Cloud Storage Pool, o StorageGRID restaura temporariamente o objeto e cria uma nova cópia no Storage Node recuperado.

Para implementar uma solução de backup:

1. Crie um único Cloud Storage Pool.
2. Configure uma regra ILM que armazene simultaneamente cópias de objetos em Storage Nodes (como cópias replicadas ou com código de apagamento) e uma única cópia do objeto no Cloud Storage Pool.
3. Adicione a regra à sua política ILM. Em seguida, simule e ative a política.

Transferir dados de camada do StorageGRID para um local externo

Você pode usar um Cloud Storage Pool para armazenar objetos fora do sistema StorageGRID. Por exemplo, suponha que você tenha um grande número de objetos que precisa reter, mas espera acessá-los raramente, se é que vai acessá-los. Você pode usar um Cloud Storage Pool para transferir os objetos para um armazenamento de menor custo e liberar espaço no StorageGRID.

Para implementar uma solução de tiering:

1. Crie um único Cloud Storage Pool.
2. Configure uma regra ILM que mova objetos raramente usados dos Storage Nodes para o Cloud Storage Pool.

3. Adicione a regra à sua política ILM. Em seguida, simule e ative a política.

Manter vários endpoints na nuvem

Você pode configurar vários endpoints do Cloud Storage Pool se quiser fazer tiering ou backup de dados de objetos em mais de uma nuvem. Os filtros nas suas regras de ILM permitem especificar quais objetos são armazenados em cada Cloud Storage Pool. Por exemplo, você pode querer armazenar objetos de alguns tenants ou buckets no Amazon S3 Glacier e objetos de outros tenants ou buckets no Azure Blob storage. Ou você pode querer mover dados entre Amazon S3 Glacier e Azure Blob storage.



Ao usar vários pontos de extremidade do Cloud Storage Pool, lembre-se de que um objeto só pode ser armazenado em um Cloud Storage Pool por vez.

Para implementar vários endpoints na nuvem:

1. Crie até 10 Cloud Storage Pools.
2. Configure as regras do ILM para armazenar os dados de objeto apropriados no momento apropriado em cada Cloud Storage Pool. Por exemplo, armazene objetos do bucket A em Cloud Storage Pool A e objetos do bucket B em Cloud Storage Pool B. Ou, armazene objetos em Cloud Storage Pool A por um determinado período e depois mova-os para Cloud Storage Pool B.
3. Adicione as regras à sua política ILM. Em seguida, simule e ative a política.

Requisitos e limites do Cloud Storage Pool no StorageGRID

Se você planeja usar um Cloud Storage Pool para mover objetos para fora do sistema StorageGRID, deve revisar as considerações para configurar e usar Cloud Storage Pools.

Considerações gerais

- Em geral, o armazenamento em nuvem para arquivamento, como Amazon S3 Glacier ou Azure Blob storage, é uma opção econômica para armazenar dados de objetos. No entanto, os custos para recuperar dados do armazenamento em nuvem para arquivamento são relativamente altos. Para obter o menor custo total, você deve considerar quando e com que frequência acessará os objetos no Cloud Storage Pool. O uso de um Cloud Storage Pool é recomendado apenas para conteúdo que você espera acessar com pouca frequência.
- O uso de Cloud Storage Pools com FabricPool não é compatível devido à latência adicional para recuperar um objeto do destino do Cloud Storage Pool.
- Objetos com o S3 Object Lock ativado não podem ser colocados em Cloud Storage Pools.
- As seguintes combinações de plataforma, autenticação e protocolo com o S3 Object lock não são compatíveis com Cloud Storage Pools:
 - **Plataformas:** Google Cloud Platform e Azure
 - **Tipos de autenticação:** acesso anônimo
 - **Protocolo:** HTTP

Considerações sobre as portas utilizadas para os Cloud Storage Pools

Para garantir que as regras do ILM possam mover objetos de e para o Cloud Storage Pool especificado, você deve configurar a(s) rede(s) que contém(êm) os Storage Nodes do seu sistema. Você deve garantir que as seguintes portas possam se comunicar com o Cloud Storage Pool.

Por padrão, os Cloud Storage Pools usam as seguintes portas:

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

Você pode especificar uma porta diferente ao criar ou editar um Cloud Storage Pool.

Se você utiliza um servidor proxy não transparente, também precisa "[configurar um servidor proxy de storage](#)" permitir que mensagens sejam enviadas para endpoints externos, como um endpoint na internet.

Considerações sobre custos

O acesso ao storage na nuvem usando um Cloud Storage Pool requer conectividade de rede com a nuvem. Você deve considerar o custo da infraestrutura de rede que usará para acessar a nuvem e provisioná-la adequadamente, com base na quantidade de dados que espera mover entre StorageGRID e a nuvem usando o Cloud Storage Pool.

Quando StorageGRID se conecta ao endpoint externo do Cloud Storage Pool, ele emite várias solicitações para monitorar a conectividade e garantir que pode executar as operações necessárias. Embora alguns custos adicionais estejam associados a essas solicitações, o custo de monitorar um Cloud Storage Pool deve representar apenas uma pequena fração do custo total de armazenar objetos no S3 ou no Azure.

Custos mais significativos podem ser incorridos se você precisar mover objetos de um endpoint externo do Cloud Storage Pool de volta para StorageGRID. Objetos podem ser movidos de volta para StorageGRID em qualquer um destes casos:

- A única cópia do objeto está em um Cloud Storage Pool e você decide armazenar o objeto no StorageGRID em vez disso. Nesse caso, você reconfigura suas regras e políticas do ILM. Quando a avaliação do ILM ocorre, o StorageGRID faz várias solicitações para recuperar o objeto do Cloud Storage Pool. O StorageGRID então cria localmente o número especificado de cópias replicadas ou com código de eliminação. Depois que o objeto é movido de volta para o StorageGRID, a cópia no Cloud Storage Pool é excluída.
- Os objetos são perdidos devido a falha no Storage Node. Se a única cópia restante de um objeto estiver em um Cloud Storage Pool, o StorageGRID restaura temporariamente o objeto e cria uma nova cópia no Storage Node recuperado.



Quando objetos são movidos de volta para StorageGRID a partir de um Cloud Storage Pool, StorageGRID envia várias solicitações ao endpoint do Cloud Storage Pool para cada objeto. Antes de mover grandes quantidades de objetos, entre em contato com o suporte técnico para obter ajuda na estimativa do tempo necessário e dos custos associados.

S3: permissões necessárias para o bucket do Cloud Storage Pool

As políticas do bucket S3 externo usado para um Cloud Storage Pool devem conceder ao StorageGRID permissão para mover um objeto para o bucket, obter o status de um objeto, restaurar um objeto do armazenamento Glacier quando necessário e mais. Idealmente, o StorageGRID deve ter acesso de controle total ao bucket (`s3:*`; no entanto, se isso não for possível, a política do bucket deve conceder as seguintes permissões S3 ao StorageGRID:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`

- s3:ListBucket
- s3:ListBucketMultipartUploads
- s3:ListMultipartUploadParts
- s3:PutObject
- s3:RestoreObject

S3: Considerações sobre o ciclo de vida do bucket externo

A movimentação de objetos entre StorageGRID e o bucket S3 externo especificado no Cloud Storage Pool é controlada pelas regras de ILM e pelas políticas de ILM ativas no StorageGRID. Em contraste, a transição de objetos do bucket S3 externo especificado no Cloud Storage Pool para Amazon S3 Glacier ou S3 Glacier Deep Archive (ou para uma solução de storage que implemente a classe de armazenamento Glacier) é controlada pela configuração de ciclo de vida desse bucket.

Se você deseja migrar objetos do Cloud Storage Pool, é necessário criar a configuração de ciclo de vida apropriada no bucket S3 externo e usar uma solução de storage que implemente a classe de armazenamento Glacier e seja compatível com a API RestoreObject do S3.

Por exemplo, suponha que você queira que todos os objetos movidos do StorageGRID para o Cloud Storage Pool sejam transferidos imediatamente para o armazenamento Amazon S3 Glacier. Você criaria uma configuração de ciclo de vida no bucket S3 externo que especifica uma única ação (**Transição**) da seguinte forma:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Essa regra faria a transição de todos os objetos do bucket para o Amazon S3 Glacier no dia em que foram criados (ou seja, no dia em que foram movidos do StorageGRID para o Cloud Storage Pool).



Ao configurar o ciclo de vida do bucket externo, nunca use ações de **Expiração** para definir quando os objetos expiram. As ações de Expiração fazem com que o sistema de storage externo exclua os objetos expirados. Se você tentar acessar um objeto expirado posteriormente no StorageGRID, o objeto excluído não será encontrado.

Se você deseja migrar objetos no Cloud Storage Pool para o S3 Glacier Deep Archive (em vez do Amazon S3 Glacier), especifique `<StorageClass>DEEP\_ARCHIVE</StorageClass>` no ciclo de vida do bucket. No entanto, esteja ciente de que você não pode usar o nível `Expedited` para restaurar objetos do S3 Glacier

Deep Archive.

Azure: considerações sobre a camada de acesso

Ao configurar uma conta de armazenamento do Azure, você pode definir o nível de acesso padrão como Hot ou Cool. Ao criar uma conta de armazenamento para uso com um Cloud Storage Pool, você deve usar o nível Hot como padrão. Embora o StorageGRID defina imediatamente o nível como Archive ao mover objetos para o Cloud Storage Pool, usar a configuração padrão Hot garante que você não será cobrado por exclusão antecipada de objetos removidos do nível Cool antes do período mínimo de 30 dias.

Azure: gerenciamento de ciclo de vida não suportado

Não utilize o gerenciamento de ciclo de vida do Azure Blob storage para o contêiner usado com um Cloud Storage Pool. As operações de ciclo de vida podem interferir nas operações do Cloud Storage Pool.

Informações relacionadas

["Criar um Cloud Storage Pool"](#)

Pools de armazenamento em nuvem e CloudMirror replication no StorageGRID

Ao começar a usar os Cloud Storage Pools, pode ser útil entender as semelhanças e diferenças entre os Cloud Storage Pools e o serviço de replicação StorageGRID CloudMirror.

	Pool de storage em nuvem	CloudMirror serviço de replicação
Qual é o objetivo principal?	Funciona como um destino de arquivamento. A cópia do objeto no Cloud Storage Pool pode ser a única cópia do objeto ou pode ser uma cópia adicional. Ou seja, em vez de manter duas cópias localmente, você pode manter uma cópia no StorageGRID e enviar uma cópia para o Cloud Storage Pool.	Permite que um locatário replique automaticamente objetos de um bucket no StorageGRID (origem) para um bucket S3 externo (destino). Cria uma cópia independente de um objeto em uma infraestrutura S3 independente.
Como é configurado?	Definido da mesma forma que os pools de storage, usando o Grid Manager ou a Grid Management API. Pode ser selecionado como local de colocação em uma regra ILM. Enquanto um pool de storage consiste em um grupo de Storage Nodes, um Cloud Storage Pool é definido usando um endpoint remoto S3 ou Azure (endereço IP, credenciais e assim por diante).	Um usuário locatário "configura a replicação CloudMirror" define um endpoint CloudMirror (endereço IP, credenciais e assim por diante) usando o Gerenciador de Locatários ou a API S3. Depois que o endpoint CloudMirror é configurado, qualquer bucket pertencente a essa conta de locatário pode ser configurado para apontar para o endpoint CloudMirror.
Quem é responsável por configurá-lo?	Normalmente, um administrador de grid	Normalmente, um usuário tenant

	Pool de storage em nuvem	CloudMirror serviço de replicação
Qual é o destino?	- Qualquer infraestrutura S3 compatível (incluindo Amazon S3) - Camada de Arquivo de Blob do Azure - Google Cloud Platform (GCP)	- Qualquer infraestrutura S3 compatível (incluindo Amazon S3) - Google Cloud Platform (GCP)
O que faz com que os objetos sejam movidos para o destino?	Uma ou mais regras ILM nas políticas ILM ativas. As regras ILM definem quais objetos StorageGRID move para o Cloud Storage Pool e quando os objetos são movidos.	O ato de ingerir um novo objeto em um bucket de origem que foi configurado com um endpoint CloudMirror. Objetos que já existiam no bucket de origem antes de o bucket ser configurado com o endpoint CloudMirror não são replicados, a menos que sejam modificados.
Como os objetos são recuperados?	Os aplicativos devem fazer solicitações ao StorageGRID para recuperar objetos que foram movidos para um Cloud Storage Pool. Se a única cópia de um objeto tiver sido transferida para armazenamento de arquivamento, o StorageGRID gerencia o processo de restauração do objeto para que ele possa ser recuperado.	Como a cópia espelhada no bucket de destino é uma cópia independente, os aplicativos podem recuperar o objeto fazendo solicitações ao StorageGRID ou ao destino S3. Por exemplo, suponha que você use a replicação CloudMirror para espelhar objetos para uma organização parceira. O parceiro pode usar seus próprios aplicativos para ler ou atualizar objetos diretamente do destino S3. Não é necessário usar o StorageGRID.
É possível ler diretamente do destino?	Não. Os objetos movidos para um Cloud Storage Pool são gerenciados pelo StorageGRID. As solicitações de leitura devem ser direcionadas ao StorageGRID (e o StorageGRID será responsável pela recuperação a partir do Cloud Storage Pool).	Sim, porque a cópia espelhada é uma cópia independente.
O que acontece se um objeto for excluído da origem?	O objeto também é excluído do Cloud Storage Pool.	A ação de exclusão não é replicada. Um objeto excluído deixa de existir no bucket do StorageGRID, mas continua existindo no bucket de destino. Da mesma forma, objetos no bucket de destino podem ser excluídos sem afetar a origem.
Como você acessa objetos após um desastre (sistema StorageGRID inoperante)?	Os nós do StorageGRID com falha precisam ser recuperados. Durante esse processo, cópias de objetos replicados podem ser restauradas usando as cópias no Cloud Storage Pool.	As cópias dos objetos no destino CloudMirror são independentes do StorageGRID, então podem ser acessadas diretamente antes que os nós do StorageGRID sejam recuperados.

Criar um Cloud Storage Pool no StorageGRID

Um pool de storage em nuvem especifica um único bucket externo do Amazon S3 ou outro provedor compatível com S3, ou ainda um contêiner de storage de Blobs do Azure.

Ao criar um pool de storage em nuvem, você especifica o nome e a localização do bucket ou contêiner externo que StorageGRID usará para armazenar objetos, o tipo de provedor de nuvem (Amazon S3/GCP ou Azure Blob storage) e as informações que o StorageGRID precisa para acessar o bucket ou contêiner externo.

StorageGRID valida o Cloud Storage Pool assim que você o salva, portanto, você deve garantir que o bucket ou contêiner especificado no Cloud Storage Pool exista e esteja acessível.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["permissões de acesso necessárias"](#).
- Você revisou o ["Considerações sobre Cloud Storage Pools"](#).
- O bucket ou contêiner externo referenciado pelo Cloud Storage Pool já existe e você tem o [informações do endpoint de serviço](#).
- Para acessar o bucket ou container, você tem a [Informações da conta para o tipo de autenticação](#) que vai escolher.

Passos

1. Selecione **ILM > Storage pools > Cloud Storage Pools**.
2. Selecione **Criar** e, em seguida, insira as seguintes informações:

Campo	Descrição
Nome do pool de storage em nuvem	Um nome que descreva brevemente o pool de storage em nuvem e sua finalidade. Use um nome que seja fácil de identificar ao configurar as regras de ILM.
Tipo de provedor	Qual provedor de nuvem você usará para este pool de storage em nuvem? • Amazon S3/GCP: Selecione esta opção para um Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) ou outro provedor compatível com S3. • Azure Blob Storage
Bucket ou container	O nome do bucket S3 externo ou do contêiner do Azure. Você não pode alterar esse valor depois que o pool de Cloud Storage é salvo.

3. Com base na sua seleção de tipo de provedor, insira as informações do endpoint de serviço.

Amazon S3/GCP

- a. Para o protocolo, selecione HTTPS ou HTTP.



Não utilize conexões HTTP para dados confidenciais.

- b. Digite o nome do host. Exemplo:

`s3-aws-region.amazonaws.com`

- c. Selecione o estilo da URL:

Opção	Descrição
Detecção automática	Tenta detectar automaticamente qual estilo de URL usar, com base nas informações fornecidas. Por exemplo, se você especificar um endereço IP, StorageGRID usará uma URL no formato de caminho. Selecione esta opção somente se você não souber qual estilo específico usar.
Estilo virtual-hosted	Use uma URL no estilo de hospedagem virtual para acessar o bucket. URLs no estilo de hospedagem virtual incluem o nome do bucket como parte do nome de domínio. Exemplo: <code>https://bucket-name.s3.company.com/key-name</code>
Estilo de caminho	Use uma URL no formato de caminho para acessar o bucket. URLs no formato de caminho incluem o nome do bucket no final. Exemplo: <code>https://s3.company.com/bucket-name/key-name</code> Nota: A opção de URL no formato de caminho não é recomendada e será descontinuada em uma versão futura do StorageGRID.

- d. Opcionalmente, insira o número da porta ou use a porta padrão: 443 para HTTPS ou 80 para HTTP.

Azure Blob Storage

- a. Usando um dos seguintes formatos, insira o URI do endpoint do serviço.

- `https://host:port`
- `http://host:port`

Exemplo: `https://myaccount.blob.core.windows.net:443`

Se você não especificar uma porta, por padrão a porta 443 é usada para HTTPS e a porta 80 é usada para HTTP.

4. Selecione **Continuar**. Em seguida, selecione o tipo de autenticação e insira as informações necessárias para o endpoint do Cloud Storage Pool:

Chave de acesso

Para Amazon S3/GCP ou outro provedor compatível com S3

- a. **ID da chave de acesso:** Insira o ID da chave de acesso da conta proprietária do bucket externo.
- b. **Chave de acesso secreta:** Digite a chave de acesso secreta.

IAM Roles Anywhere

Para o serviço AWS IAM Roles Anywhere

StorageGRID utiliza o AWS Security Token Service (STS) para gerar dinamicamente um token de curta duração para acessar recursos da AWS.

- a. **Região do AWS IAM Roles Anywhere:** selecione a região para o pool de storage em nuvem. Por exemplo, `us-east-1`.
- b. **URN da âncora de confiança:** Insira o URN da âncora de confiança que valida as solicitações de credenciais STS de curta duração. Pode ser uma CA raiz ou intermediária.
- c. **URN do perfil:** Insira o URN do perfil do IAM Roles Anywhere que lista as funções que podem ser assumidas por qualquer pessoa confiável.
- d. **URN da função:** Insira o URN da função IAM que pode ser assumida por qualquer pessoa confiável.
- e. **Duração da sessão:** Insira a duração das credenciais de segurança temporárias e da sessão de função. Insira pelo menos 15 minutos e no máximo 12 horas.
- f. **Certificado de CA do servidor** (opcional): Um ou mais certificados de CA confiáveis, em formato PEM, para verificar o servidor IAM Roles Anywhere. Se omitido, o servidor não será verificado.
- g. **Certificado de entidade final:** A chave pública, em formato PEM, do certificado X509 assinado pela trust anchor. O AWS IAM Roles Anywhere usa essa chave para emitir um token STS.
- h. **Chave privada da entidade final:** a chave privada do certificado da entidade final.

CAP (portal de acesso C2S)

Para o serviço S3 de Commercial Cloud Services (C2S)

- a. **URL de credenciais temporárias:** Insira a URL completa que StorageGRID usará para obter credenciais temporárias do servidor CAP, incluindo todos os parâmetros de API obrigatórios e opcionais atribuídos à sua conta C2S.
- b. **Certificado CA do servidor:** Selecione **Procurar** e carregue o certificado CA que StorageGRID usará para verificar o servidor CAP. O certificado deve estar codificado em PEM e ter sido emitido por uma Autoridade de Certificação (CA) governamental apropriada.
- c. **Certificado do cliente:** selecione **Procurar** e carregue o certificado que StorageGRID usará para se identificar no servidor CAP. O certificado do cliente deve estar codificado em PEM, ser emitido por uma Autoridade Certificadora (CA) governamental apropriada e ter permissão de acesso à sua conta C2S.
- d. **Chave privada do cliente:** selecione **Procurar** e carregue a chave privada codificada em PEM para o certificado do cliente.
- e. Se a chave privada do cliente estiver criptografada, insira a senha para descriptografar a chave privada do cliente. Caso contrário, deixe o campo **Senha da chave privada do cliente** em branco.



Se o certificado do cliente for criptografado, use o formato tradicional para a criptografia. O formato criptografado PKCS #8 não é compatível.

Azure Blob Storage

Somente para Azure Blob Storage, apenas com Shared Key

- Nome da conta:** Insira o nome da conta de armazenamento que é proprietária do contêiner externo
- Chave da conta:** Insira a chave secreta da conta de storage

Você pode usar o portal do Azure para encontrar esses valores.

Anônimo

Nenhuma informação adicional é necessária.

5. Selecione **Continuar**. Em seguida, escolha o tipo de verificação de servidor que você deseja usar:

Opção	Descrição
Use certificados de CA raiz no sistema operacional do nó de armazenamento	Utilize os certificados Grid CA instalados no sistema operacional para proteger as conexões.
Use um certificado CA personalizado	Utilize um certificado de CA personalizado. Selecione Procurar e carregue o certificado codificado em PEM.
Não verificar o certificado	Selecionar esta opção significa que as conexões TLS com o Cloud Storage Pool não são seguras.

6. Selecione **Salvar**.

Ao salvar um Cloud Storage Pool, StorageGRID faz o seguinte:

- Valida se o bucket ou contêiner e o endpoint do serviço existem e se podem ser acessados usando as credenciais que você especificou.
- Grava um arquivo marcador no bucket ou contêiner para identificá-lo como um Cloud Storage Pool. Nunca remova este arquivo, que tem o nome `x-ntap-sgws-cloud-pool-uuid`.

Se a validação do Cloud Storage Pool falhar, você receberá uma mensagem de erro explicando o motivo da falha. Por exemplo, um erro pode ser relatado se houver um erro de certificado ou se o bucket ou contêiner que você especificou ainda não existir.

7. Se ocorrer um erro, consulte o "[Instruções para solucionar problemas em Cloud Storage Pools](#)", resolva quaisquer problemas e tente salvar o pool de storage em nuvem novamente.

Veja os detalhes do Cloud Storage Pool no StorageGRID

Você pode visualizar os detalhes de um Cloud Storage Pool para determinar onde ele é usado e para ver quais nós e storage grades estão incluídos.

Antes de começar

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

Passos

1. Selecione **ILM > Storage pools > Cloud Storage Pools**.

A tabela de Cloud Storage Pools inclui as seguintes informações para cada Cloud Storage Pool que inclui Storage Nodes:

- **Nome:** O nome de exibição exclusivo do pool.
- **URI:** O Identificador Uniforme de Recursos do pool de storage de nuvem.
- **Tipo de provedor:** Qual provedor de nuvem é usado para este Cloud Storage Pool.
- **Contêiner:** O nome do bucket usado para o pool de storage de nuvem.
- **Uso do ILM:** Como o pool está sendo usado atualmente. Um Cloud Storage Pool pode estar ocioso ou pode estar sendo usado em uma ou mais regras de ILM, perfis de codificação de apagamento ou ambos.
- **Último erro:** O último erro detectado durante uma verificação de integridade deste pool de storage de nuvem.

2. Para visualizar os detalhes de um Cloud Storage Pool específico, selecione o nome dele.

A página de detalhes do pool é exibida.

3. Consulte a guia **Autenticação** para saber mais sobre o tipo de autenticação para este pool de storage em nuvem e para editar os detalhes de autenticação.
4. Consulte a aba **Verificação do servidor** para obter detalhes sobre a verificação, editar a verificação, baixar um novo certificado ou copiar o PEM do certificado.
5. Consulte a guia **Uso do ILM** para determinar se o Cloud Storage Pool está sendo usado em alguma regra de ILM ou perfil de codificação de apagamento.
6. Opcionalmente, acesse a **página de regras do ILM** para ["saiba mais e gerencie quaisquer regras"](#) que usam o pool de storage de nuvem.

Editar um Cloud Storage Pool no StorageGRID

Você pode editar um Cloud Storage Pool para alterar seu nome, endpoint de serviço ou outros detalhes; no entanto, não é possível alterar o bucket do S3 ou o container do Azure para um Cloud Storage Pool.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Você revisou o ["Considerações sobre Cloud Storage Pools"](#).

Passos

1. Selecione **ILM > Storage pools > Cloud Storage Pools**.

A tabela Cloud Storage Pools lista os Cloud Storage Pools existentes.

2. Selecione a caixa de seleção do Cloud Storage Pool que você deseja editar e, em seguida, selecione **Ações > Editar**.

Como alternativa, selecione o nome do Cloud Storage Pool e, em seguida, selecione **Editar**.

3. Conforme necessário, altere o nome do Cloud Storage Pool, o service endpoint, as credenciais de autenticação ou o método de verificação do certificado.



Você não pode alterar o tipo de provedor, o bucket S3 ou o contêiner do Azure para um pool de storage em nuvem.

Se você já carregou um certificado de servidor ou cliente, pode expandir o painel **Detalhes do certificado** para revisar o certificado que está em uso no momento.

4. Selecione **Salvar**.

Ao salvar um Cloud Storage Pool, o StorageGRID valida se o bucket ou contêiner e o endpoint do serviço existem e se podem ser acessados usando as credenciais que você especificou.

Se a validação do Cloud Storage Pool falhar, uma mensagem de erro será exibida. Por exemplo, um erro pode ser relatado se houver um erro de certificado.

Consulte as instruções para "[Solução de problemas em Cloud Storage Pools](#)", resolva o problema e tente salvar o pool de storage em nuvem novamente.

Remover um Cloud Storage Pool no StorageGRID

Você pode remover um Cloud Storage Pool se ele não for usado em uma regra do ILM e não contiver dados de objetos.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador web compatível](#)".
- Você tem o "[permissões de acesso necessárias](#)".

Se necessário, use o ILM para mover os dados do objeto

Se o Cloud Storage Pool que você deseja remover contiver dados de objetos, você deve usar o ILM para mover os dados para um local diferente. Por exemplo, você pode mover os dados para Storage Nodes em sua grid ou para um Cloud Storage Pool diferente.

Passos

1. Selecione **ILM > Storage pools > Cloud Storage Pools**.
2. Consulte a coluna de uso do ILM na tabela para determinar se você pode remover o Cloud Storage Pool.

Você não pode remover um pool de storage em nuvem se ele estiver sendo usado em uma regra ILM ou em um perfil de codificação de apagamento.

3. Se o Cloud Storage Pool estiver sendo usado, selecione **cloud storage pool name > uso do ILM**.
4. "[Clone cada regra ILM](#)" que atualmente coloca objetos no pool de storage em nuvem que você deseja remover.
5. Determine para onde você deseja mover os objetos existentes gerenciados por cada regra que você

clonou.

Você pode usar um ou mais pools de storage ou um Cloud Storage Pool diferente.

6. Edite cada uma das regras que você clonou.

Na Etapa 2 do assistente Criar regra ILM, selecione o novo local no campo **cópias em**.

7. "[Criar uma nova política ILM](#)" e substitua cada uma das regras antigas por uma regra clonada.

8. Ative a nova política.

9. Aguarde até que o ILM remova os objetos do pool de storage em nuvem e os coloque no novo local.

Excluir pool de storage em nuvem

Quando o pool de storage em nuvem estiver vazio e não for usado em nenhuma regra do ILM, você pode excluí-lo.

Antes de começar

- Você removeu todas as regras ILM que poderiam ter usado o pool.
- Você confirmou que o bucket S3 ou o contêiner do Azure não contém nenhum objeto.

Ocorre um erro se você tentar remover um Cloud Storage Pool que contenha objetos. Consulte "[Solucione problemas em pools de storage em nuvem](#)".



Ao criar um Cloud Storage Pool, o StorageGRID grava um arquivo marcador no bucket ou contêiner para identificá-lo como um Cloud Storage Pool. Não remova este arquivo, que tem o nome `x-ntap-sgws-cloud-pool-uuid`.

Passos

1. Selecione **ILM > Storage pools > Cloud Storage Pools**.
2. Se a coluna de uso do ILM indicar que o Cloud Storage Pool não está sendo usado, selecione a caixa de seleção.
3. Selecione **Ações > Remover**.
4. Selecione **OK**.

Solucione problemas de Cloud Storage Pools no StorageGRID

Use estas etapas de solução de problemas para ajudar a resolver erros que você possa encontrar ao criar, editar ou excluir um Cloud Storage Pool.

Determine se ocorreu um erro

StorageGRID realiza uma verificação de integridade simples em cada Cloud Storage Pool, lendo o objeto conhecido `x-ntap-sgws-cloud-pool-uuid` para garantir que o Cloud Storage Pool possa ser acessado e esteja funcionando corretamente. Quando StorageGRID encontra um erro no endpoint, realiza uma verificação de integridade a cada minuto a partir de cada Storage Node. Quando o erro é resolvido, as verificações de integridade param. Se uma verificação de integridade detectar um problema, uma mensagem será exibida na coluna Last error da tabela Cloud Storage Pools na página Storage pools.

A tabela mostra o erro mais recente detectado para cada Cloud Storage Pool e indica há quanto tempo o erro

ocorreu.

Além disso, um alerta de **erro de conectividade do Cloud Storage Pool** é acionado se a verificação de integridade detectar que um ou mais novos erros do Cloud Storage Pool ocorreram nos últimos 5 minutos. Se você receber uma notificação por e-mail para este alerta, acesse a página Storage pools (selecione **ILM > Storage pools**), revise as mensagens de erro na coluna Last error e consulte as diretrizes de solução de problemas abaixo.

Verifique se o erro foi resolvido

Após resolver quaisquer problemas subjacentes, você pode verificar se o erro foi solucionado. Na página Cloud Storage Pool, selecione o endpoint e selecione **Limpar erro**. Uma mensagem de confirmação indica que StorageGRID limpou o erro do Cloud Storage Pool.

Se o problema subjacente tiver sido resolvido, a mensagem de erro deixará de ser exibida. No entanto, se o problema subjacente não tiver sido corrigido (ou se ocorrer um erro diferente), a mensagem de erro será exibida na coluna "Último erro" dentro de alguns minutos.

Erro: a verificação de integridade falhou. Erro do endpoint.

Você pode encontrar esse erro ao habilitar o S3 Object Lock com retenção padrão para seu bucket do Amazon S3 depois de começar a usar esse bucket para um Cloud Storage Pool. Esse erro ocorre quando a operação PUT não possui um cabeçalho HTTP com um valor de checksum de carga, como Content-MD5. Esse valor de cabeçalho é exigido pela AWS para operações PUT em buckets com S3 Object Lock habilitado.

Para corrigir esse problema, siga os passos em ["Editar um pool de armazenamento em nuvem"](#) sem fazer nenhuma alteração. Essa ação aciona a validação da configuração do Cloud Storage Pool que detecta e atualiza automaticamente o sinalizador S3 Object Lock na configuração do endpoint do Cloud Storage Pool.

Erro: Este pool de armazenamento em nuvem contém conteúdo inesperado

Você pode encontrar esse erro ao tentar criar, editar ou excluir um Cloud Storage Pool. Esse erro ocorre se o bucket ou contêiner incluir o arquivo marcador `x-ntap-sgws-cloud-pool-uuid`, mas esse arquivo não tiver o campo de metadados com o UUID esperado.

Normalmente, você só verá esse erro se estiver criando um novo Cloud Storage Pool e outra instância do StorageGRID já estiver usando o mesmo Cloud Storage Pool.

Tente um destes passos para corrigir o problema:

- Se você estiver configurando um novo Cloud Storage Pool e o bucket contiver o arquivo `x-ntap-sgws-cloud-pool-uuid` e chaves de objeto adicionais semelhantes ao exemplo a seguir, crie um novo bucket e use esse novo bucket em vez disso.

Exemplo de uma chave de objeto adicional: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Se o ``x-ntap-sgws-cloud-pool-uuid`` arquivo for o único objeto no bucket, exclua esse arquivo.

Se essas etapas não se aplicarem ao seu cenário, entre em contato com o suporte.

Erro: Não foi possível criar ou atualizar o Cloud Storage Pool. Erro do endpoint

Você pode encontrar esse erro nas seguintes circunstâncias:

- Quando você tenta criar ou editar um Cloud Storage Pool.
- Ao selecionar uma combinação de plataforma, autenticação ou protocolo não compatível com o S3 Object Lock durante a configuração de um novo Cloud Storage Pool. Consulte ["Considerações sobre pools de armazenamento em nuvem"](#).

Este erro indica que um problema de conectividade ou de configuração está impedindo StorageGRID de gravar no Cloud Storage Pool.

Para corrigir o problema, revise a mensagem de erro do endpoint.

- Se a mensagem de erro contiver `Get url: EOF`, verifique se o endpoint de serviço usado para o Cloud Storage Pool não usa HTTP para um contêiner ou bucket que requer HTTPS.
- Se a mensagem de erro contiver `Get url: net/http: request canceled while waiting for connection`, verifique se a configuração de rede permite que os Storage Nodes acessem o endpoint do serviço usado para o Cloud Storage Pool.
- Se o erro for devido a uma plataforma, autenticação ou protocolo não suportado, altere para uma configuração suportada com S3 Object Lock e tente salvar o novo Cloud Storage Pool novamente.
- Para todas as outras mensagens de erro do endpoint, tente uma ou mais das seguintes opções:
 - Crie um contêiner ou bucket externo com o mesmo nome que você inseriu para o Cloud Storage Pool e tente salvar o novo Cloud Storage Pool novamente.
 - Corrija o nome do contêiner ou bucket que você especificou para o Cloud Storage Pool e tente salvar o novo Cloud Storage Pool novamente.

Erro: Falha ao analisar o certificado da CA

Você pode encontrar esse erro ao tentar criar ou editar um Cloud Storage Pool. O erro ocorre se StorageGRID não conseguir analisar o certificado inserido durante a configuração do Cloud Storage Pool.

Para corrigir o problema, verifique o certificado da Autoridade Certificadora (CA) que você forneceu para identificar possíveis problemas.

Erro: Não foi encontrado um Cloud Storage Pool com este ID

Você pode encontrar esse erro ao tentar editar ou excluir um Cloud Storage Pool. Esse erro ocorre se o endpoint retornar uma resposta 404, que pode significar uma das seguintes situações:

- As credenciais usadas para o Cloud Storage Pool não têm permissão de leitura para o bucket.
- O bucket usado para o Cloud Storage Pool não inclui o `x-ntap-sgws-cloud-pool-uuid` arquivo marcador.

Tente uma ou mais destas etapas para corrigir o problema:

- Verifique se o usuário associado à chave de acesso configurada possui as permissões necessárias.
- Edite o Cloud Storage Pool com credenciais que possuam as permissões necessárias.
- Se as permissões estiverem corretas, entre em contato com o suporte.

Erro: Não foi possível verificar o conteúdo do Cloud Storage Pool. Erro do endpoint

Você pode encontrar esse erro ao tentar excluir um Cloud Storage Pool. Esse erro indica que algum problema de conectividade ou configuração está impedindo StorageGRID de ler o conteúdo do bucket do Cloud Storage Pool.

Para corrigir o problema, revise a mensagem de erro do endpoint.

Erro: objetos já foram colocados neste bucket

Você pode encontrar esse erro ao tentar excluir um Cloud Storage Pool. Você não pode excluir um Cloud Storage Pool se ele contiver dados que foram movidos para lá pelo ILM, dados que já estavam no bucket antes de você configurar o Cloud Storage Pool ou dados que foram colocados no bucket por outra fonte após a criação do Cloud Storage Pool.

Tente uma ou mais destas etapas para corrigir o problema:

- Siga as instruções para mover objetos de volta para StorageGRID em "Ciclo de vida de um objeto do Cloud Storage Pool".
- Se você tiver certeza de que os objetos restantes não foram colocados no Cloud Storage Pool pelo ILM, exclua manualmente os objetos do bucket.



Nunca exclua manualmente objetos de um Cloud Storage Pool que possam ter sido colocados lá pelo ILM. Se você tentar acessar posteriormente um objeto excluído manualmente do StorageGRID, o objeto excluído não será encontrado.

Erro: o proxy encontrou um erro externo ao tentar acessar o Cloud Storage Pool

Você pode encontrar esse erro se tiver configurado um proxy de storage não transparente entre os Storage Nodes e o endpoint S3 externo usado para o Cloud Storage Pool. Esse erro ocorre se o servidor proxy externo não conseguir alcançar o endpoint do Cloud Storage Pool. Por exemplo, o servidor DNS pode não conseguir resolver o nome do host ou pode haver um problema de rede externa.

Tente uma ou mais destas etapas para corrigir o problema:

- Verifique as configurações do Cloud Storage Pool (**ILM > storage pools**).
- Verifique a configuração de rede do servidor proxy de storage.

Erro: o certificado X.509 está fora do período de validade

Você pode encontrar esse erro ao tentar excluir um Cloud Storage Pool. Esse erro ocorre quando a autenticação exige um certificado X.509 para garantir que o Cloud Storage Pool externo correto seja validado e que o pool externo esteja vazio antes da exclusão da configuração do Cloud Storage Pool.

Tente seguir estes passos para corrigir o problema:

- Atualize o certificado configurado para autenticação no Cloud Storage Pool.
- Certifique-se de que qualquer alerta de expiração de certificado neste Cloud Storage Pool seja resolvido.

Informações relacionadas

["Ciclo de vida de um objeto de cloud storage pool"](#)

Gerencie perfis de codificação de apagamento no StorageGRID

Você pode visualizar os detalhes de um perfil de codificação de apagamento e renomeá-lo, se necessário. Você pode desativar um perfil de codificação de apagamento caso ele não esteja sendo usado em nenhuma regra de gerenciamento do ciclo de vida das

informações (ILM).

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["permissões de acesso necessárias"](#).

Veja os detalhes do perfil de codificação de apagamento

Você pode visualizar os detalhes de um perfil de codificação de apagamento para determinar seu status, o esquema de codificação de apagamento utilizado e outras informações.

Passos

1. Selecione **Configuração > Sistema > Codificação de apagamento**.
2. Selecione o perfil. A página de detalhes do perfil é exibida.
3. Opcionalmente, visualize a guia de regras do ILM para ver uma lista das regras do ILM que usam o perfil e das políticas do ILM que usam essas regras.
4. Opcionalmente, consulte a guia Nós de Armazenamento para obter detalhes sobre cada Nó de Armazenamento no pool de storage do perfil, como o site onde está localizado e o uso de storage.

Renomear um perfil de codificação de apagamento

Você pode querer renomear um perfil de codificação de apagamento para tornar mais óbvio o que o perfil faz.

Passos

1. Selecione **Configuração > Sistema > Codificação de apagamento**.
2. Selecione o perfil que deseja renomear.
3. Selecione **Renomear**.
4. Insira um nome exclusivo para o perfil de codificação de apagamento.

O nome do perfil de codificação de apagamento é anexado ao nome do pool de storage na instrução de posicionamento de uma regra ILM.



Os nomes dos perfis de codificação de apagamento devem ser únicos. Ocorre um erro de validação se você usar o nome de um perfil existente, mesmo que esse perfil tenha sido desativado.

5. Selecione **Salvar**.

Desativar um perfil de codificação de apagamento

Você pode desativar um perfil de codificação de apagamento se não planeja mais usá-lo e se o perfil não estiver sendo usado atualmente em nenhuma regra ILM.



Confirme que não há operações de reparo de dados com codificação de eliminação ou procedimentos de desativação em andamento. Uma mensagem de erro será exibida se você tentar desativar um perfil de codificação de eliminação enquanto qualquer uma dessas operações estiver em andamento.

Sobre esta tarefa

StorageGRID impede você de desativar um perfil de codificação de apagamento se alguma das seguintes condições for verdadeira:

- O perfil de codificação de apagamento está sendo usado atualmente em uma regra ILM.
- O perfil de codificação de apagamento não é mais usado em nenhuma regra ILM, mas os dados do objeto e os fragmentos de paridade para o perfil ainda existem.

Passos

1. Selecione **Configuração > Sistema > Codificação de apagamento**.
2. Na guia Ativo, verifique a coluna **Status** para confirmar que o perfil de codificação de apagamento que você deseja desativar não está sendo usado em nenhuma regra ILM.

Você não pode desativar um perfil de codificação de apagamento se ele for usado em qualquer regra de ILM. No exemplo, o perfil 2+1 Data Center 1 é usado em pelo menos uma regra de ILM.

☐	Profile name ?	Status ?	Storage pool ?	Erasure-coding scheme ?
☐	2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
☐	New profile	Deactivated	Data Center 1	2+1

3. Se o perfil for usado em uma regra ILM, siga estas etapas:
 - a. Selecione **ILM > Regras**.
 - b. Selecione cada regra e revise o diagrama de retenção para determinar se a regra usa o perfil de codificação de apagamento que você deseja desativar.
 - c. Se a regra ILM usar o perfil de codificação de apagamento que você deseja desativar, verifique se a regra é usada em alguma política ILM.
 - d. Complete as etapas adicionais na tabela, com base em onde o perfil de erasure-coding é usado.

Onde o perfil foi utilizado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Nunca usado em nenhuma regra ILM	Não são necessárias etapas adicionais. Continue com este procedimento.	Nenhum
Em uma regra ILM que nunca foi usada em nenhuma política ILM	i. Edite ou exclua todas as regras ILM afetadas. Se você editar a regra, remova todos os posicionamentos que usam o perfil de codificação de apagamento. ii. Continue com este procedimento.	"Trabalhe com regras e políticas do ILM"

Onde o perfil foi utilizado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Em uma regra ILM que está atualmente em uma política ILM ativa	i. Clone a política. ii. Remova a regra ILM que usa o perfil de erasure-coding. iii. Adicione uma ou mais novas regras ILM para garantir que os objetos estejam protegidos. iv. Salve, simule e ative a nova política. v. Aguarde a aplicação da nova política e a movimentação dos objetos existentes para novos locais com base nas novas regras que você adicionou. Nota: Dependendo do número de objetos e do tamanho do seu sistema StorageGRID, as operações do ILM podem levar semanas ou até meses para mover os objetos para novos locais, com base nas novas regras do ILM. Embora você possa tentar desativar com segurança um perfil de codificação de apagamento enquanto ele ainda estiver associado a dados, a operação de desativação falhará. Uma mensagem de erro informará você se o perfil ainda não estiver pronto para ser desativado. vi. Edite ou exclua a regra que você removeu da política. Se você editar a regra, remova todos os posicionamentos que usam o perfil de codificação de apagamento. vii. Continue com este procedimento.	"Crie uma política ILM" "Trabalhe com regras e políticas do ILM"
Em uma regra ILM que está atualmente em uma política ILM	i. Edite a política. ii. Remova a regra ILM que usa o perfil de erasure-coding. iii. Adicione uma ou mais novas regras ILM para garantir que todos os objetos estejam protegidos. iv. Salve a política. v. Edite ou exclua a regra que você removeu da política. Se você editar a regra, remova todos os posicionamentos que usam o perfil de codificação de apagamento. vi. Continue com este procedimento.	"Crie uma política ILM" "Trabalhe com regras e políticas do ILM"

e. Atualize a página de perfis de codificação de apagamento para garantir que o perfil não seja usado em uma regra ILM.

- Se o perfil não for usado em uma regra ILM, selecione o botão de opção e selecione **Desativar**. A caixa de diálogo Desativar perfil de codificação de apagamento é exibida.



Você pode selecionar vários perfis para desativar ao mesmo tempo, desde que cada perfil não seja usado em nenhuma regra.

- Se você tem certeza de que deseja desativar o perfil, selecione **Desativar**.

Resultados

- Se StorageGRID conseguir desativar o perfil de codificação de apagamento, o status dele será "Desativado". Você não poderá mais selecionar esse perfil para nenhuma regra ILM. Você não pode reativar um perfil desativado.
- Se StorageGRID não conseguir desativar o perfil, uma mensagem de erro será exibida. Por exemplo, uma mensagem de erro será exibida se ainda houver dados de objeto associados a esse perfil. Pode ser necessário aguardar algumas semanas antes de tentar o processo de desativação novamente.

Configure regiões S3 para StorageGRID

As regras do ILM podem filtrar objetos com base nas regiões opcionais onde os buckets do S3 são criados, permitindo que você armazene objetos de diferentes regiões em diferentes locais de storage.

Se você deseja usar uma região de bucket do S3 como filtro em uma regra, primeiro precisa criar as regiões que podem ser usadas pelos buckets em seu sistema.



Você não pode alterar a região de um bucket depois que o bucket foi criado.

Antes de começar

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

Sobre esta tarefa

Ao criar um bucket S3, você pode especificar que ele seja criado em uma região específica. Especificar uma região permite que o bucket fique geograficamente próximo de seus usuários, o que pode ajudar a otimizar a latência, minimizar custos e atender a requisitos regulatórios.

Ao criar uma regra ILM, você pode querer usar a região associada a um bucket do S3 como um filtro avançado. Por exemplo, você pode criar uma regra que se aplique somente a objetos em buckets do S3 criados na `us-west-2` região. Em seguida, você pode especificar que cópias desses objetos sejam colocadas em Storage Nodes em um data center dentro dessa região para otimizar a latência.

Ao configurar regiões, siga estas diretrizes:

- Por padrão, todos os buckets são considerados pertencentes à `us-east-1` região.
- Você deve criar as regiões usando o Grid Manager antes de poder especificar uma região não padrão ao criar buckets usando o Tenant Manager ou a Tenant Management API, ou com o elemento de solicitação `LocationConstraint` para solicitações da API S3 PUT Bucket. Ocorrerá um erro se uma solicitação PUT Bucket usar uma região que não foi definida no StorageGRID.
- Você deve usar o nome exato da região ao criar o bucket do S3. Os nomes de região diferenciam maiúsculas de minúsculas. Os caracteres válidos são números, letras e hífens.



EU não é considerado um sinônimo para eu-west-1. Se você quiser usar a região EU ou eu-west-1, deve usar o nome exato.

- Não é possível excluir ou modificar uma região se ela estiver sendo usada em uma regra atribuída a qualquer política (ativa ou inativa).
- Se você usar uma região inválida como filtro avançado em uma regra ILM, não poderá adicionar essa regra a uma política.

Uma região inválida pode resultar se você usar uma região como filtro avançado em uma regra ILM, mas posteriormente excluir essa região, ou se você usar a Grid Management API para criar uma regra e especificar uma região que você não definiu.

- Se você excluir uma região depois de usá-la para criar um bucket do S3, precisará adicioná-la novamente caso queira usar o filtro avançado de Location Constraint para encontrar objetos nesse bucket.

Passos

1. Selecione **ILM > Regiões**.

A página Regiões é exibida.

2. Selecione a guia **Todas as regiões** ou **Região padrão**.

Todas as regiões

A aba **Todas as regiões** lista as regiões atualmente definidas, incluindo a região padrão definida.



Não é possível remover ou modificar a região padrão na guia **Todas as regiões**. Use a guia **Região padrão** para alterar a região padrão.

- a. Para adicionar uma região, selecione **Adicionar outra região**.
- b. Insira o nome de uma região que você deseja usar ao criar buckets do S3.

Você deve usar exatamente esse nome de região como o elemento de solicitação LocationConstraint ao criar o bucket S3 correspondente.

- c. Para remover uma região não utilizada, selecione o ícone de excluir .

Uma mensagem de erro aparece se você tentar remover uma região que está sendo usada em qualquer política (ativa ou inativa).

- d. Quando terminar de fazer as alterações, selecione **Salvar**.

Agora você pode selecionar essas regiões na seção Filtros avançados, na etapa 1 do assistente Criar regra ILM. Consulte "[Utilize filtros avançados em regras ILM](#)".

Região padrão

A aba **Região padrão** exibe a região padrão definida atualmente, a qual você pode modificar.

- a. Para alterar a região padrão, selecione o nome da região nas opções disponíveis na lista suspensa **Default region**.
- b. Selecione **Salvar**.

Criar regra ILM

Saiba mais sobre as regras ILM no StorageGRID

Para gerenciar objetos, você cria um conjunto de regras de gerenciamento do ciclo de vida das informações (ILM) e as organiza em uma política de ILM.

Cada objeto inserido no sistema é avaliado em relação à política ativa. Quando uma regra na política corresponde aos metadados de um objeto, as instruções na regra determinam quais ações StorageGRID executa para copiar e armazenar esse objeto.



Os metadados de objeto não são gerenciados pelas regras de ILM. Em vez disso, os metadados de objeto são armazenados em um banco de dados Cassandra, conhecido como repositório de metadados. Três cópias dos metadados de objeto são mantidas automaticamente em cada site para proteger os dados contra perda.

Elementos de uma regra ILM

Uma regra ILM possui três elementos:

- **Critérios de filtragem:** Os filtros básicos e avançados de uma regra definem a quais objetos a regra se aplica. Se um objeto corresponder a todos os filtros, StorageGRID aplica a regra e cria as cópias do objeto especificadas nas instruções de posicionamento da regra.
- **Instruções de posicionamento:** As instruções de posicionamento de uma regra definem o número, o tipo e a localização das cópias de objetos. Cada regra pode incluir uma sequência de instruções de posicionamento para alterar o número, o tipo e a localização das cópias de objetos ao longo do tempo. Quando o período de um posicionamento expira, as instruções do próximo posicionamento são aplicadas automaticamente pela próxima avaliação do ILM.
- **Comportamento de ingestão:** O comportamento de ingestão de uma regra permite que você escolha como os objetos filtrados pela regra são protegidos durante a ingestão (quando um cliente S3 salva um objeto na grid).

Filtragem de regras ILM

Ao criar uma regra ILM, você especifica filtros para identificar a quais objetos a regra se aplica.

No caso mais simples, uma regra pode não usar nenhum filtro. Qualquer regra que não use filtros se aplica a todos os objetos, portanto, deve ser a última (padrão) regra em uma política ILM. A regra padrão fornece instruções de storage para objetos que não correspondem aos filtros de outra regra.

- Os filtros básicos permitem que você aplique regras diferentes a grandes grupos distintos de objetos. Esses filtros permitem que você aplique uma regra a contas de tenant específicas, buckets S3 específicos ou ambos.

Os filtros básicos oferecem uma maneira simples de aplicar regras diferentes a um grande número de objetos. Por exemplo, os registros financeiros da sua empresa podem precisar ser armazenados para atender a requisitos regulatórios, enquanto os dados do departamento de marketing podem precisar ser armazenados para facilitar as operações diárias. Depois de criar contas de locatário separadas para cada departamento ou depois de segregar os dados dos diferentes departamentos em buckets S3 separados, você pode facilmente criar uma regra que se aplica a todos os registros financeiros e uma segunda regra que se aplica a todos os dados de marketing.

- Os filtros avançados oferecem controle preciso. Você pode criar filtros para selecionar objetos com base

nas seguintes propriedades do objeto:

- Tempo de ingestão
- Último tempo de acesso
- Todo ou parte do nome do objeto (chave)
- Restrição de localização (somente S3)
- Tamanho do objeto
- Metadados do usuário
- Tag de objeto (somente S3)

Você pode filtrar objetos com base em critérios muito específicos. Por exemplo, objetos armazenados pelo departamento de imagem de um hospital podem ser usados com frequência quando têm menos de 30 dias e raramente depois disso, enquanto objetos que contêm informações sobre consultas de pacientes podem precisar ser copiados para o departamento de faturamento na sede da rede de saúde. Você pode criar filtros que identificam cada tipo de objeto com base no nome do objeto, tamanho, tags de objeto S3 ou qualquer outro critério relevante e, em seguida, criar regras separadas para armazenar cada conjunto de objetos adequadamente.

Você pode combinar filtros conforme necessário em uma única regra. Por exemplo, o departamento de marketing pode querer armazenar arquivos de imagem grandes de forma diferente dos registros de fornecedores, enquanto o departamento de Recursos Humanos pode precisar armazenar registros de pessoal em uma região geográfica específica e informações de políticas de forma centralizada. Nesse caso, você pode criar regras que filtrem por conta de locatário para segregar os registros de cada departamento, enquanto usa filtros em cada regra para identificar o tipo específico de objeto ao qual a regra se aplica.

Instruções de posicionamento de regras ILM

As instruções de posicionamento determinam onde, quando e como os dados do objeto são armazenados. Uma regra ILM pode incluir uma ou mais instruções de posicionamento. Cada instrução de posicionamento se aplica a um único período de tempo.

Ao criar instruções de posicionamento:

- Você começa especificando o tempo de referência, que determina quando as instruções de posicionamento começam. O tempo de referência pode ser quando um objeto é ingerido, quando um objeto é acessado, quando um objeto versionado se torna não atual ou um tempo definido pelo usuário.
- Em seguida, você especifica quando o posicionamento será aplicado, em relação ao tempo de referência. Por exemplo, um posicionamento pode começar no dia 0 e continuar por 365 dias, em relação ao momento em que o objeto foi ingerido.
- Por fim, você especifica o tipo de cópias (replicação ou codificação de apagamento) e o local onde as cópias são armazenadas. Por exemplo, você pode querer armazenar duas cópias replicadas em dois locais diferentes.

Cada regra pode definir várias colocações para um único período de tempo e colocações diferentes para períodos de tempo diferentes.

- Para inserir objetos em vários locais durante um único período, selecione **Adicionar outro tipo ou local** para adicionar mais de uma linha para esse período.
- Para posicionar objetos em locais diferentes em períodos de tempo distintos, selecione **Adicionar outro período de tempo** para adicionar o próximo período. Em seguida, especifique uma ou mais linhas dentro do período de tempo.

O exemplo mostra duas instruções de posicionamento na página Definir posicionamentos do assistente Criar regra ILM.

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0store for 365 days

Store objects by replicating2 copies at Data Center 1, Data Center 2

and store objects by erasure coding using 6+3 EC scheme at all sites

Add other type or location

Time period 2

From Day 365store forever

Store objects by replicating2 copies at Data Center 3

Add other type or location

A primeira instrução de colocação **1** tem duas linhas para o primeiro ano:

- A primeira linha cria duas cópias replicadas do objeto em dois sites de data center.
- A segunda linha cria uma cópia 6+3 com codificação de apagamento usando todos os sites do data center.

A segunda instrução de colocação **2** cria duas cópias após um ano e guarda essas cópias para sempre.

Ao definir o conjunto de instruções de posicionamento para uma regra, você deve garantir que pelo menos uma instrução de posicionamento comece no dia 0, que não haja lacunas entre os períodos de tempo que você definiu e que a instrução de posicionamento final continue indefinidamente ou até que você não precise mais de nenhuma cópia de objeto.

À medida que cada período de tempo definido na regra expira, as instruções de posicionamento de conteúdo para o próximo período são aplicadas. Novas cópias de objetos são criadas e quaisquer cópias desnecessárias são excluídas.

Comportamento de ingestão da regra ILM

O comportamento de ingestão controla se as cópias dos objetos são colocadas imediatamente de acordo com as instruções da regra ou se cópias intermediárias são feitas e as instruções de colocação são aplicadas posteriormente. Os seguintes comportamentos de ingestão estão disponíveis para regras ILM:

- **Balanceado:** StorageGRID tenta criar todas as cópias especificadas na regra ILM durante a ingestão; se isso não for possível, cópias intermediárias são criadas e uma mensagem de sucesso é retornada ao cliente. As cópias especificadas na regra ILM são criadas sempre que possível.

- **Estrito:** Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja retornado ao cliente.
- **Confirmação dupla:** StorageGRID cria imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. As cópias especificadas na regra ILM são criadas sempre que possível.

Informações relacionadas

- ["Opções de ingestão"](#)
- ["Vantagens, desvantagens e limitações das opções de ingestão"](#)
- ["Como a consistência e as regras de ILM interagem para afetar a proteção de dados"](#)

Exemplo de regra ILM

Por exemplo, uma regra ILM poderia especificar o seguinte:

- Aplica-se somente aos objetos pertencentes ao Tenant A.
- Faça duas cópias replicadas desses objetos e armazene cada cópia em um site diferente.
- As duas cópias serão mantidas "para sempre", o que significa que StorageGRID não as excluirá automaticamente. Em vez disso, StorageGRID reterá esses objetos até que sejam excluídos por uma solicitação de exclusão do cliente ou pelo término do ciclo de vida do bucket.
- Use a opção Balanceada para o comportamento de ingestão: a instrução de posicionamento em dois sites é aplicada assim que o Tenant A salva um objeto no StorageGRID, a menos que não seja possível fazer imediatamente as duas cópias necessárias.

Por exemplo, se o Site 2 estiver inacessível quando o Tenant A salvar um objeto, StorageGRID fará duas cópias provisórias nos Storage Nodes do Site 1. Assim que o Site 2 estiver disponível, StorageGRID fará a cópia necessária nesse site.

Informações relacionadas

- ["O que é um pool de storage"](#)
- ["O que é um pool de storage em nuvem"](#)

Acesse o assistente Criar uma regra ILM no StorageGRID

As regras do ILM permitem gerenciar a alocação de dados de objetos ao longo do tempo. Para criar uma regra do ILM, você utiliza o assistente Criar uma regra do ILM.



Se você deseja criar a regra ILM padrão para uma política, siga as ["Instruções para criar uma regra ILM padrão"](#) instruções em vez disso.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Se você deseja especificar a quais contas de locatário essa regra se aplica, você tem o ["Permissão de contas de tenant"](#) ou conhece o ID da conta para cada conta.
- Se você deseja que a regra filtre objetos com base nos metadados de tempo de acesso, as atualizações de tempo de acesso devem estar habilitadas pelo bucket do S3.
- Você configurou todos os Cloud Storage Pools que planeja usar. Consulte ["Criar pool de armazenamento"](#)

em nuvem".

- Você está familiarizado com o "opções de ingestão".
- Se você precisar criar uma regra compatível para uso com o S3 Object Lock, você já está familiarizado com o "Requisitos para S3 Object Lock".
- Opcionalmente, você assistiu ao vídeo:

[Visão geral das regras do ILM](#)

Sobre esta tarefa

Ao criar regras ILM:

- Considere a topologia do sistema StorageGRID e as configurações de storage.
- Considere que tipos de cópias de objetos você deseja criar (replicadas ou com codificação de apagamento) e o número de cópias de cada objeto necessárias.
- Determine quais tipos de metadados de objeto são usados nos aplicativos que se conectam ao StorageGRID. As regras de ILM filtram objetos com base em seus metadados.
- Considere onde você deseja que as cópias dos objetos sejam colocadas ao longo do tempo.
- Decida qual opção de ingestão usar (Balanced, Strict ou Dual commit).

Passos

1. Selecione **ILM > Regras**.
2. Selecione **Criar**. "Etapa 1 (Inserir detalhes)"A tela do assistente Criar uma regra ILM é exibida.

Insira detalhes e filtros para uma regra ILM do StorageGRID

A etapa **Inserir detalhes** do assistente Criar uma regra ILM permite que você insira um nome e uma descrição para a regra e defina filtros para a regra.

Inserir uma descrição e definir filtros para a regra é opcional.

Sobre esta tarefa

Ao avaliar um objeto em relação a uma "Regra ILM" regra, StorageGRID compara os metadados do objeto com os filtros da regra. Se os metadados do objeto corresponderem a todos os filtros, StorageGRID usa a regra para colocar o objeto. Você pode criar uma regra para aplicar a todos os objetos ou especificar filtros básicos, como uma ou mais contas de tenant ou nomes de buckets, ou filtros avançados, como o tamanho do objeto ou metadados do usuário.

Passos

1. Insira um nome exclusivo para a regra no campo **Nome**.
2. Opcionalmente, insira uma breve descrição para a regra no campo **Descrição**.

Você deve descrever o propósito ou a função da regra para que possa reconhecê-la posteriormente.

3. Opcionalmente, selecione uma ou mais contas de locatário do S3 às quais esta regra se aplica. Se esta regra se aplica a todos os locatários, deixe este campo em branco.

Se você não tiver a permissão de acesso Root ou a permissão de Tenant accounts, não poderá selecionar locatários da lista. Em vez disso, insira o ID do locatário ou vários IDs como uma sequência separada por vírgulas.

4. Opcionalmente, especifique os buckets do S3 aos quais esta regra se aplica.

Se a opção **aplica a todos os buckets** estiver selecionada (padrão), a regra se aplica a todos os buckets S3.

5. Para tenants do S3, selecione opcionalmente **Sim** para aplicar a regra somente a versões de objetos mais antigas em buckets do S3 que tenham versionamento ativado.

Se você selecionar **Sim**, "Hora não atual" será selecionada automaticamente para Hora de referência em "Etapa 2 do assistente Criar uma regra ILM".



O tempo não atual aplica-se apenas a objetos S3 em buckets com versionamento ativado. Consulte "[Operações em buckets, PutBucketVersioning](#)" e "[Gerencie objetos com S3 Object Lock](#)".

Você pode usar essa opção para reduzir o impacto de storage de objetos versionados filtrando versões de objetos não atuais. Consulte "[Exemplo 4: regras e políticas do ILM para objetos versionados do S3](#)".

6. Opcionalmente, selecione **Adicionar um filtro avançado** para especificar filtros adicionais.

Se você não configurar a filtragem avançada, a regra se aplica a todos os objetos que correspondem aos filtros básicos. Para mais informações sobre filtragem avançada, consulte [Utilize filtros avançados em regras ILM](#) e [Especifique vários tipos de metadados e valores](#).

7. Selecione **Continuar**. "Etapa 2 (Definir colocações)" O assistente Criar uma regra ILM será exibido.

Utilize filtros avançados em regras ILM

A filtragem avançada permite que você crie regras ILM que se aplicam somente a objetos específicos com base em seus metadados. Ao configurar a filtragem avançada para uma regra, você seleciona o tipo de metadado que deseja corresponder, seleciona um operador e especifica um valor de metadado. Quando os objetos são avaliados, a regra ILM é aplicada somente àqueles objetos que possuem metadados que correspondem ao filtro avançado.

A tabela mostra os tipos de metadados que você pode especificar em filtros avançados, os operadores que você pode usar para cada tipo de metadados e os valores de metadados esperados.

Tipo de metadados	Operadores suportados	Valor de metadados
Tempo de ingestão	• é • não é • é antes • é em ou antes de • é depois • é em ou após	Data e hora em que o objeto foi ingerido. Nota: Para evitar problemas de recursos ao ativar uma nova política ILM, você pode usar o filtro avançado "Tempo de ingestão" em qualquer regra que possa alterar a localização de um grande número de objetos existentes. Defina o "Tempo de ingestão" para um valor maior ou igual ao horário aproximado em que a nova política entrará em vigor para garantir que os objetos existentes não sejam movidos desnecessariamente.

Tipo de metadados	Operadores suportados	Valor de metadados
Chave	• igual a • não é igual • contém • não contém • começa com • não começa com • termina com • não termina com	Toda ou parte de uma chave de objeto S3 exclusiva. Por exemplo, você pode querer encontrar objetos que terminem com <code>.txt</code> ou comecem com <code>test-object/</code>.
Último tempo de acesso	• é • não é • é antes • é em ou antes de • é depois • é em ou após	Data e hora em que o objeto foi recuperado (lido ou visualizado) pela última vez. Observação: Se você planeja "usar o último tempo de acesso" como um filtro avançado, as atualizações do tempo de acesso mais recente devem estar ativadas para o bucket do S3.
Restrição de localização (somente S3)	• igual a • não é igual	A região onde um bucket do S3 foi criado. Use ILM > Regiões para definir as regiões que são exibidas. Nota: O valor <code>us-east-1</code> corresponderá a objetos em buckets criados na região <code>us-east-1</code>, bem como a objetos em buckets que não têm região especificada. Consulte "Configurar regiões S3".
Tamanho do objeto	• igual a • não é igual • menor que • menor ou igual a • maior que • maior ou igual a	O tamanho do objeto. A codificação de apagamento é mais adequada para objetos maiores que 1 MB. Não use codificação de apagamento para objetos menores que 200 KB para evitar a sobrecarga de gerenciar fragmentos codificados por apagamento muito pequenos.

Tipo de metadados	Operadores suportados	Valor de metadados
Metadados do usuário	• contém • termina com • igual a • existe • começa com • não contém • não termina com • não é igual • não existe • não começa com	Par chave-valor, onde Nome dos metadados do usuário é a chave e Valor dos metadados é o valor. Por exemplo, para filtrar objetos que tenham metadados do usuário de <code>color=blue</code>, especifique <code>color</code> para Nome dos metadados do usuário, <code>equals</code> para o operador e <code>blue</code> para Valor dos metadados. Observação: Os nomes dos metadados do usuário não diferenciam maiúsculas de minúsculas; os valores dos metadados do usuário diferenciam maiúsculas de minúsculas.
Tag de objeto (somente S3)	• contém • termina com • igual a • existe • começa com • não contém • não termina com • não é igual • não existe • não começa com	Par chave-valor, onde Nome da tag do objeto é a chave e Valor da tag do objeto é o valor. Por exemplo, para filtrar objetos que tenham uma tag de objeto de <code>Image=True</code>, especifique <code>Image</code> para Nome da tag de objeto, <code>equals</code> para o operador e <code>True</code> para Valor da tag de objeto. Observação: Os nomes e valores das tags de objeto diferenciam maiúsculas de minúsculas. Você deve inserir esses itens exatamente como foram definidos para o objeto.

Especifique vários tipos de metadados e valores

Ao definir a filtragem avançada, você pode especificar vários tipos de metadados e vários valores de metadados. Por exemplo, se você quiser que uma regra corresponda a objetos com tamanho entre 10 MB e 100 MB, você selecionaria o tipo de metadado **Object size** e especificaria dois valores de metadados.

- O primeiro valor de metadados especifica objetos com tamanho igual ou superior a 10 MB.
- O segundo valor de metadados especifica objetos com tamanho igual ou inferior a 100 MB.

Filter group 1
Objects with all of following metadata will be evaluated by this rule:
✕

Object size

greater than or equal to

10

MB

✕

and

Object size

less than or equal to

100

MB

✕

O uso de múltiplas entradas permite que você tenha controle preciso sobre quais objetos são correspondidos. No exemplo a seguir, a regra se aplica a objetos que têm Brand A ou Brand B como valor do metadados de usuário `camera_type`. No entanto, a regra só se aplica àqueles objetos Brand B que são menores que 10 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

User metadata equals

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule:

User metadata equals

and Object size

[Add another advanced filter](#)

Defina as instruções de posicionamento para uma regra ILM do StorageGRID

A etapa **Definir posicionamentos** do assistente Criar regra ILM permite definir as instruções de posicionamento que determinam por quanto tempo os objetos são armazenados, o tipo de cópias (replicadas ou com código de apagamento), o local de armazenamento e o número de cópias.



As capturas de tela mostradas são exemplos. Seus resultados podem variar dependendo da sua versão do StorageGRID.

Sobre esta tarefa

Uma regra ILM pode incluir uma ou mais instruções de posicionamento. Cada instrução de posicionamento se aplica a um único período de tempo. Quando você usa mais de uma instrução, os períodos de tempo devem ser contíguos e pelo menos uma instrução deve começar no dia 0. As instruções podem continuar indefinidamente ou até que você não precise mais de cópias de objetos.

Cada instrução de posicionamento pode ter várias linhas se você quiser criar diferentes tipos de cópias ou usar locais diferentes durante esse período.

Neste exemplo, a regra ILM armazena uma cópia replicada no Site 1 e uma cópia replicada no Site 2 durante o primeiro ano. Após um ano, uma cópia codificada de apagamento 2+1 é criada e salva em apenas um site.

Time period 1
From Day
0
store
for
365
days

Store objects by
replicating
1
copies at
Site 1

and store objects by
replicating
1
copies at
Site 2

Add other type or location

Time period 2
From Day
365
store
forever

Store objects by
erasure coding
using
2+1 EC scheme at Site 3

Add other type or location

Passos

1. Em **Horário de referência**, selecione o tipo de horário a ser usado ao calcular o horário de início de uma instrução de posicionamento.

Opção	Descrição
Tempo de ingestão	O momento em que o objeto foi ingerido.
Último tempo de acesso	O momento em que o objeto foi recuperado (lido ou visualizado) pela última vez. Para usar esta opção, as atualizações de tempo de acesso devem estar habilitadas para o bucket S3. Consulte "Usar tempo de acesso nas regras do ILM".
Tempo de criação definido pelo usuário	Um horário especificado nos metadados definidos pelo usuário.
Tempo não atual	A opção "Tempo não atual" é selecionada automaticamente se você selecionou Sim para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com versionamento ativado)?" em "Etapa 1 do assistente Criar uma regra ILM" .

Se você deseja criar uma regra *em conformidade*, você deve selecionar **Horário de ingestão**. Consulte ["Gerencie objetos com S3 Object Lock"](#).

2. Na seção **Período e locais**, insira um horário de início e uma duração para o primeiro período.

Por exemplo, você pode querer especificar onde armazenar objetos durante o primeiro ano (*A partir do dia 0, armazenar por 365 dias*). Pelo menos uma instrução deve começar no dia 0.

3. Se você deseja criar cópias replicadas:
 - a. Na lista suspensa **Armazenar objetos por**, selecione **replicating**.
 - b. Selecione o número de cópias que você deseja fazer.

Um aviso é exibido se você alterar o número de cópias para 1. Uma regra ILM que cria apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Consulte ["Por que você não deve usar replicação de cópia única"](#).

Para evitar o risco, faça uma ou mais das seguintes ações:

- Aumente o número de cópias para o período de tempo.
- Adicione cópias a outros pools de storage ou a um Cloud Storage Pool.
- Selecione **codificação de apagamento** em vez de **replicação**.

Você pode ignorar este aviso com segurança se esta regra já criar várias cópias para todos os períodos de tempo.

- c. No campo **cópias em**, selecione os pools de storage que você deseja adicionar.

Se você especificar apenas um pool de storage, esteja ciente de que StorageGRID pode armazenar apenas uma cópia replicada de um objeto em qualquer Storage Node. Se sua grid incluir três Storage Nodes e você selecionar 4 como o número de cópias, apenas três cópias serão criadas—uma cópia para cada Storage Node.

O alerta **Implantação do ILM inviável** é acionado para indicar que a regra do ILM não pôde ser completamente aplicada.

Se você especificar mais de um pool de storage, lembre-se destas regras:

- O número de cópias não pode ser maior que o número de pools de storage.
- Se o número de cópias for igual ao número de pools de storage, uma cópia do objeto será armazenada em cada pool de storage.
- Se o número de cópias for menor que o número de pools de storage, uma cópia é armazenada no site de ingestão e, em seguida, o sistema distribui as cópias restantes para manter o uso do disco equilibrado entre os pools, garantindo que nenhum site receba mais de uma cópia de um objeto.
- Se os pools de storage se sobrepuserem (contiverem os mesmos Storage Nodes), todas as cópias do objeto poderão ser salvas em apenas um site. Por esse motivo, não especifique o pool de storage All Storage Nodes (StorageGRID 11.6 e versões anteriores) e outro pool de storage.

4. Se você deseja criar uma cópia com codificação de apagamento:

- a. Na lista suspensa **Armazenar objetos por**, selecione **erasure coding**.



A codificação de apagamento é mais adequada para objetos maiores que 1 MB. Não use codificação de apagamento para objetos menores que 200 KB para evitar a sobrecarga de gerenciar fragmentos codificados por apagamento muito pequenos.

- b. Se você não adicionou um filtro de tamanho de objeto para um valor maior que 200 KB, selecione **Anterior** para retornar à Etapa 1. Em seguida, selecione **Adicionar um filtro avançado** e defina um filtro de **Tamanho do objeto** para qualquer valor maior que 200 KB.
 - c. Selecione o pool de storage que você deseja adicionar e o esquema de codificação de apagamento

que você deseja usar.

O local de armazenamento de uma cópia com codificação de apagamento inclui o nome do esquema de codificação de apagamento, seguido pelo nome do pool de storage.

Os esquemas de codificação de apagamento disponíveis são limitados pelo número de Storage Nodes no pool de storage que você selecionar. Um **Recommended** badge aparece ao lado dos esquemas que fornecem o "[melhor proteção ou menor sobrecarga de storage](#)".

5. Opcionalmente:

- a. Selecione **Adicionar outro tipo ou local** para criar cópias adicionais em locais diferentes.
- b. Selecione **Adicionar outro período de tempo** para adicionar diferentes períodos de tempo.



A exclusão de objetos ocorre com base nas seguintes configurações:

- Os objetos são excluídos automaticamente ao final do último período, a menos que outro período termine com **forever**.
- Dependendo de "[Configurações de período de retenção de bucket e tenant](#)", os objetos podem não ser excluídos mesmo que o período de retenção termine.

6. Se você deseja armazenar objetos em um pool de Cloud Storage:

- a. Na lista suspensa **Armazenar objetos por**, selecione **replicando**.
- b. Selecione o campo **cópias em** e, em seguida, selecione um Cloud Storage Pool.

Ao usar Cloud Storage Pools, tenha em mente estas regras:

- Não é possível selecionar mais de um Cloud Storage Pool em uma única instrução de posicionamento. Da mesma forma, não é possível selecionar um Cloud Storage Pool e um pool de storage na mesma instrução de posicionamento.
- Você só pode armazenar uma cópia de um objeto em qualquer pool de storage do Cloud Storage. Uma mensagem de erro aparece se você definir **Cópias** para 2 ou mais.
- Não é possível armazenar mais de uma cópia de um objeto em qualquer Cloud Storage Pool ao mesmo tempo. Uma mensagem de erro aparece se vários posicionamentos que usam um Cloud Storage Pool tiverem datas sobrepostas ou se várias linhas no mesmo posicionamento usarem um Cloud Storage Pool.
- Você pode armazenar um objeto em um Cloud Storage Pool ao mesmo tempo em que esse objeto está sendo armazenado como cópias replicadas ou codificadas por codificação de apagamento no StorageGRID. No entanto, você deve incluir mais de uma linha na instrução de posicionamento para o período, para que possa especificar o número e os tipos de cópias para cada local.

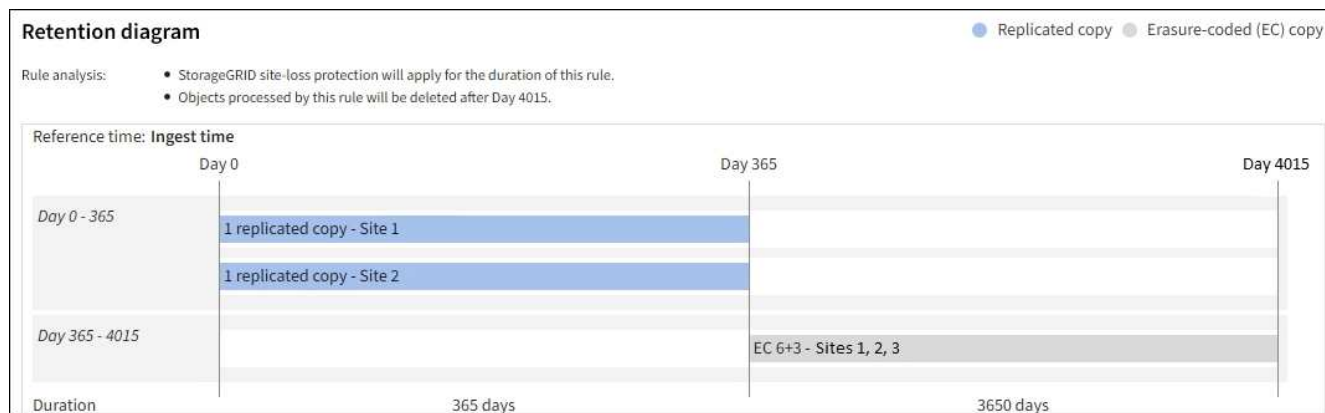
7. No diagrama de retenção, confirme suas instruções de posicionamento.

Neste exemplo, a regra ILM armazena uma cópia replicada no Site 1 e uma cópia replicada no Site 2 durante o primeiro ano. Após um ano e por mais 10 anos, uma cópia de codificação de apagamento 6+3 será salva em três sites. Após um total de 11 anos, os objetos serão excluídos do StorageGRID.

A seção de análise de regras do diagrama de retenção afirma:

- A proteção contra perda de site do StorageGRID será aplicada durante a vigência desta regra.
- Os objetos processados por esta regra serão excluídos após o dia 4015.

Consulte ["Ative a proteção contra perda de sites."](#)



8. Selecione **Continuar**. ["Etapa 3 \(Selecionar comportamento de ingestão\)"](#) do assistente Criar uma regra ILM é exibido.

Use tempo de acesso nas regras do StorageGRID ILM

Você pode usar tempo de acesso como referência em uma regra do ILM. Por exemplo, você pode querer manter os objetos visualizados nos últimos três meses em Storage Nodes locais, enquanto move os objetos que não foram visualizados recentemente para um local externo. Você também pode usar tempo de acesso como um filtro avançado se quiser que uma regra do ILM se aplique somente aos objetos que foram acessados pela última vez em uma data específica.

Sobre esta tarefa

Antes de usar tempo de acesso em uma regra ILM, revise as seguintes considerações:

- Ao usar tempo de acesso como referência, esteja ciente de que alterar o tempo de acesso de um objeto não aciona uma avaliação imediata do ILM. Em vez disso, os posicionamentos do objeto são avaliados e o objeto é movido conforme necessário quando o ILM em segundo plano avalia o objeto. Isso pode levar duas semanas ou mais após o acesso ao objeto.

Leve essa latência em consideração ao criar regras ILM com base no tempo de acesso e evite configurações que utilizem períodos curtos (menos de um mês).

- Ao usar tempo de acesso como filtro avançado ou como horário de referência, você deve habilitar as atualizações do tempo de acesso para buckets S3. Você pode usar o ["Tenant Manager"](#) ou o ["API de gerenciamento de inquilinos"](#).



As atualizações de tempo de acesso estão desativadas por padrão para buckets do S3.



Tenha em mente que habilitar as atualizações do tempo de acesso pode reduzir o desempenho, especialmente em sistemas com objetos pequenos. O impacto no desempenho ocorre porque StorageGRID precisa atualizar os objetos com novos registros de data e hora sempre que eles são recuperados.

A tabela a seguir resume se o tempo de acesso é atualizado para todos os objetos no bucket para diferentes tipos de solicitações.

Tipo de solicitação	Se o tempo de acesso é atualizado quando as atualizações do tempo de acesso estão desativadas	Se o tempo de acesso é atualizado quando as atualizações do tempo de acesso estão ativadas
Solicitação para recuperar um objeto, sua lista de controle de acesso ou seus metadados	Não	Sim
Solicitação para atualizar os metadados de um objeto	Sim	Sim
Solicitação para copiar um objeto de um bucket para outro	• Não, para a cópia original • Sim, para a cópia de destino	• Sim, para a cópia de origem • Sim, para a cópia de destino
Solicitação para concluir um upload multipart	Sim, para o objeto montado	Sim, para o objeto montado

Selecione o comportamento de ingestão para uma regra ILM do StorageGRID

A etapa **Selecionar comportamento de ingestão** do assistente Criar regra ILM permite que você escolha como os objetos filtrados por esta regra são protegidos durante a ingestão.

Sobre esta tarefa

StorageGRID pode criar cópias provisórias e enfileirar os objetos para avaliação ILM posterior, ou pode criar cópias para atender imediatamente às instruções de posicionamento da regra.

Passos

1. Selecione a opção ["comportamento de ingestão"](#) para usar.

Para obter mais informações, consulte ["Vantagens, desvantagens e limitações das opções de ingestão"](#).



Você não pode usar a opção Equilibrado ou Rigoroso se a regra usar um destes posicionamentos:

- Um pool de storage em nuvem no dia 0
- Um pool de storage em nuvem quando a regra usa um horário de criação definido pelo usuário como horário de referência

Consulte ["Exemplo 5: regras e política do ILM para comportamento de ingestão estrito"](#).

2. Selecione **Create**.

A regra ILM é criada. A regra só entra em vigor depois de ser adicionada a uma ["Política ILM"](#) e essa política ser ativada.

Para visualizar os detalhes da regra, selecione o nome da regra na página de regras do ILM.

Crie uma regra ILM padrão no StorageGRID

Antes de criar uma política ILM, você deve criar uma regra padrão para incluir na política quaisquer objetos que não correspondam a nenhuma outra regra. A regra padrão não pode usar nenhum filtro. Ela deve se aplicar a todos os tenants, todos os buckets e todas as versões de objeto.

Antes de começar

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

Sobre esta tarefa

A regra padrão é a última regra a ser avaliada em uma política ILM, portanto, não pode usar nenhum filtro. As instruções de posicionamento da regra padrão são aplicadas a quaisquer objetos que não correspondam a outra regra na política.

Neste exemplo de política, a primeira regra aplica-se apenas aos objetos pertencentes ao test-tenant-1. A regra padrão, que é a última, aplica-se aos objetos pertencentes a todas as outras contas de tenant.

Proposed policy name

Example ILM policy

Reason for change

Example

Manage rules

1. Select the rules you want to add to the policy.

2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	 EC for test-tenant-1	Tenant is test-tenant-1
Default	Default rule	

Ao criar a regra padrão, tenha em mente os seguintes requisitos:

- A regra padrão será automaticamente inserida como a última regra quando você a adicionar a uma política.
- A regra padrão não pode usar nenhum filtro básico ou avançado.
- A regra padrão deve ser aplicada a todas as versões do objeto.
- A regra padrão deve criar cópias replicadas.



Não utilize uma regra que crie cópias codificadas por apagamento como regra padrão de uma política. As regras de codificação por apagamento devem usar um filtro avançado para impedir que objetos menores sejam codificados por apagamento.

- Em geral, a regra padrão deve manter os objetos indefinidamente.
- Se você estiver usando (ou planeja habilitar) a configuração global de S3 Object Lock, a regra padrão deve estar em conformidade.

Passos

1. Selecione **ILM > Regras**.
2. Selecione **Create**.

A etapa 1 (Inserir detalhes) do assistente Criar regra ILM é exibida.

3. Insira um nome exclusivo para a regra no campo **Rule name**.
4. Opcionalmente, insira uma breve descrição para a regra no campo **Descrição**.
5. Deixe o campo **Tenant accounts** em branco.

A regra padrão deve ser aplicada a todas as contas de tenant.

6. Deixe a seleção do nome do bucket como **aplica-se a todos os buckets**.

A regra padrão deve ser aplicada a todos os buckets S3.

7. Mantenha a resposta padrão, **Não**, para a pergunta "Aplicar esta regra somente a versões antigas de objetos (em buckets do S3 com versionamento ativado)?"
8. Não adicione filtros avançados.

A regra padrão não pode especificar nenhum filtro.

9. Selecione **Next**.

A etapa 2 (Definir posicionamentos) é exibida.

10. Para o horário de referência, selecione qualquer opção.

Se você manteve a resposta padrão, **Não**, para a pergunta "Aplicar esta regra somente a versões antigas do objeto?" O tempo não atual não será incluído na lista suspensa. A regra padrão deve ser aplicada a todas as versões do objeto.

11. Especifique as instruções de posicionamento para a regra padrão.
 - A regra padrão deve reter os objetos indefinidamente. Um aviso será exibido ao ativar uma nova política se a regra padrão não reter os objetos indefinidamente. Você deve confirmar se esse é o comportamento que você espera.
 - A regra padrão deve criar cópias replicadas.



Não utilize uma regra que crie cópias codificadas por apagamento como regra padrão para uma política. As regras de codificação por apagamento devem incluir o filtro avançado **Tamanho do objeto (MB) maior que 200 KB** para impedir que objetos menores sejam codificados por apagamento.

- Se você estiver usando (ou planeja habilitar) a configuração global S3 Object Lock, a regra padrão deve ser compatível:
 - É necessário criar pelo menos duas cópias replicadas do objeto ou uma cópia com código de apagamento.
 - Essas cópias devem existir nos Storage Nodes durante toda a duração de cada linha nas instruções de posicionamento.
 - Não é possível salvar cópias de objetos em um Cloud Storage Pool.
 - Pelo menos uma linha das instruções de colocação deve começar no dia 0, usando o horário de ingestão como horário de referência.
 - Pelo menos uma linha das instruções de posicionamento deve ser "para sempre".

12. Consulte o diagrama de retenção para confirmar suas instruções de posicionamento.

13. Selecione **Continue**.

A etapa 3 (Selecionar comportamento de ingestão) aparece.

14. Selecione a opção de ingestão que você deseja usar e selecione **Criar**.

Gerenciar políticas ILM

Saiba mais sobre as políticas ILM no StorageGRID

Uma política de gerenciamento do ciclo de vida das informações (ILM, na sigla em inglês) é um conjunto ordenado de regras de ILM que determina como o sistema StorageGRID gerencia os dados dos objetos ao longo do tempo.



Uma política ILM configurada incorretamente pode resultar em perda de dados irrecuperáveis. Antes de ativar uma política ILM, revise cuidadosamente a política ILM e suas regras ILM, e depois simule a política ILM. Sempre confirme que a política ILM funcionará conforme o esperado.

Política ILM padrão

Ao instalar StorageGRID e adicionar sites, uma política ILM padrão é criada automaticamente, da seguinte forma:

- Se sua grade contiver um único site, a política padrão contém uma regra padrão que replica duas cópias de cada objeto nesse site.
- Se a sua grid contiver mais de um site, a regra padrão replica uma cópia de cada objeto em cada site.

Se a política padrão não atender aos seus requisitos de armazenamento, você pode criar suas próprias regras e políticas. Consulte ["Crie uma regra ILM"](#) e ["Crie uma política ILM"](#).

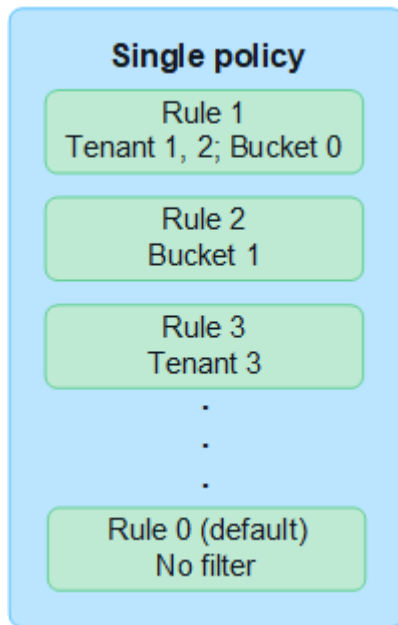
Uma ou várias políticas ILM ativas?

Você pode ter uma ou mais políticas ILM ativas simultaneamente.

Uma política

Se sua grid usar um esquema de proteção de dados simples, com poucas regras específicas para tenants e buckets, utilize uma única política ILM ativa. As regras ILM podem conter filtros para gerenciar diferentes

buckets ou tenants.



Quando você possui apenas uma política e os requisitos de um locatário mudam, é necessário criar uma nova política ILM ou clonar a política existente para aplicar as alterações, simular e, em seguida, ativar a nova política ILM. Alterações na política ILM podem resultar em movimentações de objetos que podem levar vários dias e causar latência no sistema.

Várias políticas

Para oferecer diferentes opções de qualidade de serviço aos clientes, você pode ter mais de uma política ativa simultaneamente. Cada política pode gerenciar clientes, buckets do S3 e objetos específicos. Ao aplicar ou alterar uma política para um conjunto específico de clientes ou objetos, as políticas aplicadas a outros clientes e objetos não são afetadas.

Etiquetas de política ILM

Se você deseja permitir que os locatários alternem facilmente entre várias políticas de proteção de dados por bucket, use várias políticas ILM com *tags de política ILM*. Você atribui cada política ILM a uma tag, então os locatários adicionam uma tag a um bucket para aplicar a política a esse bucket. Você só pode definir tags de política ILM em buckets S3.

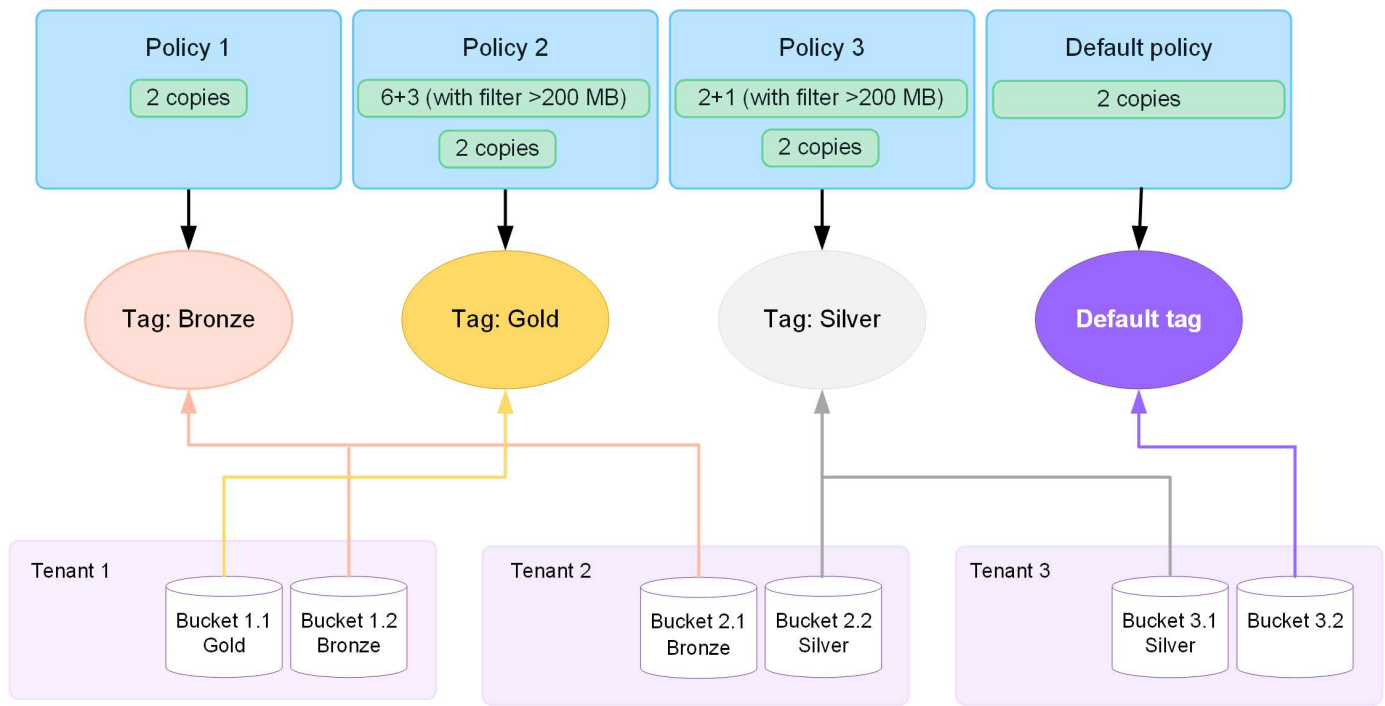
Por exemplo, você pode ter três tags chamadas Gold, Silver e Bronze. Você pode atribuir uma política ILM a cada tag, com base em quanto tempo e onde essa política armazena objetos. Os tenants podem escolher qual política usar marcando seus buckets. Um bucket com a tag Gold é gerenciado pela política Gold e recebe o nível Gold de proteção de dados e desempenho.



Você pode "[Crie no máximo 10 tags de política](#)" para sua grid.

Tag de política ILM padrão

Uma tag de política ILM padrão é criada automaticamente quando você instala StorageGRID. Cada grid deve ter uma política ativa atribuída à tag Default. A política padrão se aplica a qualquer bucket S3 sem tag.



Como uma política ILM avalia objetos?

Uma política ILM ativa controla a localização, a duração e a proteção de dados dos objetos.

Quando os clientes salvam objetos no StorageGRID, os objetos são avaliados em relação ao conjunto ordenado de regras ILM na política, da seguinte forma:

1. Se os filtros da primeira regra na política corresponderem a um objeto, o objeto é ingerido de acordo com o comportamento de ingestão dessa regra e armazenado de acordo com as instruções de posicionamento dessa regra.
2. Se os filtros da primeira regra não corresponderem ao objeto, o objeto é avaliado em relação a cada regra subsequente na política até que uma correspondência seja feita.
3. Se nenhuma regra corresponder a um objeto, o comportamento de ingestão e as instruções de posicionamento da regra padrão na política serão aplicados. A regra padrão é a última regra em uma política. A regra padrão deve se aplicar a todos os locatários, todos os buckets do S3 e todas as versões de objeto, e não pode usar nenhum filtro avançado.

Exemplo de política ILM

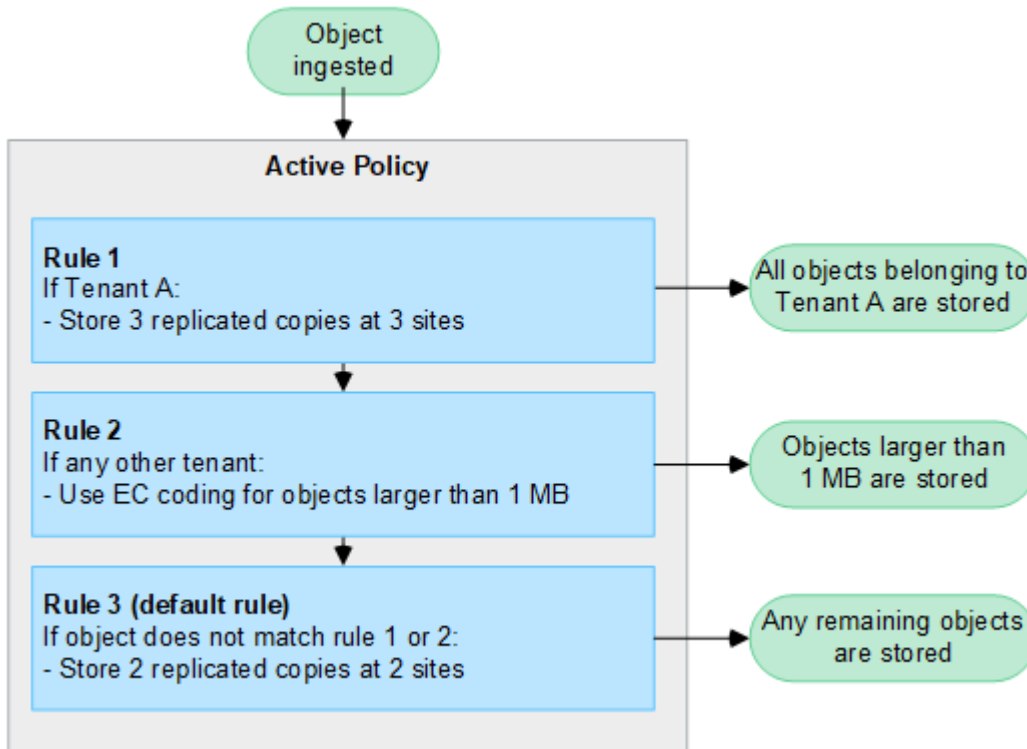
Por exemplo, uma política ILM pode conter três regras ILM que especificam o seguinte:

- **Regra 1: Cópias replicadas para Tenant A**
 - Associe todos os objetos pertencentes ao Tenant A.
 - Armazene esses objetos como três cópias replicadas em três sites.
 - Os objetos pertencentes a outros tenants não correspondem à Regra 1, portanto, são avaliados de acordo com a Regra 2.
- **Regra 2: codificação de apagamento para objetos maiores que 1 MB**
 - Corresponda a todos os objetos de outros locatários, mas somente se eles forem maiores que 1 MB. Esses objetos maiores são armazenados usando codificação de apagamento 6+3 em três sites.
 - Não corresponde a objetos de 1 MB ou menores, portanto, esses objetos são avaliados de acordo

com a Regra 3.

- **Regra 3: 2 cópias 2 centros de dados** (padrão)

- É a última e padrão regra na política. Não utiliza filtros.
- Faça duas cópias replicadas de todos os objetos que não correspondem à Regra 1 ou à Regra 2 (objetos que não pertencem ao Tenant A e que têm 1 MB ou menos).



O que são políticas ativas e inativas?

Todo sistema StorageGRID deve ter pelo menos uma política ILM ativa. Se você quiser ter mais de uma política ILM ativa, você cria tags de política ILM e atribui uma política a cada tag. Os tenants então aplicam tags aos buckets S3. A política padrão é aplicada a todos os objetos em buckets que não têm uma tag de política atribuída.

Ao criar uma política ILM pela primeira vez, você seleciona uma ou mais regras ILM e as organiza em uma ordem específica. Depois de simular a política para confirmar seu comportamento, você a ativa.

Ao ativar uma política ILM, StorageGRID usa essa política para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Objetos existentes podem ser movidos para novos locais quando as regras ILM da nova política são implementadas.

Se você ativar mais de uma política ILM simultaneamente e os locatários aplicarem tags de política aos buckets do S3, os objetos em cada bucket serão gerenciados de acordo com a política atribuída à tag.

Um sistema StorageGRID rastreia o histórico de políticas que foram ativadas ou desativadas.

Considerações para criar uma política de ILM

- Utilize apenas a política fornecida pelo sistema, Baseline 2 copies policy, em sistemas de teste. Para StorageGRID 11.6 e versões anteriores, a regra Make 2 Copies nesta política utiliza o pool de storage All Storage Nodes, que contém todos os sites. Se o seu sistema StorageGRID tiver mais de um site, duas cópias de um objeto podem ser colocadas no mesmo site.



O pool de storage All Storage Nodes é criado automaticamente durante a instalação do StorageGRID 11.6 e versões anteriores. Se você atualizar para uma versão posterior do StorageGRID, o pool All Storage Nodes ainda existirá. Se você instalar StorageGRID 11.7 ou posterior como uma nova instalação, o pool All Storage Nodes não será criado.

- Ao criar uma nova política, considere todos os diferentes tipos de objetos que podem ser inseridos em sua grid. Certifique-se de que a política inclua regras para identificar e posicionar esses objetos conforme necessário.
- Mantenha a política ILM o mais simples possível. Isso evita situações potencialmente perigosas em que os dados dos objetos não são protegidos conforme o esperado quando alterações são feitas no sistema StorageGRID ao longo do tempo.
- Certifique-se de que as regras na política estejam na ordem correta. Quando a política é ativada, os objetos novos e existentes são avaliados pelas regras na ordem em que são listadas, começando do topo. Por exemplo, se a primeira regra em uma política corresponder a um objeto, esse objeto não será avaliado por nenhuma outra regra.
- A última regra em cada política ILM é a regra ILM padrão, que não pode usar nenhum filtro. Se um objeto não for correspondido por outra regra, a regra padrão controla onde esse objeto é colocado e por quanto tempo ele é retido.
- Antes de ativar uma nova política, revise quaisquer alterações que a política esteja fazendo no posicionamento de objetos existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos são avaliados e implementados.

Crie políticas ILM no StorageGRID

Crie uma ou mais políticas de ILM para atender aos seus requisitos de qualidade de serviço.

Ter uma política ILM ativa permite aplicar as mesmas regras ILM a todos os tenants e buckets.

Ter várias políticas ILM ativas permite que você aplique as regras ILM apropriadas a tenants e buckets específicos para atender a múltiplos requisitos de qualidade de serviço.

Crie uma política ILM

Sobre esta tarefa

Antes de criar sua própria política, verifique se a "[Política ILM padrão](#)" não atende aos seus requisitos de armazenamento.



Utilize apenas as políticas fornecidas pelo sistema, 2 copies Policy (para grids de um único site) ou 1 Copy per Site (para grids de múltiplos sites), em sistemas de teste. Para StorageGRID 11.6 e versões anteriores, a regra padrão nesta política utiliza o pool de storage All Storage Nodes, que contém todos os sites. Se o seu sistema StorageGRID tiver mais de um site, duas cópias de um objeto podem ser colocadas no mesmo site.



Se o "[A configuração global de bloqueio de objeto S3 foi ativada](#)", você deve garantir que a política ILM esteja em conformidade com os requisitos dos buckets que têm S3 Object Lock ativado. Nesta seção, siga as instruções que mencionam ter S3 Object Lock ativado.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador web compatível](#)".

- Você tem o ["permissões de acesso necessárias"](#).
- Você tem ["regras ILM criadas"](#) dependendo se o S3 Object Lock está ativado.

Bloqueio de objeto S3 não ativado

- Você tem ["criou as regras ILM"](#) que deseja adicionar à política. Conforme necessário, você pode salvar uma política, criar regras adicionais e, em seguida, editar a política para adicionar as novas regras.
- Você tem ["criou uma regra ILM padrão"](#) que não contém nenhum filtro.

Bloqueio de objeto S3 ativado

- O ["A configuração global de S3 Object Lock já está ativada"](#) para o sistema StorageGRID.
- Você tem ["criou as regras ILM compatíveis e não compatíveis"](#) que deseja adicionar à política. Conforme necessário, você pode salvar uma política, criar regras adicionais e, em seguida, editar a política para adicionar as novas regras.
- Você tem ["criou uma regra ILM padrão"](#) para a política que está em conformidade.

- Opcionalmente, você assistiu ao vídeo:

[Visão geral das políticas do ILM](#)

Veja também ["Use políticas ILM"](#).

Passos

1. Selecione **ILM > Políticas**.

Se a configuração global de S3 Object Lock estiver ativada, a página de políticas do ILM indica quais regras do ILM estão em conformidade.

2. Determine como você deseja criar a política ILM.

Criar nova política

- a. Selecione **Criar policy**.

Clonar política existente

- a. Selecione a caixa de seleção da política com a qual você deseja começar e, em seguida, selecione **Clonar**.

Editar política existente

- a. Se uma política estiver inativa, você pode editá-la. Selecione a caixa de seleção da política inativa que você deseja começar, depois selecione **Editar**.

3. No campo **Policy name**, insira um nome exclusivo para a policy.
4. Opcionalmente, no campo **Motivo da alteração**, insira o motivo pelo qual você está criando uma nova política.
5. Para adicionar regras à política, selecione **Selecionar regras**. Selecione o nome de uma regra para visualizar as configurações dessa regra.

Se você estiver clonando uma política:

- As regras utilizadas pela política que você está clonando estão selecionadas.
- Se a política que você está clonando utilizava alguma regra sem filtros que não fosse a regra padrão, você será solicitado a remover todas as regras, exceto uma.
- Se a regra padrão utilizava um filtro, você será solicitado a selecionar uma nova regra padrão.
- Se a regra padrão não for a última regra, você pode movê-la para o final da nova política.

Bloqueio de objeto S3 não ativado

- a. Selecione uma regra padrão para a política. Para criar uma nova regra padrão, selecione **página de regras do ILM**.

A regra padrão se aplica a quaisquer objetos que não correspondam a outra regra na política. A regra padrão não pode usar nenhum filtro e é sempre avaliada por último.



Não utilize a regra "Make 2 Copies" como regra padrão para uma política. A regra "Make 2 Copies" utiliza um único pool de storage, All Storage Nodes, que contém todos os sites. Se o seu sistema StorageGRID tiver mais de um site, duas cópias de um objeto poderão ser colocadas no mesmo site.

Bloqueio de objeto S3 ativado

- a. Selecione uma regra padrão para a política. Para criar uma nova regra padrão, selecione **página de regras do ILM**.

A lista de regras contém apenas as regras que estão em conformidade e não utilizam nenhum filtro.



Não utilize a regra "Make 2 Copies" como regra padrão para uma política. A regra "Make 2 Copies" utiliza um único pool de storage, All Storage Nodes, que contém todos os sites. Se você utilizar essa regra, várias cópias de um objeto podem ser colocadas no mesmo site.

- b. Se você precisar de uma regra "padrão" diferente para objetos em buckets S3 não compatíveis, selecione **Incluir uma regra sem filtros para buckets S3 não compatíveis** e selecione uma regra não compatível que não use um filtro.

Por exemplo, você pode querer usar um Cloud Storage Pool para armazenar objetos em buckets que não têm S3 Object Lock ativado.



Você só pode selecionar uma regra não conforme que não use um filtro.

Veja também ["Exemplo 7: política ILM compatível para S3 Object Lock"](#).

6. Quando você terminar de selecionar a regra padrão, selecione **Continuar**.
7. Na etapa Outras regras, selecione quaisquer outras regras que você queira adicionar à política. Essas regras usam pelo menos um filtro (conta de locatário, nome do bucket, filtro avançado ou o horário de referência não atual). Em seguida, selecione **Selecionar**.

A janela Criar uma política agora lista as regras que você selecionou. A regra padrão está no final, com as outras regras acima dela.

Se o S3 Object Lock estiver ativado e você também tiver selecionado uma regra "default" não compatível, essa regra será adicionada como a penúltima regra na política.



Um aviso será exibido se alguma regra não reter objetos indefinidamente. Ao ativar essa política, você deve confirmar que deseja que StorageGRID exclua os objetos quando as instruções de posicionamento da regra padrão expirarem (a menos que um ciclo de vida de bucket mantenha os objetos por um período mais longo).

8. Arraste as linhas das regras não padrão para determinar a ordem em que essas regras serão avaliadas.

Não é possível mover a regra padrão. Se o S3 Object Lock estiver ativado, você também não pode mover a regra "default" não compatível, caso uma tenha sido selecionada.



Você deve confirmar se as regras do ILM estão na ordem correta. Quando a política é ativada, os objetos novos e existentes são avaliados pelas regras na ordem listada, começando do topo.

9. Se necessário, selecione **Selecionar regras** para adicionar ou remover regras.

10. Quando terminar, selecione **Salvar**.

11. Repita esses passos para criar políticas ILM adicionais.

12. **Simule uma política ILM**. É sempre recomendável simular uma política antes de ativá-la para garantir que ela funcione conforme o esperado.

Simule uma política

Simule uma política em objetos de teste antes de ativá-la e aplicá-la aos seus dados de produção.

Antes de começar

- Você conhece o bucket S3/chave do objeto para cada objeto que você deseja testar.

Passos

1. Utilizando um cliente S3 ou o "**Console S3**", ingira os objetos necessários para testar cada regra.
2. Na página de políticas do ILM, selecione a caixa de seleção da política e depois selecione **Simular**.
3. No campo **Objeto**, insira o S3 bucket/object-key para um objeto de teste. Por exemplo, bucket-01/filename.png.
4. Se o versionamento do S3 estiver ativado, insira opcionalmente um ID de versão para o objeto no campo **Version ID**.
5. Selecione **Simular**.
6. Na seção Resultados da Simulação, confirme que cada objeto foi correspondido pela regra correta.
7. Para determinar qual pool de storage ou perfil de codificação de apagamento está em vigor, selecione o nome da regra correspondente para acessar a página de detalhes da regra.



Analise quaisquer alterações no posicionamento de objetos replicados e codificados para apagamento existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos forem avaliados e implementados.

Resultados

Quaisquer alterações nas regras da política serão refletidas nos resultados da simulação e mostrarão a nova correspondência e a correspondência anterior. A janela "Simular política" mantém os objetos testados até que você selecione "Limpar tudo" ou o ícone de remoção  para cada objeto na lista de resultados da simulação.

Informações relacionadas

["Exemplos de simulações de políticas ILM"](#)

Ativar uma política

Ao ativar uma única política ILM, os objetos existentes e os objetos recém-ingeridos são gerenciados por essa política. Ao ativar várias políticas, as tags de política ILM atribuídas aos buckets determinam os objetos a serem gerenciados.

Antes de ativar uma nova política:

1. Simule a política para confirmar que ela se comporta conforme você espera.
2. Analise quaisquer alterações no posicionamento de objetos replicados e codificados para apagamento existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos forem avaliados e implementados.



Erros em uma política ILM podem causar perda de dados irreversível.

Sobre esta tarefa

Ao ativar uma política ILM, o sistema distribui a nova política para todos os nós. No entanto, a nova política ativa pode não entrar em vigor até que todos os nós da grid estejam disponíveis para receber a nova política. Em alguns casos, o sistema aguarda para implementar uma nova política ativa para garantir que os objetos da grid não sejam removidos acidentalmente. Especificamente:

- Se você fizer alterações de política que **auumentem a redundância ou a durabilidade dos dados**, essas alterações serão implementadas imediatamente. Por exemplo, se você ativar uma nova política que inclua uma regra de três cópias em vez de uma regra de duas cópias, essa política será implementada imediatamente porque aumenta a redundância dos dados.
- Se você fizer alterações de política que **possam diminuir a redundância ou a durabilidade dos dados**, essas alterações não serão implementadas até que todos os nós da grid estejam disponíveis. Por exemplo, se você ativar uma nova política que usa uma regra de duas cópias em vez de uma regra de três cópias, a nova política aparecerá na guia Active policy, mas não entrará em vigor até que todos os nós estejam online e disponíveis.

Passos

Siga os passos para ativar uma ou mais políticas:

Ativar uma política

Siga estes passos se você tiver apenas uma política ativa. Se você já tiver uma ou mais políticas ativas e estiver ativando políticas adicionais, siga os passos para ativar várias políticas.

1. Quando você estiver pronto para ativar uma política, selecione **ILM > Policies**.

Alternativamente, você pode ativar uma única política na página **ILM > Policy tags**.

2. Na guia Políticas, selecione a caixa de seleção da política que você deseja ativar e, em seguida, selecione **Ativar**.
3. Siga a etapa apropriada:
 - Se uma mensagem de aviso solicitar que você confirme que deseja ativar a política, selecione **OK**.
 - Se aparecer uma mensagem de aviso contendo detalhes sobre a política:
 - i. Analise os detalhes para garantir que a política gerencie os dados conforme o esperado.
 - ii. Se a regra padrão armazenar objetos por um número limitado de dias, revise o diagrama de retenção e digite esse número de dias na caixa de texto.
 - iii. Se a regra padrão armazenar objetos indefinidamente, mas uma ou mais outras regras tiverem retenção limitada, digite **sim** na caixa de texto.
 - iv. Selecione **Ativar política**.

Ativar várias políticas

Para ativar várias políticas, você deve criar etiquetas de política e atribuir uma política a cada etiqueta. Você pode criar no máximo 10 etiquetas de política para sua grid.



Quando várias tags de política estão em uso, se os tenants reatribuírem tags de política aos buckets com frequência, o desempenho do grid pode ser afetado. Se você tiver tenants não confiáveis, considere usar apenas a tag de política Default.

1. Selecione **ILM > Tags de política**.
2. Selecione **Create**.
3. Na caixa de diálogo Criar tag de política, digite um nome para a tag e, opcionalmente, uma descrição para a tag.



Os nomes e descrições das tags são visíveis para os locatários. Escolha valores que ajudem os locatários a tomar uma decisão informada ao selecionar tags de política para atribuir aos seus buckets. Por exemplo, se a política atribuída excluir objetos após um período de tempo, você pode comunicar isso na descrição. Não inclua informações confidenciais nesses campos.

4. Selecione **Criar tag**.
5. Na tabela de tags de política ILM, use o menu suspenso para selecionar uma política para atribuir à tag.
6. Se aparecerem avisos na coluna Limitações da política, selecione **Exibir detalhes da política** para revisar a política.
7. Garanta que cada política gerencie os dados conforme o esperado.

8. Selecione **Ativar políticas atribuídas**. Ou selecione **Limpar alterações** para remover a atribuição da política.
9. Na caixa de diálogo Ativar políticas com novas tags, revise as descrições de como cada tag, política e regra gerenciará os objetos. Faça as alterações necessárias para garantir que as políticas gerenciem os objetos conforme o esperado.
10. Quando tiver certeza de que deseja ativar as políticas, digite **sim** na caixa de texto, depois selecione **Ativar políticas**.

Informações relacionadas

["Exemplo 6: alterando uma política ILM"](#)

Exemplo de simulações de políticas ILM no StorageGRID

Os exemplos de simulações de políticas ILM fornecem diretrizes para estruturar e modificar simulações para seu ambiente.

Exemplo 1: verificar regras ao simular uma política ILM

Este exemplo descreve como verificar regras ao simular uma política.

Neste exemplo, a **Example ILM policy** está sendo simulada em relação aos objetos ingeridos em dois buckets. A política inclui três regras, conforme descrito a seguir:

- A primeira regra, **Duas cópias, dois anos para bucket-a**, aplica-se apenas aos objetos em bucket-a.
- A segunda regra, **Objetos EC > 1 MB**, aplica-se a todos os buckets, mas filtra objetos maiores que 1 MB.
- A terceira regra, **Duas cópias, dois data centers**, é a regra padrão. Ela não inclui nenhum filtro e não usa o Noncurrent reference time.

Após simular a política, confirme que cada objeto foi correspondido pela regra correta.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
bucket-a/bucket-a object.pdf	—	Two copies, two years for bucket-a	—	
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	

Neste exemplo:

- bucket-a/bucket-a object.pdf correspondeu corretamente à primeira regra, que filtra objetos em `bucket-a`.
- bucket-b/test object greater than 1 MB.pdf está em bucket-b, portanto não correspondeu

à primeira regra. Em vez disso, foi corretamente correspondido pela segunda regra, que filtra objetos maiores que 1 MB.

- `bucket-b/test object less than 1 MB.pdf` Não correspondeu aos filtros das duas primeiras regras, portanto, será colocado pela regra padrão, que não inclui filtros.

Exemplo 2: reordenar regras ao simular uma política ILM

Este exemplo mostra como você pode reordenar as regras para alterar os resultados ao simular uma política.

Neste exemplo, a política **Demo** está sendo simulada. Essa política, que tem como objetivo encontrar objetos que possuam metadados de usuário `series=x-men`, inclui três regras, conforme descrito a seguir:

- A primeira regra, **PNGs**, filtra nomes de chaves que terminam em `.png`.
- A segunda regra, **X-men**, aplica-se apenas a objetos do Locatário A e filtros para `series=x-men` metadados do usuário.
- A última regra, **Duas cópias em dois data centers**, é a regra padrão, que se aplica a quaisquer objetos que não correspondam às duas primeiras regras.

Passos

1. Após adicionar as regras e salvar a política, selecione **Simular**.
2. No campo **Objeto**, insira o bucket S3/chave do objeto para um objeto de teste e selecione **Simular**.

Os resultados da simulação são exibidos, mostrando que o `Havok.png` objeto foi correspondido pela regra **PNGs**.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNGs	—	X

No entanto, `Havok.png` o objetivo era testar a regra dos **X-men**.

3. Para resolver o problema, reordene as regras.
 - a. Selecione **Concluir** para fechar a janela Simular Política ILM.
 - b. Selecione **Editar** para editar a política.
 - c. Arraste a regra **X-men** para o topo da lista.
 - d. Selecione **Salvar**.
4. Selecione **Simular**.

Os objetos que você testou anteriormente são reavaliados em relação à política atualizada e os novos resultados da simulação são exibidos. No exemplo, a coluna "Regra correspondente" mostra que o `Havok.png` objeto agora corresponde à regra de metadados X-men, como esperado. A coluna "Correspondência anterior" mostra que a regra PNGs correspondeu ao objeto na simulação anterior.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	X-men	PNGs	X

Exemplo 3: corrigir uma regra ao simular uma política ILM

Este exemplo mostra como simular uma política, corrigir uma regra na política e continuar a simulação.

Neste exemplo, a política **Demo** está sendo simulada. Essa política tem como objetivo encontrar objetos que possuam `series=x-men` metadados de usuário. No entanto, resultados inesperados ocorreram ao simular essa política no objeto `Beast.jpg`. Em vez de corresponder à regra de metadados X-men, o objeto correspondeu à regra padrão, duas cópias dois data centers.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	Two copies two data centers	—	X

Quando um objeto de teste não corresponde à regra esperada na política, você deve examinar cada regra na política e corrigir quaisquer erros.

Passos

1. Selecione **Concluir** para fechar a caixa de diálogo Simular política. Na página de detalhes da política, selecione **Diagrama de retenção**. Em seguida, selecione **expandir tudo** ou **Exibir detalhes** para cada regra, conforme necessário.
2. Analise a conta do locatário da regra, o horário de referência e os critérios de filtragem.

Por exemplo, suponha que os metadados para a regra X-men foram inseridos como "x-men01" em vez de "x-men".

3. Para resolver o erro, corrija a regra da seguinte forma:
 - Se a regra fizer parte da política, você pode cloná-la ou removê-la da política e então editá-la.
 - Se a regra fizer parte da política ativa, você deve cloná-la. Você não pode editar ou remover uma regra da política ativa.
4. Execute a simulação novamente.

Neste exemplo, a regra X-men corrigida agora corresponde ao `Beast.jpg` objeto com base nos `series=x-men` metadados do usuário, como esperado.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	X-men	—	X

Gerencie tags de política ILM no StorageGRID

Você pode visualizar os detalhes da tag de política ILM, editar uma tag ou remover uma tag.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["permissões de acesso necessárias"](#).

Veja os detalhes da tag de política ILM

Para visualizar os detalhes de uma tag:

1. Selecione **ILM > Tags de política**.
2. Selecione o nome da política na tabela. A página de detalhes da tag é exibida.
3. Na página de detalhes, visualize o histórico anterior das políticas atribuídas.
4. Visualize uma política selecionando-a.

Editar tag de política ILM



Os nomes e descrições das tags são visíveis para os locatários. Escolha valores que ajudem os locatários a tomar uma decisão informada ao selecionar tags de política para atribuir aos seus buckets. Por exemplo, se a política atribuída excluir objetos após um período de tempo, você pode comunicar isso na descrição. Não inclua informações confidenciais nesses campos.

Para editar a descrição de uma etiqueta existente:

1. Selecione **ILM > Tags de política**.
2. Selecione a caixa de seleção da tag e, em seguida, selecione **Editar**.

Como alternativa, selecione o nome da tag. A página de detalhes da tag é exibida e você pode selecionar **Editar** nessa página.

3. Altere a descrição da tag conforme necessário.
4. Selecione **Salvar**.

Remover a tag de política ILM

Ao remover uma etiqueta de política, todos os buckets atribuídos a essa etiqueta terão a política Default aplicada.

Para remover uma tag:

1. Selecione **ILM > Tags de política**.
2. Selecione a caixa de seleção da tag e, em seguida, selecione **Remover**. Uma caixa de diálogo de confirmação aparece.

Como alternativa, selecione o nome da etiqueta. A página de detalhes da etiqueta é exibida e você pode selecionar **Remover** nessa página.

3. Selecione **Sim** para excluir a tag.

Informações relacionadas

["Saiba mais sobre como criar tags de política ILM"](#)

Verifique uma política ILM com pesquisa de metadados de objeto no StorageGRID

Após ativar uma política ILM, insira objetos de teste representativos no sistema StorageGRID e, em seguida, execute uma pesquisa de metadados do objeto para confirmar que as cópias estão sendo feitas conforme o esperado e colocadas nos locais corretos.

Antes de começar

Você possui um identificador de objeto, que pode ser um dos seguintes:

- **UUID:** O Identificador Universalmente Único do objeto.
- **CBID:** O identificador único do objeto no StorageGRID. Você pode obter o CBID de um objeto no log de auditoria. Insira o CBID em letras maiúsculas.
- **Bucket S3 e chave do objeto:** Quando um objeto é ingerido através da interface S3, o aplicativo cliente usa uma combinação de bucket e chave do objeto para armazenar e identificar o objeto. Se o bucket S3 for versionado e você quiser consultar uma versão específica de um objeto S3 usando o bucket e a chave do objeto, você terá o **ID da versão**.

Passos

1. Ingerir o objeto.
2. Selecione **ILM > Pesquisa de metadados do objeto**.
3. Digite o identificador do objeto no campo **Identificador**. Você pode inserir um UUID, CBID ou S3 bucket/object-key.
4. Opcionalmente, insira um ID de versão para o objeto (somente S3).
5. Selecione **Pesquisar**.

Os resultados da pesquisa de metadados do objeto são exibidos. Esta página lista os seguintes tipos de informação:

- Metadados do sistema, como ID do objeto (UUID), tipo de resultado (objeto, marcador de exclusão, bucket S3) e tamanho lógico do objeto. Consulte a captura de tela abaixo para obter mais detalhes.
- Quaisquer pares de chave-valor de metadados de usuário personalizados associados ao objeto.
- Para objetos S3, quaisquer pares de chave-valor de tag de objeto associados ao objeto.
- Para cópias de objetos replicadas, o local de armazenamento atual de cada cópia.

- Para cópias de objetos com código de apagamento, o local de armazenamento atual de cada fragmento.
- Para cópias de objetos em um Cloud Storage Pool, a localização do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
- Para objetos segmentados e objetos multipartes, é exibida uma lista dos segmentos do objeto, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, apenas os 100 primeiros segmentos são mostrados.
- Todos os metadados de objetos no formato de armazenamento interno não processado. Esses metadados brutos incluem metadados internos do sistema que não têm garantia de persistência entre versões.

6. Confirme se o objeto está armazenado no(s) local(is) correto(s) e se é o tipo de cópia correto.

Se a opção de auditoria estiver habilitada, você também pode monitorar o log de auditoria para a mensagem ORLM Object Rules Met. A mensagem de auditoria do ORLM pode fornecer mais informações sobre o status do processo de avaliação do ILM, mas não pode fornecer informações sobre a correção do posicionamento dos dados do objeto ou a integridade da política do ILM. Você deve avaliar isso por conta própria. Para obter detalhes, consulte ["Analisar registros de auditoria"](#).

O exemplo a seguir mostra os resultados da pesquisa de metadados de um objeto de teste do S3 armazenado como duas cópias replicadas.



A seguinte captura de tela é um exemplo. Seus resultados podem variar dependendo da sua versão do StorageGRID.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAIS": "2",

```

Informações relacionadas

["Utilize a API REST S3"](#)

Trabalhe com políticas ILM e regras ILM no StorageGRID

À medida que seus requisitos de armazenamento mudam, você pode precisar implementar políticas adicionais ou modificar as regras do ILM associadas a uma política. Você pode visualizar métricas do ILM para determinar o desempenho do sistema.

Antes de começar

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

Ver políticas do ILM

Para visualizar as políticas ILM ativas e inativas e o histórico de ativação das políticas:

1. Selecione **ILM > Políticas**.
2. Selecione **Políticas** para visualizar uma lista de políticas ativas e inativas. A tabela lista o nome de cada política, as tags às quais a política está atribuída e se a política está ativa ou inativa.
3. Selecione **Histórico de ativação** para visualizar uma lista das datas de início e término da ativação das políticas.
4. Selecione o nome de uma política para ver os detalhes da política.



Ao visualizar os detalhes de uma policy cujo status é Edited ou Deleted, uma mensagem aparece explicando que você está visualizando a versão da policy que estava ativa durante o período especificado e que desde então foi editada ou excluída.

Editar uma política ILM

Você só pode editar uma política inativa. Se quiser editar uma política ativa, desative-a ou crie um clone e edite o clone.

Para editar uma política:

1. Selecione **ILM > Políticas**.
2. Selecione a caixa de seleção da política que você deseja editar e, em seguida, selecione **Editar**.
3. Edite a política seguindo as instruções em "[Criar políticas de ILM](#)".
4. Simule a política antes de reativá-la.



Uma política ILM configurada incorretamente pode resultar em perda de dados irreversíveis. Antes de ativar uma política ILM, revise cuidadosamente a política ILM e suas regras ILM, e depois simule a política ILM. Sempre confirme que a política ILM funcionará conforme o esperado.

Clonar uma política ILM

Para clonar uma política ILM:

1. Selecione **ILM > Políticas**.
2. Selecione a caixa de seleção da política que você deseja clonar e, em seguida, selecione **Clonar**.
3. Crie uma nova política a partir da política que você clonou, seguindo as instruções em "[Criar políticas de ILM](#)".



Uma política ILM configurada incorretamente pode resultar em perda de dados irreversíveis. Antes de ativar uma política ILM, revise cuidadosamente a política ILM e suas regras ILM, e depois simule a política ILM. Sempre confirme que a política ILM funcionará conforme o esperado.

Remover uma política ILM

Você só pode remover uma política ILM se ela estiver inativa. Para remover uma política:

1. Selecione **ILM > Políticas**.
2. Selecione a caixa de seleção da política inativa que você deseja remover.
3. Selecione **Remove**.

Veja os detalhes da regra ILM

Para visualizar os detalhes de uma regra ILM, incluindo o diagrama de retenção e as instruções de posicionamento da regra:

1. Selecione **ILM > Regras**.
2. Selecione o nome da regra cujos detalhes você deseja visualizar. Exemplo:

2 copies 2 data centers

Compliant: No
Ingest behavior: Strict
Reference time: Noncurrent time

Clone Edit Remove

Rule detail Used in policies

Time period and placements

Retention diagram Placement instructions

Sort placements by Time period Storage pool

● Replicated copy ● Erasure-coded (EC) copy

Rule analysis: • Objects processed by this rule will not be deleted by ILM.

Reference time: Noncurrent time Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Data Center 1

EC 2+1 - Data Center 1

Duration Forever

Além disso, você pode usar a página de detalhes para clonar, editar ou remover uma regra. Você não pode editar ou remover uma regra se ela estiver sendo usada em alguma política.

Clonar uma regra ILM

Você pode clonar uma regra existente se quiser criar uma nova regra que utilize algumas das configurações da regra existente. Se precisar editar uma regra que está sendo usada em alguma política, você clona a regra e faz as alterações no clone. Depois de fazer as alterações no clone, você pode remover a regra original da política e substituí-la pela versão modificada conforme necessário.



Não é possível clonar uma regra ILM se ela foi criada usando StorageGRID versão 10.2 ou anterior.

Passos

1. Selecione **ILM > Regras**.
2. Selecione a caixa de seleção da regra que você deseja clonar e, em seguida, selecione **Clonar**. Como alternativa, selecione o nome da regra e, em seguida, selecione **Clonar** na página de detalhes da regra.
3. Atualize a regra clonada seguindo os passos para [editar uma regra ILM](#) e "[usando filtros avançados em regras ILM](#)".

Ao clonar uma regra ILM, você deve inserir um novo nome.

Editar uma regra ILM

Você pode precisar editar uma regra ILM para alterar um filtro ou uma instrução de posicionamento.

Não é possível editar uma regra se ela estiver sendo usada em alguma política ILM. Em vez disso, você pode [clonar a regra](#) e fazer as alterações necessárias na cópia clonada.



Uma política ILM configurada incorretamente pode resultar em perda de dados irrecuperáveis. Antes de ativar uma política ILM, revise cuidadosamente a política ILM e suas regras ILM, e depois simule a política ILM. Sempre confirme que a política ILM funcionará conforme o esperado.

Passos

1. Selecione **ILM > Regras**.
2. Confirme que a regra que você deseja editar não está sendo usada em nenhuma política ILM.
3. Se a regra que você deseja editar não estiver em uso, marque a caixa de seleção da regra e selecione **Ações > Editar**. Como alternativa, selecione o nome da regra e selecione **Editar** na página de detalhes da regra.
4. Conclua as etapas do assistente Editar regra ILM. Se necessário, siga as etapas para "[criando uma regra ILM](#)" e "[usando filtros avançados em regras ILM](#)".

Ao editar uma regra ILM, você não pode alterar o nome dela.

Remover uma regra ILM

Para manter a lista de regras ILM atuais gerenciável, remova quaisquer regras ILM que você provavelmente não usará.

Passos

Para remover uma regra ILM que está atualmente em uso em uma política ativa:

1. Clone a política.
2. Remova a regra ILM do clone da política.
3. Salve, simule e ative a nova política para garantir que os objetos estejam protegidos conforme o esperado.
4. Vá para as etapas para remover uma regra ILM que está sendo usada em uma política inativa.

Para remover uma regra ILM que está sendo usada em uma política inativa:

1. Selecione a política inativa.
2. Remova a regra ILM da política ou [remover a policy](#).

3. Vá para os passos para remover uma regra ILM que não está sendo usada no momento.

Para remover uma regra ILM que não está sendo usada atualmente:

1. Selecione **ILM > Regras**.
2. Confirme que a regra que você deseja remover não está sendo usada em nenhuma política.
3. Se a regra que você deseja remover não estiver em uso, selecione a regra e selecione **Ações > Remover**. Você pode selecionar várias regras e remover todas ao mesmo tempo.
4. Selecione **Sim** para confirmar que você deseja remover a regra ILM.

Visualizar métricas de ILM

Você pode visualizar métricas do ILM, como o número de objetos na fila e a taxa de avaliação. Você pode monitorar essas métricas para determinar o desempenho do sistema. Uma fila grande ou uma alta taxa de avaliação podem indicar que o sistema não está conseguindo acompanhar a taxa de ingestão, que a carga dos aplicativos cliente está excessiva ou que existe alguma condição anormal.

Passos

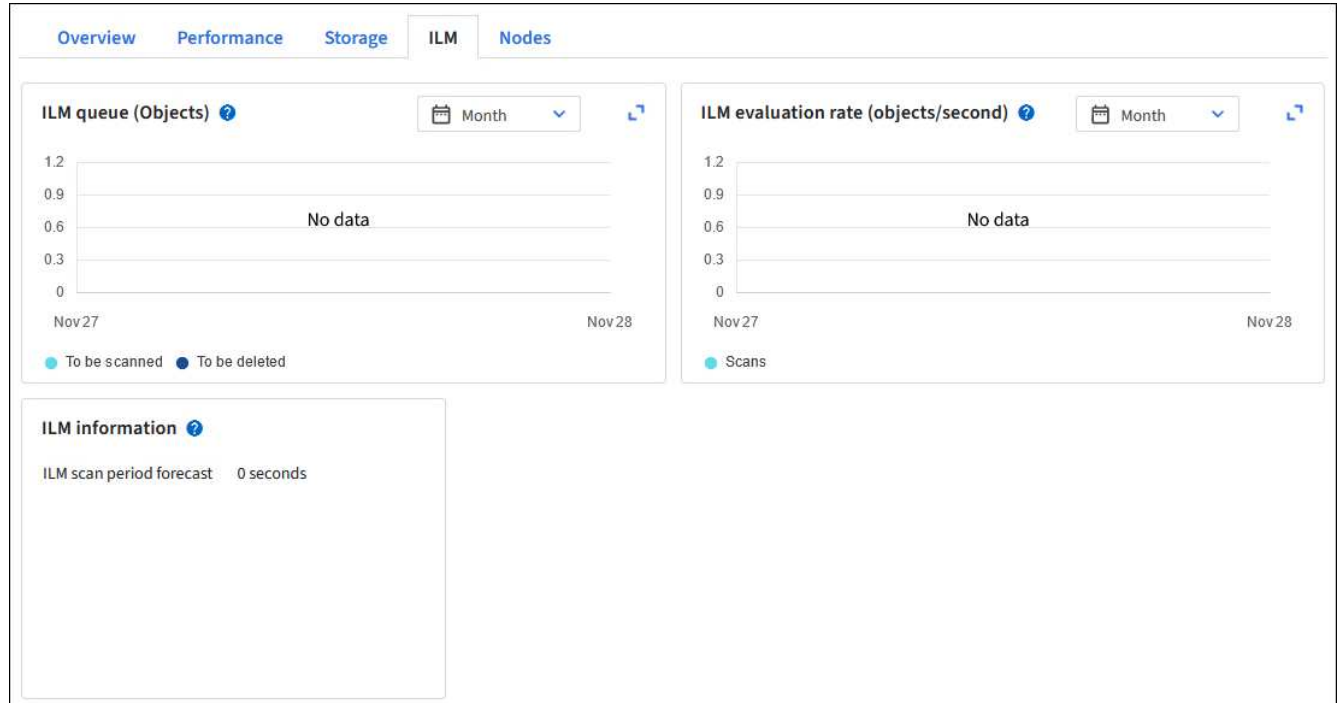
1. Selecione **Dashboard > ILM**.



Como o painel de controle pode ser personalizado, a guia ILM pode não estar disponível.

2. Monitore as métricas na guia ILM.

Você pode selecionar o ponto de interrogação (?) para ver uma descrição dos itens na guia ILM.



Use o Bloqueio de Objeto S3

Como o S3 Object Lock protege objetos no StorageGRID

Como administrador de grid, você pode habilitar o S3 Object Lock para o seu sistema StorageGRID e implementar uma política ILM compatível para ajudar a garantir que objetos em buckets S3 específicos não sejam excluídos ou sobrescritos por um período de tempo determinado.

O que é o bloqueio de objeto S3?

O recurso StorageGRID S3 Object Lock é uma solução de proteção de objetos equivalente ao S3 Object Lock do Amazon Simple Storage Service (Amazon S3).

Quando a configuração global de S3 Object Lock está habilitada para um sistema StorageGRID, uma conta de locatário S3 pode criar buckets com ou sem S3 Object Lock habilitado. Se um bucket tiver S3 Object Lock habilitado, o versionamento do bucket é obrigatório e é habilitado automaticamente.

Um bucket sem S3 Object Lock só pode conter objetos sem configurações de retenção especificadas. Nenhum objeto ingerido terá configurações de retenção.

Um bucket com S3 Object Lock pode conter objetos com e sem configurações de retenção especificadas por aplicativos cliente S3. Alguns objetos ingeridos terão configurações de retenção.

Um bucket com S3 Object Lock e retenção padrão configurada pode ter objetos carregados com configurações de retenção especificadas e novos objetos sem configurações de retenção. Os novos objetos usam a configuração padrão, pois a configuração de retenção não foi definida no nível do objeto.

Na prática, todos os objetos recém-ingерidos têm configurações de retenção quando a retenção padrão está configurada. Os objetos existentes sem configurações de retenção permanecem inalterados.

Modos de retenção

O recurso StorageGRID S3 Object Lock oferece suporte a dois modos de retenção para aplicar diferentes níveis de proteção aos objetos. Esses modos são equivalentes aos modos de retenção do Amazon S3.

- No modo de conformidade:
 - O objeto não pode ser excluído até que sua retain-until-date seja atingida.
 - A data de retenção do objeto pode ser aumentada, mas não pode ser diminuída.
 - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- Em modo de governança:
 - Usuários com permissão especial podem usar um cabeçalho de bypass em solicitações para modificar determinadas configurações de retenção.
 - Esses usuários podem excluir uma versão de objeto antes que a data de retenção seja atingida.
 - Esses usuários podem aumentar, diminuir ou remover a retain-until-date de um objeto.

Configurações de retenção para versões de objetos

Se um bucket for criado com o S3 Object Lock ativado, os usuários podem usar o aplicativo cliente S3 para, opcionalmente, especificar as seguintes configurações de retenção para cada objeto adicionado ao bucket:

- **Modo de retenção:** conformidade ou governança.

- **Data de retenção:** Se a data de retenção de uma versão de objeto for futura, o objeto pode ser recuperado, mas não pode ser excluído.
- **Guarda legal:** Aplicar uma guarda legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar aplicar uma guarda legal a um objeto relacionado a uma investigação ou disputa legal. Uma guarda legal não tem data de expiração, mas permanece em vigor até ser explicitamente removida. As guardas legais são independentes da data de retenção.



Se um objeto estiver sob guarda legal, ninguém pode excluir o objeto, independentemente do seu modo de retenção.

Para obter detalhes sobre as configurações do objeto, consulte ["Use a API REST S3 para configurar o S3 Object Lock"](#).

Configuração padrão de retenção para buckets

Se um bucket for criado com o S3 Object Lock ativado, você pode, opcionalmente, especificar as seguintes configurações padrão para o bucket:

- **Modo de retenção padrão:** conformidade ou governança.
- **Período de retenção padrão:** Por quanto tempo as novas versões de objetos adicionadas a este bucket devem ser retidas, a partir do dia em que forem adicionadas.

As configurações padrão do bucket se aplicam somente a novos objetos que não possuem suas próprias configurações de retenção. Objetos de bucket existentes não são afetados quando você adiciona ou altera essas configurações padrão.

Veja ["Crie um bucket S3"](#) e ["Atualizar retenção padrão do S3 Object Lock"](#).

Comparando o S3 Object Lock com a Compliance legada

O recurso S3 Object Lock substitui o recurso Compliance que estava disponível em versões anteriores do StorageGRID. Como o recurso S3 Object Lock está em conformidade com os requisitos do Amazon S3, ele descontinua o recurso proprietário Compliance do StorageGRID, agora denominado "legacy Compliance".



A configuração de Compliance global está obsoleta. Se você habilitou essa configuração usando uma versão anterior do StorageGRID, a configuração S3 Object Lock é habilitada automaticamente. Você pode continuar usando StorageGRID para gerenciar as configurações dos buckets compatíveis existentes; no entanto, você não pode criar novos buckets compatíveis. Para detalhes, veja ["NetApp Knowledge Base: como gerenciar buckets legados compatíveis no StorageGRID 11.5"](#).

Se você utilizou o recurso de Compliance legado em uma versão anterior do StorageGRID, consulte a tabela a seguir para saber como ele se compara ao recurso S3 Object Lock no StorageGRID.

	Bloqueio de objeto S3	Conformidade (legado)
Como esse recurso é habilitado globalmente?	No Grid Manager, selecione Configuração > Sistema > S3 Object Lock .	Não é mais suportada.

	Bloqueio de objeto S3	Conformidade (legado)
Como o recurso é habilitado para um bucket?	Os usuários devem habilitar o S3 Object Lock ao criar um novo bucket usando o Tenant Manager, a Tenant Management API ou a API REST.	Não é mais suportada.
O versionamento de buckets é suportado?	Sim. O versionamento de buckets é necessário e é ativado automaticamente quando o S3 Object Lock está habilitado para o bucket.	Não
Como o período de retenção de objetos é definido?	Os usuários podem definir uma data limite de retenção para cada versão de objeto ou podem definir um período de retenção padrão para cada bucket.	Os usuários devem definir um período de retenção para todo o bucket. O período de retenção se aplica a todos os objetos no bucket.
O período de retenção pode ser alterado?	• No modo de conformidade, a data de retenção para uma versão de objeto pode ser aumentada, mas nunca diminuída. • No modo de governança, usuários com permissões especiais podem diminuir ou até mesmo remover as configurações de retenção de um objeto.	O período de retenção de um bucket pode ser aumentado, mas nunca diminuído.
Onde a guarda legal é controlada?	Os usuários podem aplicar guarda legal ou remover guarda legal para qualquer versão de objeto no bucket.	Uma guarda legal é aplicada ao bucket e afeta todos os objetos no bucket.
Quando os objetos podem ser excluídos?	• No modo de conformidade, uma versão de objeto pode ser excluída após o retain-until-date ser atingido, desde que o objeto não esteja sob guarda legal. • No modo de governança, usuários com permissões especiais podem excluir um objeto antes que sua data de retenção seja atingida, desde que o objeto não esteja sob guarda legal.	Um objeto pode ser excluído após o período de retenção expirar, desde que o bucket não esteja sob guarda legal. Os objetos podem ser excluídos automaticamente ou manualmente.

	Bloqueio de objeto S3	Conformidade (legado)
A configuração de ciclo de vida do bucket é compatível?	Sim	Não

Fluxo de trabalho do S3 Object Lock no StorageGRID

Como administrador de grid, você deve coordenar-se de perto com os usuários locatários para garantir que os objetos sejam protegidos de uma forma que atenda aos requisitos de retenção deles.



A aplicação das configurações de locatário em toda a grid pode levar 15 minutos ou mais, dependendo da conectividade da rede, do status do nó e das operações do Cassandra.

As listas a seguir para administradores de grid e usuários locatários contêm as tarefas de alto nível para usar o recurso S3 Object Lock.

Administrador de grid

- Ative a configuração global de bloqueio de objetos S3 para todo o sistema StorageGRID.
- Garanta que as políticas de gerenciamento do ciclo de vida das informações (ILM) estejam em conformidade; ou seja, que atendam aos ["Requisitos de buckets com S3 Object Lock ativado"](#).
- Se necessário, permita que um locatário use o modo de Compliance como modo de retenção. Caso contrário, somente o modo de Governance é permitido.
- Se necessário, defina um período máximo de retenção para um tenant.

Usuário locatário

- Analise as considerações para buckets e objetos com S3 Object Lock.
- Se necessário, entre em contato com o administrador da grid para ativar a configuração global de S3 Object Lock e definir as permissões.
- Crie buckets com o S3 Object Lock ativado.
- Opcionalmente, configure as definições de retenção padrão para um bucket:
 - Modo de retenção padrão: Governança ou Conformidade, se permitido pelo administrador da grid.
 - Período de retenção padrão: deve ser menor ou igual ao período de retenção máximo definido pelo administrador da grade.
- Use o aplicativo cliente S3 para adicionar objetos e, opcionalmente, definir a retenção específica do objeto:
 - Modo de retenção. Governança ou Conformidade, se permitido pelo administrador da grid.
 - Data de retenção: deve ser menor ou igual ao permitido pelo período máximo de retenção definido pelo administrador do grid.

Requisitos do S3 Object Lock no StorageGRID

Você deve revisar os requisitos para habilitar a configuração global de S3 Object Lock, os requisitos para criar regras ILM e políticas ILM compatíveis e as restrições que StorageGRID impõe aos buckets e objetos que usam S3 Object Lock.

Requisitos para usar a configuração global de S3 Object Lock

- Você precisa habilitar a configuração global de S3 Object Lock usando o Grid Manager ou a Grid Management API antes que qualquer tenant S3 possa criar um bucket com S3 Object Lock habilitado.
- Habilitar a configuração global de S3 Object Lock permite que todas as contas de locatário do S3 criem buckets com S3 Object Lock ativado.
- Depois de ativar a configuração global de S3 Object Lock, você não poderá desativar a configuração.
- Você não pode habilitar o S3 Object Lock global a menos que a regra padrão em todas as políticas ILM ativas seja *compliant* (ou seja, a regra padrão deve estar em conformidade com os requisitos dos buckets com S3 Object Lock habilitado).
- Quando a configuração global de S3 Object Lock está ativada, você não pode criar uma nova política ILM nem ativar uma política ILM existente, a menos que a regra padrão na política seja compatível. Depois que a configuração global de S3 Object Lock for ativada, as páginas de regras ILM e políticas ILM indicam quais regras ILM são compatíveis.

Requisitos para regras ILM em conformidade

Se você deseja habilitar a configuração global de S3 Object Lock, você deve garantir que a regra padrão em todas as políticas ILM ativas esteja em conformidade. Uma regra em conformidade atende aos requisitos tanto dos buckets com S3 Object Lock habilitado quanto de quaisquer buckets existentes que tenham Compliance legado habilitada:

- É necessário criar pelo menos duas cópias replicadas do objeto ou uma cópia com código de apagamento.
- Essas cópias devem existir nos Storage Nodes durante toda a duração de cada linha nas instruções de posicionamento.
- Não é possível salvar cópias de objetos em um Cloud Storage Pool.
- Pelo menos uma linha das instruções de colocação deve começar no dia 0, usando **Horário de ingestão** como tempo de referência.
- Pelo menos uma linha das instruções de posicionamento deve ser "para sempre".

Requisitos para políticas de ILM

Quando a configuração global de S3 Object Lock está ativada, as políticas ILM ativas e inativas podem incluir regras compatíveis e não compatíveis.

- A regra padrão em uma política ILM ativa ou inativa deve estar em conformidade.
- As regras de não conformidade aplicam-se apenas a objetos em buckets que não têm o S3 Object Lock ativado ou que não têm o recurso de Compliance legado ativado.
- As regras de conformidade podem ser aplicadas a objetos em qualquer bucket; S3 Object Lock ou Compliance legado não precisam estar habilitados para o bucket.

"Exemplo de uma política ILM compatível para S3 Object Lock"

Requisitos para buckets com S3 Object Lock ativado

- Se a configuração global de S3 Object Lock estiver habilitada para o sistema StorageGRID, você pode usar o Tenant Manager, a Tenant Management API ou a S3 REST API para criar buckets com S3 Object Lock habilitado.
- Se você planeja usar o S3 Object Lock, precisa habilitar o S3 Object Lock ao criar o bucket. Você não

pode habilitar o S3 Object Lock para um bucket existente.

- Quando o S3 Object Lock está habilitado para um bucket, o StorageGRID habilita automaticamente o versionamento para esse bucket. Você não pode desabilitar o S3 Object Lock nem suspender o versionamento para o bucket.
- Opcionalmente, você pode especificar um modo de retenção padrão e um período de retenção para cada bucket usando o Tenant Manager, a Tenant Management API ou a S3 REST API. As configurações de retenção padrão do bucket se aplicam somente a novos objetos adicionados ao bucket que não têm suas próprias configurações de retenção. Você pode substituir essas configurações padrão especificando um modo de retenção e uma data de retenção para cada versão do objeto no momento do upload.
- A configuração do ciclo de vida do bucket é compatível com buckets que possuem o S3 Object Lock ativado.
- CloudMirror A replicação não é suportada para buckets com S3 Object Lock ativado.

Requisitos para objetos em buckets com S3 Object Lock ativado

- Para proteger uma versão de objeto, você pode especificar configurações de retenção padrão para o bucket ou pode especificar configurações de retenção para cada versão de objeto. As configurações de retenção em nível de objeto podem ser especificadas usando o aplicativo cliente S3 ou a API REST.
- As configurações de retenção se aplicam a versões individuais de objetos. Uma versão de objeto pode ter tanto uma configuração de data de retenção quanto de guarda legal, uma delas, mas não a outra, ou nenhuma das duas. Especificar uma data de retenção ou uma configuração de guarda legal para um objeto protege apenas a versão especificada na solicitação. Você pode criar novas versões do objeto, enquanto a versão anterior do objeto permanece bloqueada.

Ciclo de vida de objetos em buckets com S3 Object Lock ativado

Cada objeto salvo em um bucket com o S3 Object Lock ativado passa por estas etapas:

1. Ingestão de objeto

Quando uma versão de objeto é adicionada a um bucket com o S3 Object Lock ativado, as configurações de retenção são aplicadas da seguinte forma:

- Se as configurações de retenção forem especificadas para o objeto, as configurações em nível de objeto serão aplicadas. Quaisquer configurações padrão de bucket serão ignoradas.
- Se nenhuma configuração de retenção for especificada para o objeto, as configurações padrão do bucket serão aplicadas, se existirem.
- Se nenhuma configuração de retenção for especificada para o objeto ou o bucket, o objeto não estará protegido pelo S3 Object Lock.

Se as configurações de retenção forem aplicadas, tanto o objeto quanto quaisquer metadados definidos pelo usuário S3 estarão protegidos.

2. Retenção e exclusão de objetos

Várias cópias de cada objeto protegido são armazenadas pelo StorageGRID pelo período de retenção especificado. O número exato e o tipo de cópias de objeto, assim como os locais de armazenamento, são determinados pelas regras de conformidade nas políticas ILM ativas. Se um objeto protegido pode ser excluído antes de atingir sua data de retenção depende do seu modo de retenção.

- Se um objeto estiver sob guarda legal, ninguém pode excluir o objeto, independentemente do seu modo de retenção.

Informações relacionadas

- ["Crie um bucket S3"](#)
- ["Atualizar retenção padrão do S3 Object Lock"](#)
- ["Use a API REST S3 para configurar o S3 Object Lock"](#)
- ["Exemplo 7: política ILM compatível para S3 Object Lock"](#)

Ativar o S3 Object Lock globalmente no StorageGRID

Se uma conta de locatário do S3 precisar atender a requisitos regulatórios ao salvar dados de objetos, você deve habilitar o S3 Object Lock para todo o seu sistema StorageGRID. Habilitar a configuração global de S3 Object Lock permite que qualquer usuário de locatário do S3 crie e gerencie buckets e objetos com S3 Object Lock.

Antes de começar

- Você tem o ["Permissão de acesso root"](#).
- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você analisou o fluxo de trabalho de S3 Object Lock e compreende as considerações.
- Você confirmou que a regra padrão na política ILM ativa está em conformidade. Veja ["Criar uma regra ILM padrão"](#) para detalhes.

Sobre esta tarefa

Um administrador de grid deve habilitar a configuração global de Bloqueio de Objetos S3 para permitir que os usuários do tenant criem novos buckets com o Bloqueio de Objetos S3 habilitado. Depois de habilitada, essa configuração não pode ser desabilitada.

Revise as configurações de conformidade dos locatários existentes após ativar a configuração global de S3 Object Lock. Ao ativar essa configuração, as configurações de S3 Object Lock por locatário dependem da versão do StorageGRID vigente no momento em que o locatário foi criado.



A configuração de Compliance global está obsoleta. Se você habilitou essa configuração usando uma versão anterior do StorageGRID, a configuração S3 Object Lock é habilitada automaticamente. Você pode continuar usando StorageGRID para gerenciar as configurações dos buckets compatíveis existentes; no entanto, você não pode criar novos buckets compatíveis. Para detalhes, veja ["NetApp Knowledge Base: como gerenciar buckets legados compatíveis no StorageGRID 11.5"](#).

Passos

1. Selecione **Configuração > Sistema > S3 Object Lock**.

A página Configurações de bloqueio de objetos S3 é exibida.

2. Selecione **Ativar S3 Object Lock**.
3. Selecione **Aplicar**.

Uma caixa de diálogo de confirmação é exibida e lembra você de que não é possível desativar o S3 Object Lock depois que ele é ativado.

4. Se você tem certeza de que deseja ativar permanentemente o S3 Object Lock para todo o seu sistema, selecione **OK**.

Ao selecionar **OK**:

- Se a regra padrão na política ILM ativa estiver em conformidade, o S3 Object Lock agora está ativado para toda a grid e não pode ser desativado.
- Se a regra padrão não for compatível, um erro será exibido. Você deve criar e ativar uma nova política ILM que inclua uma regra compatível como regra padrão. Selecione **OK**. Em seguida, crie uma nova política, simule-a e ative-a. Consulte ["Criar política de ILM"](#) para obter instruções.

Resolva erros de consistência ao atualizar S3 Object Lock ou configurações de Compliance legadas no StorageGRID

Caso um site de data center ou vários Storage Nodes em um site fiquem indisponíveis, você poderá precisar ajudar os usuários do tenant do S3 a aplicar alterações no S3 Object Lock ou na configuração de Compliance legada.

Usuários locatários que possuem buckets com S3 Object Lock (ou Compliance legada) ativado podem alterar determinadas configurações. Por exemplo, um usuário locatário que utiliza S3 Object Lock pode precisar colocar uma versão de objeto sob guarda legal.

Quando um usuário locatário atualiza as configurações de um bucket S3 ou a versão de um objeto, StorageGRID tenta atualizar imediatamente os metadados do bucket ou do objeto em toda a grid. Se o sistema não conseguir atualizar os metadados porque um site do data center ou vários Storage Nodes estão indisponíveis, ele retorna um erro:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Para resolver esse erro, siga estes passos:

1. Tente disponibilizar todos os Storage Nodes ou sites novamente o mais rápido possível.
2. Caso não consiga disponibilizar nós de armazenamento suficientes em cada local, entre em contato com o suporte técnico, que pode ajudar você a recuperar os nós e garantir que as alterações sejam aplicadas de forma consistente em toda a grid.
3. Após a resolução do problema subjacente, lembre o usuário locatário de tentar novamente as alterações de configuração.

Informações relacionadas

- ["Use uma conta de tenant"](#)
- ["Utilize a API REST S3"](#)
- ["Recuperar e manter"](#)

Exemplos de regras e políticas de ILM

Regras e políticas do ILM para proteção básica de objetos e retenção no StorageGRID

Você pode usar as seguintes regras e a política de exemplo como ponto de partida ao

definir uma política ILM para atender aos seus requisitos de proteção e retenção de objetos.



As regras e políticas de ILM a seguir são apenas exemplos. Existem muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Regra 1 do ILM para o exemplo 1: copiar dados de objeto para dois sites

Este exemplo de regra ILM copia dados de objetos para pools de storage em dois sites.

Definição de regra	Valor de exemplo
Pools de storage em um único site	Dois pools de storage, cada um contendo sites diferentes, chamados Site 1 e Site 2.
Nome da regra	Duas cópias dois sites
Tempo de referência	Tempo de ingestão
Atribuições	Do dia 0 até a perpetuidade, mantenha uma cópia replicada no Site 1 e uma cópia replicada no Site 2.

A seção de análise de regras do diagrama de retenção afirma:

- A proteção contra perda de site do StorageGRID será aplicada durante a vigência desta regra.
- Os objetos processados por esta regra não serão excluídos pelo ILM.

Reference time ?

Ingest time

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store forever

Store objects by replicating

1

copies at Site 1

and store objects by replicating

1

copies at Site 2

Add other type or location

Add another time period

Retention diagram

Replicated copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

1 replicated copy - Site 1

1 replicated copy - Site 2

Duration

Forever

Regra 2 do ILM para o exemplo 1: Perfil de codificação de apagamento com correspondência de bucket

Este exemplo de regra ILM usa um perfil de codificação de apagamento e um bucket S3 para determinar onde e por quanto tempo o objeto é armazenado.

Definição de regra	Valor de exemplo
Pool de storage com vários sites	- Um único pool de storage em três sites (Sites 1, 2, 3) - Use o esquema de codificação de apagamento 6+3
Nome da regra	Bucket S3 finance-records
Tempo de referência	Tempo de ingestão
Atribuições	Para os objetos no bucket S3 chamado finance-records, crie uma cópia codificada de apagamento no pool especificado pelo perfil de codificação de apagamento. Mantenha essa cópia para sempre.

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store

forever

Store objects by

erasure coding

using

6+3 EC scheme at Sites 1, 2, 3

Add other type or location

Add another time period

Retention diagram

Erasure-coded (EC) copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

EC 6+3 - Sites 1, 2, 3

Forever

Política ILM para o exemplo 1

Na prática, a maioria das políticas de ILM é simples, mesmo que o sistema StorageGRID permita que você crie políticas de ILM sofisticadas e complexas.

Uma política ILM típica para uma grid multi-site pode incluir regras ILM como as seguintes:

- Na ingestão, armazene todos os objetos pertencentes ao bucket S3 nomeado `finance-records` em um pool de storage que contenha três sites. Use codificação de apagamento 6+3.
- Se um objeto não corresponder à primeira regra ILM, use a regra ILM padrão da política, "Two Copies Two Data Centers", para armazenar uma cópia desse objeto no Site 1 e uma cópia no Site 2.

Proposed policy name

Object Storage Policy

Reason for change

example 1

Manage rules

1. Select the rules you want to add to the policy.

2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	S3 Bucket finance-records	Tenant is Finance Bucket name is finance-records
Default	Two Copies Two Data Centers	—

Informações relacionadas

- ["Use políticas ILM"](#)
- ["Criar políticas de ILM"](#)

Regras e política de ILM para filtragem de tamanho de objetos EC no StorageGRID

Você pode usar as seguintes regras e políticas de exemplo como ponto de partida para definir uma política ILM que filtre por tamanho de objeto para atender aos requisitos recomendados de codificação de apagamento.



As regras e políticas de ILM a seguir são apenas exemplos. Existem muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Regra 1 do ILM para o exemplo 2: use EC para objetos maiores que 1 MB

Este exemplo de regra ILM aplica codificação de apagamento a objetos com mais de 1 MB.



A codificação de apagamento é mais adequada para objetos maiores que 1 MB. Não use codificação de apagamento para objetos menores que 200 KB para evitar a sobrecarga de gerenciar fragmentos codificados por apagamento muito pequenos.

Definição de regra	Valor de exemplo
Nome da regra	Apenas objetos de EC > 1 MB
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Tamanho do objeto superior a 1 MB
Atribuições	Crie uma cópia 2+1 com codificação de apagamento usando três sites

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼

greater than ▼

1 ⬆️⬆️⬆️⬆️⬆️⬆️⬆️⬆️⬆️

MB ▼ ✕

Regra 2 do ILM para o exemplo 2: duas cópias replicadas

Esta regra de exemplo do ILM cria duas cópias replicadas e não filtra por tamanho do objeto. Esta regra é a regra padrão da política. Como a primeira regra filtra todos os objetos maiores que 1 MB, esta regra se aplica somente a objetos com 1 MB ou menos.

Definição de regra	Valor de exemplo
Nome da regra	Duas cópias replicadas

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Nenhum
Atribuições	Do dia 0 até a perpetuidade, mantenha uma cópia replicada no Site 1 e uma cópia replicada no Site 2.

Política ILM para o exemplo 2: usar EC para objetos maiores que 1 MB

Esta política ILM de exemplo inclui duas regras ILM:

- A primeira regra de codificação de apagamento codifica todos os objetos com tamanho superior a 1 MB.
- A segunda (padrão) regra ILM cria duas cópias replicadas. Como os objetos maiores que 1 MB foram filtrados pela regra 1, a regra 2 se aplica somente a objetos com 1 MB ou menos.

Regras e política de ILM para proteger arquivos de imagem no StorageGRID

Você pode usar as seguintes regras e políticas de exemplo para garantir que imagens maiores que 1 MB sejam codificadas de apagamento e que duas cópias sejam feitas de imagens menores.



As regras e políticas de ILM a seguir são apenas exemplos. Existem muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Regra 1 do ILM para o exemplo 3: use EC para arquivos de imagem maiores que 1 MB

Este exemplo de regra ILM usa filtragem avançada para aplicar codificação de apagamento a todos os arquivos de imagem maiores que 1 MB.



A codificação de apagamento é mais adequada para objetos maiores que 1 MB. Não use codificação de apagamento para objetos menores que 200 KB para evitar a sobrecarga de gerenciar fragmentos codificados por apagamento muito pequenos.

Definição de regra	Valor de exemplo
Nome da regra	Arquivos de imagem EC > 1 MB
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Tamanho do objeto superior a 1 MB
Filtros avançados para chave	• Termina com .jpg • Termina com .png

Definição de regra	Valor de exemplo
Atribuições	Crie uma cópia 2+1 com codificação de apagamento usando três sites

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

Object size greater than 1 MB

and Key ends with .jpg

or Filter group 2 Objects with all of following metadata will be evaluated by this rule:

Object size greater than 1 MB

and Key ends with .png

Como essa regra está configurada como a primeira regra na política, a instrução de colocação de codificação de apagamento se aplica somente a arquivos .jpg e .png com mais de 1 MB.

Regra 2 do ILM para o exemplo 3: crie 2 cópias replicadas para todos os arquivos de imagem restantes

Esta regra de exemplo do ILM usa filtragem avançada para especificar que arquivos de imagem menores sejam replicados. Como a primeira regra na política já correspondeu a arquivos de imagem maiores que 1 MB, esta regra se aplica a arquivos de imagem de 1 MB ou menores.

Definição de regra	Valor de exemplo
Nome da regra	2 cópias para arquivos de imagem
Tempo de referência	Tempo de ingestão
Filtros avançados para chave	• Termina com .jpg • Termina com .png
Atribuições	Crie 2 cópias replicadas em dois pools de storage

Política ILM para o exemplo 3: melhor proteção para arquivos de imagem

Esta política ILM de exemplo inclui três regras:

- A primeira regra codifica por apagamento todos os arquivos de imagem maiores que 1 MB.
- A segunda regra cria duas cópias de quaisquer arquivos de imagem restantes (ou seja, imagens com 1 MB ou menores).
- A regra padrão se aplica a todos os objetos restantes (ou seja, quaisquer arquivos que não sejam imagens).

Rule order	Rule name	Filters
1	↕ EC image files > 1 MB	Object size is greater than 1 MB
2	↕ 2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Regras e políticas de ILM para versões não atuais de objetos S3 no StorageGRID

Se você tiver um bucket S3 com versionamento ativado, poderá gerenciar as versões desatualizadas dos objetos incluindo regras em sua política ILM que usem o "Tempo desatualizado" como tempo de referência.



Se você especificar um tempo de retenção limitado para os objetos, esses objetos serão excluídos permanentemente após o término desse período. Certifique-se de compreender por quanto tempo os objetos serão retidos.

Como mostra este exemplo, você pode controlar a quantidade de armazenamento usada por objetos versionados usando instruções de alocação diferentes para versões não atuais do objeto.



As regras e políticas de ILM a seguir são apenas exemplos. Existem muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará conforme o esperado para proteger o conteúdo contra perdas.



Para realizar a simulação da política ILM em uma versão não atual de um objeto, você precisa saber o UUID ou CBID da versão do objeto. Para encontrar o UUID e o CBID, use ["pesquisa de metadados de objetos"](#) enquanto o objeto ainda estiver atual.

Informações relacionadas

["Como os objetos são excluídos"](#)

Regra 1 do ILM para o exemplo 4: Salve três cópias por 10 anos

Este exemplo de regra ILM armazena uma cópia de cada objeto em três sites por 10 anos.

Essa regra se aplica a todos os objetos, independentemente de serem ou não versionados.

Definição de regra	Valor de exemplo
Pools de storage	Três pools de armazenamento, cada um composto por diferentes data centers, denominados Site 1, Site 2 e Site 3.
Nome da regra	Três cópias dez anos

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Atribuições	No dia 0, mantenha três cópias replicadas por 10 anos (3.652 dias), uma no Site 1, uma no Site 2 e uma no Site 3. Ao final de 10 anos, exclua todas as cópias do objeto.

Regra 2 do ILM para o exemplo 4: salve duas cópias de versões não atuais por 2 anos

Esta regra ILM de exemplo armazena duas cópias das versões não atuais de um objeto versionado do S3 por 2 anos.

Como a regra 1 do ILM se aplica a todas as versões do objeto, você deve criar outra regra para filtrar quaisquer versões não atuais.

Para criar uma regra que use "Tempo não atual" como tempo de referência, selecione **Sim** na pergunta "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com versionamento ativado)?" na Etapa 1 (Inserir detalhes) do assistente Criar uma regra ILM. Ao selecionar **Sim**, *Tempo não atual* é selecionado automaticamente como tempo de referência e você não pode selecionar um tempo de referência diferente.

1 Enter details
2 Define placements
3 Select ingest behavior

Rule name

Older Object Versions: Two Copies Two Years

Description (optional)

Older versions only

Basic filters (optional)
Specify which tenant accounts and buckets this rule applies to.

Tenant accounts ?

Select tenant accounts

Bucket name ?

matches all

Apply this rule to older object versions only (in S3 buckets with versioning enabled)? ?

☐ No
☒ Yes

Neste exemplo, apenas duas cópias das versões não atuais são armazenadas, e essas cópias serão armazenadas por dois anos.

Definição de regra	Valor de exemplo
Pools de armazenamento	Dois pools de armazenamento, cada um em um data center diferente, Site 1 e Site 2.
Nome da regra	Versões não atuais: duas cópias dois anos
Tempo de referência	Tempo não atual Selecione automaticamente quando você seleciona Sim para a pergunta, "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com versionamento ativado)?" no assistente Criar uma regra ILM.
Atribuições	No Dia 0 em relação ao tempo não atual (ou seja, a partir do dia em que a versão do objeto se torna a versão não atual), mantenha duas cópias replicadas das versões não atuais do objeto por 2 anos (730 dias), uma no Site 1 e uma no Site 2. Ao final de 2 anos, exclua as versões não atuais.

Política ILM para exemplo 4: objetos versionados do S3

Se você deseja gerenciar versões antigas de um objeto de forma diferente da versão atual, as regras que usam "Tempo não atual" como tempo de referência devem aparecer na política ILM antes das regras que se aplicam à versão atual do objeto.

Uma política ILM para objetos versionados do S3 pode incluir regras ILM como as seguintes:

- Mantenha quaisquer versões antigas (não atuais) de cada objeto por 2 anos, a partir do dia em que a versão se tornou não atual.



As regras de "Tempo não atual" devem aparecer na política antes das regras que se aplicam à versão atual do objeto. Caso contrário, as versões não atuais do objeto nunca serão correspondidas pela regra de "Tempo não atual".

- No momento da ingestão, crie três cópias replicadas e armazene uma cópia em cada um dos três locais. Mantenha cópias da versão atual do objeto por 10 anos.

Ao simular a política de exemplo, você esperaria que os objetos de teste fossem avaliados da seguinte forma:

- Qualquer versão de objeto não atual será correspondida pela primeira regra. Se uma versão de objeto não atual tiver mais de 2 anos, ela é excluída permanentemente pelo ILM (todas as cópias da versão não atual removidas do grid).
- A versão atual do objeto seria correspondida pela segunda regra. Quando a versão atual do objeto estiver armazenada por 10 anos, o processo ILM adiciona um marcador de exclusão como a versão atual do objeto e torna a versão anterior do objeto "não atual". Na próxima avaliação do ILM, essa versão não atual será correspondida pela primeira regra. Como resultado, a cópia no Site 3 é excluída e as duas cópias nos Sites 1 e 2 são armazenadas por mais 2 anos.

Regras e política de ILM para comportamento de ingestão estrito no StorageGRID

Você pode usar um filtro de local e o comportamento de ingestão estrito em uma regra para impedir que os objetos sejam salvos em um local específico do data center.

Neste exemplo, um locatário com sede em Paris não deseja armazenar alguns objetos fora da UE devido a preocupações regulatórias. Outros objetos, incluindo todos os objetos de outras contas de locatários, podem ser armazenados no data center de Paris ou no data center dos EUA.



As regras e políticas de ILM a seguir são apenas exemplos. Existem muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Informações relacionadas

- ["Opções de ingestão"](#)
- ["Criar regra ILM: selecionar comportamento de ingestão"](#)

Regra 1 do ILM para o exemplo 5: Ingestão rigorosa para garantir o data center de Paris

Este exemplo de regra ILM usa o comportamento de ingestão estrito para garantir que os objetos salvos por um locatário com sede em Paris em buckets S3 com a região definida como eu-west-3 (Paris) nunca sejam armazenados no data center dos EUA.

Esta regra aplica-se a objetos que pertencem ao locatário Paris e que têm a região do bucket S3 definida como eu-west-3 (Paris).

Definição de regra	Valor de exemplo
Conta de tenant	Tenant Paris
Filtro avançado	A restrição de local é igual a eu-west-3
Pools de storage	Local 1 (Paris)
Nome da regra	Ingestão rigorosa para garantir o data center de Paris
Tempo de referência	Tempo de ingestão
Atribuições	No dia 0, mantenha duas cópias replicadas para sempre no Site 1 (Paris)
Comportamento de ingestão	Rigoroso. Sempre utilize os posicionamentos desta regra na ingestão. A ingestão falhará se não for possível armazenar duas cópias do objeto no data center de Paris.

Strict ingest to guarantee Paris data center

Compliant: Yes
Used in active policy: No
Used in proposed policy: No

Ingest behavior: Strict
Reference time: Ingest time

Clone Edit Remove

Filters

This rule applies if:

- Tenant is Paris tenant

And it only applies if objects have this metadata:

- Location constraint is eu-west-3

Time period and placements

Retention diagram Placement instructions

Sort placements by Time period Storage pool

● Replicated copy

Rule analysis:

- StorageGRID site-loss protection will not apply from Day 0 - Forever.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Site 1

Duration

Forever

Regra 2 do ILM para o exemplo 5: ingestão balanceada para outros objetos

Esta regra de ILM de exemplo usa o comportamento de ingestão balanceada para fornecer eficiência ideal de ILM para quaisquer objetos que não correspondam à primeira regra. Duas cópias de todos os objetos correspondentes a esta regra serão armazenadas: uma no data center dos EUA e uma no data center de Paris. Se a regra não puder ser atendida imediatamente, cópias provisórias serão armazenadas em qualquer local disponível.

Esta regra aplica-se a objetos que pertencem a qualquer tenant e a qualquer região.

Definição de regra	Valor de exemplo
Conta de tenant	Ignorar
Filtro avançado	Não especificado
Pools de storage	Local 1 (Paris) e Local 2 (US)
Nome da regra	2 Cópias 2 Data Centers
Tempo de referência	Tempo de ingestão

Definição de regra	Valor de exemplo
Atribuições	No dia 0, mantenha duas cópias replicadas para sempre em dois data centers
Comportamento de ingestão	Equilibrado. Os objetos que correspondem a esta regra são colocados de acordo com as instruções de posicionamento da regra, se possível. Caso contrário, cópias provisórias são feitas em qualquer local disponível.

Política ILM para o exemplo 5: combinando comportamentos de ingestão

A política ILM de exemplo inclui duas regras com comportamentos de ingestão diferentes.

Uma política ILM que utiliza dois comportamentos de ingestão diferentes pode incluir regras ILM como as seguintes:

- Armazene os objetos pertencentes ao locatário de Paris e que tenham a região do bucket S3 definida como eu-west-3 (Paris) somente no data center de Paris. Falhe a ingestão se o data center de Paris não estiver disponível.
- Armazene todos os outros objetos (incluindo aqueles que pertencem ao locatário de Paris, mas que têm uma região de bucket diferente) tanto no data center dos EUA quanto no data center de Paris. Faça cópias provisórias em qualquer local disponível caso a instrução de posicionamento não possa ser atendida.

Ao simular a política de exemplo, você espera que os objetos de teste sejam avaliados da seguinte forma:

- Quaisquer objetos pertencentes ao locatário de Paris e que tenham a região do bucket S3 definida como eu-west-3 são correspondidos pela primeira regra e armazenados no data center de Paris. Como a primeira regra usa ingestão estrita, esses objetos nunca são armazenados no data center dos EUA. Se os nós de armazenamento no data center de Paris não estiverem disponíveis, a ingestão falha.
- Todos os outros objetos são correspondidos pela segunda regra, incluindo objetos pertencentes ao locatário de Paris e que não têm a região do bucket S3 definida como eu-west-3. Uma cópia de cada objeto é salva em cada data center. No entanto, como a segunda regra usa Balanced ingest, se um data center estiver indisponível, duas cópias provisórias são salvas em qualquer local disponível.

Como a alteração de uma política ILM afeta o desempenho do StorageGRID

Se precisar alterar sua proteção de dados ou adicionar novos sites, você pode criar e ativar uma nova política ILM.

Antes de alterar uma política, você deve entender como as mudanças nos posicionamentos do ILM podem afetar temporariamente o desempenho geral de um sistema StorageGRID.

Neste exemplo, um novo site StorageGRID foi adicionado em uma expansão e uma nova política ILM ativa precisa ser implementada para armazenar dados no novo site. Para implementar uma nova política ativa, primeiro **"criar uma política"**. Em seguida, você deve **"simular"** e depois **"ativar"** a nova política.



As regras e políticas de ILM a seguir são apenas exemplos. Existem muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Como a alteração de uma política de ILM afeta o desempenho

Ao ativar uma nova política ILM, o desempenho do seu sistema StorageGRID pode ser afetado temporariamente, especialmente se as instruções de posicionamento na nova política exigirem que muitos objetos existentes sejam movidos para novos locais.

Ao ativar uma nova política ILM, StorageGRID a utiliza para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Antes de ativar uma nova política ILM, revise quaisquer alterações no posicionamento de objetos replicados e objetos com codificação de apagamento existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos são avaliados e implementados.

Para garantir que uma nova política ILM não afete a alocação de objetos replicados e codificados para apagamento existentes, você pode "[Crie uma regra ILM com um filtro de tempo de ingestão](#)". Por exemplo, **Ingest time is on or after <date and time>**, para que a nova regra se aplique somente a objetos ingeridos na data e hora especificadas ou posteriormente.

Os tipos de alterações de política ILM que podem afetar temporariamente o desempenho do StorageGRID incluem o seguinte:

- Aplicando um perfil de codificação de apagamento diferente a objetos já codificados por apagamento.



StorageGRID considera cada perfil de codificação de apagamento como único e não reutiliza fragmentos de codificação de apagamento quando um novo perfil é usado.

- Alterar o tipo de cópias necessárias para objetos existentes; por exemplo, converter uma grande porcentagem de objetos replicados em objetos com codificação de apagamento.
- Mover cópias de objetos existentes para um local completamente diferente; por exemplo, mover um grande número de objetos para ou de um Cloud Storage Pool ou para ou de um local remoto.

Política ILM ativa, por exemplo 6: proteção de dados em dois locais

Neste exemplo, a política ILM ativa foi inicialmente projetada para um sistema StorageGRID de dois locais e utiliza duas regras ILM.

Active policy

Policy history

Policy name:

Data Protection for Two Sites (2 rules)

Reason for change :

Data protection for two sites (using 2 rules)

Start date:

2022-10-11 10:37:11 MDT

Simulate

Policy rules

Retention diagram

Rule order ?	Rule name	Filters ?
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

Nessa política de ILM, os objetos pertencentes ao Tenant A são protegidos por codificação de apagamento 2+1 em um único site, enquanto os objetos pertencentes a todos os outros tenants são protegidos em dois sites usando replicação de 2 cópias.

Regra 1: codificação de apagamento em um único site para o Tenant A

Definição de regra	Valor de exemplo
Nome da regra	Codificação de apagamento de um único local para o tenant A
Conta de tenant	Locatário A
Pool de storage	Local 1
Atribuições	codificação de apagamento 2+1 no Site 1 do dia 0 até sempre

Regra 2: replicação em dois locais para outros inquilinos

Definição de regra	Valor de exemplo
Nome da regra	Replicação em dois locais para outros tenants
Conta de tenant	Ignorar
Pools de armazenamento	Site 1 e Site 2
Atribuições	Duas cópias replicadas desde o dia 0 até a eternidade: uma cópia no Site 1 e uma cópia no Site 2.

Política ILM para exemplo 6: proteção de dados em três locais

Neste exemplo, a política ILM está sendo substituída por uma nova política para um sistema StorageGRID de três locais.

Após realizar uma expansão para adicionar o novo site, o administrador da grade criou dois novos pools de storage: um pool de storage para o Site 3 e um pool de storage contendo todos os três sites (não é o mesmo que o pool de storage padrão All Storage Nodes). Em seguida, o administrador criou duas novas regras ILM e uma nova política ILM, projetada para proteger os dados em todos os três sites.

Quando essa nova política ILM for ativada, os objetos pertencentes ao Tenant A serão protegidos por codificação de apagamento 2+1 em três sites, enquanto os objetos pertencentes a outros tenants (e objetos menores pertencentes ao Tenant A) serão protegidos em três sites usando replicação de 3 cópias.

Regra 1: codificação de apagamento em três sites para o Tenant A

Definição de regra	Valor de exemplo
Nome da regra	Codificação de apagamento de três locais para o tenant A

Definição de regra	Valor de exemplo
Conta de tenant	Locatário A
Pool de storage	Todos os 3 sites (inclui o Site 1, o Site 2 e o Site 3)
Atribuições	codificação de apagamento 2+1 em todos os 3 sites do dia 0 para sempre

Regra 2: replicação em três locais para outros tenants

Definição de regra	Valor de exemplo
Nome da regra	Replicação em três locais para outros tenants
Conta de tenant	Ignorar
Pools de armazenamento	Site 1, Site 2 e Site 3
Atribuições	Três cópias replicadas desde o dia 0 até a eternidade: uma cópia no Site 1, uma cópia no Site 2 e uma cópia no Site 3.

Ativando a política ILM para o exemplo 6

Ao ativar uma nova política ILM, os objetos existentes podem ser movidos para novos locais ou novas cópias de objetos podem ser criadas para objetos existentes, com base nas instruções de posicionamento em quaisquer regras novas ou atualizadas.



Erros em uma política de ILM podem causar perda de dados irrecuperável. Analise e simule cuidadosamente a política antes de ativá-la para confirmar que ela funcionará conforme o esperado.



Ao ativar uma nova política ILM, StorageGRID a utiliza para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Antes de ativar uma nova política ILM, revise quaisquer alterações no posicionamento de objetos replicados e objetos com codificação de apagamento existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos são avaliados e implementados.

O que acontece quando as instruções de codificação de apagamento mudam

Na política ILM atualmente ativa para este exemplo, os objetos pertencentes ao Tenant A são protegidos usando codificação de apagamento 2+1 no Site 1. Na nova política ILM, os objetos pertencentes ao Tenant A serão protegidos usando codificação de apagamento 2+1 nos Sites 1, 2 e 3.

Quando a nova política ILM é ativada, as seguintes operações ILM ocorrem:

- Novos objetos recebidos pelo Tenant A são divididos em dois fragmentos de dados e um fragmento de paridade é adicionado. Em seguida, cada um dos três fragmentos é armazenado em um site diferente.

- Os objetos existentes pertencentes ao Tenant A são reavaliados durante o processo de varredura ILM em andamento. Como as instruções de posicionamento do ILM utilizam um novo perfil de codificação de apagamento, fragmentos de codificação de apagamento totalmente novos são criados e distribuídos para os três sites.



Os fragmentos 2+1 existentes no Site 1 não são reutilizados. StorageGRID considera cada perfil de codificação de apagamento como único e não reutiliza fragmentos de codificação de apagamento quando um novo perfil é usado.

O que acontece quando as instruções de replicação mudam

Na política ILM atualmente ativa para este exemplo, os objetos pertencentes a outros locatários são protegidos usando duas cópias replicadas em pools de storage nos Sites 1 e 2. Na nova política ILM, os objetos pertencentes a outros locatários serão protegidos usando três cópias replicadas em pools de storage nos Sites 1, 2 e 3.

Quando a nova política ILM é ativada, as seguintes operações ILM ocorrem:

- Quando qualquer locatário que não seja o Tenant A ingere um novo objeto, StorageGRID cria três cópias e salva uma cópia em cada site.
- Os objetos existentes pertencentes a esses outros locatários são reavaliados durante o processo contínuo de verificação do ILM. Como as cópias de objetos existentes no Site 1 e no Site 2 continuam a atender aos requisitos de replicação da nova regra do ILM, StorageGRID precisa criar apenas uma nova cópia do objeto para o Site 3.

Impacto no desempenho de ativar esta política

Quando a política ILM deste exemplo for ativada, o desempenho geral deste StorageGRID será afetado temporariamente. Serão necessários níveis de recursos de grid superiores ao normal para criar novos fragmentos com codificação de apagamento para os objetos existentes do Tenant A e novas cópias replicadas no Site 3 para os objetos existentes de outros tenants.

Como resultado da alteração na política ILM, as solicitações de leitura e gravação do cliente podem apresentar latências temporariamente maiores que o normal. As latências retornarão aos níveis normais após a implementação completa das instruções de posicionamento em todo o grid.

Para evitar problemas de recursos ao ativar uma nova política ILM, você pode usar o filtro avançado Ingest time em qualquer regra que possa alterar a localização de um grande número de objetos existentes. Defina Ingest time para um valor maior ou igual ao horário aproximado em que a nova política entrará em vigor para garantir que os objetos existentes não sejam movidos desnecessariamente.



Contate o suporte técnico se você precisar diminuir ou aumentar a velocidade com que os objetos são processados após uma alteração na política do ILM.

Política ILM compatível para S3 Object Lock no StorageGRID

Você pode usar o bucket S3, as regras ILM e a política ILM deste exemplo como ponto de partida ao definir uma política ILM para atender aos requisitos de proteção e retenção de objetos em buckets com o S3 Object Lock ativado.



Se você utilizou o recurso de Compliance legado em versões anteriores do StorageGRID, também pode usar este exemplo para ajudar a gerenciar quaisquer buckets existentes que tenham o recurso de Compliance legado ativado.



As regras e políticas de ILM a seguir são apenas exemplos. Existem muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Informações relacionadas

- ["Gerencie objetos com S3 Object Lock"](#)
- ["Crie uma política ILM"](#)

Bucket e objetos para exemplo de S3 Object Lock

Neste exemplo, uma conta de locatário do S3 chamada Bank of ABC usou o Tenant Manager para criar um bucket com S3 Object Lock ativado para armazenar registros bancários críticos.

Definição de bucket	Valor de exemplo
Nome da conta do locatário	Bank of ABC
Nome do bucket	registros bancários
Região do bucket	us-east-1 (padrão)

Cada objeto e versão de objeto adicionados ao bucket bank-records usarão os seguintes valores para `retain-until-date` e `legal hold` configurações.

Configuração para cada objeto	Valor de exemplo
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 de dezembro de 2030) Cada versão do objeto possui sua própria <code>retain-until-date</code> configuração. Essa configuração pode ser aumentada, mas não diminuída.
<code>legal hold</code>	"DESLIGADO" (não está em vigor) Uma guarda legal pode ser aplicada ou removida de qualquer versão de um objeto a qualquer momento durante o período de retenção. Se um objeto estiver sob guarda legal, ele não poderá ser excluído, mesmo que o <code>retain-until-date</code> tenha sido atingido.

Exemplo da regra 1 do ILM para S3 Object Lock: perfil de codificação de apagamento com correspondência de bucket

Este exemplo de regra de ILM aplica-se apenas à conta de tenant S3 chamada Bank of ABC. Ela corresponde a qualquer objeto no `bank-records` bucket e, em seguida, utiliza codificação de apagamento para armazenar o objeto em Storage Nodes em três data center, usando um perfil de codificação de apagamento 6+3. Esta regra atende aos requisitos de buckets com S3 Object Lock ativado: uma cópia é mantida em Storage Nodes do dia 0 para sempre, usando o horário de ingestão como tempo de referência.

Definição de regra	Valor de exemplo
Nome da regra	Regra de conformidade: Objetos EC no bucket de registros bancários - Bank of ABC
Conta de tenant	Bank of ABC
Nome do bucket	bank-records
Filtro avançado	Tamanho do objeto (MB) maior que 1 Nota: Este filtro garante que codificação de apagamento não seja usada para objetos de 1 MB ou menores.

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Atribuições	Desde o dia 0, armazene para sempre
Perfil de codificação de apagamento	• Crie uma cópia codificada por apagamento em Storage Nodes em três sites de data center • Utiliza o esquema de codificação de apagamento 6+3

Regra ILM 2 para S3 Object Lock: regra não compatível

Este exemplo de regra ILM armazena inicialmente duas cópias replicadas de objetos em Storage Nodes. Após um ano, armazena uma cópia em um Cloud Storage Pool para sempre. Como essa regra usa um Cloud Storage Pool, ela não está em conformidade e não será aplicada aos objetos em buckets com S3 Object Lock ativado.

Definição de regra	Valor de exemplo
Nome da regra	Regra não conforme: usar o Cloud Storage Pool
Contas de locatários	Não especificado
Nome do bucket	Não especificado, mas só se aplicará a buckets que não tenham S3 Object Lock (ou o recurso legado Compliance) ativado.
Filtro avançado	Não especificado

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão

Definição de regra	Valor de exemplo
Atribuições	- No dia 0, mantenha duas cópias replicadas nos Storage Nodes no Data Center 1 e no Data Center 2 por 365 dias - Após 1 ano, mantenha uma cópia replicada em um Cloud Storage Pool para sempre

Regra 3 do ILM para S3 Object Lock: regra padrão

Esta regra de exemplo do ILM copia dados de objetos para pools de storage em dois data centers. Esta regra em conformidade foi projetada para ser a regra padrão na política do ILM. Ela não inclui filtros, não usa o tempo de referência Noncurrent e atende aos requisitos de buckets com S3 Object Lock ativado: duas cópias do objeto são mantidas nos Storage Nodes do dia 0 para sempre, usando Ingest como tempo de referência.

Definição de regra	Valor de exemplo
Nome da regra	Regra padrão de conformidade: Duas cópias dois data centers
Conta de tenant	Não especificado
Nome do bucket	Não especificado
Filtro avançado	Não especificado

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Atribuições	Do dia 0 em diante, mantenha duas cópias replicadas: uma nos Storage Nodes no Data Center 1 e outra nos Storage Nodes no Data Center 2.

Exemplo de política ILM compatível para S3 Object Lock

Para criar uma política ILM que proteja efetivamente todos os objetos do seu sistema, incluindo aqueles em buckets com S3 Object Lock ativado, você deve selecionar regras ILM que atendam aos requisitos de armazenamento de todos os objetos. Em seguida, você deve simular e ativar a política.

Adicionar regras à política

Neste exemplo, a política ILM inclui três regras ILM, na seguinte ordem:

1. Uma regra compatível que usa codificação de apagamento para proteger objetos maiores que 1 MB em um bucket específico com S3 Object Lock ativado. Os objetos são armazenados em Storage Nodes do dia 0 para sempre.
2. Uma regra não conforme que cria duas cópias replicadas de objetos em Storage Nodes por um ano e, em seguida, move uma das cópias para um Cloud Storage Pool permanentemente. Essa regra não se aplica a buckets com S3 Object Lock ativado porque utiliza um Cloud Storage Pool.
3. A regra padrão de conformidade que cria duas cópias replicadas de objetos em Storage Nodes desde o primeiro dia até indefinidamente.

Simule a política

Depois de adicionar regras à sua política, escolher uma regra padrão compatível e organizar as demais regras, você deve simular a política testando objetos do bucket com S3 Object Lock ativado e de outros buckets. Por exemplo, ao simular a política de exemplo, você espera que os objetos de teste sejam avaliados da seguinte forma:

- A primeira regra só corresponderá a objetos de teste que sejam maiores que 1 MB no bucket bank-records para o tenant Bank of ABC.
- A segunda regra corresponderá a todos os objetos em todos os buckets não compatíveis para todas as outras contas de tenant.
- A regra padrão corresponderá a estes objetos:
 - Objetos de 1 MB ou menores no bucket bank-records para o tenant Bank of ABC.
 - Objetos em qualquer outro bucket que tenha o S3 Object Lock ativado para todas as outras contas de locatário.

Ative a política

Quando você estiver completamente satisfeito de que a nova política protege os dados do objeto conforme o esperado, você pode ativá-la.

Como o ciclo de vida do bucket S3 e a política ILM interagem no StorageGRID

Dependendo da sua configuração de ciclo de vida, os objetos seguem as configurações de retenção do ciclo de vida do bucket S3 ou de uma política ILM.

Exemplo de ciclo de vida do bucket tendo prioridade sobre a política ILM

Política ILM

- Regra baseada em referência a um período anterior ao atual: no dia 0, mantenha X cópias por 20 dias
- Regra baseada na referência de tempo de ingestão (padrão): no dia 0, mantenha X cópias por 50 dias

Ciclo de vida do bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Resultado

- Um objeto chamado "docs/text" é ingerido. Ele corresponde ao filtro de ciclo de vida do bucket com o prefixo "docs/".
 - Após 100 dias, um marcador de exclusão é criado e "docs/text" se torna não atual.
 - Após 5 dias, num total de 105 dias desde a ingestão, "docs/text" é excluída.
 - Após 95 dias, totalizando 200 dias desde a ingest e 100 dias desde a criação do marcador de exclusão, o marcador de exclusão expirado é excluído.
- Um objeto chamado "video/movie" é ingerido. Ele não corresponde ao filtro e usa a política de retenção ILM.
 - Após 50 dias, um marcador de exclusão é criado e "video/movie" se torna não atual.
 - Após 20 dias, totalizando 70 dias desde a ingestão, "vídeo/filme" é excluído.
 - Após 30 dias, totalizando 100 dias desde a ingest e 50 dias desde a criação do marcador de

exclusão, o marcador de exclusão expirado é excluído.

Exemplo de ciclo de vida de bucket que implicitamente mantém para sempre

Política ILM

- Regra baseada em referência a um período anterior ao atual: no dia 0, mantenha X cópias por 20 dias
- Regra baseada na referência de tempo de ingestão (padrão): no dia 0, mantenha X cópias por 50 dias

Ciclo de vida do bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker": true}
```

Resultado

- Um objeto chamado "docs/text" é ingerido. Ele corresponde ao filtro de ciclo de vida do bucket com o prefixo "docs/".

A `Expiration`ação se aplica apenas a marcadores de exclusão expirados, o que implica manter todo o resto para sempre (começando com "docs/").

Os marcadores de exclusão que começam com "docs/" são removidos quando expiram.

- Um objeto chamado "video/movie" é ingerido. Ele não corresponde ao filtro e usa a política de retenção ILM.
 - Após 50 dias, um marcador de exclusão é criado e "video/movie" se torna não atual.
 - Após 20 dias, totalizando 70 dias desde a ingestão, "vídeo/filme" é excluído.
 - Após 30 dias, totalizando 100 dias desde a ingest e 50 dias desde a criação do marcador de exclusão, o marcador de exclusão expirado é excluído.

Exemplo de uso do ciclo de vida do bucket para duplicar o ILM e limpar marcadores de exclusão expirados

Política ILM

- Regra baseada em referência a um período anterior ao atual: no dia 0, mantenha X cópias por 20 dias
- Regra baseada na referência de tempo de ingestão (padrão): no Dia 0, mantenha X cópias para sempre

Ciclo de vida do bucket

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Resultado

- A política ILM é duplicada no ciclo de vida do bucket.
 - A regra "para sempre" da política de ILM foi projetada para remover objetos manualmente e limpar versões não atuais após 20 dias. Consequentemente, a regra de ingestão manterá os marcadores de exclusão expirados para sempre.
 - O ciclo de vida do bucket duplica o comportamento da política ILM
"ExpiredObjectDeleteMarker": true, que remove marcadores de exclusão assim que expiram
- Um objeto é ingerido. A ausência de filtro significa que o ciclo de vida do bucket se aplica a todos os objetos e substitui as configurações de retenção do ILM.

- Quando um locatário emite uma solicitação de exclusão de objeto, um marcador de exclusão é criado e o objeto se torna não atual.
- Após 20 dias, o objeto não atual é excluído e o marcador de exclusão se torna expirado.
- Logo em seguida, o marcador de exclusão expirado é excluído.

Reforço do sistema para StorageGRID

Saiba mais sobre a proteção do sistema para StorageGRID

O fortalecimento do sistema é o processo de eliminar o máximo possível de riscos de segurança de um sistema StorageGRID.

Ao instalar e configurar StorageGRID, use estas diretrizes para ajudar você a atender a quaisquer objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade.

Você já deve estar utilizando as melhores práticas padrão do setor para reforçar a segurança do sistema. Por exemplo, você usa senhas fortes para StorageGRID, usa HTTPS em vez de HTTP e habilita autenticação baseada em certificado sempre que disponível. Essas melhores práticas devem incluir segurança física e ambiental que limite o acesso físico, além de proteger o data center e a infraestrutura de suporte. Você também deve consultar todas as normas e recomendações regulamentares aplicáveis ao seu negócio e localização.

StorageGRID segue o "[NetApp Política de Gestão de Vulnerabilidades](#)". As vulnerabilidades relatadas são verificadas e tratadas de acordo com o processo de resposta a incidentes de segurança do produto.

Ao reforçar a segurança de um sistema StorageGRID, considere o seguinte:

- **Qual das três redes StorageGRID** você implementou. Todos os sistemas StorageGRID devem usar a Grid Network, mas você também pode estar usando a Admin Network, a Client Network ou ambas. Cada rede possui considerações de segurança diferentes.
- **O tipo de plataforma** que você usa para os nós individuais do seu sistema StorageGRID. Os nós do StorageGRID podem ser implementados em máquinas virtuais VMware, em um mecanismo de contêiner em hosts Linux ou como appliances de hardware dedicados. Cada tipo de plataforma tem seu próprio conjunto de práticas recomendadas de hardening.
- **Qual o nível de confiabilidade das contas dos tenants.** Se você é um provedor de serviços com contas de tenants não confiáveis, suas preocupações com segurança serão diferentes das que teria se utilizasse apenas tenants internos e confiáveis.
- **Quais requisitos e convenções de segurança** sua organização segue. Pode ser necessário cumprir requisitos regulamentares ou corporativos específicos.

Diretrizes de reforço para upgrades de software do StorageGRID

Você deve manter seu sistema StorageGRID e serviços relacionados atualizados para se defender contra ataques.

Atualizações do software StorageGRID

Sempre que possível, você deve atualizar o software StorageGRID para a versão principal mais recente ou para a versão principal anterior. Manter o StorageGRID atualizado ajuda a reduzir o tempo em que vulnerabilidades conhecidas ficam ativas e diminui a superfície geral de ataque. Além disso, as versões mais

recentes do StorageGRID geralmente contêm recursos de reforço de segurança que não estão incluídos em versões anteriores.

Consulte o "[NetApp Ferramenta de Matriz de Interoperabilidade](#)" (IMT) para determinar qual versão do software StorageGRID você deve usar. Quando um hotfix for necessário, a NetApp prioriza criar atualizações para as versões mais recentes. Alguns patches podem não ser compatíveis com versões anteriores.

- Para baixar as versões e hotfixes mais recentes do StorageGRID, acesse "[Downloads do NetApp: StorageGRID](#)".
- Para atualizar o software StorageGRID, consulte o "[instruções de atualização](#)".
- Para aplicar um hotfix, consulte o "[Procedimento de hotfix do StorageGRID](#)".

Atualizações para serviços externos

Serviços externos podem apresentar vulnerabilidades que afetam StorageGRID indiretamente. Certifique-se de que os serviços dos quais o StorageGRID depende estejam sempre atualizados. Esses serviços incluem LDAP, KMS (ou servidor KMIP), DNS e NTP.

Para obter uma lista das versões suportadas, consulte o "[NetApp Ferramenta de Matriz de Interoperabilidade](#)".

Atualizações para hipervisores

Se seus nós StorageGRID estiverem sendo executados no VMware ou em outro hipervisor, você deve garantir que o software do hipervisor e o firmware estejam atualizados.

Para obter uma lista das versões suportadas, consulte o "[NetApp Ferramenta de Matriz de Interoperabilidade](#)".

Atualizações para nós Linux

Se os seus nós StorageGRID estiverem usando plataformas host Linux, você deve garantir que as atualizações de segurança e as atualizações do kernel sejam aplicadas ao sistema operacional host. Além disso, você deve aplicar as atualizações de firmware ao hardware vulnerável assim que essas atualizações estiverem disponíveis.

Para obter uma lista das versões suportadas, consulte o "[NetApp Ferramenta de Matriz de Interoperabilidade](#)".

Diretrizes de reforço para redes StorageGRID

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

Para obter informações detalhadas sobre as redes StorageGRID, consulte o "[Tipos de rede StorageGRID](#)".

Diretrizes para rede de grid

Você deve configurar uma Grid Network para todo o tráfego interno do StorageGRID. Todos os nós do grid estão na Grid Network e devem ser capazes de se comunicar com todos os outros nós.

Ao configurar a Grid Network, siga estas diretrizes:

- Garanta que a rede esteja protegida contra clientes não confiáveis, como aqueles na internet aberta.

- Sempre que possível, utilize a Grid Network exclusivamente para tráfego interno. Tanto a Admin Network quanto a Client Network possuem restrições adicionais de firewall que bloqueiam o tráfego externo para serviços internos. O uso da Grid Network para tráfego externo de cliente é suportado, mas essa utilização oferece menos camadas de proteção.
- Se a implementação do StorageGRID abranger vários centros de dados, use uma rede privada virtual (VPN) ou equivalente na Grid Network para fornecer proteção adicional ao tráfego interno.
- Alguns procedimentos de manutenção exigem acesso secure shell (SSH) na porta 22 entre o nó de administração principal e todos os outros nós da grade. Use um firewall externo para restringir o acesso SSH a clientes confiáveis.

Diretrizes para a Rede de Administração

A Rede Administrativa é normalmente usada para tarefas administrativas (funcionários de confiança que utilizam o Grid Manager ou SSH) e para comunicação com outros serviços confiáveis, como LDAP, DNS, NTP ou KMS (ou servidor KMIP). No entanto, StorageGRID não impõe esse uso internamente.

Se você estiver usando a Admin Network, siga estas orientações:

- Bloqueie todas as portas de tráfego interno na Rede Administrativa. Consulte o ["lista de portas internas"](#).
- Caso clientes não confiáveis consigam acessar a Admin Network, bloqueie o acesso ao StorageGRID na Admin Network com um firewall externo.

Diretrizes para a rede de cliente

A Rede de Clientes é normalmente usada por locatários e para comunicação com serviços externos, como o serviço de replicação CloudMirror ou outro serviço de plataforma. No entanto, StorageGRID não impõe esse uso internamente.

Se você estiver usando a Client Network, siga estas orientações:

- Bloqueie todas as portas de tráfego interno na rede do cliente. Consulte o ["lista de portas internas"](#).
- Aceite o tráfego de entrada do cliente somente em endpoints explicitamente configurados. Veja as informações sobre ["gerenciando controles de firewall"](#).

Diretrizes de reforço para nós do StorageGRID

Os nós do StorageGRID podem ser implementados em máquinas virtuais VMware, dentro de um mecanismo de contêiner em hosts Linux ou como dispositivos de hardware dedicados. Cada tipo de plataforma e cada tipo de nó possui seu próprio conjunto de práticas recomendadas de segurança.

Controlar o acesso IPMI remoto ao BMC

Você pode habilitar ou desabilitar o acesso IPMI remoto para todos os appliances que contêm um BMC. A interface IPMI remota permite o acesso de baixo nível ao hardware dos seus appliances StorageGRID por qualquer pessoa com uma conta e senha do BMC. Se você não precisar de acesso IPMI remoto ao BMC, desabilite esta opção.

- Para controlar o acesso IPMI remoto ao BMC no Grid Manager, acesse **Configuração > Segurança > Configurações de segurança > Dispositivos**:
 - Desmarque a caixa de seleção **Ativar acesso IPMI remoto** para desativar o acesso IPMI ao BMC.

- Selecione a caixa de seleção **Habilitar acesso IPMI remoto** para habilitar o acesso IPMI ao BMC.

Para obter informações adicionais sobre o reforço da segurança do BMC, consulte a ["Reforce os Baseboard Management Controllers"](#) ficha informativa de cibersegurança da ["National Security Agency \(NSA\)"](#) e ["Agência de Segurança Cibernética e de Infraestrutura \(CISA\)"](#).

Configuração do firewall

Como parte do processo de reforço da segurança do sistema, você deve revisar as configurações do firewall externo e modificá-las para que o tráfego seja aceito somente dos endereços IP e nas portas de onde for estritamente necessário.

StorageGRID inclui um firewall interno em cada nó que aumenta a segurança da sua grid, permitindo que você controle o acesso à rede do nó. Você deve ["gerenciar controles de firewall internos"](#) para impedir o acesso à rede em todas as portas, exceto aquelas necessárias para a sua implementação específica da grid. As alterações de configuração que você faz na página de controle do firewall são aplicadas a cada nó.

Especificamente, você pode gerenciar estas áreas:

- **Endereços privilegiados:** Você pode permitir que endereços IP ou sub-redes selecionados acessem portas que estão fechadas pelas configurações na guia Gerenciar acesso externo.
- **Gerenciar acesso externo:** Você pode fechar portas que estão abertas por padrão ou reabrir portas que foram fechadas anteriormente.
- **Rede de Cliente Não Confiável:** Você pode especificar se um nó confia no tráfego de entrada da Rede de Cliente, bem como as portas adicionais que deseja abrir quando a Rede de Cliente Não Confiável estiver configurada.

Embora esse firewall interno forneça uma camada adicional de proteção contra algumas ameaças comuns, ele não elimina a necessidade de um firewall externo.

Para obter uma lista de todas as portas internas e externas usadas pelo StorageGRID, consulte ["Portas internas do StorageGRID"](#) e ["Portas usadas para comunicações externas"](#).

Desativar serviços não utilizados

Para todos os nós do StorageGRID, você deve desabilitar ou bloquear o acesso a serviços não utilizados. Por exemplo, se você não pretende usar DHCP, utilize o Grid Manager para fechar a porta 68. Selecione **Configuração > Controle de firewall > Gerenciar acesso externo**. Em seguida, altere o status da porta 68 de **Aberta** para **Fechada**.

Virtualização, contêineres e hardware compartilhado

Para todos os nós do StorageGRID, evite executar o StorageGRID no mesmo hardware físico que softwares não confiáveis. Não presuma que as proteções do hipervisor impedirão que malwares acessem dados protegidos pelo StorageGRID se tanto o StorageGRID quanto o malware estiverem no mesmo hardware físico. Por exemplo, os ataques Meltdown e Spectre exploram vulnerabilidades críticas em processadores modernos e permitem que programas roubem dados da memória no mesmo computador.

Proteja os nós durante a instalação

Não permita que usuários não confiáveis acessem os nós do StorageGRID pela rede durante a instalação. Os nós só estarão totalmente seguros após serem integrados à grid.

Limite o acesso físico ao hardware

Você deve limitar o acesso físico aos nós de hardware do StorageGRID, bem como aos hosts de máquinas virtuais VMware e hosts Linux que executam StorageGRID, somente a administradores autorizados. Alguns exemplos de controles de acesso físico incluem fechaduras, guardas, barreiras físicas e videovigilância.

Os nós de hardware appliance são projetados para serem instalados e operados somente por administradores autorizados. Não permita que administradores não autorizados acessem os nós de hardware appliance.

Diretrizes para Admin Nodes

Os nós administrativos fornecem serviços de gerenciamento, como configuração do sistema, monitoramento e registro de logs. Ao fazer login no Grid Manager ou no Tenant Manager, você está se conectando a um nó administrativo.

Siga estas diretrizes para proteger os nós de administração em seu sistema StorageGRID:

- Proteja todos os nós administrativos contra clientes não confiáveis, como aqueles na internet aberta. Garanta que nenhum cliente não confiável possa acessar qualquer nó administrativo na Grid Network, na Admin Network ou na Client Network.
- Os Grupos do StorageGRID controlam o acesso aos recursos do Grid Manager e do Tenant Manager. Conceda a cada grupo de usuários as permissões mínimas necessárias para sua função e use o modo de acesso somente leitura para impedir que os usuários alterem a configuração.
- Ao usar os endpoints do balanceador de carga StorageGRID, utilize nós de gateway em vez de nós de administração para o tráfego de clientes não confiáveis.
- Se você tiver inquilinos não confiáveis, não permita que eles tenham acesso direto ao Tenant Manager ou à Tenant Management API. Em vez disso, oriente esses inquilinos a usar um portal de inquilinos ou um sistema externo de gerenciamento de inquilinos que interaja com a Tenant Management API.
- Opcionalmente, utilize um proxy administrativo para ter mais controle sobre a comunicação do AutoSupport dos nós administrativos com o suporte da NetApp. Veja as etapas para ["Criando um proxy de administrador"](#).
- Opcionalmente, utilize as portas restritas 8443 e 9443 para separar as comunicações do Grid Manager e do Tenant Manager. Bloqueie a porta compartilhada 443 e limite as solicitações dos tenants à porta 9443 para proteção adicional.
- Opcionalmente, utilize nós de administração separados para administradores da grid e usuários locatários.

Para obter mais informações, consulte as instruções para ["Administrando StorageGRID"](#).

Diretrizes para nós de armazenamento

Os nós de armazenamento gerenciam e armazenam dados de objetos e metadados. Siga estas diretrizes para proteger os nós de armazenamento em seu sistema StorageGRID.

- Não permita que clientes não confiáveis se conectem diretamente aos Storage Nodes. Use um endpoint de balanceador de carga fornecido por um Gateway Node ou por um balanceador de carga de terceiro.
- Não habilite serviços de saída para locatários não confiáveis. Por exemplo, ao criar a conta para um locatário não confiável, não permita que ele use sua própria fonte de identidade nem permita o uso de serviços da plataforma. Consulte as etapas para ["criando uma conta de tenant"](#).
- Use um balanceador de carga de terceiros para tráfego de clientes não confiáveis. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques.

- Opcionalmente, utilize um proxy de armazenamento para obter mais controle sobre os Cloud Storage Pools e a comunicação dos serviços da plataforma dos Nós de Armazenamento com serviços externos. Veja as etapas para ["Criando um proxy de armazenamento"](#).
- Opcionalmente, conecte-se a serviços externos usando a Client Network. Em seguida, selecione **Configuration > Security > Firewall control > Untrusted Client Networks** e indique que a Client Network no Storage Node não é confiável. O Storage Node não aceita mais nenhum tráfego de entrada na Client Network, mas continua permitindo solicitações de saída para Platform Services.

Diretrizes para nós de gateway

Os nós de gateway fornecem uma interface de balanceamento de carga opcional que os aplicativos cliente podem usar para se conectar ao StorageGRID. Siga estas diretrizes para proteger quaisquer nós de gateway em seu sistema StorageGRID:

- Configure e use os endpoints do balanceador de carga. Consulte ["Considerações sobre balanceamento de carga"](#).
- Use um balanceador de carga de terceiro entre o cliente e o Gateway Node ou os Storage Nodes para tráfego de clientes não confiáveis. O balanceamento de carga de terceiro oferece mais controle e camadas adicionais de proteção contra ataques. Se você usar um balanceador de carga de terceiro, o tráfego de rede ainda pode ser configurado opcionalmente para passar por um endpoint de balanceador de carga interno ou ser enviado diretamente para os Storage Nodes.
- Se você estiver usando endpoints de balanceamento de carga, opcionalmente permita que os clientes se conectem pela Client Network. Em seguida, selecione **Configuração > Segurança > Controle de firewall > Untrusted Client Networks** e indique que a Client Network no Gateway Node não é confiável. O Gateway Node aceita tráfego de entrada apenas nas portas explicitamente configuradas como endpoints de balanceamento de carga.

Diretrizes para nós de appliance de hardware

Os dispositivos de hardware StorageGRID são projetados especificamente para uso em um sistema StorageGRID. Alguns dispositivos podem ser usados como Storage Nodes. Outros dispositivos podem ser usados como Admin Nodes ou Gateway Nodes. Você pode combinar nós de dispositivo com nós baseados em software ou implantar grids totalmente projetados, compostos exclusivamente por dispositivos.

Siga estas diretrizes para proteger quaisquer nós de hardware em seu sistema StorageGRID:

- Se o dispositivo usar SANtricity System Manager para gerenciamento do controlador de armazenamento, impeça que clientes não confiáveis acessem SANtricity System Manager pela rede.
- Se o appliance tiver um controlador de gerenciamento de placa-mãe (BMC), esteja ciente de que a porta de gerenciamento do BMC permite acesso de baixo nível ao hardware. Conecte a porta de gerenciamento do BMC somente a uma rede de gerenciamento interna segura e confiável.

Você pode estabelecer uma VLAN para isolar as conexões de rede do BMC e restringir o acesso do BMC à internet a redes confiáveis. Para obter informações adicionais sobre como impor a separação de VLANs, consulte a ["Reforce os Baseboard Management Controllers"](#) ficha informativa de segurança cibernética da ["National Security Agency \(NSA\)"](#) e ["Agência de Segurança Cibernética e de Infraestrutura \(CISA\)"](#).

Caso não haja uma rede de gerenciamento interna segura e confiável disponível, deixe a porta de gerenciamento do BMC desconectada ou bloqueada. O suporte técnico pode solicitar acesso temporário durante um chamado de suporte.

- Se o dispositivo suportar o gerenciamento remoto do hardware do controlador via Ethernet usando o padrão Intelligent Platform Management Interface (IPMI), bloqueie o tráfego não confiável na porta 623.



Você pode habilitar ou desabilitar o acesso IPMI remoto para todos os appliances que contêm um BMC. A interface IPMI remota permite acesso de baixo nível ao hardware dos seus appliances StorageGRID por qualquer pessoa com uma conta e senha do BMC. Se você não precisa de acesso IPMI remoto ao BMC, desabilite esta opção usando um dos seguintes métodos: + No Grid Manager, acesse **Configuração > Segurança > Configurações de segurança > Appliances** e desmarque a caixa de seleção **Habilitar acesso IPMI remoto**. + Na API de gerenciamento do Grid, use o endpoint privado: PUT /private/bmc.

Você também pode [desativar acesso IPMI remoto](#).

- Para modelos de dispositivos que contenham unidades NL-SAS SED, FDE ou FIPS que você gerencia com o SANtricity System Manager, "[Ative e configure SANtricity Drive Security](#)".
- Para modelos de dispositivos que contenham SSDs NVMe SED ou FIPS gerenciados pelo StorageGRID Appliance Installer e Grid Manager "[Habilitar e configurar a criptografia de unidade do StorageGRID](#)".
- Para dispositivos sem unidades SED, FDE ou FIPS, use um Servidor de Gerenciamento de Chaves (KMS) para "[Habilitar e configurar a criptografia do software StorageGRID](#)".

Informações relacionadas

["Saiba mais sobre segurança de unidades em SANtricity System Manager"](#)

Diretrizes de reforço para TLS e SSH no StorageGRID

Você deve controlar o acesso SSH, substituir os certificados TLS padrão e selecionar a política de segurança apropriada para conexões TLS e SSH.

Diretrizes de reforço para certificados

Você deve substituir os certificados padrão criados durante a instalação por seus próprios certificados personalizados.

Para muitas organizações, o certificado digital autoassinado para acesso à Web do StorageGRID não está em conformidade com suas políticas de segurança da informação. Em sistemas de produção, você deve instalar um certificado digital assinado por uma CA para uso na autenticação do StorageGRID.

Especificamente, você deve usar certificados de servidor personalizados em vez destes certificados padrão:

- **Certificado da interface de gerenciamento:** Usado para proteger o acesso ao Grid Manager, ao Tenant Manager, à Grid Management API e à Tenant Management API.
- **Certificado da API S3:** Usado para proteger o acesso aos nós de armazenamento e nós de gateway, que os aplicativos cliente S3 utilizam para carregar e baixar dados de objetos.

Veja "[Gerenciar certificados de segurança](#)" para obter detalhes e instruções.



StorageGRID gerencia os certificados usados para os endpoints do balanceador de carga separadamente. Para configurar os certificados do balanceador de carga, consulte "[Configurar pontos de extremidade do balanceador de carga](#)".

Ao usar certificados de servidor personalizados, siga estas diretrizes:

- Os certificados devem ter um *subjectAltName* que corresponda às entradas DNS para StorageGRID. Para obter detalhes, consulte a seção 4.2.1.6, "Subject Alternative Name", em "[RFC 5280: Perfil de](#)

Certificado e CRL PKIX".

- Sempre que possível, evite o uso de certificados curinga. Uma exceção a essa diretriz é o certificado para um endpoint virtual hospedado no S3, que exige o uso de um certificado curinga caso os nomes dos buckets não sejam conhecidos antecipadamente.
- Quando for necessário usar curingas em certificados, você deve tomar medidas adicionais para reduzir os riscos. Use um padrão de curinga como `*.s3.example.com`, e não use o sufixo `s3.example.com` para outros aplicativos. Esse padrão também funciona com acesso ao S3 no estilo de caminho, como `dc1-s1.s3.example.com/mybucket`.
- Defina os prazos de expiração dos certificados para valores curtos (por exemplo, 2 meses) e use a API de Gerenciamento de Grid para automatizar a rotação de certificados. Isso é especialmente importante para certificados curinga.

Além disso, os clientes devem usar verificação rigorosa de nome de host ao se comunicarem com StorageGRID.

Diretrizes de reforço para políticas de TLS e SSH

Você pode selecionar uma política de segurança para determinar quais protocolos e cifras são usados para estabelecer conexões TLS seguras com aplicativos cliente e conexões SSH seguras com serviços internos do StorageGRID.

A política de segurança controla como o TLS e o SSH criptografam os dados em trânsito. Como prática recomendada, você deve desativar as opções de criptografia que não são necessárias para a compatibilidade do aplicativo. Use a política Modern padrão, a menos que seu sistema precise estar em conformidade com Common Criteria, FIPS 140-2 ou que você precise usar outras cifras.

Veja "[Gerencie a política de TLS e SSH](#)" para obter detalhes e instruções.

Gerenciar acesso SSH externo

Para aumentar a segurança do sistema, o acesso SSH externo é bloqueado por padrão. Habilite o acesso SSH somente quando você precisar executar tarefas que exijam acesso SSH de entrada, como solução de problemas. Consulte "[Gerenciar acesso SSH externo](#)" para obter detalhes e instruções.

Diretrizes de reforço para logs, senhas e mensagens de auditoria no StorageGRID

Além de seguir as diretrizes de hardening para redes e nós do StorageGRID, você deve seguir as diretrizes de hardening para outras áreas do sistema StorageGRID.

Senha de instalação temporária

Para proteger o sistema StorageGRID durante a instalação, defina uma senha na página de senha temporária do instalador na interface de instalação do StorageGRID ou na API de Instalação. Quando definida, essa senha se aplica a todos os métodos de instalação do StorageGRID, incluindo a interface de usuário, a API de Instalação e o script `configure-storagegrid.py`.

Para obter mais informações, consulte:

- "[Instale StorageGRID em nós baseados em software](#)"
- "[Instale o appliance StorageGRID](#)"

Logs e mensagens de auditoria

Sempre proteja os logs e as mensagens de auditoria do StorageGRID de forma segura. Os logs e as mensagens de auditoria do StorageGRID fornecem informações valiosas do ponto de vista de suporte e disponibilidade do sistema. Além disso, as informações e os detalhes contidos nos logs e nas mensagens de auditoria do StorageGRID geralmente são de natureza sensível.

Configure StorageGRID para enviar eventos de segurança para um servidor syslog externo. Se estiver usando a exportação de syslog, selecione TLS e RELP/TLS para os protocolos de transporte.

Consulte ["Referência de arquivos de log"](#) para obter mais informações sobre os logs do StorageGRID. Consulte ["Mensagens de auditoria"](#) para obter mais informações sobre as mensagens de auditoria do StorageGRID.

NetApp AutoSupport

O recurso AutoSupport do StorageGRID permite que você monitore proativamente a integridade do seu sistema e envie pacotes automaticamente para o site de suporte da NetApp, para a equipe de suporte interna da sua organização ou para um parceiro de suporte. Por padrão, o envio de pacotes AutoSupport para a NetApp é ativado quando o StorageGRID é configurado pela primeira vez.

O recurso AutoSupport pode ser desativado. No entanto, a NetApp recomenda ativá-lo, pois o AutoSupport ajuda a acelerar a identificação e a resolução de problemas caso surja algum no seu sistema StorageGRID.

AutoSupport oferece suporte a HTTPS, HTTP e SMTP como protocolos de transporte. Devido à natureza sensível dos pacotes AutoSupport, a NetApp recomenda fortemente o uso de HTTPS como protocolo de transporte padrão para enviar pacotes AutoSupport para a NetApp.

Compartilhamento de recursos entre origens diferentes (CORS)

Você pode configurar o compartilhamento de recursos entre origens (CORS) para um bucket do S3 se você quiser que esse bucket e os objetos nele sejam acessíveis a aplicativos web em outros domínios. Em geral, não habilite CORS a menos que seja necessário. Se CORS for necessário, restrinja-o a origens confiáveis.

Veja os passos para ["configurando CORS para buckets e objetos"](#).

Dispositivos de segurança externos

Uma solução completa de hardening deve abordar mecanismos de segurança externos ao StorageGRID. Usar dispositivos de infraestrutura adicionais para filtrar e limitar o acesso ao StorageGRID é uma maneira eficaz de estabelecer e manter uma postura de segurança rigorosa. Esses dispositivos de segurança externos incluem firewalls, sistemas de prevenção de intrusões (IPS) e outros dispositivos de segurança.

Recomenda-se o uso de um balanceador de carga de terceiro para tráfego de clientes não confiáveis. O balanceamento de carga de terceiro oferece mais controle e camadas adicionais de proteção contra ataques.

Mitigação de ransomware

Ajude a proteger os dados dos seus objetos contra ataques de ransomware seguindo as recomendações em ["Defesa contra ransomware com StorageGRID"](#).

StorageGRID com FabricPool

Fluxo de trabalho de configuração para usar StorageGRID com FabricPool

Se você usa o software NetApp ONTAP, pode usar o NetApp FabricPool para transferir dados inativos para um sistema de storage de objetos NetApp StorageGRID.

Use estas instruções para:

- Aprenda as considerações e as melhores práticas para configurar StorageGRID para uma carga de trabalho FabricPool.
- Saiba como configurar um sistema de storage de objetos StorageGRID para uso com FabricPool.
- Aprenda como fornecer os valores necessários ao ONTAP ao conectar StorageGRID como uma camada de nuvem FabricPool.

Guia rápido para configurar StorageGRID para FabricPool

1

Planeje sua configuração

- Decida qual política de hierarquização de volumes do FabricPool você usará para transferir dados inativos do ONTAP para o StorageGRID.
- Planeje e instale um sistema StorageGRID para atender às suas necessidades de capacidade de storage e desempenho.
- Familiarize-se com o software do sistema StorageGRID, incluindo o ["Grid Manager"](#) e o ["Tenant Manager"](#).
- Analise as melhores práticas do FabricPool para ["Grupos HA"](#), ["balanceamento de carga"](#), ["ILM"](#) e ["mais"](#).
- Consulte estes recursos adicionais, que fornecem detalhes sobre como usar e configurar ONTAP e FabricPool:

["TR-4598: FabricPool Melhores Práticas em ONTAP"](#)

["Documentação ONTAP para FabricPool"](#)

2

Executar tarefas pré-requisito

Obtenha o ["Informações necessárias para conectar StorageGRID como uma camada de nuvem"](#), incluindo:

- Endereços IP
- Nomes de domínio
- Certificado SSL

Opcionalmente, configure ["federação de identidade"](#) e ["autenticação única"](#).

3

Configurar as configurações do StorageGRID

Utilize StorageGRID para obter os valores que o ONTAP precisa para se conectar à grid.

Utilizar o ["FabricPool assistente de instalação"](#) é a forma recomendada e mais rápida de configurar todos os itens, mas você também pode configurar cada entidade manualmente, se necessário.

4

Configurar ONTAP e DNS

Use ONTAP para ["adicionar uma camada de nuvem"](#) que utiliza os valores do StorageGRID. Em seguida, ["configurar entradas de DNS"](#) associe endereços IP a quaisquer nomes de domínio que você planeja usar.

5

Monitorar e gerenciar

Quando seu sistema estiver em funcionamento, execute tarefas contínuas no ONTAP e StorageGRID para gerenciar e monitorar o tiering de dados do FabricPool ao longo do tempo.

O que é FabricPool?

FabricPool é uma solução de storage híbrido ONTAP que utiliza um agregado flash de alto desempenho como camada de performance e um armazenamento de objetos como camada de nuvem. Usar agregados habilitados para FabricPool ajuda você a reduzir o custo de storage sem comprometer o desempenho, a eficiência ou a proteção.

FabricPool associa uma camada de nuvem (um armazenamento de objetos externo, como StorageGRID) a uma camada local (um agregado de armazenamento ONTAP) para criar uma coleção composta de discos. Os volumes dentro da FabricPool podem então aproveitar o tiering, mantendo os dados ativos (quentes) no storage de alto desempenho (a camada local) e transferindo os dados inativos (frios) para o armazenamento de objetos externo (a camada de nuvem).

Não são necessárias alterações arquitetônicas e você pode continuar gerenciando seus dados e ambiente de aplicativos a partir do sistema de storage ONTAP.

O que é StorageGRID?

NetApp StorageGRID é uma arquitetura de storage que gerencia dados como objetos, ao contrário de outras arquiteturas de storage, como storage de arquivos ou blocos. Os objetos são mantidos dentro de um único contêiner (como um bucket) e não são aninhados como arquivos dentro de um diretório dentro de outros diretórios. Embora o storage de objetos geralmente ofereça desempenho inferior ao storage de arquivos ou blocos, ele é significativamente mais escalável. Os buckets do StorageGRID podem armazenar petabytes de dados e bilhões de objetos.

Por que usar StorageGRID como camada de nuvem FabricPool?

FabricPool pode distribuir dados ONTAP em camadas para diversos provedores de storage de objetos, incluindo StorageGRID. Ao contrário das nuvens públicas, que podem definir um número máximo de operações de entrada/saída por segundo (IOPS) suportadas no nível do bucket ou do contêiner, o desempenho do StorageGRID escala com o número de nós em um sistema. Usar StorageGRID como uma camada de nuvem FabricPool permite que você mantenha seus dados frios em sua própria nuvem privada para obter o máximo desempenho e controle total sobre seus dados.

Além disso, uma licença FabricPool não é necessária quando você usa StorageGRID como camada de nuvem.

Informações necessárias para conectar StorageGRID como uma camada de nuvem FabricPool

Antes de poder conectar StorageGRID como uma camada de nuvem para o FabricPool, você deve executar etapas de configuração no StorageGRID e obter determinados

valores para uso no ONTAP.

Quais valores você precisa?

A tabela a seguir mostra os valores que você deve configurar no StorageGRID e como esses valores são usados pelo ONTAP e pelo servidor DNS.

Valor	Onde o valor é configurado	Onde o valor é usado
Endereços IP virtuais (VIP)	StorageGRID > Grupo HA	Entrada DNS
Porta	StorageGRID > Ponto final do balanceador de carga	ONTAP System Manager > Adicionar camada de nuvem
Certificado SSL	StorageGRID > Ponto final do balanceador de carga	ONTAP System Manager > Adicionar camada de nuvem
Nome do servidor (FQDN)	StorageGRID > Ponto final do balanceador de carga	Entrada DNS
ID da chave de acesso e chave de acesso secreta	StorageGRID > Locatário e bucket	ONTAP System Manager > Adicionar camada de nuvem
Nome do bucket/container	StorageGRID > Locatário e bucket	ONTAP System Manager > Adicionar camada de nuvem

Como obtenho esses valores?

Dependendo das suas necessidades, você pode fazer o seguinte para obter as informações de que precisa:

- Utilize ["FabricPool assistente de instalação"](#). O assistente de instalação do FabricPool ajuda você a configurar rapidamente os valores necessários no StorageGRID e gera um arquivo que você pode usar para configurar o ONTAP System Manager. O assistente orienta você pelas etapas necessárias e ajuda a garantir que suas configurações estejam em conformidade com as melhores práticas do StorageGRID e do FabricPool.
- Configure cada item manualmente. Em seguida, insira os valores no ONTAP System Manager ou na ONTAP CLI. Siga estas etapas:
 - a. ["Configure um grupo de alta disponibilidade \(HA\) para FabricPool"](#).
 - b. ["Crie um ponto de extremidade de balanceamento de carga para FabricPool"](#).
 - c. ["Crie uma conta de locatário para FabricPool"](#).
 - d. Faça login na conta do inquilino e ["Crie o bucket e as chaves de acesso para o usuário raiz"](#).
 - e. Crie uma regra ILM para FabricPool data e adicione-a às suas políticas ILM ativas. Consulte ["Configurar o ILM para dados do FabricPool"](#).
 - f. Opcionalmente, ["crie uma política de classificação de tráfego para FabricPool"](#).

Use o assistente de instalação do FabricPool

Saiba mais sobre o assistente de instalação do StorageGRID FabricPool

Você pode usar o assistente de instalação do FabricPool para configurar o StorageGRID como o storage de objetos para uma camada de nuvem FabricPool. Após concluir o assistente de instalação, você pode inserir os detalhes necessários no ONTAP System Manager.

Quando usar o assistente de instalação FabricPool

O assistente de instalação do FabricPool guia você por cada etapa da configuração do StorageGRID para uso com o FabricPool e configura automaticamente determinadas entidades para você, como as políticas de ILM e de classificação de tráfego. Como parte da conclusão do assistente, você faz o download de um arquivo que pode ser usado para inserir valores no ONTAP System Manager. Use o assistente para configurar seu sistema mais rapidamente e para garantir que suas configurações estejam em conformidade com as melhores práticas do StorageGRID e do FabricPool.

Supondo que você tenha permissão de acesso à raiz, você pode concluir o assistente de instalação do FabricPool ao começar a usar o StorageGRID Grid Manager, ou pode acessá-lo e concluí-lo posteriormente. Dependendo dos seus requisitos, você também pode configurar alguns ou todos os itens necessários manualmente e, em seguida, usar o assistente para reunir os valores que ONTAP precisa em um único arquivo.



Utilize o assistente de instalação do FabricPool, a menos que você saiba que tem requisitos especiais ou que sua implementação exigirá personalização significativa.

Antes de usar o assistente

Confirme se você concluiu essas etapas prévias.

Revisar as melhores práticas

- Você tem uma compreensão geral do ["Informações necessárias para conectar StorageGRID como uma camada de nuvem"](#).
- Você analisou as melhores práticas do FabricPool para:
 - ["Grupos de alta disponibilidade \(HA\)"](#)
 - ["Balanceamento de carga"](#)
 - ["Regras e política do ILM"](#)

Obtenha endereços IP e configure interfaces VLAN

Se você for configurar um grupo de HA, você sabe a quais nós ONTAP se conectará e qual rede StorageGRID será usada. Você também sabe quais valores inserir para o CIDR da sub-rede, endereço IP do gateway e endereços IP virtuais (VIP).

Se você planeja usar uma LAN virtual para segregar o tráfego do FabricPool, você já configurou a interface VLAN. Veja ["Configurar interfaces VLAN"](#).

Configurar a federação de identidades e o SSO (Single Sign-On)

Se você planeja usar federação de identidade ou logon único (SSO) para seu sistema StorageGRID, você habilitou esses recursos. Você também sabe qual grupo federado deve ter acesso à raiz para a conta do tenant que ONTAP usará. Consulte ["Use federação de identidades"](#) e ["Configure o single sign-on \(SSO\)"](#).

Obtenha e configure nomes de domínio

- Você sabe qual domínio totalmente qualificado (FQDN) usar para o StorageGRID. As entradas do servidor DNS mapearão esse FQDN para os endereços IP VIP do grupo de HA que você criar usando o assistente. Consulte ["Configurar servidor DNS"](#).
- Se você planeja usar solicitações no estilo de hospedagem virtual do S3, você tem ["nomes de domínio de endpoint S3 configurados"](#). ONTAP usa URLs no estilo de caminho por padrão, mas é recomendado usar solicitações no estilo de hospedagem virtual.

Analise os requisitos do balanceador de carga e do certificado de segurança

Se você planeja usar o balanceador de carga StorageGRID, já revisou as informações gerais ["Considerações sobre balanceamento de carga"](#). Você já possui os certificados que irá carregar ou os valores necessários para gerar um certificado.

Se você planeja usar um endpoint de balanceador de carga externo (terceiro), você precisa ter o domínio totalmente qualificado (FQDN), a porta e o certificado desse balanceador de carga.

Confirme a configuração do pool de storage ILM

Se você instalou StorageGRID 11.6 ou anterior, já configurou o pool de storage que usará. Em geral, você deve criar um pool de storage para cada site do StorageGRID que usará para armazenar dados do ONTAP.



Este pré-requisito não se aplica se você instalou inicialmente StorageGRID 11.7 ou 11.8. Ao instalar inicialmente qualquer uma dessas versões, os pools de storage são criados automaticamente para cada site.

Relação entre ONTAP e a camada de nuvem StorageGRID

O assistente FabricPool orienta você no processo de criação de um único tier de nuvem StorageGRID que inclui um tenant StorageGRID, um conjunto de chaves de acesso e um bucket StorageGRID. Você pode anexar esse tier de nuvem StorageGRID a um ou mais tiers locais ONTAP.

A prática recomendada geralmente consiste em conectar uma única camada de nuvem a várias camadas locais em um cluster. No entanto, dependendo dos seus requisitos, você pode optar por usar mais de um bucket ou até mesmo mais de um StorageGRID tenant para as camadas locais em um único cluster. O uso de buckets e tenants diferentes permite isolar os dados e o acesso aos dados entre as camadas locais do ONTAP, mas é um pouco mais complexo de configurar e gerenciar.

NetApp não recomenda conectar uma única camada de nuvem a camadas locais em vários clusters.



Para obter as melhores práticas de uso do StorageGRID com NetApp MetroCluster™ e FabricPool Mirror, consulte ["TR-4598: FabricPool Melhores Práticas em ONTAP"](#).

Opcional: use um bucket diferente para cada camada local

Para usar mais de um bucket para as camadas locais em um cluster ONTAP, adicione mais de uma camada de nuvem StorageGRID no ONTAP. Cada camada de nuvem compartilha o mesmo grupo de HA, endpoint do balanceador de carga, tenant e chaves de acesso, mas usa um contêiner diferente (bucket StorageGRID). Siga estas etapas gerais:

1. No StorageGRID Grid Manager, conclua o assistente de instalação do FabricPool para o primeiro nível de nuvem.

2. No ONTAP System Manager, adicione uma camada de nuvem e use o arquivo que você baixou do StorageGRID para fornecer os valores necessários.
3. No StorageGRID Tenant Manager, faça login no locatário que foi criado pelo assistente e crie um segundo bucket.
4. Conclua o assistente FabricPool novamente. Selecione o grupo HA existente, o endpoint do balanceador de carga e o tenant. Em seguida, selecione o novo bucket que você criou manualmente. Crie uma nova regra ILM para o novo bucket e ative uma política ILM para incluir essa regra.
5. A partir do ONTAP, adicione uma segunda camada de nuvem, mas forneça o novo nome do bucket.

Opcional: use um locatário e um bucket diferentes para cada camada local

Para usar mais de um tenant e diferentes conjuntos de chaves de acesso para as camadas locais em um cluster ONTAP, adicione mais de uma camada de nuvem StorageGRID no ONTAP. Cada camada de nuvem compartilha o mesmo grupo de HA, o mesmo endpoint do balanceador de carga, mas usa um tenant, chaves de acesso e contêiner (StorageGRID bucket) diferentes. Siga estas etapas gerais:

1. No StorageGRID Grid Manager, conclua o assistente de instalação do FabricPool para o primeiro nível de nuvem.
2. No ONTAP System Manager, adicione uma camada de nuvem e use o arquivo que você baixou do StorageGRID para fornecer os valores necessários.
3. Conclua o assistente FabricPool novamente. Selecione o grupo HA existente e o endpoint do balanceador de carga. Crie um novo tenant e um novo bucket. Crie uma nova regra ILM para o novo bucket e ative uma política ILM para incluir essa regra.
4. A partir do ONTAP, adicione uma segunda camada de nuvem, mas forneça a nova chave de acesso, chave secreta e nome do bucket.

Acesse e conclua o assistente de instalação do StorageGRID FabricPool

Você pode usar o assistente de instalação do FabricPool para configurar o StorageGRID como o storage de objetos para um tier de nuvem do FabricPool.

Antes de começar

- Você revisou as "[Considerações e requisitos](#)" para usar o assistente de instalação do FabricPool.



Se você deseja configurar StorageGRID para uso com qualquer outro aplicativo cliente S3, acesse "[Use o assistente de instalação S3](#)".

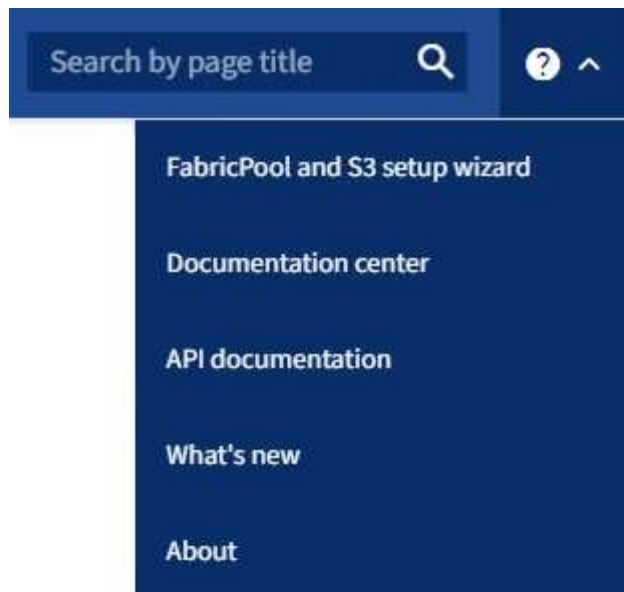
- Você tem o "[Permissão de acesso root](#)".

Acesse o assistente

Você pode concluir o assistente de instalação do FabricPool ao começar a usar o StorageGRID Grid Manager ou pode acessá-lo e concluí-lo posteriormente.

Passos

1. Faça login no Gerenciador de Grade usando um "[navegador web compatível](#)".
2. Se o banner **FabricPool and S3 assistente de instalação** aparecer no painel, selecione o link no banner. Se o banner não aparecer mais, selecione o ícone de ajuda na barra de cabeçalho no Grid Manager e selecione **FabricPool and S3 assistente de instalação**.



3. Na seção FabricPool da página do assistente de instalação FabricPool e S3, selecione **Configurar agora**.

Etapas 1 de 9: Configurar grupo HA aparece.

Etapas 1 de 9: configurar grupo de alta disponibilidade

Um grupo de alta disponibilidade (HA) é uma coleção de nós que cada um contém o serviço StorageGRID Load Balancer. Um grupo HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo de alta disponibilidade (HA) para ajudar a manter as conexões de dados do FabricPool disponíveis. Um grupo HA usa endereços IP virtuais (VIPs) para fornecer acesso de alta disponibilidade ao serviço Load Balancer. Se a interface ativa no grupo HA falhar, uma interface de backup pode gerenciar a carga de trabalho com pouco impacto nas operações do FabricPool.

Para obter detalhes sobre esta tarefa, consulte ["Gerenciar grupos de alta disponibilidade"](#) e ["Melhores práticas para grupos de alta disponibilidade"](#).

Passos

1. Se você planeja usar um balanceador de carga externo, não precisa criar um grupo de alta disponibilidade. Selecione **Ignorar esta etapa** e vá para [Etapa 2 de 9: configurar o endpoint do balanceador de carga](#).
2. Para usar o balanceador de carga StorageGRID, crie um novo grupo HA ou utilize um grupo HA existente.

Criar grupo HA

- Para criar um novo grupo HA, selecione **Criar grupo HA**.
- Na etapa **Inserir detalhes**, preencha os seguintes campos.

Campo	Descrição
Nome do grupo HA	Um nome de exibição exclusivo para este grupo HA.
Descrição (opcional)	A descrição deste grupo HA.

- Na etapa **Adicionar interfaces**, selecione as interfaces de nó que você deseja usar neste grupo de alta disponibilidade.

Use os cabeçalhos das colunas para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

Você pode selecionar um ou mais nós, mas só pode selecionar uma interface para cada nó.

- Na etapa **Priorizar interfaces**, determine a interface principal e quaisquer interfaces de backup para este grupo de alta disponibilidade.

Arraste as linhas para alterar os valores na coluna **Ordem de prioridade**.

A primeira interface da lista é a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.

Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços VIP (IP virtual) são movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP são movidos para a próxima interface de backup e assim por diante. Quando as falhas forem resolvidas, os endereços VIP retornam para a interface disponível de maior prioridade.

- Na etapa **Inserir endereços IP**, preencha os seguintes campos.

Campo	Descrição
CIDR da sub-rede	O endereço da sub-rede VIP na notação CIDR—um endereço IPv4 seguido por 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.
Endereço IP do gateway (opcional)	Opcional. Se os endereços IP do ONTAP usados para acessar o StorageGRID não estiverem na mesma sub-rede que os endereços VIP do StorageGRID, insira o endereço IP do gateway local do StorageGRID VIP. O endereço IP do gateway local deve estar dentro da sub-rede VIP.

Campo	Descrição
Endereço IP virtual	Insira pelo menos um e no máximo dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP e todos estarão ativos ao mesmo tempo na interface ativa. Pelo menos um endereço deve ser IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

f. Selecione **Criar grupo HA** e, em seguida, selecione **Concluir** para retornar ao assistente de instalação do FabricPool.

g. Selecione **Continuar** para ir para a etapa do balanceador de carga.

Usar grupo HA existente

a. Para usar um grupo HA existente, selecione o nome do grupo HA na lista suspensa **Selecionar um grupo HA**.

b. Selecione **Continuar** para ir para a etapa do balanceador de carga.

Etapa 2 de 9: configurar o endpoint do balanceador de carga

StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de aplicativos cliente, como FabricPool. O balanceamento de carga maximiza a velocidade e a capacidade de conexão em vários Storage Nodes.

Você pode usar o serviço StorageGRID Load Balancer, que existe em todos os nós Gateway e Admin, ou pode se conectar a um balanceador de carga externo (de terceiro). Recomenda-se usar o balanceador de carga StorageGRID.

Para obter detalhes sobre esta tarefa, consulte o geral "[Considerações sobre balanceamento de carga](#)" e o "[melhores práticas para balanceamento de carga para FabricPool](#)".

Passos

1. Selecione ou crie um endpoint de balanceador de carga do StorageGRID ou use um balanceador de carga externo.

Criar endpoint

- Selecione **Criar endpoint**.
- Na etapa **Inserir detalhes do endpoint**, preencha os seguintes campos.

Campo	Descrição
Nome	Um nome descritivo para o endpoint.
Porta	A porta do StorageGRID que você deseja usar para balanceamento de carga. Este campo tem como padrão 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada. Se você inserir 80 ou 443, o endpoint será configurado apenas nos nós de Gateway, pois essas portas são reservadas nos nós de Admin. Nota: Portas usadas por outros serviços de grid não são permitidas. Veja o "Referência da porta de rede".
Tipo de cliente	Deve ser S3 .
Protocolo de rede	Selecione HTTPS. Nota: A comunicação com StorageGRID sem criptografia TLS é suportada, mas não recomendada.

- Na etapa **Selecionar modo de vinculação**, especifique o modo de vinculação. O modo de vinculação controla como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

Modo	Descrição
Global (padrão)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer Gateway Node ou Admin Node, o endereço IP virtual (VIP) de qualquer grupo HA em qualquer rede ou um FQDN correspondente. Use a configuração Global (padrão), a menos que precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este endpoint. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA que você selecionar para os endpoints não se sobreponham.
Interfaces de nó	Os clientes devem usar os endereços IP (ou os FQDNs correspondentes) das interfaces de nó selecionadas para acessar este endpoint.

Modo	Descrição
Tipo de nó	Dependendo do tipo de nó que você selecionar, os clientes devem usar o endereço IP (ou o FQDN correspondente) de qualquer Nó de Administração ou o endereço IP (ou o FQDN correspondente) de qualquer Nó de Gateway para acessar este endpoint.

d. Na etapa **Acesso do locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de locatário podem usar este endpoint para acessar seus buckets. Permitir todos os locatários é quase sempre a opção apropriada para o endpoint do balanceador de carga usado para FabricPool. Você deve selecionar esta opção se estiver usando o assistente de instalação FabricPool para um novo sistema StorageGRID e ainda não tiver criado nenhuma conta de locatário.
Permitir locatários selecionados	Somente as contas de locatário selecionadas podem usar este endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar este endpoint para acessar seus buckets. Todos os outros locatários podem usar este endpoint.

e. Na etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Fazer upload do certificado (recomendado)	Use esta opção para carregar um certificado de servidor assinado por uma CA, a chave privada do certificado e, opcionalmente, um pacote de CA.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Veja "Configurar pontos de extremidade do balanceador de carga" para detalhes sobre o que inserir.
Use o certificado StorageGRID S3	Esta opção está disponível apenas se você já tiver carregado ou gerado uma versão personalizada do certificado global do StorageGRID. Consulte "Configurar certificados da API S3" para detalhes.

f. Selecione **Concluir** para retornar ao assistente de instalação do FabricPool.

g. Selecione **Continuar** para ir para a etapa de tenant e bucket.



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

Usar o endpoint do balanceador de carga existente

- Selecione o nome de um endpoint existente na lista suspensa **Select a load balancer endpoint**.
- Selecione **Continuar** para ir para a etapa de tenant e bucket.

Use um balanceador de carga externo

- Preencha os seguintes campos para o balanceador de carga externo.

Campo	Descrição
FQDN	O domínio totalmente qualificado (FQDN) do balanceador de carga externo.
Porta	O número da porta que FabricPool usará para se conectar ao balanceador de carga externo.
Certificado	Copie o certificado do servidor para o balanceador de carga externo e cole-o neste campo.

- Selecione **Continuar** para ir para a etapa de tenant e bucket.

Etapa 3 de 9: inquilino e bucket

Um tenant é uma entidade que pode usar aplicativos S3 para armazenar e recuperar objetos no StorageGRID. Cada tenant possui seus próprios usuários, chaves de acesso, buckets, objetos e um conjunto específico de recursos. Você deve criar um tenant do StorageGRID antes de criar o bucket que o FabricPool usará.

Um bucket é um contêiner usado para armazenar os objetos e metadados de um locatário. Embora alguns locatários possam ter vários buckets, o assistente permite que você crie ou selecione apenas um locatário e um bucket por vez. Você pode usar o Tenant Manager posteriormente para adicionar quaisquer buckets adicionais de que precisar.

Você pode criar um novo locatário e bucket para FabricPool ou pode selecionar um locatário e bucket existentes. Se você criar um novo locatário, o sistema cria automaticamente o ID da chave de acesso e a chave de acesso secreta para o usuário raiz do locatário.

Para obter detalhes sobre esta tarefa, consulte ["Crie uma conta de locatário para FabricPool"](#) e ["Crie um bucket S3 e obtenha uma chave de acesso"](#).

Passos

Crie um novo tenant e bucket ou selecione um tenant existente.

Novo tenant e bucket

1. Para criar um novo locatário e bucket, insira um **Nome do locatário**. Por exemplo, `FabricPool tenant`.
2. Defina acesso à raiz para a conta do locatário, com base em se o seu sistema StorageGRID usa ["federação de identidade"](#), ["autenticação única \(SSO\)"](#) ou ambos.

Opção	Faça isso
Se a federação de identidades não estiver ativada	Especifique a senha a ser usada ao fazer login no tenant como usuário raiz.
Se a federação de identidades estiver ativada	a. Selecione um grupo federado existente para ter permissão de acesso à raiz para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no tenant como usuário raiz.
Se a federação de identidades e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter permissão de acesso à raiz para o locatário. Nenhum usuário local pode fazer login.

3. Em **Nome do bucket**, insira o nome do bucket que o FabricPool usará para armazenar os dados do ONTAP. Por exemplo, `fabricpool-bucket`.



Não é possível alterar o nome do bucket depois de criá-lo.

4. Selecione a **Região** para este bucket.

Use a região padrão (`us-east-1`) a menos que você pretenda usar o ILM no futuro para filtrar objetos com base na região do bucket.

5. Selecione **Criar e Continuar** para criar o locatário e o bucket e ir para a etapa de download de dados

Selecione o locatário e o bucket

A conta de locatário existente deve ter pelo menos um bucket que não tenha o versionamento ativado. Você não pode selecionar uma conta de locatário existente se não houver nenhum bucket para esse locatário.

1. Selecione o tenant existente na lista suspensa **Tenant name**.
2. Selecione o bucket existente na lista suspensa **Nome do bucket**.

FabricPool não suporta versionamento de objetos, portanto, os buckets com versionamento ativado não são exibidos.



Não selecione um bucket que tenha o S3 Object Lock ativado para uso com FabricPool.

3. Selecione **Continuar** para ir para a etapa de download de dados.

Etapa 4 de 9: Baixar as configurações do ONTAP

Nesta etapa, você faz o download de um arquivo que pode usar para inserir valores no ONTAP System Manager.

Passos

1. Opcionalmente, selecione o ícone de copiar () para copiar o ID da chave de acesso e a chave de acesso secreta para a área de transferência.

Esses valores estão incluídos no arquivo baixado, mas você pode salvá-los separadamente.

2. Selecione **Baixar configurações do ONTAP** para baixar um arquivo de texto que contém os valores que você inseriu até o momento.

O `ONTAP\_FabricPool\_settings\_bucketname.txt` arquivo inclui as informações necessárias para configurar StorageGRID como o storage de objetos para uma camada de nuvem FabricPool, incluindo:

- Detalhes da conexão do balanceador de carga, incluindo o nome do servidor (FQDN), porta e certificado
- Nome do bucket
- ID da chave de acesso e chave de acesso secreta para o usuário raiz da conta do tenant

3. Salve as chaves copiadas e o arquivo baixado em um local seguro.



Não feche esta página até que você tenha copiado ambas as chaves de acesso, baixado as configurações do ONTAP ou ambos. As chaves não estarão disponíveis após você fechar esta página. Certifique-se de salvar essas informações em um local seguro, pois elas podem ser usadas para obter dados do seu sistema StorageGRID.

4. Selecione a caixa de seleção para confirmar que você baixou ou copiou o ID da chave de acesso e a chave de acesso secreta.
5. Selecione **Continuar** para ir para a etapa do pool de storage ILM.

Etapa 5 de 9: selecione um pool de storage

Um pool de storage é um grupo de Storage Nodes. Ao selecionar um pool de storage, você determina quais nós o StorageGRID usará para armazenar os dados em camadas do ONTAP.

Para obter detalhes sobre esta etapa, consulte "[Crie um pool de storage](#)".

Passos

1. Na lista suspensa **Site**, selecione o site do StorageGRID que você deseja usar para os dados armazenados em camadas a partir do ONTAP.
2. Na lista suspensa **pool de storage**, selecione o pool de storage para esse site.

O pool de storage de um site inclui todos os Storage Nodes desse site.

3. Selecione **Continuar** para ir para a etapa da regra ILM.

Etapa 6 de 9: Revisar a regra ILM para FabricPool

As regras de gerenciamento de ciclo de vida da informação (ILM) controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos no seu sistema StorageGRID.

O assistente de instalação do FabricPool cria automaticamente a regra ILM recomendada para uso do FabricPool. Essa regra se aplica somente ao bucket que você especificou. Ela utiliza codificação de apagamento 2+1 em um único site para armazenar os dados que são transferidos de nível do ONTAP.

Para obter detalhes sobre esta etapa, consulte ["Criar regra ILM"](#) e ["Melhores práticas para usar o ILM com FabricPool data"](#).

Passos

1. Analise os detalhes da regra.

Campo	Descrição
Nome da regra	Gerado automaticamente e não pode ser alterado
Descrição	Gerado automaticamente e não pode ser alterado
Filtro	O nome do bucket Essa regra se aplica somente aos objetos salvos no bucket que você especificou.
Tempo de referência	Tempo de ingestão A instrução de posicionamento começa quando os objetos são salvos inicialmente no bucket.
Instrução de posicionamento	Use codificação de apagamento 2+1

2. Classifique o diagrama de retenção por **Período de tempo** e **pool de storage** para confirmar a instrução de colocação.
 - O **período de tempo** para a regra é **Dia 0 - para sempre**. **Dia 0** significa que a regra é aplicada quando os dados são transferidos em camadas a partir do ONTAP. **Para sempre** significa que o StorageGRID ILM não excluirá dados que foram transferidos em camadas a partir do ONTAP.
 - O **storage pool** para a regra é o storage pool que você selecionou. **EC 2+1** significa que os dados serão armazenados usando codificação de apagamento 2+1. Cada objeto será salvo como dois fragmentos de dados e um fragmento de paridade. Os três fragmentos de cada objeto serão salvos em Storage Nodes diferentes em um único site.
3. Selecione **Criar e Continuar** para criar esta regra e ir para a etapa de política ILM.

Etapa 7 de 9: revisar e ativar a política ILM

Após o assistente de instalação do FabricPool criar a regra ILM para uso do FabricPool, ele cria uma política ILM. Você deve simular e revisar cuidadosamente essa política antes de ativá-la.

Para obter detalhes sobre esta etapa, consulte ["Criar política de ILM"](#) e ["Melhores práticas para usar o ILM com FabricPool data"](#).



Ao ativar uma nova política ILM, StorageGRID usa essa política para gerenciar o posicionamento, a duração e a proteção de dados de todos os objetos na grade, incluindo objetos existentes e objetos recém-ingeridos. Em alguns casos, ativar uma nova política pode fazer com que objetos existentes sejam movidos para novos locais.



Para evitar perda de dados, não utilize uma regra ILM que expire ou exclua dados da camada de nuvem FabricPool. Defina o período de retenção como **permanente** para garantir que os objetos FabricPool não sejam excluídos pelo StorageGRID ILM.

Passos

1. Opcionalmente, atualize o **Nome da política** gerado pelo sistema. Por padrão, o sistema acrescenta "+ FabricPool" ao nome da sua política ativa ou inativa, mas você pode fornecer seu próprio nome.
2. Analise a lista de regras na política inativa.
 - Se sua grade não tiver uma política ILM inativa, o assistente criará uma política inativa clonando sua política ativa e adicionando a nova regra no topo.
 - Se sua grade já tiver uma política ILM inativa e essa política usar as mesmas regras e a mesma ordem que a política ILM ativa, o assistente adiciona a nova regra ao topo da política inativa.
 - Se a sua política inativa contiver regras diferentes ou uma ordem diferente da política ativa, o assistente criará uma nova política inativa clonando a sua política ativa e adicionando a nova regra no topo.
3. Analise a ordem das regras na nova política inativa.

Como a regra FabricPool é a primeira, quaisquer objetos no bucket FabricPool são colocados antes que as outras regras da política sejam avaliadas. Objetos em quaisquer outros buckets são colocados pelas regras subsequentes da política.

4. Analise o diagrama de retenção para aprender como diferentes objetos serão retidos.
 - a. Selecione **expandir tudo** para ver um diagrama de retenção para cada regra na política inativa.
 - b. Selecione **Período** e **pool de storage** para revisar o diagrama de retenção. Confirme que quaisquer regras aplicáveis ao bucket ou locatário FabricPool retêm os objetos **para sempre**.
5. Após revisar a política inativa, selecione **Ativar e continuar** para ativar a política e prosseguir para a etapa de classificação de tráfego.



Erros em uma política ILM podem causar perda de dados irreparável. Revise a política cuidadosamente antes de ativar.

Etapa 8 de 9: criar política de classificação de tráfego

Como opção, o assistente de instalação do FabricPool pode criar uma política de classificação de tráfego que você pode usar para monitorar a carga de trabalho do FabricPool. A política criada pelo sistema usa uma regra de correspondência para identificar todo o tráfego de rede relacionado ao bucket que você criou. Essa política monitora apenas o tráfego; ela não limita o tráfego para o FabricPool ou qualquer outro cliente.

Para obter detalhes sobre esta etapa, consulte ["Crie uma política de classificação de tráfego para FabricPool"](#).

Passos

1. Analise a política.
2. Se você deseja criar essa política de classificação de tráfego, selecione **Criar e continuar**.

Assim que o FabricPool começar a transferir dados para o StorageGRID, você pode acessar a página de Políticas de Classificação de Tráfego para visualizar as métricas de tráfego de rede dessa política. Depois, você também pode adicionar regras para limitar outras cargas de trabalho e garantir que a carga de trabalho do FabricPool tenha a maior parte da largura de banda.

3. Caso contrário, selecione **Ignorar esta etapa**.

Etapa 9 de 9: revisar o resumo

O resumo fornece detalhes sobre os itens que você configurou, incluindo o nome do balanceador de carga, do locatário e do bucket, a política de classificação de tráfego e a política ILM ativa,

Passos

1. Analise o resumo.
2. Selecione **Concluir**.

Próximos passos

Após concluir o assistente FabricPool, execute estas etapas adicionais.

Passos

1. Acesse "[Configurar ONTAP System Manager](#)" para inserir os valores salvos e concluir o lado ONTAP da conexão. Você deve adicionar StorageGRID como uma camada de nuvem, conectar a camada de nuvem a uma camada local para criar um FabricPool e definir as políticas de tiering de volume.
2. Acesse "[Configurar o servidor DNS](#)" e certifique-se de que o DNS inclua um registro para associar o nome do servidor StorageGRID (domínio totalmente qualificado) a cada endereço IP do StorageGRID que você utilizará.
3. Acesse "[Outras práticas recomendadas para StorageGRID e FabricPool](#)" para aprender as melhores práticas para logs de auditoria do StorageGRID e outras opções de configuração global.

Configure StorageGRID manualmente

Crie um grupo de alta disponibilidade (HA) para FabricPool no StorageGRID

Ao configurar StorageGRID para uso com FabricPool, você pode opcionalmente criar um ou mais grupos de alta disponibilidade (HA). Um grupo HA é uma coleção de nós que cada um contém o serviço StorageGRID Load Balancer. Um grupo HA pode conter Gateway Nodes, Admin Nodes ou ambos.

Você pode usar um grupo de alta disponibilidade (HA) para ajudar a manter as conexões de dados do FabricPool disponíveis. Um grupo HA usa endereços IP virtuais (VIPs) para fornecer acesso altamente disponível ao serviço de balanceamento de carga. Se a interface ativa no grupo HA falhar, uma interface de backup pode gerenciar a carga de trabalho com pouco impacto nas operações do FabricPool.

Para obter detalhes sobre esta tarefa, consulte "[Gerenciar grupos de alta disponibilidade](#)". Para usar o assistente de instalação FabricPool para concluir esta tarefa, acesse "[Acesse e conclua o assistente de instalação do FabricPool](#)".

Antes de começar

- Você revisou o "[Melhores práticas para grupos de alta disponibilidade](#)".
- Você está conectado ao Gerenciador de Grade usando um "[navegador web compatível](#)".

- Você tem o ["Permissão de acesso root"](#).
- Se você planeja usar uma VLAN, você criou a interface VLAN. Veja ["Configurar interfaces VLAN"](#).

Passos

1. Selecione **Configuração > Rede > Grupos de alta disponibilidade**.
2. Selecione **Create**.
3. Na etapa **Inserir detalhes**, preencha os seguintes campos.

Campo	Descrição
Nome do grupo HA	Um nome de exibição exclusivo para este grupo HA.
Descrição (opcional)	A descrição deste grupo HA.

4. Na etapa **Adicionar interfaces**, selecione as interfaces de nó que você deseja usar neste grupo de alta disponibilidade.

Use os cabeçalhos das colunas para classificar as linhas ou insira um termo de pesquisa para localizar interfaces mais rapidamente.

Você pode selecionar um ou mais nós, mas só pode selecionar uma interface para cada nó.

5. Na etapa **Priorizar interfaces**, determine a interface principal e quaisquer interfaces de backup para este grupo de alta disponibilidade.

Arraste as linhas para alterar os valores na coluna **Ordem de prioridade**.

A primeira interface da lista é a interface primária. A interface primária é a interface ativa, a menos que ocorra uma falha.

Se o grupo HA incluir mais de uma interface e a interface ativa falhar, os endereços VIP (IP virtual) são movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP são movidos para a próxima interface de backup e assim por diante. Quando as falhas forem resolvidas, os endereços VIP retornam para a interface disponível de maior prioridade.

6. Na etapa **Inserir endereços IP**, preencha os seguintes campos.

Campo	Descrição
CIDR da sub-rede	O endereço da sub-rede VIP na notação CIDR—um endereço IPv4 seguido por 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.
Endereço IP do gateway (opcional)	Opcional. Se os endereços IP do ONTAP usados para acessar o StorageGRID não estiverem na mesma sub-rede que os endereços VIP do StorageGRID, insira o endereço IP do gateway local do StorageGRID VIP. O endereço IP do gateway local deve estar dentro da sub-rede VIP.

Campo	Descrição
Endereço IP virtual	Insira pelo menos um e no máximo dez endereços VIP para a interface ativa no grupo HA. Todos os endereços VIP devem estar dentro da sub-rede VIP. Pelo menos um endereço deve ser IPv4. Opcionalmente, você pode especificar endereços IPv4 e IPv6 adicionais.

7. Selecione **Criar grupo HA** e, em seguida, selecione **Concluir**.

Crie um ponto de extremidade de balanceamento de carga para FabricPool no StorageGRID

StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de aplicativos cliente, como FabricPool. O balanceamento de carga maximiza a velocidade e a capacidade de conexão em vários Storage Nodes.

Ao configurar StorageGRID para uso com FabricPool, você deve configurar um endpoint de balanceador de carga e carregar ou gerar um certificado de endpoint de balanceador de carga, que é usado para proteger a conexão entre ONTAP e StorageGRID.

Para usar o assistente de instalação do FabricPool para concluir esta tarefa, acesse ["Acesse e conclua o assistente de instalação do FabricPool"](#).

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).
- Você revisou o geral ["Considerações sobre balanceamento de carga"](#) assim como o ["melhores práticas para balanceamento de carga para FabricPool"](#).

Passos

1. Selecione **Configuração > Rede > Pontos de extremidade do balanceador de carga**.
2. Selecione **Create**.
3. Na etapa **Inserir detalhes do endpoint**, preencha os seguintes campos.

Campo	Descrição
Nome	Um nome descritivo para o endpoint.

Campo	Descrição
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo tem como padrão 10433 para o primeiro endpoint que você criar, mas você pode inserir qualquer porta externa não utilizada. Se você inserir 80 ou 443, o endpoint será configurado apenas nos nós de Gateway. Essas portas são reservadas nos nós de Administração. Nota: Portas usadas por outros serviços de grid não são permitidas. Veja o "Referência da porta de rede". Você fornecerá esse número ao ONTAP ao conectar StorageGRID como uma camada de nuvem FabricPool.
Tipo de cliente	Selecione S3 .
Protocolo de rede	Selecione HTTPS. Nota: A comunicação com StorageGRID sem criptografia TLS é suportada, mas não recomendada.

4. Na etapa **Selecionar modo de vinculação**, especifique o modo de vinculação. O modo de vinculação controla como o endpoint é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

Modo	Descrição
Global (padrão)	Os clientes podem acessar o endpoint usando o endereço IP de qualquer Gateway Node ou Admin Node, o endereço IP virtual (VIP) de qualquer grupo HA em qualquer rede ou um FQDN correspondente. Use a configuração Global (padrão), a menos que precise restringir a acessibilidade deste endpoint.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este endpoint. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA que você selecionar para os endpoints não se sobreponham.
Interfaces de nó	Os clientes devem usar os endereços IP (ou os FQDNs correspondentes) das interfaces de nó selecionadas para acessar este endpoint.
Tipo de nó	Dependendo do tipo de nó que você selecionar, os clientes devem usar o endereço IP (ou o FQDN correspondente) de qualquer Nó de Administração ou o endereço IP (ou o FQDN correspondente) de qualquer Nó de Gateway para acessar este endpoint.

5. Na etapa **Acesso do locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os locatários (padrão)	Todas as contas de locatário podem usar este endpoint para acessar seus buckets. Permitir todos os locatários é quase sempre a opção apropriada para o endpoint do balanceador de carga usado para FabricPool. Você deve selecionar esta opção se ainda não tiver criado nenhuma conta de locatário.
Permitir locatários selecionados	Somente as contas de locatário selecionadas podem usar este endpoint para acessar seus buckets.
Bloquear locatários selecionados	As contas de locatário selecionadas não podem usar este endpoint para acessar seus buckets. Todos os outros locatários podem usar este endpoint.

6. Na etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Fazer upload do certificado (recomendado)	Use esta opção para carregar um certificado de servidor assinado por uma CA, a chave privada do certificado e, opcionalmente, um pacote de CA.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Veja "Configurar pontos de extremidade do balanceador de carga" para detalhes sobre o que inserir.
Use o certificado StorageGRID S3	Esta opção está disponível apenas se você já tiver carregado ou gerado uma versão personalizada do certificado global do StorageGRID. Consulte "Configurar certificados da API S3" para detalhes.

7. Selecione **Create**.



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

Crie uma conta de locatário para FabricPool no StorageGRID

Você precisa criar uma conta de locatário no Grid Manager para uso do FabricPool.

As contas de locatário permitem que os aplicativos cliente armazenem e recuperem objetos no StorageGRID. Cada conta de locatário possui seu próprio ID de conta, grupos e usuários autorizados, buckets e objetos.

Para obter detalhes sobre esta tarefa, consulte ["Criar conta de locatário"](#). Para usar o assistente de instalação FabricPool para concluir esta tarefa, acesse ["Acesse e conclua o assistente de instalação do FabricPool"](#).

Antes de começar

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

Passos

1. Selecione **Tenants**.
2. Selecione **Create**.
3. Para as etapas Inserir detalhes, insira as seguintes informações.

Campo	Descrição
Nome	Um nome para a conta do locatário. Os nomes dos locatários não precisam ser exclusivos. Quando a conta do locatário é criada, ela recebe um ID de conta numérico exclusivo.
Descrição (opcional)	Uma descrição para ajudar a identificar o tenant.
Tipo de cliente	Deve ser S3 para FabricPool.
Cota de armazenamento (opcional)	Deixe este campo em branco para FabricPool.

4. Para a etapa Selecionar permissões:

- a. Não selecione **Permitir serviços da plataforma**.

FabricPool os inquilinos normalmente não precisam usar serviços de plataforma, como CloudMirror replicação.

- b. Opcionalmente, selecione **Usar sua própria fonte de identidade**.

- c. Não selecione **Permitir S3 Select**.

FabricPool os inquilinos normalmente não precisam usar o S3 Select.

- d. Opcionalmente, selecione **Usar conexão de federação de grid** para permitir que o tenant use uma ["conexão de federação de grid"](#) para clonagem de conta e replicação entre grids. Em seguida, selecione a conexão de federação de grid a ser usada.

5. Na etapa Definir acesso à raiz, especifique qual usuário terá a permissão inicial de acesso à raiz para a conta do locatário, com base em se seu sistema StorageGRID usa ["federação de identidade"](#), ["autenticação única \(SSO\)"](#) ou ambos.

Opção	Faça isso
Se a federação de identidades não estiver ativada	Especifique a senha a ser usada ao fazer login no tenant como usuário raiz.
Se a federação de identidades estiver ativada	a. Selecione um grupo federado existente para ter permissão de acesso à raiz para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no tenant como usuário raiz.

Opção	Faça isso
Se a federação de identidades e o logon único (SSO) estiverem ativados	Selecione um grupo federado existente para ter permissão de acesso à raiz para o locatário. Nenhum usuário local pode fazer login.

6. Selecione **Criar locatário**.

Crie um bucket S3 e obtenha as chaves de acesso para FabricPool no StorageGRID

Antes de usar StorageGRID com uma carga de trabalho FabricPool, você deve criar um bucket S3 para seus dados FabricPool. Você também precisa obter uma chave de acesso e uma chave de acesso secreta para a conta de tenant que você usará para FabricPool.

Para obter detalhes sobre esta tarefa, consulte ["Criar bucket S3"](#) e ["Crie suas próprias chaves de acesso S3"](#). Para usar o assistente de instalação FabricPool para concluir esta tarefa, acesse ["Acesse e conclua o assistente de instalação do FabricPool"](#).

Antes de começar

- Você criou uma conta de locatário para uso do FabricPool.
- Você tem acesso à raiz à conta do locatário.

Passos

1. Faça login no Tenant Manager.

Você pode fazer o seguinte:

- Na página Contas do Locatário no Grid Manager, selecione o link **Sign in** do tenant e insira suas credenciais.
- Digite a URL da conta do tenant em um navegador da web e insira suas credenciais.

2. Crie um bucket S3 para os dados do FabricPool.

Você deve criar um bucket exclusivo para cada cluster ONTAP que planeja usar.

- Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3) > Buckets**.
- Selecione **Create bucket**.
- Insira o nome do bucket do StorageGRID que você deseja usar com FabricPool. Por exemplo, `fabricpool-bucket`.



Não é possível alterar o nome do bucket depois de criá-lo.

d. Selecione a região para este bucket.

Por padrão, todos os buckets são criados na `us-east-1` região. Se a região padrão estiver configurada para uma região diferente de `us-east-1`, essa outra região será selecionada inicialmente na lista suspensa.

e. Selecione **Continue**.

f. Selecione **Create bucket**.



Não selecione **Habilitar versionamento de objetos** para o bucket FabricPool. Da mesma forma, não edite um bucket FabricPool para usar **Disponível** ou uma consistência diferente da padrão. A consistência recomendada para buckets FabricPool é **Leitura após nova gravação**, que é a consistência padrão para um novo bucket.

3. Crie uma chave de acesso e uma chave de acesso secreta.

- a. Selecione **STORAGE (S3) > My access keys**.
- b. Selecione **Criar chave**.
- c. Selecione **Criar chave de acesso**.
- d. Copie o ID da chave de acesso e a chave de acesso secreta para um local seguro ou selecione **Baixar .csv** para salvar um arquivo de planilha contendo o ID da chave de acesso e a chave de acesso secreta.

Você deverá inserir esses valores no ONTAP ao configurar StorageGRID como uma FabricPool cloud tier.



Se você gerar uma nova chave de acesso e uma nova chave de acesso secreta no StorageGRID no futuro, insira as novas chaves no ONTAP antes de excluir os valores antigos do StorageGRID. Caso contrário, o ONTAP pode perder temporariamente o acesso ao StorageGRID.

Configure StorageGRID ILM para dados do FabricPool

Você pode usar este exemplo simples de política como ponto de partida para suas próprias regras e política de ILM.

Este exemplo pressupõe que você esteja projetando as regras ILM e uma política ILM para um sistema StorageGRID com quatro nós de armazenamento em um único data center em Denver, Colorado. Os dados do FabricPool neste exemplo usam um bucket chamado `fabricpool-bucket`.



As regras e a política de ILM a seguir são apenas exemplos. Existem muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar que ela funcionará conforme o esperado para proteger o conteúdo contra perda. Para saber mais, consulte ["Gerencie objetos com ILM"](#).



Para evitar perda de dados, não utilize uma regra ILM que expire ou exclua dados da camada de nuvem FabricPool. Defina o período de retenção como **permanente** para garantir que os objetos FabricPool não sejam excluídos pelo StorageGRID ILM.

Antes de começar

- Você revisou o ["Melhores práticas para usar ILM com FabricPool data"](#).
- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso ILM ou root"](#).
- Se você atualizou para StorageGRID 12.0 a partir de uma versão do StorageGRID anterior à 11.7, você já configurou o pool de storage que vai usar. Em geral, você deve criar um pool de storage para cada site do

StorageGRID que vai usar para armazenar dados. (A partir da versão 11.7, pools de storage são criados automaticamente para cada site.)



Este pré-requisito não se aplica se você instalou inicialmente StorageGRID 11.7 ou 11.8. Ao instalar inicialmente qualquer uma dessas versões, os pools de storage são criados automaticamente para cada site.

Passos

1. Crie uma regra ILM que se aplique somente aos dados em `fabricpool-bucket`. Esta regra de exemplo cria cópias com codificação de apagamento.

Definição de regra	Valor de exemplo
Nome da regra	codificação de apagamento 2 + 1 para dados do FabricPool
Nome do bucket	<code>fabricpool-bucket</code> Você também pode filtrar pela conta do locatário FabricPool.
Filtros avançados	Tamanho do objeto superior a 0,2 MB. Nota: FabricPool grava apenas objetos de 4 MB, mas você precisa adicionar um filtro de tamanho de objeto porque esta regra usa codificação de apagamento.
Tempo de referência	Tempo de ingestão
Período e locais	Desde o primeiro dia, armazene para sempre Armazene objetos por meio de codificação de apagamento usando o esquema EC 2+1 em Denver e retenha esses objetos no StorageGRID para sempre.  Para evitar perda de dados, não utilize uma regra ILM que expire ou exclua dados da camada de nuvem FabricPool.
Comportamento de ingestão	Equilibrado

2. Crie uma regra ILM padrão que criará duas cópias replicadas de quaisquer objetos que não correspondam à primeira regra. Não selecione um filtro básico (conta de tenant ou nome do bucket) nem filtros avançados.

Definição de regra	Valor de exemplo
Nome da regra	Duas cópias replicadas
Nome do bucket	<i>none</i>

Definição de regra	Valor de exemplo
Filtros avançados	<i>none</i>
Tempo de referência	Tempo de ingestão
Período e locais	Desde o primeiro dia, armazene para sempre Armazene objetos replicando 2 cópias em Denver.
Comportamento de ingestão	Equilibrado

3. Crie uma política ILM e selecione as duas regras. Como a regra de replicação não usa nenhum filtro, ela pode ser a regra padrão (última) da política.
4. Ingerir objetos de teste no grid.
5. Simule a política com os objetos de teste para verificar o comportamento.
6. Ative a política.

Quando essa política é ativada, StorageGRID coloca os dados dos objetos da seguinte forma:

- Os dados em camadas do FabricPool `fabricpool-bucket` serão codificados por apagamento usando o esquema de codificação de apagamento 2+1. Dois fragmentos de dados e um fragmento de paridade serão colocados em três nós de armazenamento diferentes.
- Todos os objetos em todos os outros buckets serão replicados. Duas cópias serão criadas e colocadas em dois Storage Nodes diferentes.
- As cópias serão mantidas no StorageGRID permanentemente. StorageGRID ILM não excluirá esses objetos.

Crie uma política de classificação de tráfego para FabricPool no StorageGRID

Opcionalmente, você pode criar uma política de classificação de tráfego do StorageGRID para otimizar a qualidade do serviço para a carga de trabalho do FabricPool.

Para obter detalhes sobre esta tarefa, consulte ["Gerenciar políticas de classificação de tráfego"](#). Para usar o assistente de instalação FabricPool para concluir esta tarefa, acesse ["Acesse e conclua o assistente de instalação do FabricPool"](#).

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).

Sobre esta tarefa

As melhores práticas para criar uma política de classificação de tráfego para FabricPool dependem da carga de trabalho, conforme a seguir:

- Se você planeja distribuir os dados da carga de trabalho principal do FabricPool para o StorageGRID, você deve garantir que a carga de trabalho do FabricPool tenha a maior parte da largura de banda. Você pode criar uma política de classificação de tráfego para limitar todas as outras cargas de trabalho.



Em geral, as operações de leitura do FabricPool são mais importantes para priorizar do que as operações de escrita.

Por exemplo, se outros clientes S3 utilizarem este sistema StorageGRID, você deverá criar uma política de classificação de tráfego. Você pode limitar o tráfego de rede para os outros buckets, tenants, sub-redes IP ou endpoints de balanceadores de carga.

- Em geral, você não deve impor limites de qualidade do serviço a nenhuma carga de trabalho FabricPool; você deve limitar apenas as outras cargas de trabalho.
- Os limites impostos a outras cargas de trabalho devem levar em conta o comportamento dessas cargas. Os limites impostos também variam de acordo com o tamanho e os recursos da sua grid e com a quantidade esperada de utilização.

Passos

1. Selecione **Configuração > Rede > Classificação de tráfego**.
2. Selecione **Create**.
3. Insira um nome e uma descrição (opcional) para a política e selecione **Continuar**.
4. Na etapa Adicionar regras correspondentes, adicione pelo menos uma regra.
 - a. Selecione **Adicionar regra**
 - b. Em Tipo, selecione **Ponto de extremidade do balanceador de carga** e selecione o ponto de extremidade do balanceador de carga que você criou para FabricPool.

Você também pode selecionar a conta do locatário FabricPool ou o bucket.
 - c. Se você deseja que esta política de tráfego limite o tráfego para os outros endpoints, selecione **Correspondência inversa**.
5. Opcionalmente, adicione um ou mais limites para controlar o tráfego de rede correspondente à regra.



StorageGRID coleta métricas mesmo que você não adicione nenhum limite, assim você pode entender as tendências de tráfego.

- a. Selecione **Adicionar um limite**.
 - b. Selecione o tipo de tráfego que você deseja limitar e o limite a ser aplicado.
6. Selecione **Continue**.
 7. Leia e revise a política de classificação de tráfego. Use o botão **Anterior** para voltar e fazer as alterações necessárias. Quando você estiver satisfeito com a política, selecione **Salvar e continuar**.

Após o término

"[Visualizar métricas de tráfego de rede](#)" para verificar se as políticas estão aplicando os limites de tráfego que você espera.

Configure o System Manager do ONTAP para adicionar o StorageGRID como uma camada de nuvem FabricPool

Após obter as informações necessárias do StorageGRID, você pode acessar o ONTAP para adicionar o StorageGRID como uma camada de nuvem.

Antes de começar

- Se você concluiu o assistente de instalação do FabricPool, você tem o arquivo `ONTAP_FabricPool_settings_bucketname.txt` que baixou.
- Se você configurou StorageGRID manualmente, você tem o nome de domínio totalmente qualificado (FQDN) que está usando para StorageGRID ou o endereço VIP para o grupo HA do StorageGRID, o número da porta para o endpoint do balanceador de carga, o certificado do balanceador de carga, o ID da chave de acesso e a chave secreta para o usuário raiz da conta do tenant, e o nome do bucket que o ONTAP usará nesse tenant.

Acesse ONTAP System Manager

Estas instruções descrevem como usar ONTAP System Manager para adicionar StorageGRID como uma camada de nuvem. Você pode realizar a mesma configuração usando a ONTAP CLI. Para obter instruções, acesse "[Documentação ONTAP para FabricPool](#)".

Passos

1. Acesse o System Manager do cluster ONTAP que você deseja migrar para o StorageGRID.
2. Faça login como administrador do cluster.
3. Navegue até **ARMAZENAMENTO > Níveis > Adicionar Nível de Nuvem**.
4. Selecione **StorageGRID** na lista de provedores de armazenamento de objetos.

Insira os valores do StorageGRID

Veja "[Documentação ONTAP para FabricPool](#)" para mais informações.

Passos

1. Preencha o formulário Adicionar Nível de Nuvem, usando o `ONTAP_FabricPool_settings_bucketname.txt` arquivo ou os valores que você obteve manualmente.

Campo	Descrição
Nome	Insira um nome exclusivo para este nível de nuvem. Você pode aceitar o valor padrão.
Estilo de URL	Se você "nomes de domínio de endpoint S3 configurados"selecionar URL virtual no estilo de hospedagem. URL no formato de caminho é o padrão para ONTAP, mas o uso de solicitações no formato de hospedagem virtual é recomendado para StorageGRID. Você deve usar URL no formato de caminho se fornecer um endereço IP em vez de um nome de domínio no campo Server name (FQDN).

Campo	Descrição
Nome do servidor (FQDN)	Insira o nome de domínio totalmente qualificado (FQDN) que você está usando para StorageGRID ou o endereço IP VIP para o grupo HA do StorageGRID. Por exemplo, <code>s3.storagegrid.company.com</code>. Observe o seguinte: • O endereço IP ou nome de domínio que você especificar aqui deve corresponder ao certificado que você carregou ou gerou para o endpoint do balanceador de carga do StorageGRID. • Se você fornecer um nome de domínio, o registro DNS deve corresponder a cada endereço IP que você usará para se conectar ao StorageGRID. Consulte "Configurar o servidor DNS".
SSL	Ativado (padrão).
Certificado de armazenamento de objetos	Cole o certificado PEM que você está usando para o endpoint do balanceador de carga StorageGRID, incluindo: <pre>-----BEGIN CERTIFICATE----- e -----END CERTIFICATE-----.</pre> Nota: Se uma autoridade certificadora intermediária emitiu o certificado StorageGRID, você deve fornecer o certificado da autoridade certificadora intermediária. Se o certificado StorageGRID foi emitido diretamente pela autoridade certificadora raiz, você deve fornecer o certificado da autoridade certificadora raiz.
Porta	Insira a porta usada pelo endpoint do balanceador de carga do StorageGRID. ONTAP usará essa porta ao se conectar ao StorageGRID. Por exemplo, 10433.
Chave de acesso e chave secreta	Insira o ID da chave de acesso e a chave de acesso secreta do usuário raiz da conta de locatário do StorageGRID. Dica: Se você gerar uma nova chave de acesso e uma nova chave de acesso secreta no StorageGRID no futuro, insira as novas chaves no ONTAP antes de excluir os valores antigos do StorageGRID. Caso contrário, o ONTAP pode perder temporariamente o acesso ao StorageGRID.
Nome do contêiner	Insira o nome do bucket StorageGRID que você criou para uso com este tier ONTAP.

2. Conclua a configuração final do FabricPool no ONTAP.

- Anexe um ou mais agregados à camada de nuvem.
- Opcionalmente, crie uma política de tiering de volume.

Configure as entradas do servidor DNS para StorageGRID com FabricPool

Após configurar os grupos de alta disponibilidade, os endpoints do balanceador de carga

e os nomes de domínio dos endpoints do S3, você deve garantir que o DNS inclua as entradas necessárias para StorageGRID. Você deve incluir uma entrada DNS para cada nome no certificado de segurança e para cada endereço IP que você possa usar.

Consulte ["Considerações sobre balanceamento de carga"](#).

Entradas DNS para o nome do servidor StorageGRID

Adicione entradas DNS para associar o nome do servidor StorageGRID (domínio totalmente qualificado) a cada endereço IP do StorageGRID que você utilizará. Os endereços IP que você insere no DNS dependem de você estar usando um grupo de HA de nós de balanceamento de carga:

- Se você configurou um grupo HA, ONTAP se conectará aos endereços IP virtuais desse grupo HA.
- Se você não estiver usando um grupo HA, ONTAP pode se conectar ao serviço StorageGRID Load Balancer usando o endereço IP de qualquer Gateway Node ou Admin Node.
- Se o nome do servidor for resolvido para mais de um endereço IP, ONTAP estabelece conexões de cliente com todos os endereços IP (até um máximo de 16 endereços IP). Os endereços IP são selecionados em um método round-robin quando as conexões são estabelecidas.

Entradas DNS para solicitações virtuais no estilo hosted

Se você definiu ["Nomes de domínio de endpoint S3"](#) e utilizará solicitações virtuais no estilo de hospedagem, adicione entradas DNS para todos os nomes de domínio de endpoint S3 necessários, incluindo quaisquer nomes curinga.

Melhores práticas do StorageGRID para FabricPool

Melhores práticas para grupos de alta disponibilidade (HA) do StorageGRID com FabricPool

Antes de anexar o StorageGRID como uma camada de nuvem FabricPool, conheça os grupos de alta disponibilidade (HA) do StorageGRID e revise as práticas recomendadas para usar grupos de HA com o FabricPool.

O que é um grupo HA?

Um grupo de alta disponibilidade (HA) é um conjunto de interfaces de vários StorageGRID Gateway Nodes, Admin Nodes ou ambos. Um grupo HA ajuda a manter as conexões de dados do cliente disponíveis. Se a interface ativa no grupo HA falhar, uma interface de backup pode gerenciar a carga de trabalho com pouco impacto nas operações do FabricPool.

Cada grupo de alta disponibilidade (HA) fornece acesso altamente disponível aos serviços compartilhados nos nós associados. Por exemplo, um grupo HA composto por interfaces apenas em nós de gateway ou em nós de administração e nós de gateway fornece acesso altamente disponível ao serviço de Load Balancer compartilhado.

Para saber mais sobre grupos de alta disponibilidade, consulte ["Gerencie grupos de alta disponibilidade \(HA\)"](#).

Utilizando grupos HA

As melhores práticas para criar um grupo de alta disponibilidade (HA) do StorageGRID para FabricPool dependem da carga de trabalho.

- Se você planeja usar FabricPool com dados de carga de trabalho primária, deve criar um grupo de alta disponibilidade (HA) que inclua pelo menos dois nós de balanceamento de carga para evitar interrupções na recuperação de dados.
- Se você planeja usar a política de camadas de volume somente para snapshots da FabricPool ou camadas de desempenho locais não primárias (por exemplo, locais de recuperação de desastres ou destinos NetApp SnapMirror®), você pode configurar um grupo de alta disponibilidade com apenas um nó.

Estas instruções descrevem como configurar um grupo HA para Active-Backup HA (um nó é ativo e um nó é backup). No entanto, você pode preferir usar DNS Round Robin ou Active-Active HA. Para saber os benefícios dessas outras configurações de HA, consulte ["Opções de configuração para grupos de alta disponibilidade"](#).

Melhores práticas para balanceamento de carga do StorageGRID com FabricPool

Antes de adicionar StorageGRID como uma camada de nuvem FabricPool, revise as práticas recomendadas para usar balanceadores de carga com FabricPool.

Para obter informações gerais sobre o balanceador de carga StorageGRID e o certificado do balanceador de carga, consulte ["Considerações sobre balanceamento de carga"](#).

Melhores práticas para acesso do locatário ao endpoint do balanceador de carga usado para FabricPool

Você pode controlar quais tenants podem usar um endpoint de balanceamento de carga específico para acessar seus buckets. Você pode permitir todos os tenants, permitir alguns tenants ou bloquear alguns tenants. Ao criar um endpoint de balanceamento de carga para uso do FabricPool, selecione **Permitir todos os tenants**. ONTAP criptografa os dados colocados nos buckets do StorageGRID, portanto, essa camada extra de segurança oferece pouca proteção adicional.

Melhores práticas para o certificado de segurança

Ao criar um endpoint de balanceador de carga do StorageGRID para uso com o FabricPool, você fornece o certificado de segurança que permitirá que o ONTAP se autentique com o StorageGRID.

Na maioria dos casos, a conexão entre ONTAP e StorageGRID deve usar criptografia TLS (Transport Layer Security). Usar FabricPool sem criptografia TLS é suportado, mas não é recomendado. Ao selecionar o protocolo de rede para o endpoint do balanceador de carga do StorageGRID, selecione **HTTPS**. Em seguida, forneça o certificado de segurança que permitirá que o ONTAP se autentique com o StorageGRID.

Para saber mais sobre o certificado do servidor para um endpoint de balanceamento de carga:

- ["Gerenciar certificados de segurança"](#)
- ["Considerações sobre balanceamento de carga"](#)
- ["Diretrizes de reforço para certificados de servidor"](#)

Adicionar certificado ao ONTAP

Ao adicionar StorageGRID como uma FabricPool camada de nuvem, você deve instalar o mesmo certificado no cluster ONTAP, incluindo o certificado raiz e quaisquer certificados de autoridade de certificação (CA) subordinada.

Gerenciar expiração de certificados



Se o certificado usado para proteger a conexão entre ONTAP e StorageGRID expirar, FabricPool vai parar de funcionar temporariamente e o ONTAP vai perder temporariamente o acesso aos dados transferidos para o StorageGRID.

Para evitar problemas com a expiração do certificado, siga estas boas práticas:

- Monitore atentamente quaisquer alertas que avisem sobre a proximidade da expiração de certificados, como os alertas **Expiração do certificado do endpoint do balanceador de carga** e **Expiração do certificado global do servidor para S3 API**.
- Mantenha sempre as versões do certificado do StorageGRID e do ONTAP sincronizadas. Se você substituir ou renovar o certificado usado para um endpoint do balanceador de carga, deverá substituir ou renovar o certificado equivalente usado pelo ONTAP para a camada de nuvem.
- Use um certificado de uma Autoridade Certificadora (CA) assinada publicamente. Se você usar um certificado assinado por uma CA, você pode usar a API de gerenciamento de grid para automatizar a rotação de certificados. Isso permite que você substitua certificados prestes a expirar sem interrupções.
- Se você gerou um certificado autoassinado do StorageGRID e esse certificado está prestes a expirar, você deve substituí-lo manualmente tanto no StorageGRID quanto no ONTAP antes que o certificado existente expire. Se um certificado autoassinado já expirou, desative a validação de certificado no ONTAP para evitar perda de acesso.

Veja ["NetApp Knowledge Base: como configurar um novo certificado de servidor autoassinado do StorageGRID em uma implantação existente do ONTAP FabricPool"](#) as instruções.

Melhores práticas para usar StorageGRID ILM com FabricPool data

Se você estiver usando FabricPool para transferir dados para o StorageGRID, você deve entender os requisitos para usar o gerenciamento do ciclo de vida das informações (ILM) do StorageGRID com os dados do FabricPool.



FabricPool não tem conhecimento das regras ou políticas de gerenciamento do ciclo de vida das informações (ILM) do StorageGRID. A perda de dados pode ocorrer se a política de gerenciamento do ciclo de vida das informações do StorageGRID estiver configurada incorretamente. Para obter informações detalhadas, consulte ["Use regras ILM para gerenciar objetos"](#) e ["Criar políticas de ILM"](#).

Diretrizes para o uso do ILM com FabricPool

Ao usar o assistente de instalação do FabricPool, o assistente cria automaticamente uma nova regra ILM para cada bucket S3 que você cria e adiciona essa regra a uma política inativa. Você é solicitado a ativar a política. A regra criada automaticamente segue as melhores práticas recomendadas: utiliza codificação de apagamento 2+1 em um único site.

Se você estiver configurando StorageGRID manualmente em vez de usar o assistente de instalação do FabricPool, revise estas diretrizes para garantir que suas regras e políticas de ILM sejam adequadas aos dados do FabricPool e às necessidades da sua empresa. Talvez seja necessário criar novas regras e atualizar suas políticas de ILM ativas para atender a essas diretrizes.

- Você pode usar qualquer combinação de regras de replicação e codificação de apagamento para proteger os dados da camada de nuvem.

A prática recomendada é usar codificação de apagamento 2+1 em um site para proteção de dados com

boa relação custo-benefício. A codificação de apagamento usa mais CPU, mas oferece significativamente menos capacidade de storage do que a replicação. Os esquemas 4+1 e 6+1 usam menos capacidade do que o esquema 2+1. No entanto, os esquemas 4+1 e 6+1 são menos flexíveis se você precisar adicionar Storage Nodes durante a expansão da grid. Para obter detalhes, consulte ["Adicionar capacidade de storage para objetos com codificação de apagamento"](#).

- Cada regra aplicada aos dados do FabricPool deve usar codificação de apagamento ou criar pelo menos duas cópias replicadas.



Uma regra ILM que cria apenas uma cópia replicada para qualquer período de tempo coloca os dados em risco de perda permanente. Se existir apenas uma cópia replicada de um objeto, esse objeto será perdido se um Storage Node falhar ou apresentar um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

- Se você precisar ["remover dados do FabricPool do StorageGRID"](#), use ONTAP para recuperar todos os dados do volume FabricPool e promovê-lo para a camada de desempenho.



Para evitar perda de dados, não utilize uma regra ILM que expire ou exclua FabricPool dados da camada de nuvem. Defina o período de retenção em cada regra ILM como **permanente** para garantir que os objetos FabricPool não sejam excluídos pelo StorageGRID ILM.

- Não crie regras que movam os dados da camada de nuvem do FabricPool para fora do bucket para outro local. Você não pode usar um Cloud Storage Pool para mover dados do FabricPool para outro armazenamento de objetos.



O uso de Cloud Storage Pools com FabricPool não é compatível devido à latência adicional para recuperar um objeto do destino do Cloud Storage Pool.

- A partir do ONTAP 9.8, você pode criar tags de objeto opcionais para ajudar a classificar e ordenar dados em camadas, facilitando o gerenciamento. Por exemplo, você pode definir tags apenas em volumes FabricPool conectados ao StorageGRID. Em seguida, ao criar regras ILM no StorageGRID, você pode usar o filtro avançado de tag de objeto para selecionar e posicionar esses dados.

Melhores práticas para configurações globais do StorageGRID com FabricPool

Ao configurar um sistema StorageGRID para uso com o FabricPool, você pode precisar alterar outras opções do StorageGRID. Antes de alterar uma configuração global, considere como a alteração afetará outros aplicativos S3.

Destinos de mensagens e log de auditoria

FabricPool cargas de trabalho geralmente têm uma alta taxa de operações de leitura, o que pode gerar um grande volume de mensagens de auditoria.

- Se você não precisar de um registro das operações de leitura do cliente para FabricPool ou qualquer outro aplicativo S3, opcionalmente acesse **Configuração > Monitoramento > Servidor de auditoria e syslog**. Altere a configuração **Leituras do cliente para Erro** para diminuir o número de mensagens de auditoria registradas no log de auditoria. Consulte ["Configurar o gerenciamento de logs e o servidor syslog externo"](#) para obter detalhes.
- Se você possui uma grade grande, utiliza vários tipos de aplicativos S3 ou deseja reter todos os dados de

auditoria, configure um servidor syslog externo e salve as informações de auditoria remotamente. Usar um servidor externo minimiza o impacto no desempenho do registro de mensagens de auditoria sem reduzir a integridade dos dados de auditoria. Consulte ["Considerações para servidor syslog externo"](#) para obter detalhes.

Criptografia de objetos

Ao configurar o StorageGRID, você pode opcionalmente habilitar a ["opção global para criptografia de objetos armazenados"](#) se a criptografia de dados for necessária para outros clientes StorageGRID. Os dados que são transferidos do FabricPool para o StorageGRID já estão criptografados, portanto, habilitar a configuração do StorageGRID não é necessário. As chaves de criptografia do lado do cliente pertencem ao ONTAP.

Compressão de objetos

Ao configurar o StorageGRID, não habilite o ["opção global para compactar objetos armazenados"](#). Os dados que são transferidos do FabricPool para o StorageGRID já estão compactados. Usar a opção do StorageGRID não reduzirá ainda mais o tamanho de um objeto.

Bloqueio de objeto S3

Se a configuração global de S3 Object Lock estiver habilitada para seu sistema StorageGRID, não habilite ["Bloqueio de objeto S3"](#) ao criar buckets FabricPool. S3 Object Lock não é compatível com buckets FabricPool.

Consistência do bucket

Para FabricPool buckets, a consistência recomendada é **Read-after-new-write**, que é a consistência padrão para um novo bucket. Não edite FabricPool buckets para usar **Available** ou **Strong-site**.

Tiering do FabricPool

Se um nó do StorageGRID usar armazenamento atribuído de um sistema NetApp ONTAP, confirme que o volume não possui uma política de tiering FabricPool habilitada. Por exemplo, se um nó do StorageGRID estiver em execução em um host VMware, certifique-se de que o volume que suporta o datastore para o nó do StorageGRID não possui uma política de tiering FabricPool habilitada. Desabilitar o tiering FabricPool para volumes usados com nós do StorageGRID simplifica a solução de problemas e as operações de storage.



Nunca use FabricPool para hierarquizar qualquer dado relacionado ao StorageGRID de volta para o próprio StorageGRID. Hierarquizar dados do StorageGRID de volta para o StorageGRID aumenta a complexidade operacional e de solução de problemas.

Remova os dados do FabricPool do StorageGRID

Se você precisar remover os dados do FabricPool que estão atualmente armazenados no StorageGRID, deve usar o ONTAP para recuperar todos os dados do volume FabricPool e promovê-los para a camada de desempenho.

Antes de começar

- Você revisou as instruções e considerações em ["Promover dados para a camada de desempenho"](#).
- Você está usando ONTAP 9.8 ou posterior.
- Você está usando um ["navegador web compatível"](#).
- Você pertence a um grupo de usuários do StorageGRID para a conta de locatário FabricPool que possui o

["Gerenciar todos os buckets ou permissão de acesso à raiz".](#)

Sobre esta tarefa

Estas instruções explicam como mover dados do StorageGRID de volta para o FabricPool. Você executa este procedimento usando ONTAP e StorageGRID Tenant Manager.

Passos

1. A partir do ONTAP, execute o comando `volume modify`.

Defina `tiering-policy` para `none` para interromper o novo tiering e defina `cloud-retrieval-policy` para `promote` para retornar todos os dados que foram previamente movidos para StorageGRID.

Consulte ["Promova todos os dados de um volume FabricPool para o nível de desempenho"](#).

2. Aguarde a conclusão da operação.

Você pode usar o `volume object-store` comando com a `tiering` opção para ["Verifique o status da promoção do tier de performance"](#).

3. Quando a operação de promoção estiver concluída, faça login no StorageGRID Tenant Manager para a conta do locatário FabricPool.
4. Selecione **Exibir buckets** no painel ou selecione **STORAGE (S3) > Buckets**.
5. Confirme que o bucket do FabricPool agora está vazio.
6. Se o balde estiver vazio, ["excluir o bucket"](#).

Depois que você terminar

Ao excluir o bucket, o tiering do FabricPool para o StorageGRID não poderá mais continuar. No entanto, como o tier local ainda está vinculado ao tier de nuvem do StorageGRID, o ONTAP System Manager retornará mensagens de erro indicando que o bucket está inacessível.

Para evitar essas mensagens de erro, faça um dos seguintes procedimentos:

- Use o recurso FabricPool Mirror para conectar uma camada de nuvem diferente ao agregado.
- Mova os dados do agregado FabricPool para um agregado não FabricPool e, em seguida, exclua o agregado não utilizado.

Consulte o ["Documentação ONTAP para FabricPool"](#) para obter instruções.

Informações sobre direitos autorais

Copyright © 2026 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 SOBRESSAIENTES; 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.