



Configurar e gerenciar

StorageGRID software

NetApp
December 03, 2025

Índice

Configurar e gerenciar um sistema StorageGRID	1
Administrar StorageGRID	1
Administrar StorageGRID	1
Comece a usar o Grid Manager	1
Controle o acesso ao StorageGRID	32
Usar federação de grade	80
Gerenciar segurança	117
Gerenciar inquilinos	186
Configurar conexões do cliente	206
Gerenciar redes e conexões	247
Usar AutoSupport	266
Gerenciar nós de armazenamento	281
Gerenciar nós de administração	295
Gerenciar objetos com ILM	298
Gerenciar objetos com ILM	298
ILM e ciclo de vida do objeto	299
Criar e atribuir níveis de armazenamento	321
Use pools de armazenamento	324
Use pools de armazenamento em nuvem	332
Gerenciar perfis de codificação de eliminação	353
Configurar regiões (opcional e somente S3)	356
Criar regra ILM	358
Gerenciar políticas de ILM	374
Trabalhar com políticas e regras do ILM	391
Usar bloqueio de objeto S3	395
Exemplo de regras e políticas do ILM	403
Endurecimento do sistema	422
Considerações gerais para o reforço do sistema	422
Diretrizes de reforço para atualizações de software	423
Diretrizes de proteção para redes StorageGRID	424
Diretrizes de proteção para nós do StorageGRID	425
Diretrizes de proteção para TLS e SSH	428
Outras diretrizes de endurecimento	429
Configurar StorageGRID para FabricPool	431
Configurar StorageGRID para FabricPool	431
Informações necessárias para anexar o StorageGRID como uma camada de nuvem	433
Use o assistente de configuração do FabricPool	434
Configurar o StorageGRID manualmente	447
Configurar o ONTAP System Manager	457
Configurar o servidor DNS	459
Melhores práticas do StorageGRID para FabricPool	460
Remover dados do FabricPool do StorageGRID	464

Configurar e gerenciar um sistema StorageGRID

Administrar StorageGRID

Administrar StorageGRID

Use estas instruções para configurar e administrar um sistema StorageGRID .

Sobre estas instruções

As principais tarefas para configurar e administrar o 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
- Configurar e gerenciar redes StorageGRID
- Configurar AutoSupport
- Gerenciar configurações do nó

Antes de começar

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

Comece a usar o Grid Manager

Requisitos do navegador da Web

Você deve usar um navegador da web compatível.

Navegador da web	Versão mínima suportada
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

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

Largura do navegador	Pixels
Mínimo	1024
Ótimo	1280

Sign in no Grid Manager

Você acessa a página de login do Grid Manager inserindo o nome de 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 fazer login no Grid Manager em qualquer nó de administração para gerenciar o sistema StorageGRID. No entanto, alguns procedimentos de manutenção só podem ser executados no nó de administração principal.

Conectar ao grupo HA

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

Usar SSO

As etapas de login são ligeiramente diferentes se "[o logon único \(SSO\) foi configurado](#)".

Sign in no Grid Manager no primeiro nó de administração

Antes de começar

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

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

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

Para acessar o Grid Manager em uma porta diferente da porta padrão para HTTPS (443), inclua o número da porta no 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 da Web compatível.
2. Na barra de endereço do navegador, digite o URL do Grid Manager.
3. Se você receber um alerta de segurança, instale o certificado usando o assistente de instalação do navegador. Ver "[Gerenciar certificados de segurança](#)".

4. Sign in no Grid Manager.

A tela de login exibida depende se o logon único (SSO) foi configurado para StorageGRID.

Não usar SSO

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



The screenshot shows the login interface for NetApp StorageGRID Grid Manager. At the top, the NetApp logo is followed by 'StorageGRID®' and 'Grid Manager' in a large font. Below this, there are two input fields: 'Username' and 'Password'. The 'Username' field has a blue border and a cursor. Below the 'Password' field is a blue 'Sign in' button. At the bottom, there are three links: 'Tenant sign in', 'NetApp support', and 'NetApp.com'.

Usando SSO

- Se o StorageGRID estiver usando SSO e esta for a primeira vez que você acessou a URL neste navegador:
 - i. Selecione * Sign in*. Você pode deixar o 0 no campo Conta.



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

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

Sign in with your organizational account

Sign in

- Se o StorageGRID estiver usando SSO e você tiver acessado anteriormente o Grid Manager ou uma conta de locatário:
 - i. Digite **0** (o ID da conta do Grid Manager) ou selecione **Grid Manager** se ele aparecer na lista de contas recentes.

The image shows a web interface for NetApp StorageGRID. At the top, the logo "NetApp StorageGRID®" is displayed. Below it is the heading "Sign in". Under the heading, there is a section labeled "Recent" with a dropdown menu showing "Grid Manager". Below that is a section labeled "Account" with a text input field containing the number "0". At the bottom of the form is a blue button labeled "Sign in". Below the button, there is a link "NetApp support | NetApp.com".

NetApp StorageGRID®

Sign in

Recent

Grid Manager ▼

Account

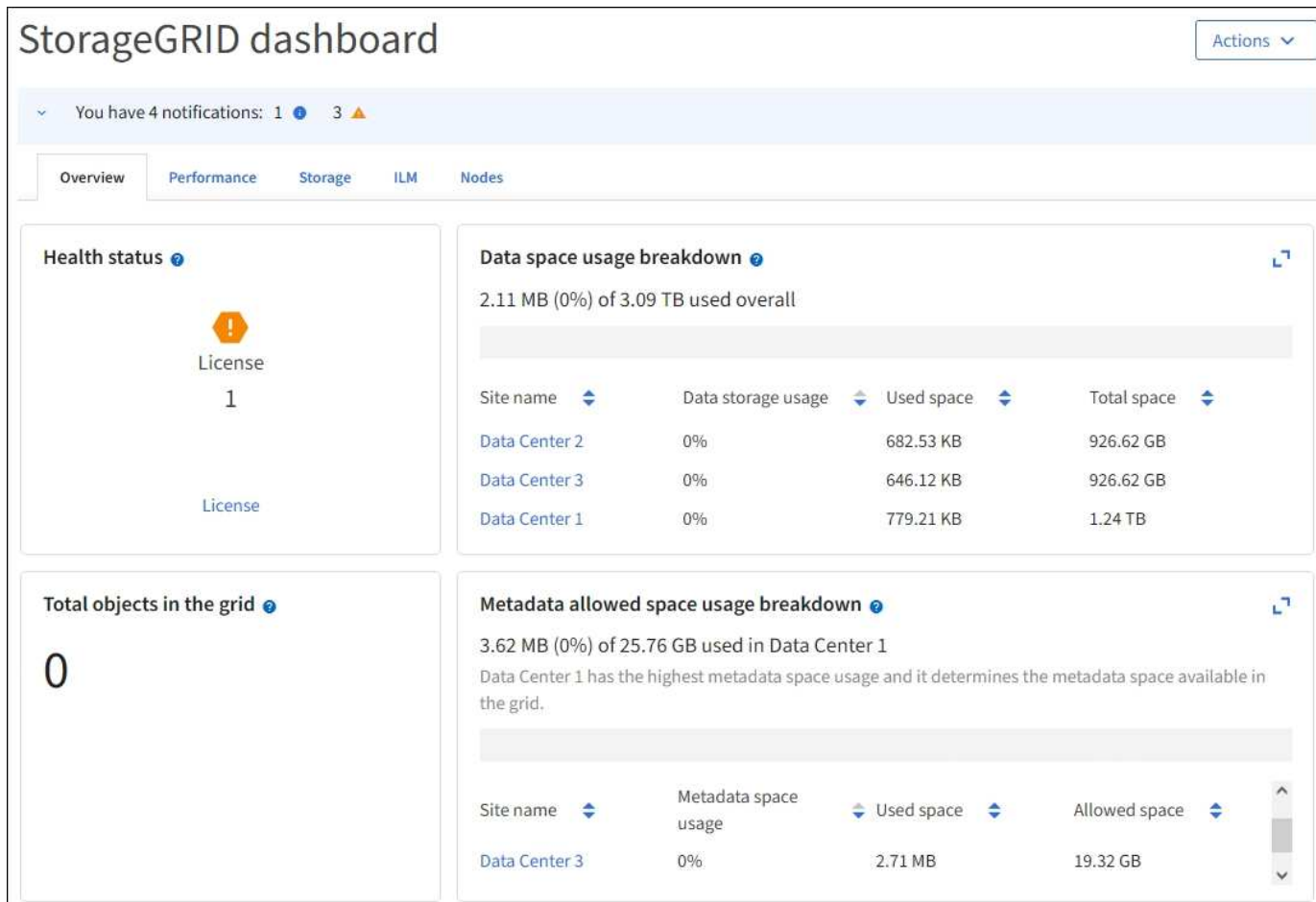
0

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Selecione * Sign in*.
- iii. Sign in com suas credenciais SSO padrão na página de login SSO da sua organização.

Quando você estiver conectado, a página inicial do Grid Manager será exibida, incluindo o painel. Para saber quais informações são fornecidas, consulte "[Visualizar e gerenciar o painel](#)".



Entre em outro nó de administração

Siga estas etapas para fazer login em outro nó de administração.

Não usar SSO

Passos

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

Usando SSO

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

Passos

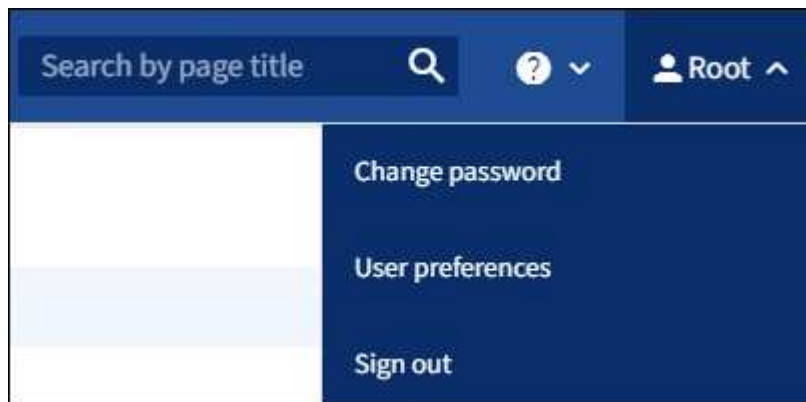
1. Digite o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração na barra de endereços do navegador.
2. Se sua sessão SSO expirou, insira suas credenciais novamente.

Sair do Grid Manager

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

Passos

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



2. Selecione **Sair**.

Opção	Descrição
SSO não está em uso	Você está desconectado do nó de administração. A página de login do Grid Manager é exibida. Observação: se você tiver entrado em mais de um nó de administração, será necessário sair de cada nó.
SSO habilitado	Você está desconectado de todos os nós de administração que estava acessando. A página de login do StorageGRID é exibida. Grid Manager é listado como padrão no menu suspenso Contas recentes, e o campo ID da conta mostra 0. Observação: Se o SSO estiver habilitado e você também estiver conectado ao Gerenciador de locatários, você também deverá "sair da conta do inquilino" para "sair do SSO".

Alterar sua senha

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

Antes de começar

Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".

Sobre esta tarefa

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

não será possível 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**.

Ver informações da licença do StorageGRID

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

Antes de começar

Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .

Sobre esta tarefa

Se houver um problema com a licença de software para este sistema StorageGRID , o cartão de status de integridade no painel incluirá 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 seguindo um destes procedimentos:
 - Selecione **MANUTENÇÃO** > **Sistema** > **Licença**.
 - No cartão Status de integridade no painel, selecione o ícone Status da licença ou o link **Licença**.

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

2. Veja os detalhes somente leitura da licença atual:

- ID do sistema StorageGRID , que é o número de identificação exclusivo para esta instalação do StorageGRID
- Número de série da licença
- Tipo de licença, **Perpétua** ou **Assinatura**
- Capacidade de armazenamento licenciada da rede
- Capacidade de armazenamento suportada
- Data de término da licença. **N/A** aparece para uma licença perpétua.
- Data de término do suporte

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

- Conteúdo do arquivo de texto da licença

Atualizar informações da licença do StorageGRID

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

Antes de começar

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

Passos

1. Selecione **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 a API

Use a API de gerenciamento de grade

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

Recursos de nível superior

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

- `/grid`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas.
- `/org`: O acesso é restrito a usuários que pertencem a um grupo LDAP local ou federado para uma conta de locatário. Para obter detalhes, consulte ["Use uma conta de inquilino"](#).
- `/private`: O acesso é restrito aos usuários do Grid Manager e é baseado nas permissões de grupo configuradas. As APIs privadas estão sujeitas a alterações sem aviso prévio. Os endpoints privados do StorageGRID também ignoram a versão da API da solicitação.

Emitir solicitações de API

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

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

Antes de começar

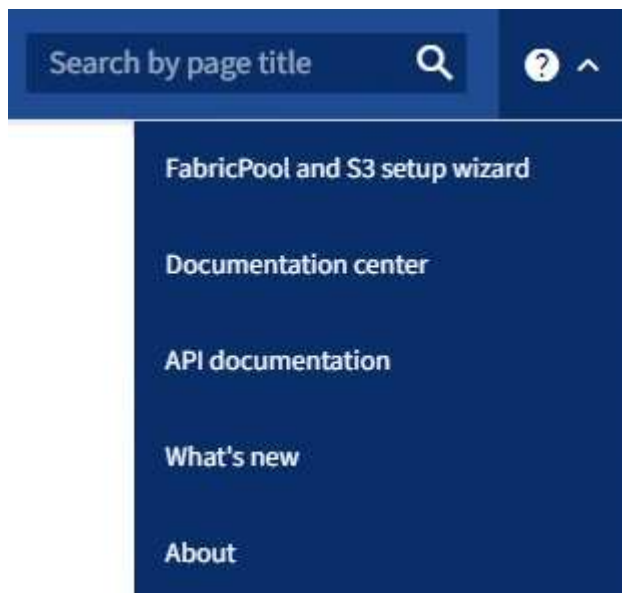
- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).



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

Passos

1. No cabeçalho do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API**.



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

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

3. Selecione a operação desejada.

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

4. Selecione uma ação HTTP para ver os detalhes da solicitação, incluindo a URL do ponto de extremidade, uma lista de quaisquer parâmetros obrigatórios ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as respostas possíveis.

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 usuário. Então,

obtenha esses valores. Talvez seja necessário emitir uma solicitação de API diferente primeiro para obter as informações necessárias.

6. Determine se você precisa modificar o corpo da solicitação de exemplo. Se sim, você pode selecionar **Modelo** para saber os requisitos de cada campo.
7. Selecione **Experimentar**.
8. Forneça quaisquer parâmetros necessários ou modifique o corpo da solicitação conforme necessário.
9. Selecione **Executar**.
10. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

Operações da API de gerenciamento de grade

A API de gerenciamento de grade organiza as operações disponíveis nas seguintes seções.



Esta lista inclui apenas operações disponíveis na API pública.

- **contas**: Operações para gerenciar contas de locatários de armazenamento, incluindo a criação de novas contas e a recuperação do uso de armazenamento para uma determinada conta.
- **alert-history**: Operações em alertas resolvidos.
- **alert-receivers**: Operações em receptores de notificação de alerta (e-mail).
- **alert-rules**: Operações em regras de alerta.
- **alert-silences**: Operações em silêncios de alerta.
- **alertas**: Operações em alertas.
- **audit**: Operações para listar e atualizar a configuração de auditoria.
- **auth**: Operações para realizar autenticação de sessão do usuário.

A API de gerenciamento de grade oferece suporte ao esquema de autenticação de token de portador. 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. Este token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("Autorização: Token do portador"). O token expira após 16 horas.



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

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

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

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



Métricas que incluem *private* em seus nomes são destinados apenas para uso interno. Essas métricas estão sujeitas a alterações entre as versões do StorageGRID sem aviso prévio.

- **node-details**: Operações em detalhes do nó.
- **node-health**: Operações 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 de Protocolo de Tempo de Rede (NTP).
- **objetos**: Operações em objetos e metadados de objetos.
- **recuperação**: Operações para o procedimento de recuperação.
- **recovery-package**: Operações para baixar o pacote de recuperação.
- **regiões**: Operações para visualizar e criar regiões.
- **s3-object-lock**: Operações nas configurações globais de bloqueio de objetos do S3.
- **server-certificate**: Operações para visualizar e atualizar certificados do servidor do Grid Manager.
- **snmp**: Operações na configuração SNMP atual.
- **storage-watermarks**: Marcas d'água do nó de armazenamento.
- **traffic-classes**: Operações para políticas de classificação de tráfego.
- **untrusted-client-network**: Operações na configuração de rede de cliente não confiável.

- **usuários:** Operações para visualizar e gerenciar usuários do Grid Manager.

Controle de versão da API de gerenciamento de grade

A API de gerenciamento de grade usa controle de versão para oferecer suporte a atualizações sem interrupções.

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 alterada quando são feitas alterações que *não são compatíveis* com versões mais antigas. A versão secundária da API é alterada quando são feitas alterações que *são compatíveis* com versões mais antigas. Alterações compatíveis incluem a adição de novos pontos de extremidade ou novas propriedades.

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

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

Quando você instala o software StorageGRID pela primeira vez, somente a versão mais recente da API é habilitada. No entanto, ao atualizar para uma nova versão de recurso do StorageGRID, você continua tendo acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID .



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

Solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Obsoleto: verdadeiro"
- O corpo da resposta JSON inclui "deprecated": true
- Um aviso obsoleto foi adicionado ao nms.log. Por exemplo:

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

Determinar quais versões de API são suportadas na versão atual

Use o GET `/versions` Solicitação de API para retornar uma lista das principais versões de API suportadas. Esta solicitação está localizada na seção **config** da documentação da API do 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 de 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 substituirá o valor do caminho.

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

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

Proteja-se contra falsificação de solicitação entre sites (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra o StorageGRID usando tokens CSRF para aprimorar a autenticação que usa 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 efetuar login.

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

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

Para habilitar o recurso, defina o `csrfToken` parâmetro para `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 `GridCsrfToken` O cookie é definido com um valor aleatório para logins no Grid Manager e o `AccountCsrfToken` O cookie é definido com um valor aleatório para logins 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 terminais que aceitam um corpo codificado em formulário: A `csrfToken` parâmetro do corpo da solicitação codificado em formulário.

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



Solicitações que tenham um cookie de token CSRF definido também aplicarão 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 logon único estiver habilitado

Use a API se o logon único estiver habilitado (Active Directory)

Se você tem "[configurou e habilitou o logon único \(SSO\)](#)" e você usa o Active Directory como o provedor de SSO, você deve emitir uma série de solicitações de API para obter um token de autenticação válido para a API de gerenciamento de grade ou a API de gerenciamento de locatários.

Sign in na API se o logon único estiver habilitado

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

Antes de começar

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

Sobre esta tarefa

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

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

- Um exemplo de fluxo de trabalho de solicitações curl.

O fluxo de trabalho do curl pode expirar se você o executar muito lentamente. Você pode ver o erro: `A valid SubjectConfirmation was not found on this Response`.



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

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

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
 - Use o `storagegrid-ssoauth.py` Script Python. Vá para o passo 2.
 - Use solicitações curl. Vá para a etapa 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 do SSO
- O domínio onde o StorageGRID está instalado
- O endereço para StorageGRID
- O ID da conta do locatário, se você quiser acessar a API de gerenciamento de locatários.

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

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

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

3. Se você quiser usar solicitações curl, use o seguinte procedimento.
 - a. Declare as variáveis necessárias para fazer 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 grade, use 0 como TENANTACCOUNTID.

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

Este exemplo mostra uma solicitação POST para uma URL de autenticação assinada para TENANTACCOUNTID. Os resultados serão repassados 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 é codificada por URL, mas não inclui a camada adicional de codificação JSON.

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

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

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

- d. Obtenha uma URL completa que inclua o ID de solicitação do cliente do AD FS.

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

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

A resposta inclui o ID 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 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 seu sistema SSO, a postagem do formulário também conterá a segunda senha ou outras credenciais.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=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='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

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

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

Os cabeçalhos de resposta conterão informações de sessão do AD FS para uso posterior em caso de 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="PHNhbWxwOlJlc3Bvb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

- i. Salve o SAMLResponse do campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb25zZT4='
```

- j. Usando o salvo SAMLResponse , faça um StorageGRID/api/saml-response solicitação para gerar

um token de autenticação StorageGRID .

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

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

A resposta inclui o token de autenticação.

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

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

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

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

Sair da API se o logon único estiver habilitado

Se o logon único (SSO) estiver habilitado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatários. Estas instruções se aplicam se você estiver usando o Active Directory como provedor de identidade SSO

Sobre esta tarefa

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

Passos

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


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

Um URL de logout é retornado:

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

2. Salve o URL de logout.

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

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

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

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

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

4. Exclua o token portador do StorageGRID .

A exclusão do token portador do StorageGRID funciona da mesma forma que sem o SSO. Se `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
```

UM 204 No Content a resposta indica que o usuário está desconectado.

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

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

Se você tem "[configurou e habilitou o logon único \(SSO\)](#)" e você usa o Azure como o provedor de SSO, você pode usar dois scripts de exemplo para obter um token de autenticação válido para a API de Gerenciamento de Grade ou a API de Gerenciamento de Locatários.

Sign in na API se o logon único do Azure estiver habilitado

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

Antes de começar

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

Sobre esta tarefa

Para obter um token de autenticação, você pode usar os seguintes scripts de exemplo:

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

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

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

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

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

Passos

1. Instale as dependências necessárias, da seguinte forma:

- a. Instale o Node.js (veja "<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 executá-lo.

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

3. Quando solicitado, insira valores para os seguintes argumentos (ou passe-os usando parâmetros):
 - O endereço de e-mail SSO usado para fazer login no Azure
 - O endereço para StorageGRID
 - O ID da conta do locatário, se você quiser acessar a API de gerenciamento de locatários
4. Quando solicitado, digite a senha e esteja preparado para fornecer uma autorização MFA ao Azure, se solicitado.

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

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

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



O script pressupõe que o MFA seja feito usando o Microsoft Authenticator. Talvez seja necessário modificar o script para oferecer suporte a outras formas de MFA (como inserir um código recebido em uma mensagem de texto).

O token de autorização 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 usado.

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

Se você tem "[configurou e habilitou o logon único \(SSO\)](#)" e você usa o PingFederate como provedor de SSO, você deve emitir uma série de solicitações de API para obter um token de autenticação válido para a API de gerenciamento de grade ou a API de gerenciamento de locatários.

Sign in na API se o logon único estiver habilitado

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

Antes de começar

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

Sobre esta tarefa

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

- O `storagegrid-ssoauth.py` Script Python, que está localizado no diretório de arquivos de instalação do StorageGRID(`./rpms` para Red Hat Enterprise Linux, `./debs` para Ubuntu ou Debian, e `./vsphere` para VMware).
- Um exemplo de fluxo de trabalho de solicitações curl.

O fluxo de trabalho do curl pode expirar se você o executar muito lentamente. Você pode ver o erro: `A valid SubjectConfirmation was not found on this Response.`



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

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

Passos

1. Selecione um dos seguintes métodos para obter um token de autenticação:
 - Use o `storagegrid-ssoauth.py` Script Python. Vá para o passo 2.
 - Use solicitações curl. Vá para a etapa 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 do SSO
- O domínio onde o StorageGRID está instalado. Este campo não é usado para PingFederate. Você pode deixar em branco ou inserir qualquer valor.
- O endereço para StorageGRID
- O ID da conta do locatário, se você quiser acessar a API de gerenciamento de locatários.

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

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

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

3. Se você quiser usar solicitações curl, use o seguinte procedimento.
 - a. Declare as variáveis necessárias para fazer 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 grade, use 0 como TENANTACCOUNTID.

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

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

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

A resposta para este exemplo inclui uma URL assinada que é codificada por URL, mas não inclui a camada adicional de codificação JSON.

```
{
  "apiVersion": "3.0",
  "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

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

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

- d. Exporte a resposta e o cookie e faça eco da resposta:

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

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

e. Exporte o valor 'pf.adapterId' e repita a resposta:

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

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

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

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

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

g. Exporte o valor 'action':

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

h. Enviar cookies junto com as credenciais:

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

i. Salve o SAMLResponse do campo oculto:

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

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

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

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

A resposta inclui o token de autenticação.

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

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

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

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

Sair da API se o logon único estiver habilitado

Se o logon único (SSO) estiver habilitado, você deverá emitir uma série de solicitações de API para sair da API de gerenciamento de grade ou da API de gerenciamento de locatários. Estas instruções se aplicam se você estiver usando o PingFederate como provedor de identidade SSO

Sobre esta tarefa

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

Passos

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

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

Um URL de logout é retornado:

```
{
  "apiVersion": "3.0",
  "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2021-10-12T22:20:30.839Z",
  "status": "success"
}
```

2. Salve o URL de logout.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

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

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

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

A exclusão do token portador do StorageGRID funciona da mesma forma que sem o SSO. Se `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
```

UM 204 No Content a resposta indica que o usuário está desconectado.

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


Desativar recursos com a API

Você pode usar a API de gerenciamento de grade para desativar completamente determinados 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 Recursos Desativados permite que você impeça o acesso a determinados recursos no sistema StorageGRID . Desativar um recurso é a única maneira de impedir que o usuário root ou usuários que pertencem a grupos de administradores com permissão de **acesso root** possam usar esse recurso.

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

_A Empresa A é uma provedora de serviços que aluga a capacidade de armazenamento do seu sistema StorageGRID criando contas de locatário. Para proteger a segurança dos objetos de seus locatários, a Empresa A quer garantir que seus próprios funcionários nunca possam acessar nenhuma conta de locatário após a conta ter sido implantada.

_A empresa A pode atingir esse objetivo usando o sistema Desativar recursos na API de gerenciamento de grade. Ao desativar completamente o recurso **Alterar senha raiz do locatário** no Grid Manager (tanto na IU quanto na API), a Empresa A garante que os usuários administradores — incluindo o usuário raiz e os usuários pertencentes a grupos com a permissão **Acesso raiz** — não possam alterar a senha de nenhum usuário raiz da conta do locatário.

Passos

1. Acesse a documentação do Swagger para a API de gerenciamento de grade. Ver "[Use a API de gerenciamento de grade](#)".
2. Localize o ponto de extremidade Desativar recursos.
3. Para desativar um recurso, como Alterar senha raiz do locatário, envie um corpo para a API como este:

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

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

Reativar recursos desativados

Por padrão, você pode usar a API de gerenciamento de grade para reativar um recurso que foi desativado. Entretanto, se você quiser impedir que recursos desativados sejam reativados, você pode desativar o próprio 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 do Swagger para a API de gerenciamento de grade.
2. Localize o ponto de extremidade Desativar recursos.
3. Para reativar todos os recursos, envie um corpo para a API como este:

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

Quando essa 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 do usuário, e qualquer solicitação de API que tente alterar a senha raiz de um locatário será bem-sucedida, supondo que o usuário tenha a permissão de gerenciamento **Acesso raiz** ou **Alterar senha raiz do locatário**.



O exemplo anterior faz com que *todos* os recursos desativados sejam reativados. Se outros recursos que devem permanecer desativados tiverem sido desativados, você deverá 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

Controle de acesso ao StorageGRID

Você controla quem pode acessar o 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 senhas de grade.

Controle o acesso ao Grid Manager

Você determina quem pode acessar o Grid Manager e a Grid Management API importando grupos e usuários de um serviço de federação de identidade ou configurando grupos e usuários locais.

Usando ["federação de identidade"](#) faz a configuração ["grupos"](#) e ["Usuários"](#) mais rápido e permite que os usuários façam login no StorageGRID usando credenciais familiares. Você pode configurar a federação de identidade se usar o Active Directory, o OpenLDAP ou o Oracle Directory Server.



Entre em contato com o suporte técnico se quiser usar outro serviço LDAP v3.

Você determina quais tarefas cada usuário pode executar atribuindo diferentes ["permissões"](#) para cada grupo. Por exemplo, você pode querer que usuários em um grupo possam gerenciar regras de ILM e usuários em 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 para ser somente leitura. Usuários em um grupo somente leitura podem apenas visualizar configurações e recursos. Eles não podem fazer nenhuma alteração ou executar nenhuma operação no Grid Manager ou na Grid Management API.

Habilitar logon único

O sistema StorageGRID oferece suporte ao logon único (SSO) usando o padrão Security Assertion Markup Language 2.0 (SAML 2.0). Depois de você ["configurar e habilitar o SSO"](#), todos os usuários devem ser autenticados por um provedor de identidade externo antes de poderem acessar o Grid Manager, o Tenant Manager, a Grid Management API ou a Tenant Management API. 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 de grade e chaves de criptografia para o sistema StorageGRID . Você pode ["alterar a senha"](#) conforme necessário.

Alterar senhas do console do nó

Cada nó na sua grade tem uma senha exclusiva do console do nó, que você precisa para efetuar login no nó como "admin" usando SSH, ou como usuário root em uma conexão de console físico/VM. Conforme necessário, você pode ["alterar a senha do console do nó"](#) para cada nó.

Alterar a senha de provisionamento

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 informações de topologia de grade, senhas de console de nós de grade e chaves de criptografia para o sistema StorageGRID .

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem permissões de acesso de manutenção ou root.
- Você tem 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 `Passwords.txt` arquivo. Certifique-se de documentar a senha de provisionamento e mantê-la em um local seguro.

Passos

1. Selecione **CONFIGURAÇÃO > Controle de acesso> Senhas de 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. As senhas diferenciam maiúsculas de minúsculas.
5. Armazene a nova senha de provisionamento em um local seguro. É necessário para procedimentos de instalação, expansão e manutenção.
6. Digite novamente a nova senha e selecione **Salvar**.

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



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

7. Selecione **Pacote de recuperação**.
8. Digite 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 Recovery Package permite restaurar o sistema caso ocorra uma falha.

Alterar senhas do console do nó

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

Antes de começar

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

Sobre esta tarefa

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



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

Acesse o assistente

Passos

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

Digite a senha de provisionamento

Passos

1. Digite a senha de provisionamento para sua grade.
2. Selecione **Continuar**.

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 neste arquivo se o processo de alteração de senha falhar para qualquer nó.

Passos

1. Selecione **Baixar pacote de recuperação**.
2. 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 .

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

Você não pode cancelar este processo depois que ele for iniciado.

Alterar senhas do console do nó

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

Passos

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



Não substitua o antigo Pacote de Recuperação.

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

4. Marque a caixa de seleção para indicar que você baixou o novo Pacote de Recuperação e verificou o conteúdo.
5. Selecione **Alterar senhas do console do nó** e aguarde até que todos os nós sejam atualizados com as novas senhas. Isso pode levar alguns minutos.

Se as senhas forem alteradas para todos os nós, um banner verde de sucesso será exibido. Vá para o próximo passo.

Se houver um erro durante o processo de atualização, uma mensagem de banner listará o número de nós que não tiveram suas senhas alteradas. O sistema repetirá automaticamente o processo em qualquer nó cuja senha não tenha sido alterada. Se o processo terminar com alguns nós ainda sem uma senha alterada, o botão **Repetir** será exibido.

Se a atualização da senha falhar para um ou mais nós:

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



Tentar novamente altera apenas as senhas do console do nó nos nós que falharam durante tentativas anteriores de alteração de senha.

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

Alterar senhas de acesso SSH para nós de administração

Alterar as senhas de acesso SSH para 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 nós usando autenticação segura e sem senha.

Use uma chave SSH para efetuar login em um nó como `admin` ou para o usuário `root` em uma VM ou conexão de console físico.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Permissão de acesso de manutenção ou root"](#) .
- Você tem 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 são armazenadas no `Passwords.txt` arquivo no Pacote de Recuperação. As chaves estão listadas na coluna Senha desse arquivo.

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

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO > Controle de acesso > Senhas de grade**.
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 se o processo de alteração de chave falhar para qualquer nó.

Passos

1. Digite a senha de provisionamento para sua grade.
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 **Continuar**.
5. Quando a caixa de diálogo de confirmação aparecer, selecione **Sim** se estiver pronto para começar a

alterar as chaves de acesso SSH.



Você não pode cancelar este 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 novo arquivo do pacote de recuperação(.zip) para dois locais seguros, protegidos e separados.
3. Quando o download for concluído:
 - a. Abra o .zip arquivo.
 - b. Confirme se você pode acessar o 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 substitua o antigo Pacote de Recuperação.

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, um banner verde de sucesso será exibido.

Se houver um erro durante o processo de atualização, uma mensagem de banner listará o número de nós que não tiveram suas chaves alteradas. O sistema repetirá automaticamente o processo em qualquer nó cuja chave não tenha sido alterada. Se o processo terminar com alguns nós ainda sem uma chave alterada, o botão **Repetir** será exibido.

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

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

Tentar novamente altera apenas as chaves de acesso SSH nos nós que falharam durante 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.

Usar federação de identidade

O uso da federação de identidades agiliza a configuração de grupos e usuários e permite que os usuários façam login no StorageGRID usando credenciais familiares.

Configurar federação de identidade para o Grid Manager

Você pode configurar a federação de identidade no Grid Manager se quiser que grupos de administradores e usuários sejam gerenciados em outro sistema, como Active Directory, Azure Active Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Antes de começar

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



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

- Se você planeja usar o OpenLDAP, deverá configurar o servidor OpenLDAP. Ver [Diretrizes para configurar um servidor OpenLDAP](#) .
- Se você planeja habilitar o logon único (SSO), você revisou o ["requisitos e considerações para logon único"](#) .
- Se você planeja usar o Transport Layer Security (TLS) para comunicações com o servidor LDAP, o provedor de identidade está usando o TLS 1.2 ou 1.3. Ver ["Cifras suportadas para conexões TLS de saída"](#) .

Sobre esta tarefa

Você pode configurar uma fonte de identidade para o Grid Manager se quiser importar grupos de outro sistema, como Active Directory, Azure AD, 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 Grid Manager e executar tarefas com base nas permissões de gerenciamento atribuídas ao grupo.
- Grupos de usuários locatários para locatários que não usam sua própria fonte de identidade. Usuários em grupos de locatários podem entrar no Gerenciador de Locatários e executar tarefas com base nas permissões atribuídas ao grupo no Gerenciador de Locatários. Ver ["Criar conta de inquilino"](#) e ["Use uma conta de inquilino"](#) para mais detalhes.

Digite a configuração

Passos

1. Selecione **CONFIGURAÇÃO > Controle de acesso > Federação de identidade**.
2. Selecione **Ativar federação de identidade**.
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

Azure

OpenLDAP

Other

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

4. Se você selecionou **Outro**, preencha os campos na seção Atributos LDAP. Caso contrário, vá para a próxima etapa.
 - **Nome exclusivo do usuário:** O nome do atributo que contém o identificador exclusivo de um usuário LDAP. Este atributo é equivalente a `sAMAccountName` para o 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 exclusivo permanente de um usuário LDAP. Este atributo é equivalente a `objectGUID` para o Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando o 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 hifens são ignorados.
 - **Nome exclusivo do grupo:** O nome do atributo que contém o identificador exclusivo de um grupo LDAP. Este atributo é equivalente a `sAMAccountName` para o Active Directory e `cn` para OpenLDAP. Se você estiver configurando o Oracle Directory Server, insira `cn`.
 - **UUID do grupo:** O nome do atributo que contém o identificador exclusivo permanente de um grupo LDAP. Este atributo é equivalente a `objectGUID` para o Active Directory e `entryUUID` para OpenLDAP. Se você estiver configurando o 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 hifens 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 nome de 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 distinto (DN) do usuário que se conectará ao servidor LDAP.

Para o Active Directory, você também pode especificar o Nome de logon de nível inferior ou o Nome principal do usuário.

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

- `sAMAccountName` ou `uid`
- `objectGUID`, `entryUUID`, ou `nsuniqueid`

- `cn`
 - `memberOf`ou `isMemberOf`
 - **Active Directory:** `objectSid`, `primaryGroupID`, `userAccountControl`, e `userPrincipalName`
 - **Azul:** `accountEnabled` e `userPrincipalName`
- **Senha:** A senha associada ao nome de usuário.



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

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



Os valores de **Nome exclusivo do grupo** devem ser exclusivos dentro do **DN base do grupo** ao qual pertencem.

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



Os valores de **Nome exclusivo do usuário** devem ser exclusivos dentro do **DN base do usuário** ao qual pertencem.

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

É recomendável fornecer o **formato de nome de usuário de associação** porque ele pode permitir que os usuários efetuem login caso o StorageGRID não consiga se associar à conta de serviço.

Insira um destes padrões:

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

Inclua **[USERNAME]** exatamente como escrito.

6. Na seção Segurança da Camada de Transporte (TLS), selecione uma configuração de segurança.

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



O uso da opção **Não usar TLS** não é suportado se o seu servidor Active Directory impõe 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 conexões.
 - **Usar certificado CA personalizado:** Use um certificado de segurança personalizado.

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

Teste a conexão e salve a configuração

Depois de inserir todos os valores, você deve testar a conexão antes de salvar a configuração. O StorageGRID verifica as configurações de conexão do servidor LDAP e o formato do nome de usuário de vinculação, se você forneceu um.

Passos

1. Selecione **Testar conexão**.
2. Se você não forneceu um formato de nome de usuário de vinculação:
 - A mensagem "Teste de conexão bem-sucedido" será exibida se as configurações de conexão forem válidas. Selecione **Salvar** para salvar a configuração.
 - A mensagem "não foi possível estabelecer a conexão de teste" aparece 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 vinculado, insira o nome de usuário e a senha de um usuário federado válido.

Por exemplo, digite seu próprio nome de usuário e senha. Não inclua nenhum caractere especial 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](#)

- A mensagem "Teste de conexão bem-sucedido" será 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 a senha de teste forem inválidos. Resolva quaisquer problemas e teste a conexão novamente.

Forçar sincronização com a fonte de identidade

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

Passos

1. Acesse a página da Federação de Identidade.
2. Selecione **Servidor de sincronização** no topo da página.

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



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

Desabilitar federação de identidade

Você pode desabilitar temporária ou permanentemente a federação de identidade para grupos e usuários. Quando a federação de identidade está desabilitada, não há comunicação entre o StorageGRID e a origem da identidade. No entanto, todas as configurações que você definiu serão mantidas, permitindo que você reative facilmente a federação de identidades no futuro.

Sobre esta tarefa

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

- Usuários federados não poderão fazer login.
- Usuários federados que estão conectados no momento manterão acesso ao sistema StorageGRID até que sua sessão expire, mas não poderão fazer login depois que sua sessão expirar.
- A sincronização entre o sistema StorageGRID e a fonte de identidade não ocorrerá, e alertas não serão gerados para contas que não foram sincronizadas.
- A caixa de seleção **Habilitar federação de identidade** será desabilitada se o logon único (SSO) estiver definido como **Habilitado** ou **Modo Sandbox**. O status do SSO na página de logon único deve ser **Desativado** antes que você possa desabilitar a federação de identidades. Ver "[Desativar logon único](#)".

Passos

1. Acesse a página da Federação de Identidade.
2. Desmarque a caixa de seleção **Ativar federação de identidade**.

Diretrizes para configurar um servidor OpenLDAP

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



Para fontes de identidade que não sejam ActiveDirectory ou Azure, o StorageGRID não bloqueará automaticamente o acesso ao S3 para usuários desabilitados externamente. Para bloquear o acesso ao S3, exclua todas as chaves S3 do usuário ou remova o usuário de todos os grupos.

Sobreposições de membro e reintegração

As sobreposições memberof e refint devem ser habilitadas. Para obter mais informações, consulte as instruções para manutenção de associação de grupo reverso no <http://www.openldap.org/doc/admin24/index.html> ["Documentação do OpenLDAP: Guia do Administrador da Versão 2.4"] .

Indexação

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

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

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

Veja as informações sobre manutenção de associação de grupo reverso no <http://www.openldap.org/doc/admin24/index.html> ["Documentação do OpenLDAP: Guia do Administrador da Versão 2.4"] .

Gerenciar grupos de administradores

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

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)" .
- Você tem "[permissões de acesso específicas](#)" .
- Se você planeja importar um grupo federado, você configurou a federação de identidade 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 Grid Manager e na Grid Management API.

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 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 pode atualizar posteriormente, conforme necessário. Por exemplo, "Usuários de Manutenção" ou "Administradores de ILM".
3. Digite um nome exclusivo para o grupo, que você não poderá atualizar posteriormente.
4. Selecione **Continuar**.

Grupo federado

Passos

1. Selecione **Grupo federado**.
2. Digite o nome do grupo que você deseja importar, exatamente como ele aparece na fonte de identidade configurada.
 - Para o Active Directory e o Azure, use o sAMAccountName.
 - Para OpenLDAP, use o CN (Nome Comum).
 - Para outro LDAP, use o nome exclusivo apropriado para o servidor LDAP.
3. Selecione **Continuar**.

Gerenciar permissões de grupo

Passos

1. Para **Modo de acesso**, selecione se os usuários do grupo podem alterar as configurações e executar operações no Grid Manager e na Grid Management API ou se eles podem apenas visualizar as configurações e os 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 configurações e recursos. Eles não podem fazer nenhuma alteração ou executar nenhuma operação no Grid Manager ou na Grid Management API. Usuários locais somente leitura podem alterar suas próprias senhas.



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

2. Selecione um ou mais "[permissões do grupo de administração](#)".

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 você estiver criando um grupo local, selecione **Continuar**. Se você 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, você pode salvar o grupo sem adicionar usuários. Você pode adicionar este grupo ao usuário na página Usuários. Ver "[Gerenciar usuários](#)" para mais detalhes.

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

Ver e editar grupos de administradores

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

- Para visualizar informações básicas de todos os grupos, revise a tabela na página Grupos.
- 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. Marque a caixa de seleção do grupo. b. Selecione Ações > Exibir detalhes do grupo .	Selecione o nome do grupo na tabela.
Editar nome de exibição (somente grupos locais)	a. Marque a caixa de seleção do grupo. b. Selecione Ações > Editar nome do grupo . c. Digite o novo nome. d. Selecione Salvar alterações .	a. Selecione o nome do grupo para exibir os detalhes. b. Selecione o ícone de edição  . c. Digite o novo nome. d. Selecione Salvar alterações .
Editar modo de acesso ou permissões	a. Marque a caixa de seleção do grupo. b. Selecione Ações > Exibir detalhes do grupo . c. Opcionalmente, altere o Modo de acesso do grupo. d. Opcionalmente, selecione ou desmarque " permissões do grupo de administração ". e. Selecione Salvar alterações .	a. Selecione o nome do grupo para exibir os detalhes. b. Opcionalmente, altere o Modo de acesso do grupo. c. Opcionalmente, selecione ou desmarque " permissões do grupo de administração ". d. Selecione Salvar alterações .

Duplicar um grupo

Passos

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

Excluir um grupo

Você pode excluir um grupo de administradores quando quiser removê-lo 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 Grupos, marque a caixa de seleção de cada grupo que deseja remover.
2. Selecione **Ações > Excluir grupo**.
3. Selecione **Excluir grupos**.

Permissões do grupo de administração

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

- Sign in no Grid Manager
- Ver o painel
- Ver as páginas dos nós
- Ver alertas atuais e resolvidos
- Alterar sua própria senha (somente usuários locais)
- Veja certas 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 as configurações e executar operações ou se eles podem apenas visualizar as configurações e os recursos relacionados. Se um usuário pertencer a vários grupos e qualquer grupo estiver definido como **Somente leitura**, o usuário terá acesso somente leitura a todas as configurações e recursos selecionados.

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

Acesso root

Esta permissão fornece acesso a todos os recursos de administração da grade.

Alterar senha raiz do locatário

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



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

Configuração da página de topologia de grade

Esta permissão fornece acesso às guias Configuração na página **SUPORTE > Ferramentas > Topologia de grade**.



A página de topologia de grade foi descontinuada e será removida em uma versão futura.

ILM

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

- Regras
- Políticas
- Tags de política
- Pools de armazenamento
- Graus de armazenamento
- Regiões
- Pesquisa de metadados de objetos



Os usuários devem ter as permissões **Outra configuração de grade** e **Configuração da página de topologia de grade** para gerenciar níveis de armazenamento.

Manutenção

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

- **CONFIGURAÇÃO > Controle de acesso:**
 - Senhas de grade
- **CONFIGURAÇÃO > Rede:**
 - Nomes de domínio de endpoint S3
- **MANUTENÇÃO > Tarefas:**
 - Descomissionamento
 - Expansão
 - Verificação de existência de objeto
 - Recuperação
- **MANUTENÇÃO > Sistema:**

- Pacote de recuperação
- Atualização de software
- **SUPORTE > Ferramentas:**
 - Registros

Usuários que não têm permissão de Manutenção podem visualizar, mas não editar, estas páginas:

- **MANUTENÇÃO > Rede:**
 - Servidores DNS
 - Rede de grade
 - 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

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

Consulta de métricas

Esta permissão fornece acesso a:

- **SUPORTE > Ferramentas > página Métricas**
- Consultas de métricas personalizadas do Prometheus usando a seção **Métricas** da API de gerenciamento de grade
- Cartões do painel do Grid Manager que contêm métricas

Pesquisa de metadados de objetos

Esta permissão fornece acesso à página **ILM > Consulta de metadados do objeto**.

Outra configuração de grade

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



Para ver essas opções adicionais, os usuários também devem ter a permissão **Configuração da página de topologia de grade**.

- **ILM:**

- Graus de armazenamento
- **CONFIGURAÇÃO > Sistema:**
- **SUORTE > Outros:**
 - Custo do link

Administrador do dispositivo de armazenamento

Esta permissão fornece:

- Acesso ao E-Series SANtricity System Manager em dispositivos de armazenamento por meio do Grid Manager.
- A capacidade de executar tarefas de solução de problemas e manutenção na guia Gerenciar unidades para dispositivos que oferecem suporte a essas operações.

Contas de inquilinos

Esta permissão fornece a capacidade de:

- Acesse a página de inquilinos, onde você pode criar, editar e remover contas de inquilinos
- Ver políticas de classificação de tráfego existentes
- Exibir cartões do painel do Grid Manager que contêm detalhes do locatário

Gerenciar usuários

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

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da 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 pode criar somente usuários locais. Use a fonte de identidade externa para gerenciar usuários e grupos federados.

O Grid Manager inclui um usuário local predefinido, chamado "root". Você não pode remover o usuário root.



Se o logon único (SSO) estiver habilitado, 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. Digite o nome completo do usuário, um nome de usuário exclusivo e uma senha.
2. Opcionalmente, selecione **Sim** se este usuário não quiser ter acesso ao Grid Manager ou à Grid Management API.
3. Selecione **Continuar**.

Atribuir a grupos

Passos

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

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. Ver "[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 ao grupo. Você também pode impedir temporariamente que um usuário acesse o Grid Manager e a Grid Management API.

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

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

Todas as edições serão aplicadas na próxima vez que o usuário sair e entrar novamente no Grid Manager.



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. Marque a caixa de seleção para o usuário. b. Selecione Ações > Exibir detalhes do usuário .	Selecione o nome do usuário na tabela.

Tarefa	Menu de ações	Página de detalhes
Editar nome completo (somente usuários locais)	a. Marque a caixa de seleção para o usuário. b. Selecione Ações > Editar nome completo. c. Digite o novo nome. d. Selecione Salvar alterações.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione o ícone de edição . c. Digite o novo nome. d. Selecione Salvar alterações.
Negar ou permitir acesso ao StorageGRID	a. Marque a caixa de seleção para o usuário. b. Selecione Ações > Exibir detalhes do usuário. c. Selecione a aba 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 Salvar alterações.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a aba 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 Salvar alterações.
Alterar senha (somente usuários locais)	a. Marque a caixa de seleção para o usuário. b. Selecione Ações > Exibir detalhes do usuário. c. Selecione a aba Senha. d. Digite uma nova senha. e. Selecione Alterar senha.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a aba Senha. c. Digite uma nova senha. d. Selecione Alterar senha.
Alterar grupos (somente usuários locais)	a. Marque a caixa de seleção para o usuário. b. Selecione Ações > Exibir detalhes do usuário. c. Selecione a aba 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 Salvar alterações.	a. Selecione o nome do usuário para exibir os detalhes. b. Selecione a aba 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 Salvar alterações.

Duplicar um usuário

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

Passos

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

Excluir um usuário

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



Você não pode excluir o usuário root.

Passos

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

Use o logon único (SSO)

Configurar logon único

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

Como funciona o logon único

O sistema StorageGRID oferece suporte ao logon único (SSO) usando o padrão Security Assertion Markup Language 2.0 (SAML 2.0).

Antes de habilitar o logon único (SSO), revise como os processos de login e logout do StorageGRID são afetados quando o SSO está habilitado.

Sign in quando o SSO estiver habilitado

Quando o SSO estiver habilitado e você fizer login no StorageGRID, você será redirecionado para a página SSO da sua organização para validar suas credenciais.

Passos

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

A página de Sign in do StorageGRID é exibida.

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



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- Se você já acessou o Grid Manager ou o Tenant Manager, será solicitado que você selecione uma conta recente ou insira um ID de conta:



Tenant Manager

Recent

Account

Sign in

[NetApp support](#) | [NetApp.com](#)



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

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

- Para acessar o Grid Manager, deixe o campo **ID da conta** em branco, digite **0** como ID da conta 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*

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

Sign in with your organizational account

someone@example.com

Password

Sign in

4. Sign in com suas credenciais de SSO.

Se suas credenciais de SSO estiverem corretas:

- O provedor de identidade (IdP) fornece uma resposta de autenticação ao StorageGRID.
- O StorageGRID valida a resposta de autenticação.
- Se a resposta for válida e você pertencer a um grupo federado com permissões de acesso ao StorageGRID, você será conectado ao Grid Manager ou ao Tenant Manager, dependendo da conta selecionada.



Se a conta de serviço estiver 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, se você tiver permissões adequadas.

Você não precisa inserir novamente suas credenciais de SSO.

Sair quando o SSO estiver habilitado

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

Passos

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

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

Se você estiver conectado a...	E você sai de...	Você está desconectado 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 Azure para SSO, poderá levar alguns minutos para sair de todos os nós de administração.
Gerenciador de locatários em um ou mais nós administrativos	Gerenciador de inquilinos em qualquer nó de administração	Gerenciador de inquilinos em todos os nós administrativos
Tanto o Grid Manager quanto o Tenant Manager	Gerenciador de grade	Somente o Grid Manager. Você também deve sair do Gerenciador de Locatários para sair do SSO.



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

Requisitos e considerações para logon único

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

Requisitos do provedor de identidade

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

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

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

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Diretório ativo	• Diretório ativo • Azul • PingFederate
Azul	Azul

Requisitos do AD FS

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

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



O Windows Server 2016 deve estar usando o ["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 o Azure

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

Requisitos de certificado do servidor

Por padrão, o StorageGRID usa um certificado de interface de gerenciamento em cada nó de administração para proteger o acesso ao Grid Manager, ao Tenant Manager, à Grid Management API e à Tenant Management API. Ao configurar relações de confiança de terceira parte confiável (AD FS), aplicativos empresariais (Azure) ou conexões de provedor de serviços (PingFederate) para o StorageGRID, você usa o certificado do servidor como o certificado de assinatura para solicitações do StorageGRID .

Se você ainda não o fez ["configurou um certificado personalizado para a interface de gerenciamento"](#) , você deve fazer isso agora. Quando você instala um certificado de servidor personalizado, ele é usado para todos os nós de administração e você pode usá-lo em todos os trusts de terceiros confiáveis do StorageGRID , aplicativos empresariais ou conexões SP .



Não é recomendado usar o certificado de servidor padrão de um nó de administração em uma conexão de confiança de terceira parte, aplicativo empresarial ou SP . Se o nó falhar e você recuperá-lo, um novo certificado de servidor padrão será gerado. Antes de poder fazer login no nó recuperado, você deve atualizar a confiança da parte confiável, o aplicativo empresarial ou a conexão SP com o novo certificado.

Você pode acessar o certificado do servidor de um nó de administração efetuando login no shell de comando

do nó e indo para `/var/local/mgmt-api` diretório. Um certificado de servidor personalizado é denominado `custom-server.crt`. O certificado do servidor padrão do nó é denominado `server.crt`.

Requisitos portuários

O logon 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 logon único. Ver ["Controle de acesso em firewall externo"](#).

Confirme se os usuários federados podem fazer login

Antes de habilitar o logon único (SSO), você deve confirmar se pelo menos um usuário federado pode fazer login no Grid Manager e no Tenant Manager para qualquer conta de locatário existente.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Você já configurou a federação de identidade.

Passos

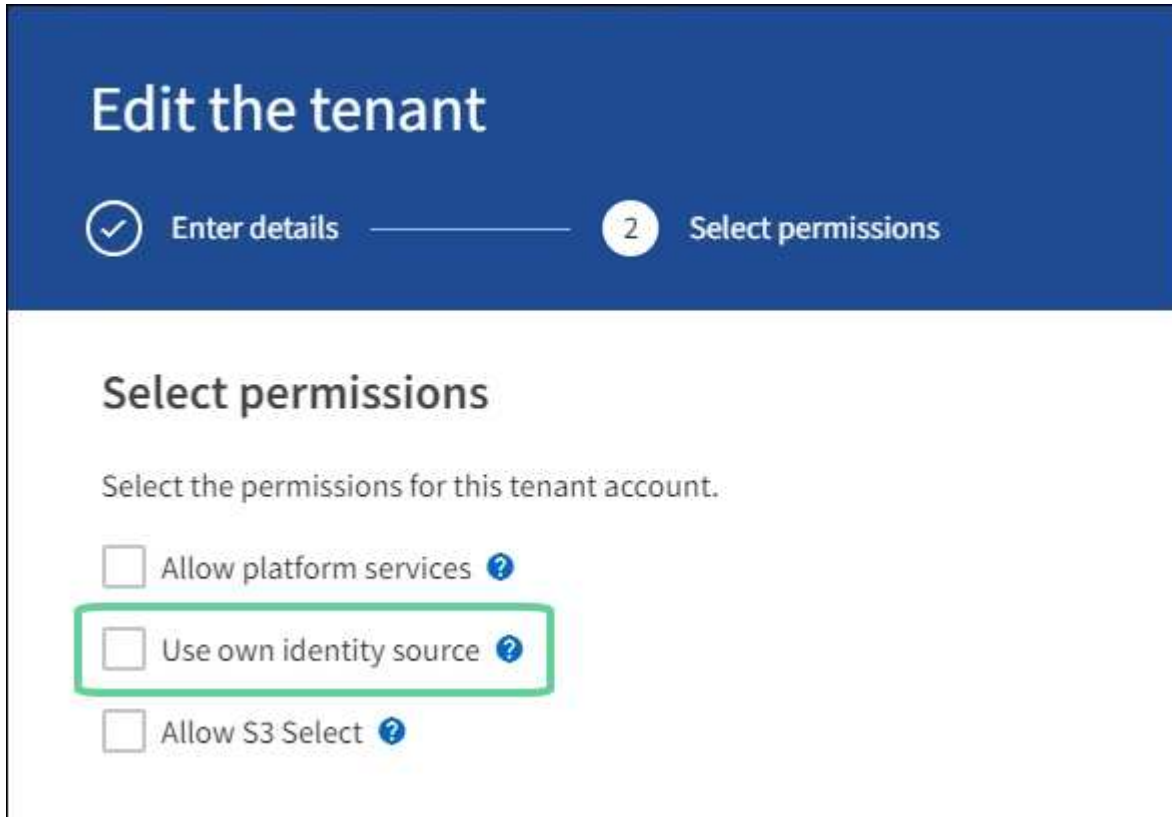
1. Se houver contas de locatários existentes, confirme se nenhum deles está usando sua própria fonte de identidade.



Quando você habilita o SSO, uma fonte de identidade configurada no Tenant Manager é substituída pela fonte de identidade configurada no Grid Manager. Os usuários pertencentes à fonte de identidade do locatário não poderão mais fazer login, a menos que tenham uma conta com a fonte de identidade do Grid Manager.

- a. Sign in no Gerenciador de Inquilinos para cada conta de inquilino.
 - b. Selecione **GERENCIAMENTO DE ACESSO > Federação de identidade**.
 - c. Confirme se a caixa de seleção **Ativar federação de identidade** não está marcada.
 - d. Se for o caso, confirme se quaisquer 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 tenha recebido a permissão de acesso Root.
 - c. Sair.
 - d. Confirme se você pode fazer login novamente no Grid Manager como um usuário no grupo federado.
 3. Se houver contas de locatário existentes, confirme se um usuário federado com permissão de acesso Root pode fazer login:
 - a. No Grid Manager, selecione **LOCATÁRIOS**.
 - 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 caixa e selecione **Salvar**.



The screenshot shows a web interface titled "Edit the tenant". At the top, there is a progress bar with two steps: "Enter details" (marked with a checkmark) and "2 Select permissions" (marked with a circle containing the number 2). Below the progress bar, the section is titled "Select permissions" with the instruction "Select the permissions for this tenant account." There are three checkboxes listed: "Allow platform services" with a question mark icon, "Use own identity source" with a question mark icon (this checkbox is highlighted with a green rectangular box), and "Allow S3 Select" with a question mark icon.

A página do inquilino é exibida.

- Selecione a conta do locatário, selecione * Sign in* e entre na conta do locatário como usuário root local.
- No Gerenciador de inquilinos, selecione **GERENCIAMENTO DE ACESSO > Grupos**.
- Certifique-se de que pelo menos um grupo federado do Grid Manager tenha recebido a permissão de acesso Root para este locatário.
- Sair.
- Confirme se você pode fazer login novamente no locatário como um usuário no grupo federado.

Informações relacionadas

- ["Requisitos e considerações para logon único"](#)
- ["Gerenciar grupos de administradores"](#)
- ["Use uma conta de inquilino"](#)

Usar o modo sandbox

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

Antes de começar

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

Tipo de serviço LDAP configurado	Opções para provedor de identidade SSO
Diretório ativo	• Diretório ativo • Azul • PingFederate
Azul	Azul

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

- A resposta do Active Directory ou PingFederate inclui um identificador universalmente exclusivo (UUID) para o usuário.
- A resposta do Azure inclui um Nome Principal do Usuário (UPN).

Para permitir que o StorageGRID (o provedor de serviços) e o provedor de identidade SSO se comuniquem com segurança sobre solicitações de autenticação do usuário, você deve configurar determinadas configurações no StorageGRID. Em seguida, você deve usar o software do provedor de identidade SSO para criar uma parte confiável (AD FS), aplicativo empresarial (Azure) ou provedor de serviços (PingFederate) para cada nó de administração. Por fim, você deve retornar ao StorageGRID para habilitar o SSO.

O modo sandbox facilita a execução dessa configuração de ida e volta e o teste de todas as suas configurações antes de habilitar o SSO. Quando você usa o modo sandbox, os usuários não conseguem fazer login usando SSO.

Acessar o modo sandbox

Passos

1. Selecione **CONFIGURAÇÃO > Controle de acesso > Logon único**.

A página de logon único é exibida, com a opção **Desativado** selecionada.

Single Sign-on

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

SSO status ⓘ ☒ Disabled ☐ Sandbox Mode ☐ Enabled

Save



Se as opções de Status do SSO não aparecerem, confirme se você configurou o provedor de identidade como a fonte de identidade federada. Ver "[Requisitos e considerações para login único](#)".

2. Selecione **Modo Sandbox**.

A seção Provedor de Identidade é exibida.

Insira os detalhes do provedor de identidade

Passos

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

Diretório ativo

- a. Insira o **Nome do serviço de federação** para o provedor de identidade, exatamente como ele aparece no Serviço de Federação do Active Directory (AD FS).



Para localizar o nome do serviço de federação, acesse o Gerenciador do Windows Server. Selecione **Ferramentas > Gerenciamento do AD FS**. No menu Ação, selecione **Editar propriedades do serviço de federação**. O nome do serviço da federação é mostrado no segundo campo.

- b. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração de 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 esta configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **Certificado CA**.

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



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

- c. Na seção Parte Confiável, especifique o **Identificador da parte confiável** para StorageGRID. Este valor controla o nome que você usa para cada parte confiável no AD FS.

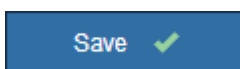
- Por exemplo, se sua grade tiver apenas um nó de administração e você não pretende adicionar mais nós de administração no futuro, insira `SG` ou `StorageGRID` .
- Se sua grade incluir mais de um nó de administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]` . Isso gera uma tabela que mostra o identificador da parte confiável para cada nó de administração no seu sistema, com base no nome do host do nó.



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

- d. Selecione **Salvar**.

Uma marca de seleção verde aparece no botão **Salvar** por alguns segundos.



Azul

- a. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração de 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 esta configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **Certificado CA**.

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



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

- b. Na seção Aplicativo Corporativo, especifique o **Nome do aplicativo corporativo** para StorageGRID. Este valor controla o nome que você usa para cada aplicativo empresarial no Azure AD.

- Por exemplo, se sua grade tiver apenas um nó de administração e você não pretende adicionar mais nós de administração no futuro, insira `SG` ou `StorageGRID`.
- Se sua grade incluir mais de um nó de administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Isso gera uma tabela que mostra um nome de aplicativo corporativo para cada nó de administração no seu sistema, com base no nome do host do nó.



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

- c. Siga os passos em ["Crie aplicativos corporativos no Azure AD"](#) para criar um aplicativo corporativo para cada nó administrativo listado na tabela.
- d. No Azure AD, copie a URL de metadados da federação para cada aplicativo empresarial. Em seguida, cole esta URL no campo **URL de metadados da federação** correspondente no StorageGRID.
- e. Depois de copiar e colar uma URL de metadados de federação para todos os nós de administração, selecione **Salvar**.

Uma marca de seleção verde aparece no botão **Salvar** por alguns segundos.



PingFederate

- a. Especifique qual certificado TLS será usado para proteger a conexão quando o provedor de identidade enviar informações de configuração de 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 esta configuração, copie o texto do certificado personalizado e cole-o na caixa de texto **Certificado CA**.

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



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

- b. Na seção Provedor de serviços (SP), especifique o * ID de conexão do SP * para StorageGRID. Este valor controla o nome que você usa para cada conexão SP no PingFederate.

- Por exemplo, se sua grade tiver apenas um nó de administração e você não pretende adicionar mais nós de administração no futuro, insira `SG` ou `StorageGRID`.
- Se sua grade incluir mais de um nó de administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]`. Isso gera uma tabela que mostra o ID de conexão do SP para cada nó de administração no seu sistema, com base no nome do host 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 entrar e sair com segurança de qualquer nó de administração.

- c. Especifique a URL de metadados da federação para cada nó administrativo no campo **URL de metadados da federação**.

Use o seguinte formato:

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

- d. Selecione **Salvar**.

Uma marca de seleção verde aparece no botão **Salvar** por alguns segundos.

Save ✓

Configurar trusts de terceira parte confiável, aplicativos corporativos ou conexões SP

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

O StorageGRID pode permanecer no modo sandbox pelo tempo que for necessário. No entanto, quando o **Modo Sandbox** é selecionado na página de logon único, o SSO é desabilitado para todos os usuários do StorageGRID. Somente usuários locais podem fazer login.

Siga estas etapas para configurar confiança de partes confiáveis (Active Directory), aplicativos empresariais completos (Azure) ou configurar conexões SP (PingFederate).

Diretório ativo

Passos

1. Acesse os Serviços de Federação do Active Directory (AD FS).
2. Crie um ou mais trusts de parte confiável para o StorageGRID, usando cada identificador de parte confiável mostrado na tabela na página de logon único do StorageGRID .

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

Para obter instruções, acesse ["Criar relações de confiança de terceira parte confiável no AD FS"](#) .

Azul

Passos

1. Na página de logon único do nó de administração no qual você está conectado no momento, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para quaisquer outros nós de administração na sua grade, repita estas etapas:
 - a. Sign in no nó.
 - b. Selecione **CONFIGURAÇÃO > Controle de acesso > Logon único**.
 - c. Baixe e salve os metadados SAML para esse nó.
3. Acesse o Portal do Azure.
4. Siga os passos em ["Crie aplicativos corporativos no Azure AD"](#) para carregar o arquivo de metadados SAML para cada nó de administração em seu aplicativo empresarial do Azure correspondente.

PingFederate

Passos

1. Na página de logon único do nó de administração no qual você está conectado no momento, selecione o botão para baixar e salvar os metadados SAML.
2. Em seguida, para quaisquer outros nós de administração na sua grade, repita estas etapas:
 - a. Sign in no nó.
 - b. Selecione **CONFIGURAÇÃO > Controle de acesso > Logon único**.
 - c. Baixe e salve os metadados SAML para esse nó.
3. Acesse PingFederate.
4. ["Crie uma ou mais conexões de provedor de serviços \(SP\) para StorageGRID"](#) . Use o ID de conexão SP para cada nó de administração (mostrado na tabela na página de logon único do StorageGRID) 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 conexões SSO

Antes de impor o uso do logon único para todo o seu sistema StorageGRID , você deve confirmar se o logon único e o logout único estão configurados corretamente para cada nó de administração.

Diretório ativo

Passos

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

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

Sandbox mode

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

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

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

2. Selecione o link ou copie e cole o URL em um navegador para acessar a página de login do seu provedor de identidade.
3. Para confirmar que você pode usar o SSO para fazer login no StorageGRID, selecione * Sign in em um dos seguintes sites*, selecione o identificador de parte confiável para seu nó de administração principal e selecione * Sign in*.

You are not signed in.

☐ Sign in to this site.

☒ Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

4. Digite seu nome de usuário e senha federados.

- Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.

✓ Single sign-on authentication and logout test completed successfully.

- Se a operação SSO não for bem-sucedida, uma mensagem de erro será exibida. Resolva o problema, limpe os cookies do navegador e tente novamente.

5. Repita essas etapas para verificar a conexão SSO para cada nó de administração na sua grade.

Azul

Passos

1. Acesse a página de login único no portal do Azure.
2. Selecione **Testar este aplicativo**.
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.

✓ Single sign-on authentication and logout test completed successfully.

- Se a operação SSO não for bem-sucedida, uma mensagem de erro será exibida. Resolva o problema, limpe os cookies do navegador e tente novamente.
4. Repita essas etapas para verificar a conexão SSO para cada nó de administração na sua grade.

PingFederate

Passos

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

Selecione e teste um link por vez.

Sandbox mode

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

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

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

2. Insira as credenciais de um usuário federado.
 - Se as operações de login e logout do SSO forem bem-sucedidas, uma mensagem de sucesso será exibida.
- ✓ Single sign-on authentication and logout test completed successfully.
- Se a operação SSO não for bem-sucedida, uma mensagem de erro será exibida. Resolva o problema, limpe os cookies do navegador e tente novamente.
3. Selecione o próximo link para verificar a conexão SSO para cada nó de administração na sua grade.

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

Habilitar logon único

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



Quando o SSO estiver habilitado, todos os usuários deverão 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 o StorageGRID.

Passos

1. Selecione **CONFIGURAÇÃO > Controle de acesso > Logon único**.
2. Altere o status do SSO para **Habilitado**.
3. Selecione **Salvar**.
4. Revise a mensagem de aviso e selecione **OK**.

O logon único agora está habilitado.



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

Criar relações de confiança de terceira parte confiável no AD FS

Você deve usar os Serviços de Federação do Active Directory (AD FS) para criar uma parte confiável para cada nó de administração no seu sistema. Você pode criar trusts de terceira parte confiável usando comandos do PowerShell, importando metadados SAML do StorageGRID ou inserindo os dados manualmente.

Antes de começar

- Você configurou o logon único para o StorageGRID e selecionou **AD FS** como o tipo de SSO.
- O **modo sandbox** é selecionado na página de logon único no Grid Manager. Ver "[Usar o modo sandbox](#)".
- Você conhece o nome de domínio totalmente qualificado (ou o endereço IP) e o identificador da parte confiável para cada nó de administração no seu sistema. Você pode encontrar esses valores na tabela de detalhes dos Nós de administração na página de logon único do StorageGRID .



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

- Você tem experiência na criação de relações de confiança de partes confiáveis no AD FS ou tem acesso à documentação do Microsoft AD FS.
- Você está usando o snap-in Gerenciamento do AD FS e pertence ao grupo Administradores.
- Se você estiver criando a confiança da parte confiável manualmente, terá o certificado personalizado que foi carregado para a interface de gerenciamento do StorageGRID ou saberá como fazer login em um nó de administração a partir do shell de comando.

Sobre esta tarefa

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

Crie uma confiança de terceira parte confiável usando o Windows PowerShell

Você pode usar o Windows PowerShell para criar rapidamente uma ou mais relações de confiança de terceira parte confiável.

Passos

1. No menu Iniciar do Windows, selecione com o botão direito do mouse o 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 ele aparece na página de Logon Único. Por exemplo, SG-DC1-ADM1.
- Para *Admin_Node_FQDN*, insira o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)

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

A ferramenta de gerenciamento do AD FS é exibida.

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

A lista de trusts de partes confiáveis é exibida.

5. Adicione uma Política de Controle de Acesso à confiança da parte confiável recém-criada:
 - a. Localize a parte confiável que você acabou de criar.
 - b. Clique com o botão direito do mouse no trust 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 Reivindicações ao Trust de Parte Confiável recém-criado:
 - a. Localize a parte confiável que você acabou de criar.
 - b. Clique com o botão direito do mouse no trust e selecione **Editar política de emissão de reivindicações**.
 - 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 ID de nome** ou **UPN para ID de nome**.

- f. Para o Attribute Store, selecione **Active Directory**.
 - g. Na coluna Atributo LDAP da tabela Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.
 - h. Na coluna Tipo de reivindicação de saída da tabela Mapeamento, selecione **ID do nome** 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 parte confiável para abrir suas propriedades.
 - b. Confirme se os campos nas guias **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 essas etapas para configurar uma parte confiável para todos os nós de administração no seu sistema StorageGRID .
9. Quando terminar, retorne ao StorageGRID e teste todos os trusts de terceiros para confirmar se estão configurados corretamente. Ver "[Usar o modo Sandbox](#)" para obter instruções.

Crie uma parte confiável importando metadados da federação

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

Passos

1. No Gerenciador do Windows Server, selecione **Ferramentas** e, em seguida, selecione **Gerenciamento do AD FS**.
2. Em Ações, selecione **Adicionar confiança de terceira parte confiável**.
3. Na página de boas-vindas, escolha **Reivindicações cientes** e selecione **Iniciar**.
4. Selecione **Importar dados sobre a parte confiável publicados on-line ou em uma rede local**.
5. Em **Endereço de metadados da federação (nome do host ou URL)**, digite o local dos metadados SAML para este nó de administração:

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

Para *Admin_Node_FQDN*, insira o nome de domínio totalmente qualificado para o mesmo nó de administração. (Se necessário, você pode usar o endereço IP do nó. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)

6. Conclua o assistente de Relying Party Trust, salve o trust da parte confiável e feche o assistente.



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

7. Adicione uma regra de reivindicação:
- a. Clique com o botão direito do mouse no trust e selecione **Editar política de emissão de reivindicações**.

- 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 ID de nome** ou **UPN para ID de nome**.

- e. Para o Attribute Store, selecione **Active Directory**.
- f. Na coluna Atributo LDAP da tabela Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.
- g. Na coluna Tipo de reivindicação de saída da tabela Mapeamento, selecione **ID do nome** 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 parte confiável para abrir suas propriedades.
- b. Confirme se os campos nas guias **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 essas etapas para configurar uma parte confiável para todos os nós de administração no seu sistema StorageGRID .

10. Quando terminar, retorne ao StorageGRID e teste todos os trusts de terceiros para confirmar se estão configurados corretamente. Ver "[Usar o modo Sandbox](#)" para obter instruções.

Crie uma parte confiável manualmente

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

Passos

- 1. No Gerenciador do Windows Server, selecione **Ferramentas** e, em seguida, selecione **Gerenciamento do AD FS**.
- 2. Em Ações, selecione **Adicionar confiança de terceira parte confiável**.
- 3. Na página de boas-vindas, escolha **Reivindicações cientes** e selecione **Iniciar**.
- 4. Selecione **Inserir dados sobre a parte confiável manualmente** e selecione **Avançar**.
- 5. Conclua o assistente Relying Party Trust:

- a. Insira um nome de exibição para este nó de administração.

Para consistência, use o Identificador de Parte Confiável para o Nó de Administração, exatamente como ele aparece na página de Logon Único no Grid Manager. Por exemplo, SG-DC1-ADM1 .

- b. Ignore a etapa para configurar um certificado de criptografia de token opcional.
- c. Na página Configurar URL, marque a caixa de seleção **Ativar suporte para o protocolo SAML 2.0 WebSSO**.
- d. Digite a URL do ponto de extremidade do serviço SAML para o nó de administração:

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

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

- e. Na página Configurar Identificadores, especifique o Identificador de Parte Confiável para o mesmo Nó de Administração:

Admin_Node_Identifier

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

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

A caixa de diálogo Editar política de emissão de reivindicações é exibida.



Se a caixa de diálogo não aparecer, clique com o botão direito do mouse no trust e selecione **Editar política de emissão de reivindicações**.

6. Para iniciar o assistente de Regra 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 ID de nome** ou **UPN para ID de nome**.
 - c. Para o Attribute Store, selecione **Active Directory**.
 - d. Na coluna Atributo LDAP da tabela Mapeamento, digite **objectGUID** ou selecione **User-Principal-Name**.
 - e. Na coluna Tipo de reivindicação de saída da tabela Mapeamento, selecione **ID do nome** na lista suspensa.
 - f. Selecione **Concluir** e selecione **OK**.
7. Clique com o botão direito do mouse na parte confiável para abrir suas propriedades.
8. Na guia **Endpoints**, configure o endpoint para logout único (SLO):
 - a. Selecione **Adicionar SAML**.
 - b. Selecione **Tipo de endpoint > Logout SAML**.
 - c. Selecione **Vinculação > Redirecionamento**.
 - d. No campo **URL confiável**, insira a URL usada para logout único (SLO) deste nó de administração:

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

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. No entanto, se você inserir um endereço IP aqui, esteja ciente de que deverá atualizar ou recriar essa parte confiável se esse endereço IP mudar.)

a. Selecione **OK**.

9. Na aba **Assinatura**, especifique o certificado de assinatura para esta parte confiável:

a. Adicione o certificado personalizado:

- Se você tiver o certificado de gerenciamento personalizado que carregou no StorageGRID, selecione esse certificado.
- Se você não tiver o certificado personalizado, faça login no nó de administração, vá para `/var/local/mgmt-api` diretório do nó de administração e adicione o `custom-server.crt` arquivo de certificado.



Usando o certificado padrão do nó de administração(`server.crt`) não é recomendado. Se o nó de administração falhar, o certificado padrão será regenerado quando você recuperar o nó, e você precisará atualizar a confiança da parte confiável.

b. Selecione **Aplicar** e selecione **OK**.

As propriedades da Parte Confiável são salvas e fechadas.

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

11. Quando terminar, retorne ao StorageGRID e teste todos os trusts de terceiros para confirmar se estão configurados corretamente. Ver "[Usar o modo sandbox](#)" para obter instruções.

Crie aplicativos corporativos no Azure AD

Use o Azure AD para criar um aplicativo empresarial para cada nó de administração no seu sistema.

Antes de começar

- Você começou a configurar o logon único para o StorageGRID e selecionou **Azure** como o tipo de SSO.
- O **modo sandbox** é selecionado na página de logon único no Grid Manager. Ver "[Usar o modo sandbox](#)".
- Você tem o **Nome do aplicativo corporativo** para cada nó de administração no seu sistema. Você pode copiar esses valores da tabela de detalhes do nó de administração na página de logon único do StorageGRID .



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

- Você tem experiência na criação de aplicativos corporativos no Azure Active Directory.
- Você tem uma conta do Azure com uma assinatura ativa.
- Você tem uma das seguintes funções na conta do Azure: Administrador global, Administrador de aplicativos em nuvem, Administrador de aplicativos ou proprietário da entidade de serviço.

Acessar o Azure AD

Passos

1. Faça login no "[Portal do Azure](#)".

2. Navegar para "[Diretório Ativo do Azure](#)".
3. Selecione "[Aplicações empresariais](#)".

Crie aplicativos corporativos e salve a configuração do StorageGRID SSO

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

Passos

1. Repita as etapas a seguir para cada nó de administração.
 - a. No painel Aplicativos empresariais do Azure, selecione **Novo aplicativo**.
 - b. Selecione **Criar seu próprio aplicativo**.
 - c. Para o nome, insira o **Nome do aplicativo corporativo** que você copiou da tabela de detalhes do nó de administração na página de logon único do StorageGRID.
 - d. Deixe o botão de opção **Integrar qualquer outro aplicativo que você não encontrar na galeria (Não galeria)** selecionado.
 - e. Selecione **Criar**.
 - f. Selecione o link **Começar** em **2. Configure a caixa de logon único** ou selecione o link **Logon único** na margem esquerda.
 - g. Selecione a caixa **SAML**.
 - h. Copie o **App Federation Metadata URL**, que você pode encontrar em **Step 3 SAML Signing Certificate**.
 - i. Acesse a página de logon único do StorageGRID e cole a URL no campo **URL de metadados da federação** que corresponde ao **Nome do aplicativo corporativo** que você usou.
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 de logon único do StorageGRID.

Baixe metadados SAML para cada nó de administração

Depois que a configuração do SSO for salva, você poderá baixar um arquivo de metadados SAML para cada nó de administração no seu sistema StorageGRID.

Passos

1. Repita essas etapas para cada nó de administração.
 - a. Sign in no StorageGRID a partir do nó de administração.
 - b. Selecione **CONFIGURAÇÃO > Controle de acesso > Logon único**.
 - c. Selecione o botão para baixar os metadados SAML para esse nó de administração.
 - d. Salve o arquivo que você carregará no Azure AD.

Carregar metadados SAML para cada aplicativo empresarial

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

Passos

1. Retorne ao Portal do Azure.
2. Repita estas etapas para cada aplicativo corporativo:



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

- a. Acesse a página Propriedades do aplicativo empresarial.
 - b. Defina **Atribuição necessária** como **Não** (a menos que você queira configurar as atribuições separadamente).
 - c. Acesse 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 depois selecione **X** para fechar o painel. Você retornará à página Configurar logon único com SAML.
3. Siga os passos em "[Usar o modo sandbox](#)" para testar cada aplicação.

Criar conexões de provedor de serviços (SP) no PingFederate

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

Antes de começar

- Você configurou o logon único para o StorageGRID e selecionou **Ping Federate** como o tipo de SSO.
- O **modo sandbox** é selecionado na página de logon único no Grid Manager. Ver "[Usar o modo sandbox](#)".
- Você tem o * ID de conexão SP * para cada nó de administração no seu sistema. Você pode encontrar esses valores na tabela de detalhes dos Nós de administração na página de logon único do StorageGRID.
- Você baixou os **metadados SAML** para cada nó de administração no seu sistema.
- Você tem experiência na criação de conexões SP no PingFederate Server.
- Você tem https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html ["Guia de Referência do Administrador"] para o servidor PingFederate. A documentação do PingFederate fornece instruções e explicações detalhadas passo a passo.
- Você tem o "[Permissão de administrador](#)" para o servidor PingFederate.

Sobre esta tarefa

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

Pré-requisitos completos no PingFederate

Antes de criar as conexões SP que você usará para o StorageGRID, você deve concluir as tarefas de pré-requisito no PingFederate. Você usará 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 o PingFederate ao servidor LDAP do AD FS. Use os valores que você usou quando "[configurando federação de identidade](#)" em 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 credenciais de senha

Caso ainda não tenha feito isso, crie um validador de credenciais de senha.

- **Tipo:** LDAP Nome de usuário Senha Validador de credenciais
- **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. Vá para **Autenticação > Integração > Adaptadores IdP**.
2. Selecione **Criar nova instância**.
3. Na guia Tipo, selecione **Adaptador IdP de formulário HTML**.
4. Na guia Adaptador IdP, selecione **Adicionar uma nova linha para 'Validadores de credenciais'**.
5. Selecione o [validador de credenciais de senha](#) que você criou.
6. Na guia Atributos do adaptador, selecione o atributo **nome de usuário** para **Pseudônimo**.
7. Selecione **Salvar**.

Criar ou importar certificado de assinatura

Caso ainda não tenha feito isso, crie ou importe o certificado de assinatura.

Passos

1. Vá para **Segurança > Chaves e Certificados de Assinatura e Descriptografia**.
2. Crie ou importe o certificado de assinatura.

Crie uma conexão SP no PingFederate

Ao criar uma conexão SP no PingFederate, você importa os metadados SAML baixados do StorageGRID para o nó de administração. O arquivo de metadados contém muitos dos valores específicos 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 com segurança de qualquer nó. Use estas instruções para criar a primeira conexão SP . Então vá para [Criar conexões SP adicionais](#) para criar quaisquer conexões adicionais que você precisar.

Escolha o tipo de conexão SP

Passos

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

Importar metadados SP

Passos

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

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

4. Selecione **Avançar**.

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 *** SP-initiated SSO***, *** SP-initial SLO***, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selecione **Avançar**.
4. Na aba Assertion Lifetime, não faça alterações.
5. Na guia Criação de Asserção, selecione **Configurar Criação de Asserção**.
 - a. Na guia Mapeamento de Identidade, selecione **Padrão**.
 - 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 estender o contrato, selecione **Excluir** para remover o `urn:oid` , que não é usado.

Instância do adaptador de mapa

Passos

1. Na guia Mapeamento de fonte de autenticação, selecione **Mapear nova instância do adaptador**.
2. Na guia Instância do adaptador, selecione **o instância do adaptador** você criou.
3. Na guia Método de mapeamento, selecione **Recuperar atributos adicionais de um armazenamento de dados**.
4. Na guia Origem do atributo e pesquisa de usuário, selecione **Adicionar origem do atributo**.
5. Na guia Armazenamento de dados, forneça uma descrição e selecione **o armazenamento de dados** você adicionou.
6. Na guia Pesquisa de diretório LDAP:
 - Insira o **DN base**, que deve corresponder exatamente ao valor inserido 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 atributo binário LDAP, selecione **Base64** para o atributo **objectGUID**.
8. Na guia Filtro LDAP, digite **sAMAccountName=\${username}**.
9. Na guia Cumprimento de contrato de atributo, selecione **LDAP (atributo)** no menu suspenso Origem e selecione **objectGUID** ou **userPrincipalName** no menu suspenso Valor.
10. Revise e salve a origem do atributo.
11. Na guia Fonte do atributo Failsave, selecione **Abortar a transação SSO**.
12. Revise o resumo e selecione **Concluído**.
13. Selecione **Concluído**.

Configurar as definições do protocolo

Passos

1. Na guia * Conexão SP * > * SSO do navegador * > * Configurações do protocolo *, selecione * Definir configurações do protocolo *.
2. Na guia URL do serviço de consumidor de asserção, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**POST** para vinculação e `/api/saml-response` para URL do ponto de extremidade).
3. Na guia URLs do serviço SLO, aceite os valores padrão, que foram importados dos metadados SAML do StorageGRID (**REDIRECT** para vinculação e `/api/saml-logout` para URL do ponto de extremidade).
4. Na guia Ligações SAML permitidas, desmarque **ARTIFACT** e **SOAP**. Somente **POST** e **REDIRECT** são necessários.
5. Na guia Política de Assinatura, deixe as caixas de seleção **Exigir que as solicitações de autenticação sejam assinadas** e **Sempre assinar declaração** marcadas.
6. Na guia Política de Criptografia, selecione **Nenhum**.
7. Revise o resumo e selecione **Concluído** para salvar as configurações do protocolo.
8. Revise o resumo e selecione **Concluído** para salvar as configurações de SSO do navegador.

Configurar credenciais

Passos

1. Na guia Conexão SP , selecione **Credenciais**.
2. Na guia Credenciais, selecione **Configurar credenciais**.
3. Selecione o [certificado de assinatura](#) que você criou ou importou.
4. Selecione **Avançar** para ir para **Gerenciar configurações de verificação de assinatura**.
 - a. Na guia Modelo de confiança, selecione **Não ancorado**.
 - b. Na guia Certificado de verificação de assinatura, revise as informações do certificado de assinatura, que foram importadas dos metadados SAML do StorageGRID .
5. Revise 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 na sua grade. Você carrega novos metadados para cada cópia.



As conexões SP para diferentes nós administrativos 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. Selecione 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 **Avançar**.
 - d. Selecione **Salvar**.
4. Resolva o erro devido ao atributo não utilizado:
 - a. Selecione a nova conexão.
 - b. Selecione **Configurar SSO do navegador > Configurar criação de asserção > Contrato de atributo**.
 - c. Exclua a entrada para **urn:oid**.
 - d. Selecione **Salvar**.

Desativar logon único

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

Antes de começar

- Você está conectado ao Grid Manager usando um [navegador da web compatível](#) .

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

Passos

1. Selecione **CONFIGURAÇÃO > Controle de acesso > Logon único**.

A página de logon único é exibida.

2. Selecione a opção **Desativado**.
3. Selecione **Salvar**.

Uma mensagem de aviso aparece indicando que usuários locais agora poderão fazer login.

4. Selecione **OK**.

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

Desabilitar temporariamente e reabilitar o logon único para um nó de administração

Talvez você não consiga fazer login no Grid Manager se o sistema de logon único (SSO) ficar inativo. Nesse caso, você pode desabilitar temporariamente e reabilitar o SSO para um nó de administração. Para desabilitar e reabilitar o SSO, você deve acessar o shell de comando do nó.

Antes de começar

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

Sobre esta tarefa

Depois de desabilitar o SSO para um nó de administração, você pode entrar no Grid Manager como usuário root local. 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.



Desabilitar o SSO para um nó administrativo não afeta as configurações de SSO para nenhum outro nó administrativo na grade. A caixa de seleção **Habilitar SSO** na página Login Único no Grid Manager permanece selecionada, e todas as configurações de SSO existentes são mantidas, a menos que você as atualize.

Passos

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

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 nó de administração.

3. Confirme que você deseja desabilitar o SSO.

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

4. Em um navegador da Web, acesse o Grid Manager no mesmo nó de administração.

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

5. Sign in com o nome de usuário root e a senha do usuário root local.
6. Se você desativou o SSO temporariamente porque precisava corrigir a configuração do SSO:
 - a. Selecione **CONFIGURAÇÃO > Controle de acesso > Logon único**.
 - b. Altere as configurações de SSO incorretas ou desatualizadas.
 - c. Selecione **Salvar**.

Selecionar **Salvar** na página Login Único reativa automaticamente o SSO para toda a grade.

7. Se você desativou o SSO temporariamente porque precisava acessar o Grid Manager 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 qualquer uma das seguintes etapas:

- Execute o seguinte comando: `enable-saml`

Uma mensagem indica que o comando se aplica somente a este nó de administração.

Confirme que você deseja habilitar o SSO.

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

- Reinicie o nó da grade: `reboot`

8. Em um navegador da web, acesse o Grid Manager no mesmo nó de administração.
9. Confirme se a página de Sign in do StorageGRID aparece e se você deve inserir suas credenciais de SSO para acessar o Grid Manager.

Usar federação de grade

O que é federação de grade?

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

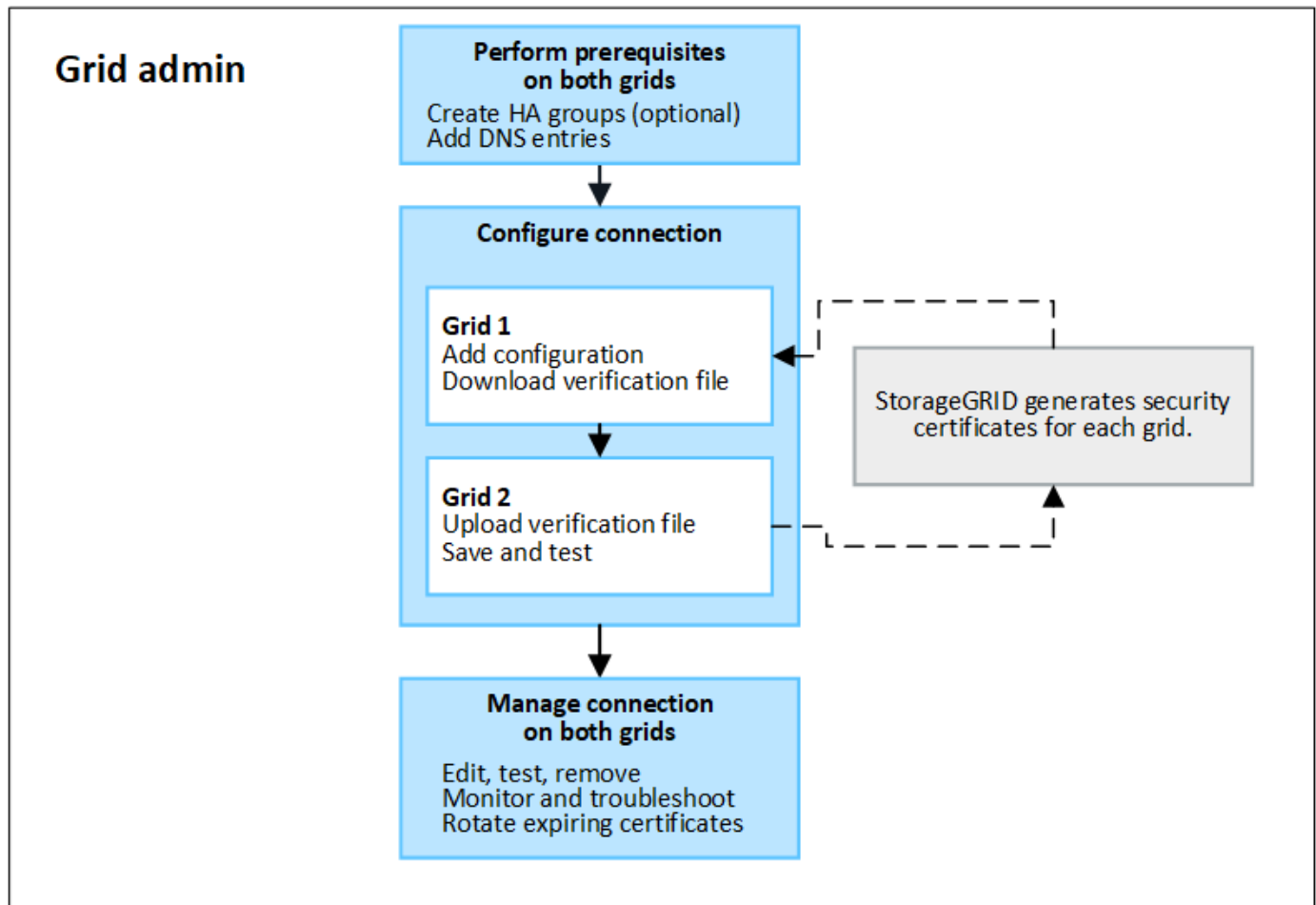
O que é uma conexão de federação de rede?

Uma conexão de federação de grade é uma conexão bidirecional, confiável e segura entre nós de

administração e gateway em dois sistemas StorageGRID .

Fluxo de trabalho para federação de grade

O diagrama de fluxo de trabalho resume as etapas para configurar uma conexão de federação de grade entre duas grades.



Considerações e requisitos para conexões de federação de rede

- As grades usadas para federação de grade devem executar versões do StorageGRID que sejam idênticas ou não tenham mais de uma diferença de versão principal entre elas.

Para obter detalhes sobre os requisitos de versão, consulte o ["Notas de lançamento"](#) .

- Uma grade pode ter uma ou mais conexões de federação de grade com outras grades. Cada conexão de federação de rede é independente de quaisquer outras conexões. Por exemplo, se a Grade 1 tiver uma conexão com a Grade 2 e uma segunda conexão com a Grade 3, não há conexão implícita entre a Grade 2 e a Grade 3.
- As conexões de federação de rede são bidirecionais. Depois que a conexão for estabelecida, você pode monitorar e gerenciar a conexão de qualquer uma das redes.
- Pelo menos uma conexão de federação de grade deve existir antes que você possa usar ["clone de conta"](#) ou ["replicação entre grades"](#) .

Requisitos de rede e endereço IP

- As conexões de federação de grade podem ocorrer na Rede de grade, na Rede de administração ou na Rede de cliente.
- Uma conexão de federação de rede conecta uma rede a outra. A configuração de cada grade especifica um ponto de extremidade de federação de grade na outra grade que consiste em nós de administração, nós de gateway ou ambos.
- A melhor prática é conectar "[grupos de alta disponibilidade \(HA\)](#)" de nós de gateway e de administração em cada grade. O uso de grupos HA ajuda a garantir que as conexões da federação de grade permanecerão online caso os nós fiquem indisponíveis. Se a interface ativa em qualquer grupo HA falhar, a conexão poderá usar uma interface de backup.
- Não é recomendado criar uma conexão de federação de grade que use o endereço IP de um único nó de administração ou nó de gateway. Se o nó ficar indisponível, a conexão da federação de rede também ficará indisponível.
- "[Replicação entre grades](#)" de objetos requer que os nós de armazenamento em cada grade sejam capazes de acessar os nós de administração e gateway configurados na outra grade. Para cada grade, confirme se todos os nós de armazenamento têm uma rota de alta largura de banda como nós de administração ou nós de gateway usados para a conexão.

Use FQDNs para balancear a carga da conexão

Para um ambiente de produção, use nomes de domínio totalmente qualificados (FQDNs) para identificar cada grade na conexão. Em seguida, crie as entradas DNS apropriadas, da seguinte forma:

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

Quando você usa várias entradas de DNS, as solicitações para usar a conexão são balanceadas de carga, da seguinte maneira:

- As entradas de DNS mapeadas para os endereços VIP de vários grupos HA são balanceadas de carga entre os nós ativos nos grupos HA.
- As entradas de DNS que mapeiam os endereços IP de vários nós de administração ou nós de gateway são balanceadas de carga entre os nós mapeados.

Requisitos portuários

Ao criar uma conexão de federação de grade, você pode especificar qualquer número de porta não utilizado de 23000 a 23999. Ambas as grades nesta conexão usarão a mesma porta.

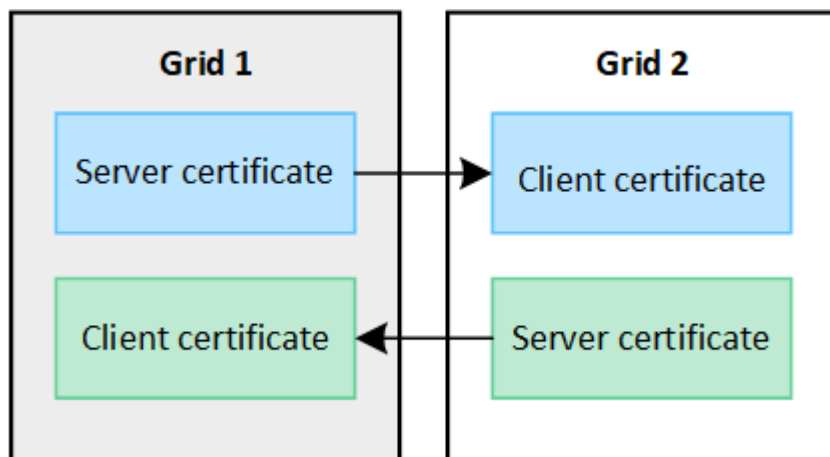
Você deve garantir que nenhum nó em nenhuma das grades use esta porta para outras conexões.

Requisitos do certificado

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

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

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



Por padrão, os certificados são válidos por 730 dias (2 anos). Quando esses certificados estiverem próximos da data de expiração, o alerta **Expiração do certificado de federação de grade** lembrará você de rotacionar os certificados, o que pode ser feito usando o Grid Manager.



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

Saber mais

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

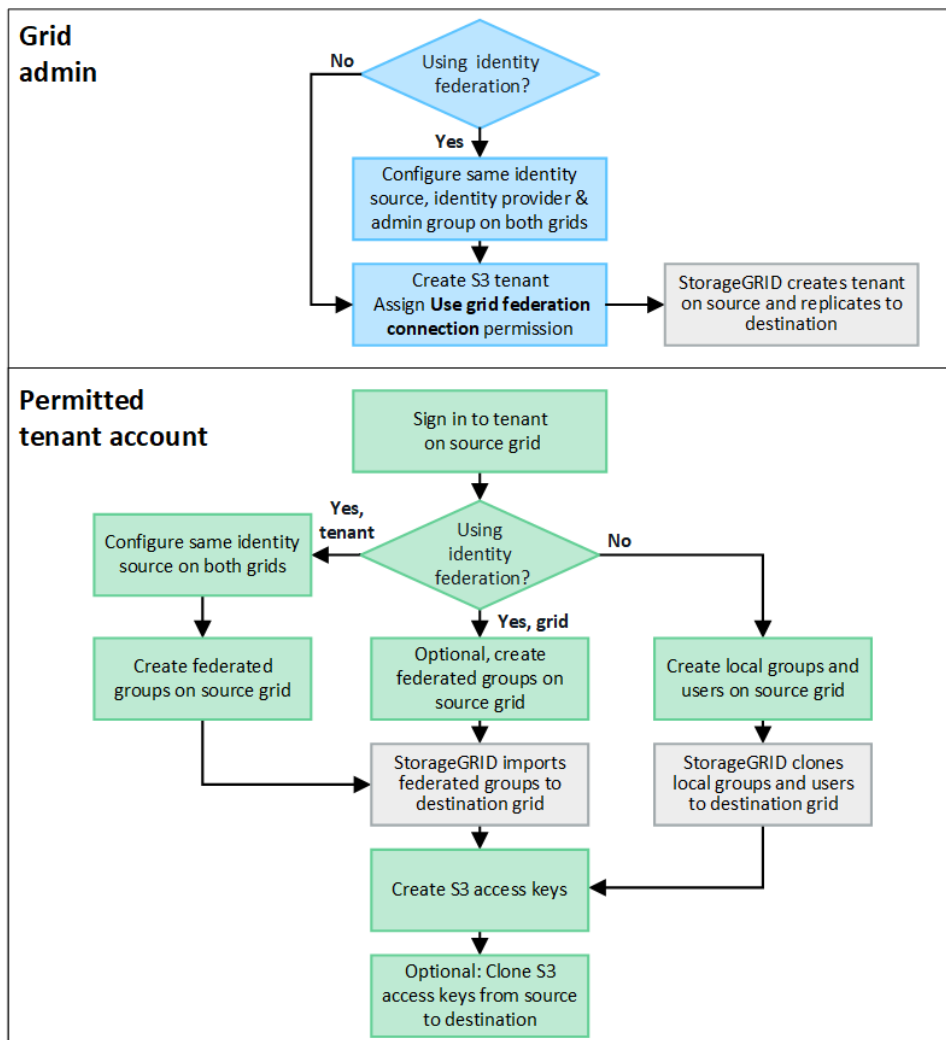
O que é clone de conta?

O clone 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 rede"](#).

É necessário clonar a conta para ["replicação entre grades"](#). A clonagem de informações de conta de um sistema StorageGRID de origem para um sistema StorageGRID de destino garante que usuários e grupos de locatários possam acessar os buckets e objetos correspondentes em qualquer grade.

Fluxo de trabalho para clonagem de conta

O diagrama de fluxo de trabalho mostra as etapas que os administradores de grade e os locatários permitidos executarão para configurar a clonagem da conta. Essas etapas são realizadas após a ["a conexão da federação de rede está configurada"](#).



Fluxo de trabalho de administração de grade

As etapas que os administradores da grade executam dependem se os sistemas StorageGRID no "conexão de federação de rede" use logon único (SSO) ou federação de identidade.

Configurar SSO para clonagem de conta (opcional)

Se qualquer sistema StorageGRID na conexão de federação de grade usar SSO, ambas as grades deverão usar SSO. Antes de criar as contas de locatário para federação de grade, os administradores de grade das grades de origem e destino do locatário devem executar estas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grades. Ver "[Usar federação de identidade](#)".
2. Configure o mesmo provedor de identidade SSO (IdP) para ambas as grades. Ver "[Configurar logon único](#)".
3. "[Crie o mesmo grupo de administração](#)" em ambas as grades importando o mesmo grupo federado.

Ao criar o locatário, você selecionará esse grupo para ter a permissão de acesso Root inicial para as contas do locatário de origem e 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 grade para clone de conta (opcional)

Se qualquer sistema StorageGRID usar federação de identidade sem SSO, ambas as grades deverão usar federação de identidade. Antes de criar as contas de locatário para federação de grade, os administradores de grade das grades de origem e destino do locatário devem executar estas etapas.

Passos

1. Configure a mesma fonte de identidade para ambas as grades. Ver "[Usar federação de identidade](#)".
2. Opcionalmente, se um grupo federado tiver permissão de acesso Root inicial para as contas de locatário de origem e de destino, "[crie o mesmo grupo de administração](#)" em ambas as grades importando o mesmo grupo federado.



Se você atribuir permissão de acesso Root a um grupo federado que não existe em ambas as grades, o locatário não será replicado para a grade de destino.

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

Criar conta de locatário S3 permitida

Depois de configurar opcionalmente o SSO ou a federação de identidade, um administrador de grade executa estas etapas para determinar quais locatários podem replicar objetos de bucket para outros sistemas StorageGRID.

Passos

1. Determine qual grade você deseja que seja a grade de origem do locatário para operações de clonagem de conta.

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

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

Se essa permissão for atribuída, as contas de locatário de origem e de destino deverão configurar a mesma fonte de identidade antes de criar grupos federados. Grupos federados adicionados ao locatário de origem não podem ser clonados para o locatário de destino, a menos que ambas as grades usem a mesma origem de identidade.

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

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

- 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 Root para o locatário, esse grupo será clonado para o locatário de destino.
- Se você selecionou um usuário local para ter permissão de acesso Root para o locatário, esse usuário será clonado para o locatário de destino. Entretanto, a senha desse usuário não é clonada.

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

Fluxo de trabalho de conta de inquilino permitido

Depois que um locatário com a permissão **Usar conexão de federação de grade** for replicado para a grade de destino, as contas de locatário permitidas poderão executar estas etapas para clonar grupos de locatários, usuários e chaves de acesso do S3.

Passos

1. Sign in na conta do locatário na grade 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, o StorageGRID os clona automaticamente para o locatário de destino, mas nenhuma clonagem ocorre 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.

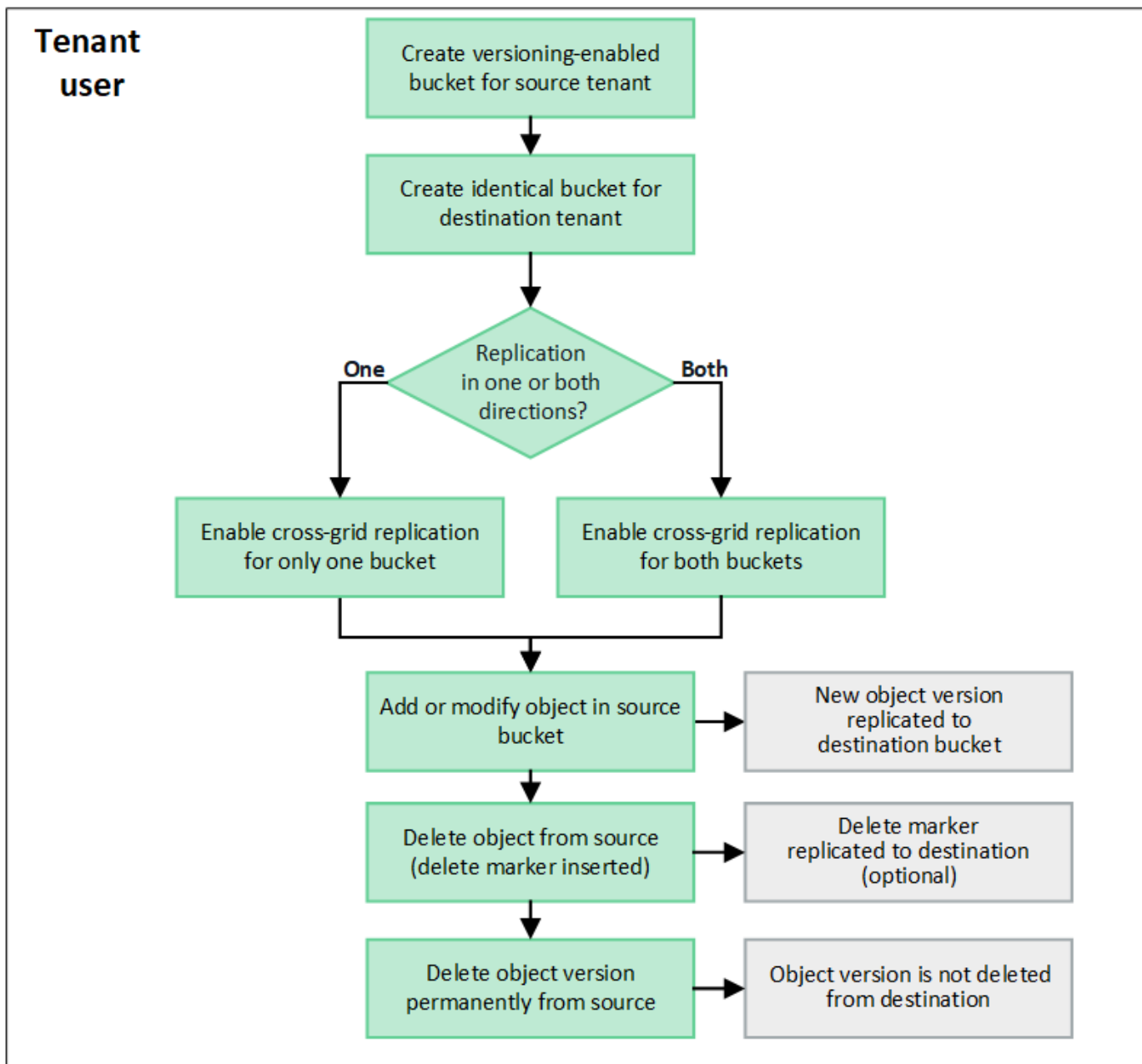
Para obter detalhes sobre o fluxo de trabalho da conta de locatário permitida e saber como grupos, usuários e chaves de acesso S3 são clonados, consulte ["Clonar grupos de locatários e usuários"](#) e ["Clonar chaves de acesso S3 usando a API"](#) .

O que é replicação entre redes?

A replicação entre grades é a replicação automática de objetos entre buckets S3 selecionados em dois sistemas StorageGRID que estão conectados em um ["conexão de federação de rede"](#) . ["Clone de conta"](#) é necessário para replicação entre grades.

Fluxo de trabalho para replicação entre grades

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



Requisitos para replicação entre redes

Se uma conta de locatário tiver a permissão **Usar conexão de federação de grade** para usar um ou mais ["conexões de federação de rede"](#), um usuário locatário com permissão de acesso Root pode criar buckets idênticos nas contas de locatário correspondentes em cada grade. Esses baldes:

- Deve ter o mesmo nome, mas pode ter regiões diferentes
- Deve ter o controle de versão habilitado
- Deve ter o bloqueio de objeto S3 desabilitado
- Deve estar vazio

Depois que ambos os buckets forem criados, a replicação entre grades poderá ser configurada para um ou ambos os buckets.

Saber mais

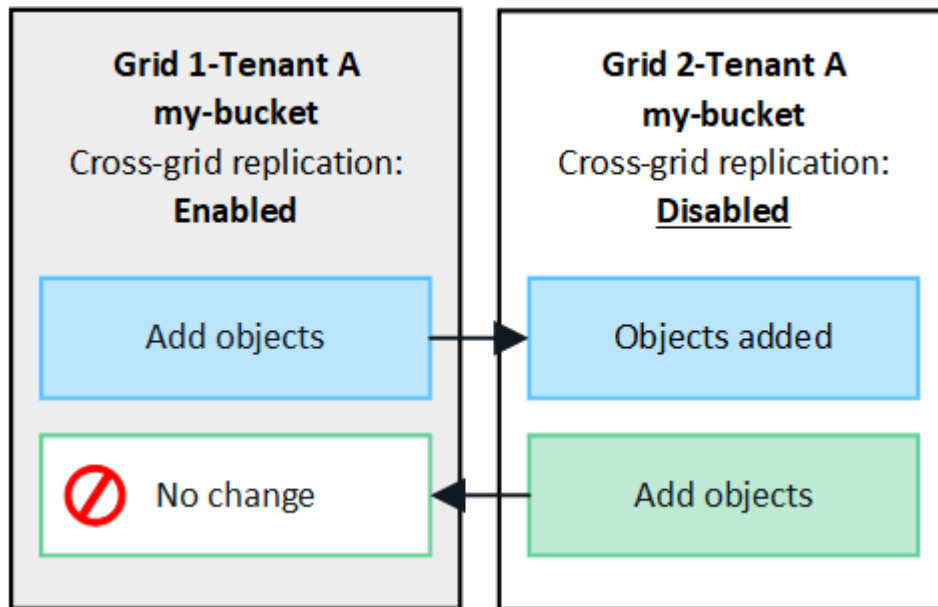
"Gerenciar replicação entre redes"

Como funciona a replicação entre redes

A replicação entre grades pode ser configurada para ocorrer em uma direção ou em ambas as direções.

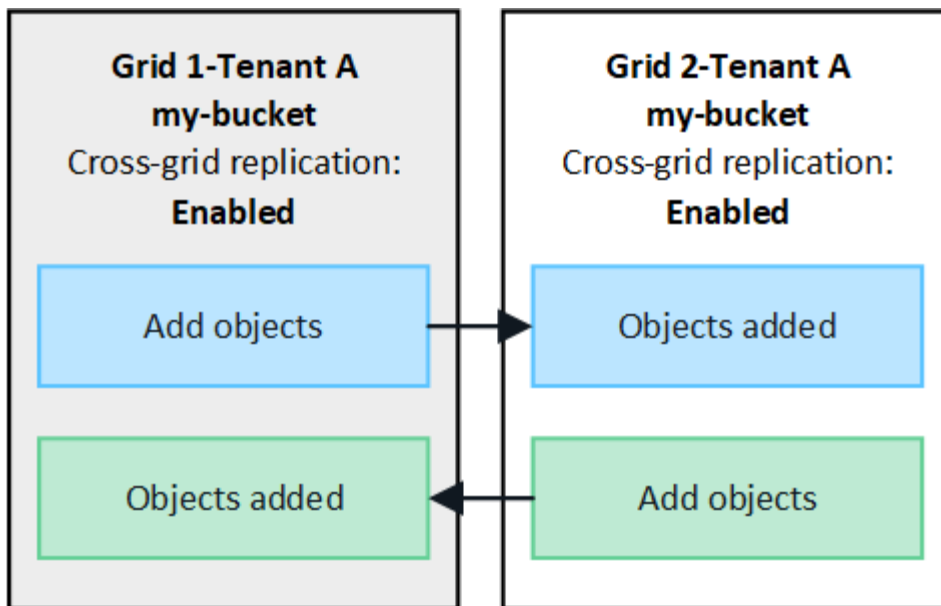
Replicação em uma direção

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 para `my-bucket` da Grade 1 para a Grade 2, mas não é habilitado na outra direção.



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 que tem a replicação entre grades habilitada, acontece o seguinte:

1. O StorageGRID replica automaticamente o objeto do bucket de origem para o bucket de destino. O tempo para executar esta 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 StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta, que terá um dos seguintes valores: O cliente S3 pode verificar o status de replicação de um objeto emitindo uma solicitação `GetObject` ou `HeadObject`. A resposta inclui um StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta, que terá um dos seguintes valores:

Grade	Status de replicação
Fonte	• CONCLUÍDO: A replicação foi bem-sucedida para todas as conexões de rede. • PENDENTE: O objeto não foi replicado para pelo menos uma conexão de grade. • FALHA: A replicação não está pendente para nenhuma conexão de rede e pelo menos uma falhou com uma falha permanente. Um usuário deve resolver o erro.
Destino	REPLICA: O objeto foi replicado da grade de origem.



O StorageGRID não oferece suporte a `x-amz-replication-status` cabeçalho.

2. O StorageGRID usa as políticas de ILM ativas de cada grade para gerenciar os objetos, assim como faria com qualquer outro objeto. Por exemplo, o Objeto A na Grade 1 pode ser armazenado como duas cópias replicadas e retido para sempre, enquanto a cópia do Objeto A que foi replicada na Grade 2 pode ser

armazenada usando codificação de eliminação 2+1 e excluída após três anos.

O que acontece quando objetos são excluídos?

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

- O cliente S3 emite uma solicitação de exclusão.
- Um usuário do Gerenciador de Inquilinos seleciona o "[Excluir objetos no bucket](#)" opção para remover todos os objetos de um bucket.
- O bucket tem 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 o StorageGRID exclui um objeto devido a uma operação Excluir objetos no bucket, expiração do ciclo de vida do bucket ou expiração do posicionamento do ILM, o objeto replicado nunca é excluído da outra grade em uma conexão de federação de grade. No entanto, os marcadores de exclusão adicionados ao bucket de origem pelas exclusões do cliente S3 podem, opcionalmente, ser replicados para o bucket de destino.

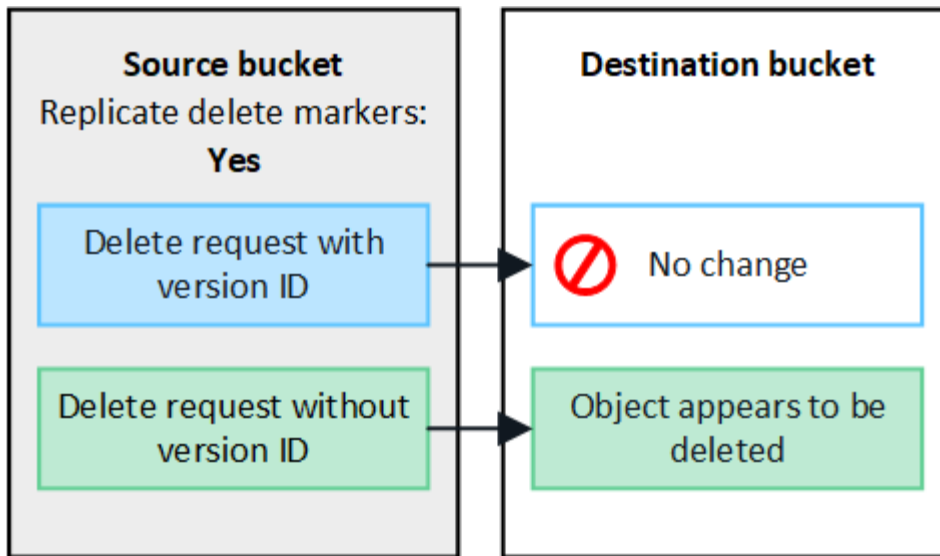
Para entender o que acontece quando um cliente S3 exclui objetos de um bucket que tem a replicação entre grades habilitada, revise como os clientes S3 excluem objetos de buckets que têm o controle de versão habilitado, da seguinte maneira:

- 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, o StorageGRID não excluirá nenhuma versão de 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 falhará com `404 No Object Found`
 - Uma solicitação `GetObject` com um ID de versão válido será bem-sucedida e retornará a versão do objeto solicitada.

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

- Se a solicitação de exclusão incluir um ID de versão, essa versão do objeto será removida permanentemente da grade de origem. No entanto, o 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, o StorageGRID poderá, opcionalmente, replicar o marcador de exclusão, com base em como a replicação entre grades estiver configurada para o bucket:
 - Se você optar por replicar marcadores de exclusão (padrão), um marcador de exclusão será adicionado ao bucket de origem e replicado no bucket de destino. Na verdade, o objeto parece ter sido excluído em ambas as grades.
 - Se você optar por não replicar os marcadores de exclusão, um marcador de exclusão será adicionado ao bucket de origem, mas não será replicado no bucket de destino. Na verdade, objetos que são excluídos na grade de origem não são excluídos na grade de destino.

Na figura, **Replicar marcadores de exclusão** foi definido como **Sim** quando "[a replicação entre grades foi habilitada](#)". Solicitações de exclusão para o bucket de origem que incluem um ID de versão não excluirão objetos do bucket de destino. Solicitações de exclusão para o bucket de origem que não incluem um ID de versão aparecerão para excluir objetos no bucket de destino.



Se você deseja manter as exclusões de objetos sincronizadas entre as grades, crie as correspondentes ["Configurações do ciclo de vida S3"](#) para os baldes 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 de bucket padrão ou configurar a criptografia em toda a grade. Você pode adicionar, modificar ou remover configurações de criptografia padrão de bucket ou de toda a 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 StorageGRID) ao adicionar os objetos ao bucket de origem. Use o `x-amz-server-side-encryption` cabeçalho da solicitação e especificar AES256. Ver ["Use criptografia do lado do servidor"](#).



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

Para usar a criptografia padrão para um bucket, use uma solicitação `PutBucketEncryption` e defina o `SSEAlgorithm` parâmetro para AES256. A criptografia em nível de bucket se aplica a todos os objetos ingeridos sem o `x-amz-server-side-encryption` cabeçalho da solicitação. Ver ["Operações em baldes"](#).

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



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

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

1. Use o `x-amz-server-side-encryption` cabeçalho de ingestão, se presente.
2. Se um cabeçalho de ingestão não estiver presente, use a configuração de criptografia padrão do bucket,

se configurada.

3. Se uma configuração de bucket não estiver configurada, use a configuração de criptografia em toda a grade, se configurada.
4. Se uma configuração para toda a grade não estiver presente, não criptografe o objeto de origem.

Ao determinar como criptografar objetos replicados, o 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 em toda a grade do destino, se configurada.
4. Se uma configuração para toda a grade não estiver presente, não criptografe o objeto de destino.

PutObjectTagging e DeleteObjectTagging não são suportados

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

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

Como objetos segmentados são replicados

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

Comparar a replicação entre grades e a replicação do CloudMirror

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

	Replicação entre grades	Serviço de replicação CloudMirror
Qual é o objetivo principal?	Um sistema StorageGRID atua como um sistema de recuperação de desastres. Objetos em um bucket podem ser replicados entre as grades 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). A replicação do CloudMirror cria uma cópia independente de um objeto em uma infraestrutura S3 independente. Essa cópia independente não é usada como backup, mas geralmente é processada na nuvem.

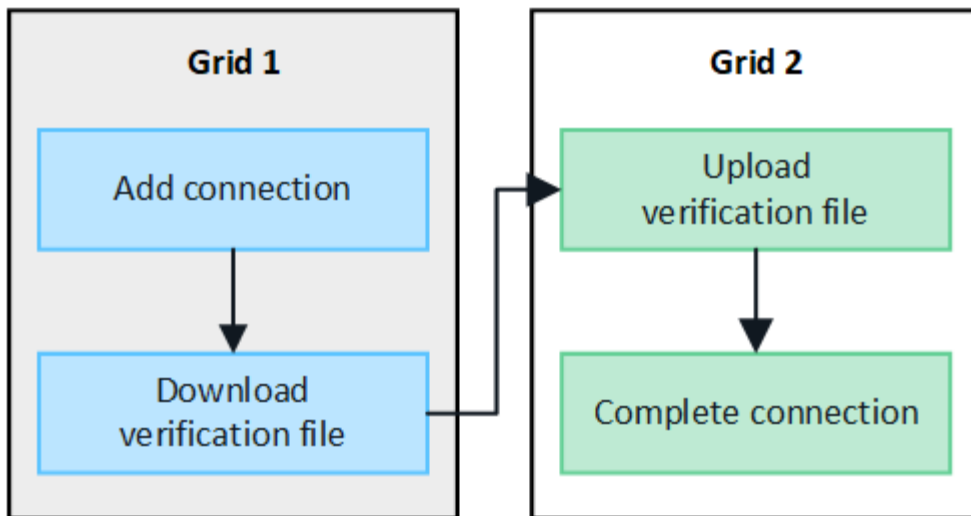
	Replicação entre grades	Serviço de replicação CloudMirror
Como é configurado?	1. Configure uma conexão de federação de grade entre duas grades. 2. Adicione novas contas de locatários, que são clonadas automaticamente para a outra grade. 3. Adicione novos grupos de locatários e usuários, que também são clonados. 4. Crie buckets correspondentes em cada grade e permita que a replicação entre grades ocorra em uma ou ambas as direções.	1. Um usuário locatário configura a replicação do CloudMirror definindo um ponto de extremidade do CloudMirror (endereço IP, credenciais e assim por diante) usando o Gerenciador de Locatários ou a API do S3. 2. Qualquer bucket pertencente a essa conta de locatário pode ser configurado para apontar para o ponto de extremidade do CloudMirror.
Quem é responsável por configurá-lo?	• Um administrador de grade configura a conexão e os inquilinos. • 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 grade.	• Qualquer infraestrutura S3 compatível (incluindo Amazon S3). • Plataforma de nuvem do Google (GCP)
O controle de versão do objeto é necessário?	Sim, tanto o bucket de origem quanto o de destino devem ter o controle de versão de objetos habilitado.	Não, a replicação do CloudMirror oferece suporte a qualquer combinação de buckets versionados e não versionados na origem e 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 do CloudMirror. Objetos que existiam no bucket de origem antes do bucket ser configurado com o endpoint do CloudMirror não são replicados, a menos que sejam modificados.
Como os objetos são replicados?	A replicação entre grades 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 ambas as grades.	A replicação do CloudMirror não requer buckets habilitados para controle de versão, portanto, o CloudMirror só pode manter a ordenação de uma chave dentro de um site. Não há garantias de que a ordem será mantida para solicitações de um objeto em um site diferente.
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 (consulte "Recomendações para uso de serviços de plataforma").

	Replicação entre grades	Serviço de replicação CloudMirror
Os metadados do sistema do objeto são replicados?	Sim, quando um objeto é replicado para outra grade, seus metadados do sistema também são replicados. Os metadados serão idênticos em ambas as grades.	Não, quando um objeto é replicado para o bucket externo, seus metadados do sistema são atualizados. Os metadados serão diferentes entre os locais, dependendo do horário de ingestão e do comportamento da infraestrutura independente do S3.
Como os objetos são recuperados?	Os aplicativos podem recuperar ou ler objetos fazendo uma solicitação ao bucket em qualquer grade.	Os aplicativos podem recuperar ou ler objetos fazendo uma solicitação ao StorageGRID ou ao destino S3. Por exemplo, suponha que você use a replicação do 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 .
O que acontece se um objeto for excluído?	- Solicitações de exclusão que incluem um ID de versão nunca são replicadas para a grade de destino. - Solicitações de exclusão que não incluem um ID de versão adicionam um marcador de exclusão ao bucket de origem, que pode ser replicado opcionalmente para a grade de destino. - Se a replicação entre grades for configurada para apenas uma direção, os objetos no bucket de destino poderão ser excluídos sem afetar a origem.	Os resultados variam de acordo com o estado de versão dos buckets de origem e destino (que não precisam ser os mesmos): - Se ambos os buckets forem versionados, uma solicitação de exclusão adicionará um marcador de exclusão em ambos os locais. - Se apenas o bucket de origem for versionado, uma solicitação de exclusão adicionará um marcador de exclusão à origem, mas não ao destino. - Se nenhum dos buckets tiver versão, uma solicitação de exclusão excluirá o objeto da origem, mas não do destino. Da mesma forma, objetos no bucket de destino podem ser excluídos sem afetar a origem.

Criar conexões de federação de grade

Você pode criar uma conexão de federação de grade entre dois sistemas StorageGRID se quiser clonar detalhes do locatário e replicar dados do objeto.

Conforme mostrado na figura, a criação de uma conexão de federação de grade inclui etapas em ambas as grades. Adicione a conexão em uma grade e complete-a na outra grade. Você pode começar em qualquer grade.



Antes de começar

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

Adicionar conexão

Execute estas etapas em qualquer um dos dois sistemas StorageGRID .

Passos

1. Sign in no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
3. Selecione **Adicionar conexão**.
4. Insira os detalhes da conexão.

Campo	Descrição
Nome da conexão	Um nome exclusivo para ajudar você a reconhecer essa conexão, por exemplo, "Grade 1-Grade 2".
FQDN ou IP para esta grade	Um dos seguintes: • O FQDN da rede na qual você está conectado no momento • Um endereço VIP de um grupo HA nesta grade • Um endereço IP de um nó de administração ou nó de gateway nesta grade. O IP pode estar em qualquer rede que a grade 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 de 23000 a 23999. Ambas as grades nesta conexão usarão a mesma porta. Você deve garantir que nenhum nó em nenhuma das grades use esta porta para outras conexões.
Dias de validade do certificado para esta grade	O número de dias que você deseja que os certificados de segurança desta grade na conexão sejam válidos. O valor padrão é 730 dias (2 anos), mas você pode inserir qualquer valor de 1 a 762 dias. O StorageGRID gera automaticamente certificados de cliente e servidor para cada grade quando você salva a conexão.
Senha de provisionamento para esta grade	A senha de provisionamento para a grade na qual você está conectado.
FQDN ou IP para a outra rede	Um dos seguintes: • O FQDN da rede à qual você deseja se conectar • Um endereço VIP de um grupo HA na outra grade • Um endereço IP de um nó de administração ou nó de gateway na outra grade. O IP pode estar em qualquer rede que a grade de origem possa alcançar.

5. Selecione **Salvar e continuar**.

6. Para a etapa Baixar arquivo de verificação, selecione **Baixar arquivo de verificação**.

Após a conexão ser concluída na outra rede, você não poderá mais baixar o arquivo de verificação de nenhuma delas.

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 confidenciais e devem ser armazenados e transmitidos com segurança.

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

9. Confirme se a nova conexão é exibida e se seu **Status da conexão** é **Aguardando conexão**.

10. Fornecer o *connection-name.grid-federation* arquivo para o administrador da grade para a outra grade.

Conexão completa

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

Passos

1. Sign in no Grid Manager a partir do nó de administração principal.

2. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
3. Selecione **Carregar arquivo de verificação** para acessar a página de Carregar.
4. Selecione **Carregar arquivo de verificação**. Em seguida, navegue e selecione o arquivo que foi baixado da primeira grade(`connection-name.grid-federation`).

Os detalhes da conexão são mostrados.

5. Opcionalmente, insira um número diferente de dias válidos para os certificados de segurança desta grade. A entrada **Dias de validade do certificado** assume como padrão o valor inserido na primeira grade, mas cada grade pode usar datas de validade diferentes.

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



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

6. Digite a senha de provisionamento da grade na qual você está conectado no momento.
7. Selecione **Salvar e testar**.

Os certificados são gerados e a conexão é testada. Se a conexão for válida, uma mensagem de sucesso será exibida e a nova conexão será listada na página Federação do Grid. O **Status da conexão** será **Conectado**.

Se uma mensagem de erro for exibida, resolva quaisquer problemas. Ver "[Solucionar erros de federação de grade](#)".

8. Vá para a página da federação da grade na primeira grade e atualize o navegador. Confirme se o **Status da conexão** agora é **Conectado**.
9. Após a conexão ser estabelecida, exclua com segurança todas as cópias do arquivo de verificação.

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

Depois que você terminar

- Revise as considerações para "[gerenciamento de inquilinos permitidos](#)".
- "[Crie uma ou mais novas contas de inquilino](#)", atribua a permissão **Usar conexão de federação de grade** e selecione a nova conexão.
- "[Gerenciar a conexão](#)" conforme necessário. Você pode editar valores de conexão, testar uma conexão, girar certificados de conexão ou remover uma conexão.
- "[Monitore a conexão](#)" como parte de suas atividades normais de monitoramento do StorageGRID.
- "[Solucionar problemas de conexão](#)", incluindo a resolução de quaisquer alertas e erros relacionados à clonagem de conta e à replicação entre redes.

Gerenciar conexões de federação de grade

O gerenciamento de conexões de federação de grade entre sistemas StorageGRID inclui a edição de detalhes de conexão, a rotação de certificados, a remoção de permissões de locatário e a remoção de conexões não utilizadas.

Antes de começar

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

Editar uma conexão de federação de grade

Você pode editar uma conexão de federação de grade entrando no nó de administração principal em qualquer grade na conexão. Depois de fazer alterações na primeira grade, você deve baixar um novo arquivo de verificação e enviá-lo para a outra grade.



Enquanto a conexão estiver sendo editada, as solicitações de clonagem de conta ou replicação entre redes continuarão a usar as configurações de conexão existentes. Todas as edições feitas na primeira grade são salvas localmente, mas não são usadas até que sejam carregadas na segunda grade, salvas e testadas.

Comece a editar a conexão

Passos

1. Sign in no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **NÓS** e confirme se todos os outros nós de administração no seu sistema estão online.



Quando você edita uma conexão de federação de grade, o StorageGRID tenta salvar um arquivo de "configuração de candidato" em todos os nós de administração na primeira grade. Se este arquivo não puder ser salvo em todos os nós de administração, uma mensagem de aviso aparecerá quando você selecionar **Salvar e testar**.

3. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
4. Edite os detalhes da conexão usando o menu **Ações** na página Federação de grade ou na página de detalhes de uma conexão específica. Ver ["Criar conexões de federação de grade"](#) para 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 um nome de conexão para exibir seus detalhes.
- b. Selecione **Editar**.
- c. Insira as novas informações.

5. Digite a senha de provisionamento da grade 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 grade.

7. Selecione **Baixar arquivo de verificação**.

Para baixar este arquivo mais tarde, 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 grade.

10. Confirme se o **Status da conexão** é **Edição pendente**.



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

11. Fornecer o *connection-name.grid-federation* arquivo para o administrador da grade para a outra grade.

Finalizar edição da conexão

Conclua a edição da conexão carregando o arquivo de verificação na outra grade.

Passos

1. Sign in no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
3. Selecione **Carregar arquivo de verificação** para acessar a página de upload.
4. Selecione **Carregar arquivo de verificação**. Em seguida, navegue e selecione o arquivo que foi baixado da primeira grade.
5. Digite a senha de provisionamento da grade na qual você está conectado no momento.
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. Revise a mensagem e resolva quaisquer problemas.

7. Feche o assistente para retornar à página Federação de grade.
8. Confirme se o **Status da conexão** é **Conectado**.
9. Vá para a página da federação da grade na primeira grade e atualize o navegador. Confirme se 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 grade

Passos

1. Sign in no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
3. Teste a conexão usando o menu **Ações** na página de federação da grade 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 um nome de conexão para exibir seus detalhes.
- b. Selecione **Testar conexão**.

4. Revise o status da conexão:

Status da conexão	Descrição
Conectado	Ambas as redes estão conectadas e se comunicando 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 grade, mas a conexão ainda está usando a configuração existente. Para concluir a edição, carregue o novo arquivo de verificação na outra grade.
Aguardando conexão	Você configurou a conexão nesta grade, mas a conexão não foi concluída na outra grade. Baixe o arquivo de verificação desta grade e carregue-o na outra grade.
Desconhecido	A conexão está em um estado desconhecido, possivelmente devido a um problema de rede ou 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 corrigido.

Rotular certificados de conexão

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



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

Passos

1. Sign in no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
2. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
3. Em qualquer uma das guias da página Federação da grade, selecione o nome da conexão para exibir seus detalhes.
4. Selecione a aba **Certificados**.

5. Selecione **Girar certificados**.
6. Especifique por quantos dias os novos certificados devem ser válidos.
7. Digite a senha de provisionamento da grade na qual você está conectado.
8. Selecione **Girar certificados**.
9. Conforme necessário, repita essas etapas na outra grade da conexão.

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

Remover uma conexão de federação de grade

Você pode remover uma conexão de federação de grade de qualquer grade na conexão. Conforme mostrado na figura, você deve executar etapas de pré-requisito em ambas as grades para confirmar que a conexão não está sendo usada por nenhum locatário em nenhuma delas.



Antes de remover uma conexão, observe o seguinte:

- Remover uma conexão não exclui nenhum item que já tenha sido copiado entre grades. Por exemplo, usuários, grupos e objetos locatários que existem em ambas as grades não são excluídos de nenhuma delas quando a permissão do locatário é removida. Se você quiser excluir esses itens, deverá excluí-los manualmente de ambas as grades.
- Quando você remove uma conexão, a replicação de todos os objetos com replicação pendente (ingeridos, mas ainda não replicados para a outra grade) falhará permanentemente.

Desabilitar replicação para todos os buckets de locatários

Passos

1. A partir de qualquer grade, faça login no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
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 algum inquilino listado, instrua todos os inquilinos a "[desabilitar replicação entre redes](#)" para todos os seus buckets em ambas as grades na conexão.



Não é possível remover a permissão **Usar conexão de federação de grade** se algum bucket de locatário tiver replicação entre grades habilitada. Cada conta de locatário deve desabilitar a replicação entre grades para seus buckets em ambas as grades.

Remover permissão para cada inquilino

Depois que a replicação entre grades for desabilitada para todos os buckets de locatários, remova a **Permissão de federação de uso de grade** de todos os locatários em ambas as grades.

Passos

1. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
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 grade** de cada locatário. Ver "[Gerenciar inquilinos permitidos](#)".
4. Repita essas etapas para os inquilinos permitidos na outra grade.

Remover conexão

Passos

1. Quando nenhum inquilino em nenhuma das redes estiver usando a conexão, selecione **Remover**.
2. Revise a mensagem de confirmação e selecione **Remover**.
 - Se a conexão puder ser removida, uma mensagem de sucesso será exibida. A conexão da federação de rede agora foi removida de ambas as redes.
 - Se a conexão não puder ser removida (por exemplo, se ela ainda estiver em uso ou se houver um erro de conexão), uma mensagem de erro será exibida. Você pode fazer qualquer um dos seguintes:
 - Resolva o erro (recomendado). Ver "[Solucionar erros de federação de grade](#)".
 - Remova a conexão à força. Veja a próxima seção.

Remover uma conexão de federação de grade à força

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

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

Passos

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

Uma mensagem de sucesso é exibida. Esta conexão de federação de rede não pode mais ser usada. No entanto, os buckets de locatários ainda podem ter a replicação entre grades habilitada e algumas cópias de objetos podem já ter sido replicadas entre as grades na conexão.
2. Da outra grade na conexão, efetue login no Grid Manager a partir do nó de administração principal.
3. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
4. Selecione o nome da conexão para exibir seus detalhes.
5. Selecione **Remover** e **Sim**.
6. Selecione **Forçar remoção** para remover a conexão desta grade.

Gerenciar os inquilinos permitidos para federação de rede

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

Antes de começar

- Você está conectado ao Grid Manager em qualquer uma das grades usando um "[navegador da web](#)".

compatível" .

- Você tem o "[Permissão de acesso root](#)" para a grade na qual você está conectado.
- Você tem "[criou uma conexão de federação de grade](#)" entre duas grades.
- Você revisou os fluxos de trabalho para "[clone de conta](#)" e "[replicação entre grades](#)" .
- Conforme necessário, você já configurou o logon único (SSO) ou a federação de identidade para ambas as grades na conexão. Ver "[O que é clone de conta](#)" .

Criar um inquilino 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 para "[criar um novo locatário S3](#)" ou "[editar uma conta de inquilino](#)" e observe o seguinte:

- Você pode criar o locatário de qualquer grade 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 grade** e depois salvo na primeira grade, um locatário idêntico é replicado automaticamente para a outra grade. A grade onde o locatário é replicado é a *grade de destino do locatário*.
- Os inquilinos 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 de um usuário root local não é copiada para a grade de destino.



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

- Depois que o novo locatário ou o locatário editado estiver disponível em ambas as grades, os usuários locatários poderão executar estas operações:
 - Na grade de origem do locatário, crie grupos e usuários locais, que serão clonados automaticamente na grade de destino do locatário. Ver "[Clonar grupos de locatários e usuários](#)" .
 - Crie novas chaves de acesso S3, que podem ser opcionalmente clonadas para a grade de destino do locatário. Ver "[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. Ver "[Gerenciar replicação entre redes](#)" .

Ver um inquilino permitido

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

Passos

1. Selecione **LOCATÁRIOS**.
2. Na página Inquilinos, selecione o nome do inquilino para visualizar a página de detalhes do inquilino.

Se esta for a grade de origem do locatário (ou seja, se o locatário foi criado nesta grade), um banner aparecerá para lembrá-lo de que o locatário foi clonado em outra grade. Se você editar ou excluir este

locatário, suas alterações não serão sincronizadas com a outra grade.

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](#)  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 aba **Federação de grade** para [monitorar a conexão da federação de rede](#) .

Editar um inquilino permitido

Se você precisar editar um locatário que tenha a permissão **Usar conexão de federação de grade**, siga as instruções gerais para [editando uma conta de locatário](#) e observe o seguinte:

- Se um locatário tiver a permissão **Usar conexão de federação de grade**, você poderá editar os detalhes do locatário de qualquer grade na conexão. Entretanto, quaisquer alterações que você fizer não serão copiadas para a outra grade. Se quiser manter os detalhes do inquilino sincronizados entre as grades, você deve fazer as mesmas edições em ambas as grades.
- Não é possível limpar a permissão **Usar conexão de federação de grade** quando você estiver editando um locatário.
- Não é possível selecionar uma conexão de federação de grade diferente ao editar um locatário.

Excluir um inquilino permitido

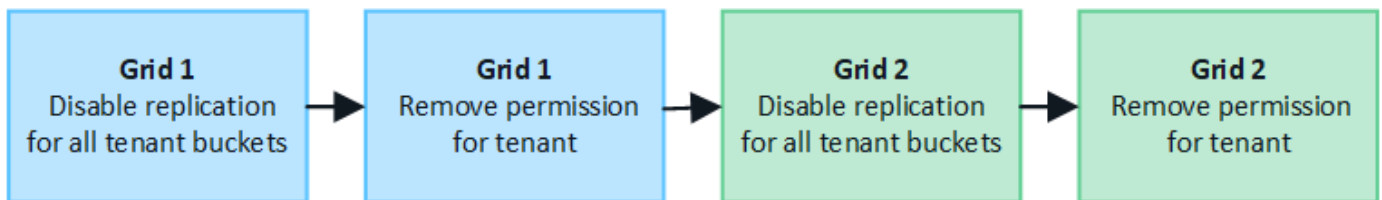
Se você precisar remover um locatário que tenha a permissão **Usar conexão de federação de grade**, siga as instruções gerais para [excluindo uma conta de inquilino](#) e observe o seguinte:

- Antes de remover o locatário original na grade de origem, você deve remover todos os buckets da conta na grade de origem.
- Antes de remover o locatário clonado na grade de destino, você deve remover todos os buckets da conta na grade de destino.
- Se você remover o locatário original ou clonado, a conta não poderá mais ser usada para replicação entre redes.
- Se você estiver removendo o locatário original na grade de origem, quaisquer grupos de locatários, usuários ou chaves que foram clonados na grade de destino não serão afetados. 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 se novos grupos ou usuários forem adicionados ao locatário original.

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

Remover permissão de conexão de federação de grade

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



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

- Você não pode remover a permissão **Usar conexão de federação de grade** se algum dos buckets do locatário tiver a replicação entre grades habilitada. A conta do locatário deve primeiro desabilitar a replicação entre redes para todos os seus buckets.
- Remover a permissão **Usar conexão de federação de grade** não exclui nenhum item que já tenha sido replicado entre grades. Por exemplo, quaisquer usuários, grupos e objetos de locatários que existam em ambas as grades não serão excluídos de nenhuma delas quando a permissão do locatário for removida. Se você quiser excluir esses itens, deverá excluí-los manualmente de ambas as grades.
- Se você quiser reativar essa permissão com a mesma conexão de federação de grade, exclua esse locatário na grade de destino primeiro; caso contrário, reativar essa permissão resultará em um erro.



Reativar a permissão **Usar conexão de federação de grade** torna a grade local a grade de origem e aciona a clonagem para a grade remota especificada pela conexão de federação de grade selecionada. Se a conta do locatário já existir na grade remota, a clonagem resultará em um erro de conflito.

Antes de começar

- Você está usando um "navegador da web compatível" .
- Você tem o "Permissão de acesso root" para ambas as grades.

Desabilitar replicação para buckets de locatários

Como primeira etapa, desabilite a replicação entre grades para todos os buckets de locatários.

Passos

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



Não é possível remover a permissão **Usar conexão de federação de grade** se algum bucket de locatário tiver replicação entre grades habilitada. O locatário deve desabilitar a replicação entre grades para seus buckets em ambas as grades.

Remover permissão para inquilino

Depois que a replicação entre grades for desabilitada para buckets de locatários, você poderá remover a permissão do locatário para usar a conexão de federação de grade.

Passos

1. Sign in 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 da federação da grade

- a. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
- b. Selecione o nome da conexão para exibir sua página de detalhes.
- c. Na aba **Inquilinos permitidos**, selecione o botão de opção para o inquilino.
- d. Selecione **Remover permissão**.

Página de inquilinos

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

3. Revise 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 pode mais usar a conexão de federação de rede.
 - Se um ou mais buckets de locatários ainda tiverem a replicação entre grades habilitada, um erro será exibido.

 **Remove permission to use grid federation connection** 

Are you sure you want to prevent **Tenant A** from performing account sync and cross-grid replication using grid federation connection **Grid 1-Grid 2**?

- Removing this permission does not delete any items that have already been copied to the other grid.
- After removing this permission for the tenant on this grid, go to the other grid and remove the permission for the corresponding tenant account.

 Connection '5427cbf8-0dd0-4b83-a2c8-e5e23cc49cc5' is used by bucket 'my-cgr-bucket' for cross-grid replication, so it can't be removed. From Tenant Manager, remove the cross-grid configuration from the tenant bucket and retry.

 Using **Force remove** removes the tenant's permission to use the grid federation connection even if tenant buckets still have cross-grid replication enabled. When the permission is removed, data in these buckets can no longer be copied between the grids.

Cancel

Force remove

Remove

Você pode fazer qualquer um dos seguintes:

- (Recomendado.) Sign in no Gerenciador de locatários e desative a replicação para cada um dos buckets do locatário. Ver "[Gerenciar replicação entre redes](#)". Em seguida, repita as etapas para remover a permissão **Usar conexão de rede**.
 - Remova a permissão à força. Veja a próxima seção.
4. Vá para a outra grade e repita essas etapas para remover a permissão do mesmo locatário na outra grade.

Remover a permissão à força

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

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

- Se você remover a permissão **Usar conexão de federação de grade** à força, todos os objetos que estiverem com replicação pendente para a outra grade (ingeridos, mas ainda não replicados) continuarão sendo replicados. Para evitar que esses objetos em processo cheguem ao bucket de destino, você deve

remover a permissão do locatário na outra grade também.

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

Passos

1. Sign in no Grid Manager a partir do nó de administração principal.
2. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
3. Selecione o nome da conexão para exibir sua página de detalhes.
4. Na aba **Inquilinos permitidos**, selecione o botão de opção para o inquilino.
5. Selecione **Remover permissão**.
6. Revise 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 rede.

7. Conforme necessário, vá para a outra grade e repita essas etapas para forçar a remoção da permissão para a mesma conta de locatário na outra grade. Por exemplo, você deve repetir essas etapas na outra grade para evitar que objetos em processo cheguem ao bucket de destino.

Solucionar erros de federação de grade

Pode ser necessário solucionar alertas e erros relacionados a conexões de federação de grade, clonagem de conta e replicação entre grades.

Alertas e erros de conexão de federação de rede

Você pode receber alertas ou enfrentar erros com suas conexões de federação de rede.

Depois de fazer qualquer alteração para resolver um problema de conexão, teste a conexão para garantir que o status da conexão retorne para **Conectado**. Para obter instruções, consulte "[Gerenciar conexões de federação de grade](#)".

Alerta de falha de conexão da federação de rede

Emitir

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

Detalhes

Este alerta indica que a conexão da federação de rede entre as redes não está funcionando.

Ações recomendadas

1. Revise as configurações na página Federação de grade para ambas as grades. Confirme se todos os valores estão corretos. Ver "[Gerenciar conexões de federação de grade](#)".
2. Revise os certificados usados para a conexão. Certifique-se de que não haja alertas para certificados de federação de grade expirados e que os detalhes de cada certificado sejam válidos. Veja as instruções para rotação de certificados de conexão em "[Gerenciar conexões de federação de grade](#)".
3. Confirme se todos os nós de administração e gateway em ambas as grades estão on-line e disponíveis. Resolva quaisquer alertas que possam estar afetando esses nós e tente novamente.
4. Se você forneceu um nome de domínio totalmente qualificado (FQDN) para a grade local ou remota,

confirme se o servidor DNS está online e disponível. Ver "[O que é federação de grade?](#)" para requisitos de rede, endereço IP e DNS.

Alerta de expiração do certificado de federação de rede

Emitir

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

Detalhes

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

Ações recomendadas

Veja as instruções para rotação de certificados de conexão em "[Gerenciar conexões de federação de grade](#)".

Erro ao editar uma conexão de federação de grade

Emitir

Ao editar uma conexão de federação de grade, 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

Quando você edita uma conexão de federação de grade, o StorageGRID tenta salvar um arquivo de "configuração de candidato" em todos os nós de administração na primeira grade. Uma mensagem de aviso será exibida se este arquivo não puder ser salvo em todos os nós administrativos, por exemplo, porque um nó administrativo está offline.

Ações recomendadas

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

Erros de clonagem de conta

Não é possível fazer login em uma conta de locatário clonada

Emitir

Você não pode entrar em uma conta de locatário clonada. A mensagem de erro na página de login do Gerenciador de locatários é "Suas credenciais para esta conta eram inválidas. Por favor, tente novamente."

Detalhes

Por motivos de segurança, quando uma conta de locatário é clonada da grade de origem do locatário para a grade de destino do locatário, a senha definida para o usuário raiz local do locatário não é clonada. Da mesma forma, quando um locatário cria usuários locais em sua grade de origem, as senhas dos usuários locais não são clonadas para a grade de destino.

Ações recomendadas

Antes que o usuário root possa efetuar login na grade de destino do locatário, um administrador de grade deve primeiro "[alterar a senha do usuário root local](#)" na grade 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 locais](#)" nas instruções de uso do Gerenciador de Inquilinos.

Inquilino criado sem um clone

Emitir

Você vê a mensagem "Locatário criado sem um clone" após criar um novo locatário com a permissão **Usar conexão de federação de grade**.

Detalhes

Esse problema pode ocorrer se as atualizações do status da conexão forem atrasadas, o que pode fazer com que uma conexão não saudável seja listada como **Conectada**.

Ações recomendadas

1. Revise o motivo listado na mensagem de erro e resolva quaisquer problemas de rede ou outros que possam estar impedindo o funcionamento da conexão. Ver [Alertas e erros de conexão da federação de rede](#).
2. Siga as instruções para testar uma conexão de federação de rede em "[Gerenciar conexões de federação de grade](#)" para confirmar se o problema foi corrigido.
3. Na grade de origem do locatário, selecione **LOCATÁRIOS**.
4. Localize a conta do locatário que não foi clonada.
5. Selecione o nome do inquilino para exibir a página de detalhes.
6. Selecione **Repetir clonagem da conta**.

Tenants > test

test

Tenant ID: 0040 2213 8117 4859 6503

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

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 será clonada para a outra grade.

Alertas e erros de replicação entre grades

Último erro mostrado para conexão ou locatário

Emitir

Quando "[visualizando uma conexão de federação de grade](#)" (ou quando "[gerenciando os inquilinos permitidos](#)" para uma conexão), você percebe um erro na coluna **Último erro** na página de detalhes da conexão. Por exemplo:

Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64
Port: 23000
Remote hostname (other grid): 10.96.130.76
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	2022-12-22 16:19:20 MST 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 and S3 Object Lock disabled. (logID 13916508109026943924) Check for errors



Last error



Tenant A

2022-12-22 16:19:20 MST

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 and S3 Object Lock disabled. (logID 13916508109026943924)

[Check for errors](#)

Detalhes

Para cada conexão de federação de grade, a coluna **Último erro** mostra o erro mais recente ocorrido, se houver, quando os dados de um locatário estavam sendo replicados para a outra grade. Esta coluna mostra apenas o último erro de replicação entre grades que ocorreu; erros anteriores que possam ter ocorrido não serão mostrados. Um erro nesta coluna pode ocorrer por um destes 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 tem o controle de versão suspenso.
- O bucket de destino foi recriado pela mesma conta, mas agora não tem versão.

Ações recomendadas

Se uma mensagem de erro aparecer na coluna **Último erro**, siga estas etapas:

1. Revise o texto da mensagem.
2. Execute todas as ações recomendadas. Por exemplo, se o controle de versão foi suspenso no bucket de destino para replicação entre grades, reative o controle de versão para esse bucket.
3. Selecione a conta de conexão ou locatário na tabela.
4. Selecione **Limpar erro**.
5. Selecione **Sim** para limpar a mensagem e atualizar o status do sistema.

- Espere de 5 a 6 minutos e então ingira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.



Para garantir que a mensagem de erro seja apagada, aguarde pelo menos 5 minutos após o registro de data e hora na mensagem antes de ingerir um novo objeto.



Depois de limpar o erro, um novo **Último erro** pode aparecer se os objetos forem ingeridos em um bucket diferente que também tenha um erro.

- Para determinar se algum objeto não foi replicado devido ao erro do bucket, consulte "[Identificar e tentar novamente operações de replicação com falha](#)".

Alerta de falha permanente de replicação entre redes

Emitir

O alerta **Falha permanente de 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. Esse alerta geralmente é causado por uma alteração no bucket de origem ou de destino.

Ações recomendadas

- Sign in na grade onde o alerta foi acionado.
- Vá para **CONFIGURAÇÃO > Sistema > Federação de grade** e localize o nome da conexão listado no alerta.
- Na guia Inquilinos permitidos, observe a coluna **Último erro** para determinar quais contas de inquilinos apresentam erros.
- Para saber mais sobre a falha, consulte as instruções em "[Monitorar conexões de federação de rede](#)" para revisar as métricas de replicação entre grades.
- Para cada conta de locatário afetada:
 - Veja as instruções em "[Monitorar a atividade do inquilino](#)" para confirmar que o locatário não excedeu sua cota na grade de destino para replicação entre grades.
 - Conforme necessário, aumente a cota do locatário na grade de destino para permitir que novos objetos sejam salvos.
- Para cada locatário afetado, faça login no Gerenciador de Locatários em ambas as grades para poder comparar a lista de buckets.
- Para cada bucket que tenha replicação entre grades habilitada, confirme o seguinte:
 - Há um bucket correspondente para o mesmo locatário na outra grade (é necessário usar o nome exato).
 - Ambos os buckets têm o controle de versão de objetos habilitado (o controle de versão não pode ser suspenso em nenhuma das grades).
 - Ambos os buckets têm o bloqueio de objeto S3 desabilitado.
 - Nenhum bucket está no estado **Excluindo objetos: somente leitura**.
- Para confirmar se o problema foi resolvido, consulte as instruções em "[Monitorar conexões de federação de rede](#)" para revisar as métricas de replicação entre grades ou executar estas etapas:

- a. Volte para a página da federação Grid.
- b. Selecione o inquilino afetado e selecione **Limpar erro** na coluna **Último erro**.
- c. Selecione **Sim** para limpar a mensagem e atualizar o status do sistema.
- d. Espere de 5 a 6 minutos e então ingira um novo objeto no balde. Confirme se a mensagem de erro não reaparece.



Para garantir que a mensagem de erro seja apagada, aguarde pelo menos 5 minutos após o registro de data e hora na mensagem antes de ingerir um novo objeto.



Pode levar até um dia para que o alerta desapareça após ser resolvido.

- a. Vá para "[Identificar e tentar novamente operações de replicação com falha](#)" para identificar quaisquer objetos ou excluir marcadores que não foram replicados para a outra grade e tentar replicar novamente conforme necessário.

Alerta de recurso de replicação entre grades indisponível

Emitir

O alerta **Recurso de replicação entre grades indisponível** foi acionado.

Detalhes

Este alerta indica que solicitações de replicação entre grades estão pendentes porque um recurso não está disponível. Por exemplo, pode haver um erro de rede.

Ações recomendadas

1. Monitore o alerta para ver se o problema se resolve sozinho.
2. Se o problema persistir, determine se alguma das grades tem um alerta **Falha na conexão da federação da grade** para a mesma conexão ou um alerta **Não foi possível comunicar com o nó** para um nó. Este alerta pode ser resolvido quando você resolver esses alertas.
3. Para saber mais sobre a falha, consulte as instruções em "[Monitorar conexões de federação de rede](#)" para revisar as métricas de replicação entre grades.
4. Se você não conseguir resolver o alerta, entre em contato com o suporte técnico.

A replicação entre redes continuará normalmente após o problema ser resolvido.

Identificar e tentar novamente operações de replicação com falha

Depois de resolver o alerta **Falha permanente de replicação entre grades**, você deve determinar se algum objeto ou marcador de exclusão falhou ao ser replicado para a outra grade. Você pode então reingerir esses objetos ou usar a API de gerenciamento de grade 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 erros de federação de grade](#)".

Determinar se algum objeto não foi replicado

Para determinar se algum objeto ou marcador de exclusão não foi replicado para a outra grade, você pode pesquisar no log de auditoria por "[CGRR \(Solicitação de Replicação Entre Redes\)](#)" mensagens. Esta mensagem é adicionada ao log quando o StorageGRID falha ao replicar um objeto, objeto multiparte 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 `Passwords.txt` arquivo.
- Você sabe o endereço IP do nó de administração principal.

Passos

1. Efetue login no nó de administração principal:

- a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- b. Digite a senha listada no `Passwords.txt` arquivo.
- c. Digite o seguinte comando para alternar para root: `su -`
- d. Digite a senha listada no `Passwords.txt` arquivo.

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

2. Pesquise no `audit.log` por mensagens CGRR e use a ferramenta `audit-explain` para formatar os resultados.

Por exemplo, este comando pesquisa todas as mensagens CGRR nos últimos 30 minutos e usa 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 tem 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 para operações de "replicar objeto" e os três últimos erros são para operações de "replicar marcador de exclusão".

```

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 redes CGRR	O nome da solicitação
inquilino	ID da conta do inquilino
conexão	O ID da conexão da federação de grade
operação	O tipo de operação de replicação que estava sendo tentada: • replicar objeto • replicar marcador de exclusão • replicar objeto multiparte
balde	O nome do balde
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

Depois de 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:

- Ingira novamente cada objeto no bucket de origem.
- Use a API privada de gerenciamento de grade, conforme descrito.

Passos

1. Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API**.
2. Selecione **Ir para documentação da API privada**.



Os pontos de extremidade 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 ponto de extremidade:

```
POST /private/cross-grid-replication-retry-failed
```

4. Selecione **Experimentar**.
5. Na caixa de texto **corpo**, substitua a entrada de exemplo para **versionID** por uma ID de versão do audit.log que corresponda a uma solicitação de replicação entre grades com falha.

Certifique-se de manter as aspas duplas ao redor 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 grade.

Você pode monitorar operações de repetição de duas maneiras:

- Use um S3 "**CabeçaObjeto**" ou "**ObterObjeto**" solicitar. A resposta inclui o StorageGRID específico `x-ntap-sg-cgr-replication-status` cabeçalho de resposta, que terá um dos seguintes valores:

Grade	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	REPLICA: O objeto foi replicado da grade de origem.

- Use a API privada de gerenciamento de grade, conforme descrito.

Passos

1. Na seção **cross-grid-replication-advanced** da documentação da API privada, selecione o seguinte ponto de extremidade:

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Selecione **Experimentar**.
3. Na seção Parâmetro, insira o ID da versão que você usou no `cross-grid-replication-retry-failed` solicitar.
4. Selecione **Executar**.
5. Confirme se o código de resposta do servidor é **200**.
6. Revise o status da replicação, que será um dos seguintes:
 - **PENDENTE:** O objeto ainda não foi replicado.
 - **CONCLUÍDO:** A replicação foi bem-sucedida.
 - **FALHOU:** A replicação falhou com uma falha permanente. Um usuário deve resolver o erro.

Gerenciar segurança

Gerenciar segurança

Você pode configurar várias configurações de segurança no Grid Manager para ajudar a proteger seu sistema StorageGRID .

Gerenciar criptografia

O StorageGRID oferece diversas opções para criptografar dados. Você deve ["revise os métodos de criptografia disponíveis"](#) para determinar quais atendem aos seus requisitos de proteção de dados.

Gerenciar certificados

Você pode ["configurar e gerenciar os certificados do servidor"](#) usado para conexões HTTP ou certificados de cliente usados para autenticar uma identidade de cliente ou usuário no servidor.

Configurar servidores de gerenciamento de chaves

Usando um ["servidor de gerenciamento de chaves"](#) permite proteger os dados do StorageGRID 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 possa se comunicar com o KMS.



Para usar o gerenciamento de chaves de criptografia, você deve habilitar a configuração **Criptografia de nó** para cada dispositivo durante a instalação, antes que o dispositivo seja adicionado à grade.

Gerenciar configurações de proxy

Se você estiver usando serviços de plataforma S3 ou pools de armazenamento em nuvem, poderá configurar um "[servidor proxy de armazenamento](#)" entre os nós de armazenamento e os pontos de extremidade S3 externos. Se você enviar pacotes AutoSupport usando HTTPS ou HTTP, você pode configurar um "[servidor proxy de administração](#)" entre nós administrativos e suporte técnico.

Firewalls de controle

Para aumentar a segurança do seu sistema, você pode controlar o acesso aos nós de administração do StorageGRID abrindo ou fechando portas específicas no "[firewall externo](#)". Você também pode controlar o acesso da rede a cada nó configurando seu "[firewall interno](#)". Você pode impedir o acesso em todas as portas, exceto aquelas necessárias para sua implantação.

Revise os métodos de criptografia do StorageGRID

O StorageGRID oferece diversas opções para criptografar dados. Você deve revisar 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 StorageGRID e " habilitar 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). Esta chave criptografa e descriptografa a chave de criptografia de dados (DEK) em cada volume.	Nós de dispositivos que têm Criptografia de Nó ativada durante a instalação. Todos os dados no dispositivo são protegidos contra perda física ou remoção do data center. Observação: o gerenciamento de chaves de criptografia com um KMS só é suportado por nós de armazenamento e dispositivos de serviços.

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 poderá definir uma senha para a unidade durante a instalação. Quando você define uma senha para uma 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, vá para Configurar Hardware > Criptografia de Unidade para definir uma senha de unidade que se aplique a todas as unidades autocriptografadas e gerenciadas StorageGRID em um nó.	Dispositivos que contêm unidades de autocriptografia. Todos os dados nas unidades protegidas são protegidos contra perda física ou remoção do data center. A criptografia de unidade não se aplica a unidades gerenciadas SANtricity. Se você tiver um dispositivo de armazenamento com unidades de autocriptografia e controladores SANtricity, poderá habilitar a segurança da unidade no SANtricity.
Impulsione a segurança no SANtricity System Manager	Se o recurso Drive Security estiver habilitado para seu dispositivo StorageGRID, você poderá usar "Gerente do Sistema SANtricity" para criar e gerenciar a chave de segurança. A chave é necessária para acessar os dados nas unidades protegidas.	Dispositivos de armazenamento que possuem unidades de criptografia completa de disco (FDE) ou unidades de autocriptografia. Todos os dados nas unidades protegidas são protegidos contra perda física ou remoção do data center. Não pode ser usado com alguns dispositivos de armazenamento ou com quaisquer dispositivos de serviço.
Criptografia de objetos armazenados	Você habilita o "Criptografia de objetos armazenados" opção no Grid Manager. Quando ativado, todos os novos objetos que não são criptografados no nível do bucket ou no nível do objeto são criptografados durante a ingestão.	Dados de objeto S3 recém-ingерidos. Objetos armazenados existentes não são criptografados. Metadados de objetos e outros dados confidenciais não são criptografados.

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de bucket S3	Você emite uma solicitação PutBucketEncryption para habilitar a criptografia para o bucket. Todos os novos objetos que não são criptografados no nível do objeto são criptografados durante a ingestão.	Somente dados de objetos S3 recém-ingeridos. A criptografia deve ser especificada para o bucket. Objetos de bucket existentes não são criptografados. Metadados de objetos e outros dados confidenciais não são criptografados. "Operações em baldes"
Criptografia do lado do servidor de objetos S3 (SSE)	Você emite uma solicitação S3 para armazenar um objeto e incluir o <code>x-amz-server-side-encryption</code> cabeçalho da solicitação.	Somente dados de objetos S3 recém-ingeridos. A criptografia deve ser especificada para o objeto. Metadados de objetos e outros dados confidenciais não são criptografados. O StorageGRID gerencia as chaves. "Use criptografia do lado do servidor"
Criptografia do lado do servidor de objetos S3 com chaves fornecidas pelo cliente (SSE-C)	Você emite uma solicitação S3 para armazenar um objeto e 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 de objetos e outros dados confidenciais não são criptografados. As chaves são gerenciadas fora do StorageGRID. "Use criptografia do lado do servidor"

Opção de criptografia	Como funciona	Aplica-se a
Criptografia de volume externo ou armazenamento de dados	Use um método de criptografia fora do StorageGRID para criptografar um volume ou armazenamento de dados inteiro, se sua plataforma de implantação oferecer suporte a ele.	Todos os dados de objetos, metadados e dados de configuração do sistema, supondo que cada volume ou armazenamento de dados seja criptografado. Um método de criptografia externa fornece controle mais rígido sobre algoritmos e chaves de criptografia. Pode ser combinado com os outros métodos listados.
Criptografia de objetos fora do StorageGRID	Use um método de criptografia fora do StorageGRID para criptografar dados de objetos e metadados antes que eles sejam ingeridos no StorageGRID.	Somente dados de objeto e metadados (os dados de configuração do sistema não são criptografados). Um método de criptografia externa fornece controle mais rígido sobre 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 de suas necessidades, você pode usar mais de um método de criptografia por vez. Por exemplo:

- Você pode usar um KMS para proteger nós de dispositivos e também usar o recurso de segurança de unidade no SANtricity System Manager para "criptografar duas vezes" dados nas unidades de autcriptografia nos mesmos dispositivos.
- Você pode usar um KMS para proteger dados em nós de dispositivos e também usar a opção Criptografia de objetos armazenados para criptografar todos os objetos quando eles são ingeridos.

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

Gerenciar certificados

Gerenciar certificados de segurança

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

O StorageGRID usa dois tipos de certificados de segurança:

- **Certificados de servidor** são necessários quando você usa conexões HTTPS. Os certificados de servidor são usados para estabelecer conexões seguras entre clientes e servidores, autenticando a identidade de um servidor para seus clientes e fornecendo um caminho de comunicação seguro para dados. O servidor e o cliente têm uma cópia do certificado.
- **Certificados de cliente** autenticam a identidade de um cliente ou usuário no servidor, fornecendo autenticação mais segura do que apenas senhas. Os certificados do 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 verifica este certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão com o servidor usando a mesma chave pública.

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

Certificado Grid CA padrão

O StorageGRID inclui uma autoridade de certificação (CA) integrada que gera um certificado de CA de grade interno 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 são totalmente compatíveis com as políticas de segurança de informações da sua organização. Embora você possa usar o certificado Grid CA para um ambiente de não produção, a prática recomendada para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa. Conexões não seguras sem certificado também são suportadas, mas não são recomendadas.

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



O StorageGRID também inclui certificados de CA do sistema operacional que são os mesmos em todas as grades. Em ambientes de produção, certifique-se de especificar um certificado personalizado assinado por uma autoridade de certificação externa no lugar do certificado de CA do sistema operacional.

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

Certificados de segurança de acesso

Você pode acessar informações sobre todos os certificados 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 guia na página Certificados para obter informações sobre cada categoria de certificado e acessar as configurações do certificado. Você pode acessar uma aba se tiver a ["permissão apropriada"](#) .

- **Global:** Protege o acesso ao StorageGRID de navegadores da web e clientes de API externos.
- **Grid CA:** protege o tráfego interno do StorageGRID .
- **Cliente:** protege conexões entre clientes externos e o banco de dados StorageGRID Prometheus.
- **Pontos de extremidade do balanceador de carga:** protege conexões entre clientes S3 e o balanceador de carga StorageGRID .
- **Inquilinos:** protege conexões com servidores de federação de identidade ou de pontos de extremidade de serviço de plataforma para recursos de armazenamento S3.
- **Outro:** Protege 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 de navegadores da web e clientes externos da API S3. Dois certificados globais são gerados inicialmente pela autoridade de certificação StorageGRID durante a instalação. A melhor prática para um ambiente de produção é usar certificados personalizados assinados por uma autoridade de certificação externa.

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

As informações sobre os certificados globais instalados incluem:

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

Você pode:

- Substitua os certificados padrão por certificados personalizados assinados por uma autoridade de certificação externa para melhorar a segurança da grade:
 - ["Substituir o certificado de interface de gerenciamento gerado pelo StorageGRID padrão"](#) usado para conexões do Grid Manager e do Tenant Manager.
 - ["Substituir o certificado da API S3"](#) usado para conexões de nó de armazenamento e ponto de extremidade do balanceador de carga (opcional).
- ["Restaurar o certificado da interface de gerenciamento padrão"](#) .
- ["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 de interface de gerenciamento"](#) ou ["Certificado S3 API"](#) .

Grade CA

O [Certificado Grid CA](#) , 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 validade do certificado e o conteúdo do certificado.

Você pode ["copiar ou baixar o certificado Grid CA"](#) , mas você não pode alterá-lo.

Cliente

[Certificados de cliente](#), gerado por uma autoridade de certificação externa, protege as conexões entre ferramentas de monitoramento externo e o banco de dados StorageGRID Prometheus.

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

Você pode:

- ["Carregue ou gere um novo certificado de cliente."](#)
- Selecione um nome de certificado para exibir os detalhes do certificado, onde você pode:
 - ["Alterar o nome do certificado do cliente."](#)
 - ["Defina a permissão de acesso do Prometheus."](#)
 - ["Carregue e substitua o certificado do cliente."](#)
 - ["Copie ou baixe o certificado do cliente."](#)
 - ["Remova o certificado do cliente."](#)
- Selecione **Ações** para rapidamente ["editar"](#) , ["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 ponto de extremidade do balanceador de carga](#) protegem as conexões entre clientes S3 e o serviço StorageGRID Load Balancer em nós de gateway e nós de administração.

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



Alterações em um certificado de ponto de extremidade podem levar até 15 minutos para serem aplicadas a todos os nós.

Você pode:

- ["Exibir um ponto de extremidade do balanceador de carga"](#), incluindo os detalhes do seu certificado.
- ["Especifique um certificado de ponto de extremidade do balanceador de carga para FabricPool."](#)
- ["Use o certificado global da API S3"](#) em vez de gerar um novo certificado de ponto de extremidade do balanceador de carga.

Inquilinos

Os inquilinos podem usar [certificados de servidor de federação de identidade](#) ou [certificados de ponto de extremidade de serviço de plataforma](#) para proteger suas conexões com o StorageGRID.

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

Você pode:

- ["Selecione um nome de inquilino para fazer login no Gerenciador de Inquilinos"](#)
- ["Selecione um nome de locatário para visualizar os detalhes da federação de identidade do locatário"](#)
- ["Selecione um nome de locatário para visualizar os detalhes dos serviços da plataforma de locatários"](#)
- ["Especifique um certificado de ponto de extremidade de serviço de plataforma durante a criação"](#)

do ponto de extremidade"

Outro

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

- [Certificados de pool de armazenamento em nuvem](#)
- [Certificados de notificação de alerta por e-mail](#)
- [Certificados de servidor syslog externo](#)
- [Certificados de conexão de federação de rede](#)
- [Certificados de federação de identidade](#)
- [Certificados do servidor de gerenciamento de chaves \(KMS\)](#)
- [Certificados de logon único](#)

As informações indicam o tipo de certificado que uma função usa e as datas de expiração dos certificados de servidor e cliente, conforme aplicável. Selecionar um nome de 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 a permissão "[permissão apropriada](#)".

Você pode:

- ["Especifique um certificado de pool de armazenamento em nuvem para S3, C2S S3 ou Azure"](#)
- ["Especificar um certificado para notificações de alerta por e-mail"](#)
- ["Use um certificado para um servidor syslog externo"](#)
- ["Girar certificados de conexão de federação de rede"](#)
- ["Visualizar e editar um certificado de federação de identidade"](#)
- ["Carregar certificados de servidor e cliente do servidor de gerenciamento de chaves \(KMS\)"](#)
- ["Especificar manualmente um certificado SSO para uma parte confiável"](#)

Detalhes do certificado de segurança

Cada tipo de certificado de segurança é descrito abaixo, com links para as instruções de implementação.

Certificado de interface de gerenciamento

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre os navegadores da Web do cliente e a interface de gerenciamento do StorageGRID , permitindo que os usuários acessem o Grid Manager e o Tenant Manager sem avisos de segurança. Este certificado também autentica conexões da API de gerenciamento de grade e da API de gerenciamento de locatários. Você pode usar o certificado padrão criado durante a instalação ou carregar um certificado personalizado.	CONFIGURAÇÃO > Segurança > Certificados , selecione a aba Global e então selecione Certificado de interface de gerenciamento	"Configurar certificados de interface de gerenciamento"

Certificado S3 API

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica conexões seguras do cliente S3 com um nó de armazenamento e com pontos de extremidade do balanceador de carga (opcional).	CONFIGURAÇÃO > Segurança > Certificados , selecione a aba Global e então selecione Certificado S3 API	"Configurar certificados da API S3"

Certificado Grid CA

Veja o [Descrição do certificado CA de grade padrão](#) .

Certificado de cliente administrador

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Cliente	Instalado em cada cliente, permitindo que o 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 aba Cliente	"Configurar certificados de cliente"

Certificado de ponto de extremidade 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 em nós de gateway e nós de administração. Você pode carregar ou gerar um certificado do balanceador de carga ao configurar um ponto de extremidade do balanceador de carga. Os aplicativos cliente usam o certificado do balanceador de carga ao se conectar ao StorageGRID para salvar e recuperar dados de objetos. Você também pode usar uma versão personalizada do global Certificado S3 API certificado para autenticar conexões com o serviço Load Balancer. Se o certificado global for usado para autenticar conexões do balanceador de carga, você não precisará carregar ou gerar um certificado separado para cada ponto de extremidade do balanceador de carga. Observação: O certificado usado para autenticação do balanceador de carga é o certificado mais usado 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 do balanceador de carga para o FabricPool"

Certificado de ponto de extremidade do Cloud Storage Pool

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

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 o StorageGRID que é usado para notificações de alerta. • Se as comunicações com o servidor SMTP exigirem o Transport Layer Security (TLS), você deverá especificar o certificado CA do servidor de e-mail. • Especifique um certificado de cliente somente se o servidor de e-mail SMTP exigir certificados de cliente para autenticação.	ALERTAS > Configuração de e-mail	"Configurar 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. Observação: Um certificado de servidor syslog externo não é necessário 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 rede

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentique e criptografe as informações enviadas entre o sistema StorageGRID atual e outra grade em uma conexão de federação de grade.	CONFIGURAÇÃO > Sistema > Federação de grade	• "Criar conexões de federação de grade" • "Girar certificados de conexão"

Certificado de federação de identidade

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre o StorageGRID e um provedor de identidade externo, como Active Directory, OpenLDAP ou Oracle Directory Server. Usado para federação de identidade, o que permite que grupos de administradores e usuários sejam gerenciados por um sistema externo.	CONFIGURAÇÃO > Controle de Acesso > Federação de Identidade	"Usar federação de identidade"

Certificado do servidor de gerenciamento de chaves (KMS)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor e cliente	Autentica a conexão entre o StorageGRID e um servidor de gerenciamento de chaves externo (KMS), que fornece chaves de criptografia para os nós do dispositivo StorageGRID .	CONFIGURAÇÃO > Segurança > Servidor de gerenciamento de chaves	"Adicionar servidor de gerenciamento de chaves (KMS)"

Certificado de ponto de extremidade 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 inquilinos > ARMAZENAMENTO (S3) > Pontos de extremidade de serviços de plataforma	"Criar ponto de extremidade de serviços de plataforma" "Editar ponto de extremidade dos serviços da plataforma"

Certificado de logon único (SSO)

Tipo de certificado	Descrição	Localização de navegação	Detalhes
Servidor	Autentica a conexão entre serviços de federação de identidade, como os Serviços de Federação do Active Directory (AD FS) e o StorageGRID , que são usados para solicitações de logon único (SSO).	CONFIGURAÇÃO > Controle de acesso > Logon único	"Configurar logon único"

Exemplos de certificados

Exemplo 1: serviço de balanceador de carga

Neste exemplo, o StorageGRID atua como servidor.

1. Você configura um ponto de extremidade do balanceador de carga e carrega ou gera um certificado de servidor no StorageGRID.

2. Você configura uma conexão de cliente S3 com o ponto de extremidade do balanceador de carga e carrega o mesmo certificado para o cliente.
3. Quando o cliente deseja salvar ou recuperar dados, ele se conecta ao ponto de extremidade do balanceador de carga usando HTTPS.
4. O StorageGRID responde com o certificado do servidor, que contém uma chave pública, e com uma assinatura baseada na chave privada.
5. O cliente verifica este certificado comparando a assinatura do servidor com a assinatura em sua cópia do certificado. Se as assinaturas corresponderem, o cliente inicia uma sessão usando a mesma chave pública.
6. O cliente envia dados do objeto para StorageGRID.

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

Neste exemplo, o StorageGRID atua como cliente.

1. Usando o software externo Key Management Server, você configura o StorageGRID como um cliente KMS e obtém um certificado de servidor assinado pela CA, um certificado de cliente público e a chave privada para o certificado de cliente.
2. Usando o Grid Manager, você configura um servidor KMS e carrega os certificados do servidor e do cliente e a chave privada do cliente.
3. Quando um nó StorageGRID precisa de uma chave de criptografia, ele faz uma solicitação ao servidor KMS que inclui dados do certificado e uma assinatura 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

O sistema StorageGRID suporta certificados personalizados criptografados com RSA ou ECDSA (Algoritmo de Assinatura Digital de Curva Elíptica).



O tipo de cifra da política de segurança deve corresponder ao tipo de certificado do servidor. Por exemplo, cifras RSA exigem certificados RSA, e cifras ECDSA exigem certificados ECDSA. Ver ["Gerenciar certificados de segurança"](#). Se você configurar uma política de segurança personalizada que não seja compatível com o certificado do servidor, você poderá ["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 de interface de gerenciamento

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

Sobre esta tarefa

Por padrão, cada nó de administração recebe um certificado assinado pela CA da grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de interface de gerenciamento

personalizado comum e pela 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 multidomínio se os clientes precisarem verificar o nome do host ao se conectar ao Grid Manager e ao Tenant Manager. Defina o certificado personalizado de forma que ele corresponda a todos os nós de administração na grade.

Você precisa concluir a configuração no servidor e, dependendo da autoridade de certificação raiz (CA) que estiver usando, os usuários também podem precisar instalar o certificado Grid CA no navegador da Web que usarão para acessar o Grid Manager e o Tenant Manager.



Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiração do certificado do servidor para a Interface de Gerenciamento** é acionado quando este certificado do servidor está prestes a expirar. Conforme necessário, você pode visualizar quando o certificado atual expira selecionando **CONFIGURAÇÃO > Segurança > Certificados** e verificando 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 mostrará um erro de certificado sem uma opção para ignorar se ocorrer qualquer uma das seguintes situações:

- Seu certificado de interface de gerenciamento personalizado expira.
- 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 de interface de gerenciamento**.
3. Selecione **Usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os arquivos de certificado do servidor necessários.

a. Selecione **Carregar certificado**.

b. Carregue os arquivos de certificado do servidor necessários:

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



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

- **Pacote CA:** Um único arquivo opcional contendo os certificados de cada autoridade certificadora intermediária emissora (CA). O arquivo deve conter cada um dos arquivos de certificado 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 será exibido em sua própria guia.

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

Especifique o nome do arquivo do certificado e o local do 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 e colá-lo em outro lugar.

d. Selecione **Salvar**. + O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao 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 de certificação externa.

a. Selecione **Gerar certificado**.

b. Especifique as informações do certificado:

Campo	Descrição
Nome de domínio	Um ou mais nomes de domínio totalmente qualificados a serem incluídos no certificado. Use um * como curinga para representar vários nomes de domínio.

Campo	Descrição
IP	Um ou mais endereços IP a serem incluídos no certificado.
Assunto (opcional)	Assunto X.509 ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (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. Observação: 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 ver os metadados do certificado gerado.

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

e. Selecione **Salvar**. + O certificado de interface de gerenciamento personalizado é usado para todas as novas conexões subsequentes ao Grid Manager, Tenant Manager, Grid Manager API ou Tenant Manager API.

5. Atualize a página para garantir que o navegador da web esteja atualizado.



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

6. Depois de adicionar um certificado de interface de gerenciamento personalizado, a página Certificado da interface de gerenciamento exibe informações detalhadas do certificado que está em uso. + Você pode baixar ou copiar o certificado PEM conforme necessário.

Restaurar o certificado da interface de gerenciamento padrão

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 de interface de gerenciamento**.
3. Selecione **Usar certificado padrão**.

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

4. Atualize a página para garantir que o navegador da web esteja atualizado.

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

Se for 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 `Passwords.txt` arquivo.

Sobre esta tarefa

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

Passos

1. Obtenha o nome de domínio totalmente qualificado (FQDN) de cada nó de administração.
2. Efetue login no nó de administração principal:
 - a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
 - b. Digite a senha listada no `Passwords.txt` arquivo.
 - c. Digite o seguinte comando para alternar para root: `su -`
 - d. Digite a senha listada no `Passwords.txt` arquivo.

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

3. Configure o StorageGRID com um novo certificado autoassinado.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- Para `--domains`, use curingas para representar os nomes de domínio totalmente qualificados de todos os nós de administração. Por exemplo, `*.ui.storagegrid.example.com` usa o curinga `*` para representar `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
- Definir `--type` para `management` para 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 o StorageGRID; caso contrário, o cliente poderá rejeitar o certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
```

A saída resultante contém o certificado público necessário para seu cliente de API de gerenciamento.

4. Selecione e copie o certificado.

Inclua as tags BEGIN e END na sua seleção.

5. Saia do shell de comando. `$ exit`

6. Confirme se o certificado foi configurado:

- Acesse o Grid Manager.
- Selecione **CONFIGURAÇÃO > Segurança > Certificados**
- Na guia **Global**, selecione **Certificado de interface de gerenciamento**.

7. Configure seu cliente de gerenciamento para usar o certificado público que você copiou. Inclua as tags 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 lugar.

Passos

- Selecione **CONFIGURAÇÃO > Segurança > Certificados**.
- Na guia **Global**, selecione **Certificado de interface de gerenciamento**.
- Selecione a aba **Servidor** ou **Pacote de CA** e então baixe ou copie o certificado.

Baixar arquivo de certificado ou pacote de CA

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

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

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

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

Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote CA PEM

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

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

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

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

Por exemplo: `storagegrid_certificate.pem`

Configurar certificados da API S3

Você pode substituir ou restaurar o certificado do servidor usado para conexões do cliente S3 com nós de armazenamento ou com pontos de extremidade do balanceador de carga. O certificado de servidor personalizado de substituição é específico para sua organização.



Os detalhes do Swift foram removidos desta versão do site de documentação. Ver ["StorageGRID 11.8: Configurar certificados S3 e Swift API"](#) .

Sobre esta tarefa

Por padrão, cada nó de armazenamento recebe um certificado de servidor X.509 assinado pela CA da grade. Esses certificados assinados pela CA podem ser substituídos por um único certificado de servidor personalizado comum e pela chave privada correspondente.

Um único certificado de servidor personalizado é usado para todos os nós de armazenamento, portanto, você deve especificar o certificado como um certificado curinga ou multidomínio se os clientes precisarem verificar o nome do host ao se conectar ao ponto de extremidade de armazenamento. Defina o certificado personalizado de forma que ele corresponda a todos os nós de armazenamento na grade.

Após concluir a configuração no servidor, talvez você também precise instalar o certificado Grid CA no cliente

S3 API que você usará para acessar o sistema, dependendo da autoridade de certificação raiz (CA) que estiver usando.



Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiração do certificado de servidor global para API S3** é acionado quando o certificado do servidor raiz está prestes a expirar. Conforme necessário, você pode visualizar quando o certificado atual expira selecionando **CONFIGURAÇÃO > Segurança > Certificados** e verificando a data de expiração do certificado da API 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 guia **Global**, selecione **Certificado S3 API**.
3. Selecione **Usar certificado personalizado**.
4. Carregue ou gere o certificado.

Carregar certificado

Carregue os arquivos de certificado do servidor necessários.

a. Selecione **Carregar certificado**.

b. Carregue os arquivos de certificado do servidor necessários:

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



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

- **Pacote CA:** Um único arquivo opcional contendo os certificados de cada autoridade certificadora emissora intermediária. O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados na ordem da cadeia de certificados.

c. Selecione os detalhes do certificado para exibir os metadados e o PEM para cada certificado de API S3 personalizado que foi carregado. Se você carregou um pacote de CA opcional, cada certificado será exibido em sua própria guia.

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

Especifique o nome do arquivo do certificado e o local do 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 e colá-lo 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 a serem incluídos no certificado. Use um * como curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a serem incluídos no certificado.

Campo	Descrição
Assunto (opcional)	Assunto X.509 ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (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. Observação: 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 exibir os metadados e o PEM do certificado S3 API personalizado que foi gerado.

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

e. Selecione **Salvar**.

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

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

6. Atualize a página para garantir que o navegador da web esteja atualizado.

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

Restaurar o certificado padrão da API S3

Você pode voltar a usar o certificado padrão da API S3 para conexões de cliente S3 com nós de armazenamento. No entanto, você não pode usar o certificado padrão da API S3 para um ponto de extremidade do balanceador de carga.

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Certificados**.
2. Na guia **Global**, selecione **Certificado S3 API**.
3. Selecione **Usar certificado padrão**.

Quando você restaura 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 nós de armazenamento.

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 de API S3 personalizado tiver sido usado para conexões de ponto de extremidade do balanceador de carga, será exibida uma lista de pontos de extremidade do balanceador de carga que não estarão mais acessíveis usando o certificado de API S3 padrão. 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 da 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 guia **Global**, selecione **Certificado S3 API**.
3. Selecione a aba **Servidor** ou **Pacote de CA** e então baixe ou copie o certificado.

Baixar arquivo de certificado ou pacote de CA

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

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

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

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

Por exemplo: `storagegrid_certificate.pem`

Copiar certificado ou pacote CA PEM

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

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

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

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

Por exemplo: `storagegrid_certificate.pem`

Informações relacionadas

- ["Usar API REST do S3"](#)
- ["Configurar nomes de domínio de endpoint S3"](#)

Copie o certificado Grid CA

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

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da 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 CA do sistema StorageGRID .

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Certificados** e então selecione a aba **Grid CA**.

2. Na seção **Certificado PEM**, baixe ou copie o certificado.

Baixar arquivo de certificado

Baixe o certificado .pem arquivo.

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

Por exemplo: `storagegrid_certificate.pem`

Certificado de cópia PEM

Copie o texto do certificado para colar em outro lugar.

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

Por exemplo: `storagegrid_certificate.pem`

Configurar certificados StorageGRID para FabricPool

Para clientes S3 que realizam validação estrita de nome de host e não oferecem suporte à desabilitação da validação estrita de nome de host, como clientes ONTAP que usam FabricPool, você pode gerar ou carregar um certificado de servidor ao configurar o ponto de extremidade do balanceador de carga.

Antes de começar

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

Sobre esta tarefa

Ao criar um ponto de extremidade do balanceador de carga, você pode gerar um certificado de servidor autoassinado ou carregar um certificado assinado por uma autoridade de certificação (CA) conhecida. Em ambientes de produção, você deve usar um certificado assinado por uma CA conhecida. Certificados assinados por uma CA podem ser rotacionados sem interrupções. Eles também são mais seguros porque oferecem melhor proteção contra ataques do tipo man-in-the-middle.

As etapas a seguir fornecem diretrizes gerais para clientes S3 que usam o FabricPool. Para obter informações e procedimentos mais detalhados, consulte ["Configurar StorageGRID para FabricPool"](#) .

Passos

- Opcionalmente, configure um grupo de alta disponibilidade (HA) para uso pelo FabricPool .
- Crie um ponto de extremidade do balanceador de carga S3 para o FabricPool usar.

Ao criar um ponto de extremidade do balanceador de carga HTTPS, você será solicitado a carregar seu certificado de servidor, a chave privada do certificado e o pacote de CA opcional.

3. Anexe o StorageGRID como uma camada de nuvem no ONTAP.

Especifique a porta do ponto de extremidade 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 uma CA intermediária emitiu o certificado StorageGRID, você deverá fornecer o certificado da CA intermediária. Se o certificado StorageGRID foi emitido diretamente pela CA raiz, você deve fornecer o certificado da CA raiz.

Configurar certificados de cliente

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 precisar acessar o StorageGRID usando uma ferramenta de monitoramento externa, você deverá carregar ou gerar um certificado de cliente usando o Grid Manager e copiar as informações do certificado para a ferramenta externa.

Ver ["Gerenciar certificados de segurança"](#) e ["Configurar certificados de servidor personalizados"](#).



Para garantir que as operações não sejam interrompidas por um certificado de servidor com falha, o alerta **Expiração de certificados de cliente configurados na página Certificados** é acionado quando este certificado de servidor está prestes a expirar. Conforme necessário, você pode visualizar quando o certificado atual expira selecionando **CONFIGURAÇÃO > Segurança > Certificados** e verificando 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 Grid Manager usando um ["navegador da web compatível"](#).
- Para configurar um certificado de cliente:
 - Você tem o endereço IP ou nome de domínio do nó de administração.
 - Se você configurou o certificado da interface de gerenciamento do StorageGRID, terá 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 no 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, será necessário criar uma nova.
- Para editar um certificado de cliente:
 - Você tem o endereço IP ou nome de domínio do nó de administração.
 - Para carregar seu próprio certificado ou um novo certificado, a chave privada, o certificado do cliente e a CA (se usada) estão disponíveis no seu computador local.

Adicionar certificados de cliente

Para adicionar o certificado do cliente, use um destes procedimentos:

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

Certificado de interface de gerenciamento já configurado

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

Passos

1. No Grid Manager, selecione **CONFIGURAÇÃO > Segurança > Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione **Adicionar**.
3. Digite um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir Prometheus**.
5. Selecione **Continuar**.
6. Para a etapa **Anexar certificados**, carregue o certificado da interface de gerenciamento.
 - a. Selecione **Carregar certificado**.
 - b. Selecione **Navegar** 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 PEM do certificado.
 - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.
 - c. Selecione **Criar** para salvar o certificado no Grid Manager.

O novo certificado aparece na aba 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 de administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para o Prometheus que use um certificado de cliente emitido por uma CA e uma chave privada.

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 **Adicionar**.
4. Digite um nome de certificado.
5. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione

Permitir Prometheus.

6. Selecione **Continuar**.
7. Para a etapa **Anexar certificados**, carregue o certificado do cliente, a chave privada e os arquivos do pacote da CA:
 - a. Selecione **Carregar certificado**.
 - b. Selecione **Navegar** e selecione o certificado do cliente, a chave privada e os arquivos do pacote CA(.pem).
 - Selecione **Detalhes do certificado do cliente** para exibir os metadados do certificado e o PEM do certificado.
 - Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.
 - c. Selecione **Criar** para salvar o certificado no Grid Manager.

Os novos certificados aparecem na aba Cliente.

8. [Configurar uma ferramenta de monitoramento externa](#), como Grafana.

Certificado gerado pelo Grid Manager

Use este procedimento para adicionar um certificado de cliente de administrador se um certificado de interface de gerenciamento não tiver sido configurado e você planeja adicionar um certificado de cliente para o Prometheus que use a função de geração de certificado no Grid Manager.

Passos

1. No Grid Manager, selecione **CONFIGURAÇÃO > Segurança > Certificados** e, em seguida, selecione a guia **Cliente**.
2. Selecione **Adicionar**.
3. Digite um nome de certificado.
4. Para acessar as métricas do Prometheus usando sua ferramenta de monitoramento externa, selecione **Permitir Prometheus**.
5. Selecione **Continuar**.
6. Para a etapa **Anexar certificados**, selecione **Gerar certificado**.
7. Especifique as informações do certificado:
 - **Assunto** (opcional): Assunto X.509 ou nome distinto (DN) do proprietário do certificado.
 - **Dias válidos**: O número de dias em que o certificado gerado é válido, a partir do momento em que ele é gerado.
 - **Adicionar extensões de uso de chave**: Se selecionado (padrão e recomendado), as extensões de uso de chave e de uso de chave estendida 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 e colá-lo em outro lugar.
- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado e colá-la 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 do download.

10. Selecione **Criar** para salvar o certificado no Grid Manager.

O novo certificado aparece na aba Cliente.

11. No Grid Manager, selecione **CONFIGURAÇÃO > Segurança > Certificados** e, em seguida, selecione a guia **Global**.
12. Selecione **Certificado de interface de gerenciamento**.
13. Selecione **Usar certificado personalizado**.
14. Carregue os arquivos `certificate.pem` e `private_key.pem` do [detalhes do certificado do cliente](#) etapa. Não há necessidade de fazer upload do pacote CA.
 - a. Selecione **Carregar certificado** e depois selecione **Continuar**.
 - b. Carregar cada arquivo de certificado (`.pem`).
 - c. 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

1. Configure as seguintes configurações na sua ferramenta de monitoramento externa, como o Grafana.
 - a. **Nome:** Digite um nome para a conexão.

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

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

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

- c. Habilite **Autenticação de cliente TLS** e **Com certificado CA**.

- d. Em Detalhes de autenticação TLS/SSL, copie e cole: +
 - Certificado CA da interface de gerenciamento para **CA Cert**
 - O certificado do cliente para **Client Cert**
 - A chave privada para **Chave do Cliente**

e. **ServerName**: Digite 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 monitorar o StorageGRID"](#).

Editar certificados de cliente

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

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Certificados** e então selecione a aba **Cliente**.

As datas de expiração dos certificados e as permissões de acesso do Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já tiver expirado, uma mensagem será exibida na tabela e um alerta será disparado.

2. Selecione o certificado que você deseja editar.
3. Selecione **Editar** e depois selecione **Editar nome e permissão**
4. Digite um nome de certificado.
5. Para acessar as 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 carregar um novo certificado quando o atual expirar.

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Certificados** e então selecione a aba **Cliente**.

As datas de expiração dos certificados e as permissões de acesso do Prometheus estão listadas na tabela. Se um certificado expirar em breve ou já tiver expirado, uma mensagem será exibida na tabela e um alerta será disparado.

2. Selecione o certificado que você deseja editar.

3. Selecione **Editar** e depois 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. Carregar o nome do certificado do cliente(.pem).

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

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

Por exemplo: storagegrid_certificate.pem

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo 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 distinto (DN) do proprietário do certificado.
- **Dias válidos**: O número de dias em que o certificado gerado é válido, a partir do momento em que ele é gerado.
- **Adicionar extensões de uso de chave**: Se selecionado (padrão e recomendado), as extensões de uso de chave e de uso de chave estendida 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.

- c. Selecione **Gerar**.
- d. 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 e colá-lo em outro

lugar.

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar chave privada** para copiar a chave privada do certificado e colá-la 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 do download.

e. Selecione **Criar** para salvar o certificado no Grid Manager.

O novo certificado aparece na aba Cliente.

Baixar ou copiar certificados de cliente

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

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Certificados** e então selecione a aba **Cliente**.
2. Selecione o certificado que você deseja copiar ou baixar.
3. Baixe ou copie o certificado.

Baixar arquivo de certificado

Baixe o certificado `.pem` arquivo.

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

Por exemplo: `storagegrid_certificate.pem`

Certificado de cópia

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 então selecione a aba **Cliente**.
2. Selecione o certificado que você deseja remover.
3. Selecione **Excluir** e depois confirme.



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

Após a remoção de um certificado, os clientes que o utilizaram devem especificar um novo certificado de cliente para acessar o banco de dados StorageGRID Prometheus.

Configurar definições de segurança

Gerenciar a política TLS e SSH

A política 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 TLS e SSH criptografam dados em movimento. Em geral, use a política de compatibilidade Moderna (padrão), a menos que seu sistema precise ser compatível com os Critérios Comuns ou você precise usar outras cifras.



Alguns serviços do StorageGRID não foram atualizados para usar as cifras nessas políticas.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da 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 TLS e SSH** mostra as políticas disponíveis. A política atualmente ativa é indicada por uma marca de seleção verde no bloco de políticas.



2. Revise os blocos para saber mais sobre as políticas disponíveis.

Política	Descrição
Compatibilidade moderna (padrão)	Use a política padrão se precisar de criptografia forte e a menos que tenha requisitos especiais. Esta política é compatível com a maioria dos clientes TLS e SSH.
Compatibilidade com legados	Use esta política se precisar de opções adicionais de compatibilidade para clientes mais antigos. As opções adicionais nesta política podem torná-la menos segura do que a política de compatibilidade moderna.
Crítérios comuns	Use esta política se precisar da certificação Common Criteria.
FIPS estrito	Use esta política se você precisar de certificação Common Criteria e usar o NetApp Cryptographic Security Module 3.0.8 para conexões de clientes externos com endpoints do balanceador de carga, Tenant Manager e Grid Manager. Usar esta política pode reduzir o desempenho. Observação: Depois de selecionar esta política, todos os nós devem ser "reiniciado de forma contínua" para ativar o Módulo de Segurança Criptográfica NetApp . Use Manutenção > Reinicialização contínua para iniciar e monitorar reinicializações.
Personalizado	Crie uma política personalizada se precisar aplicar suas próprias cifras.

3. Para ver detalhes sobre as cifras, protocolos e algoritmos de cada política, selecione **Exibir detalhes**.
4. Para alterar a política atual, selecione **Usar política**.

Uma marca de seleção verde aparece ao lado de **Política atual** no bloco de políticas.

Crie uma política de segurança personalizada

Você pode criar uma política personalizada se precisar aplicar suas próprias cifras.

Passos

1. No bloco da política mais semelhante à política personalizada que você deseja criar, selecione **Exibir detalhes**.
2. Selecione **Copiar para a área de transferência** e depois 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, talvez não consiga 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. Efetue login em um nó de administração:

- Digite o seguinte comando: `ssh admin@Admin_Node_IP`
- Digite a senha listada no `Passwords.txt` arquivo.
- Digite o seguinte comando para alternar para root: `su -`
- Digite a senha listada no `Passwords.txt` arquivo.

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

2. Execute o seguinte comando:

```
restore-default-cipher-configurations
```

3. Em um navegador da Web, acesse o Grid Manager no mesmo nó de administração.

4. Siga os passos em [Selecione uma política de segurança](#) para configurar a política novamente.

Configurar a segurança da rede e do objeto

Você pode configurar a segurança de rede e de objetos para criptografar objetos armazenados, impedir determinadas solicitações do S3 ou permitir que conexões de clientes com nós de armazenamento usem HTTP em vez de HTTPS.

Criptografia de objetos armazenados

A criptografia de objetos armazenados permite a criptografia de todos os dados de 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 ativa a configuração, todos os objetos recém-ingерidos são criptografados, mas nenhuma alteração é feita nos objetos armazenados existentes. Se você desabilitar a criptografia, os objetos criptografados atualmente permanecerão criptografados, mas os objetos recém-ingерidos não serão criptografados.

A configuração de criptografia de objeto armazenado se aplica somente a objetos do S3 que não foram criptografados pela criptografia em nível de bucket ou de objeto.

Para obter mais detalhes sobre os métodos de criptografia 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** é selecionada, as seguintes solicitações são negadas.

API REST S3

- Solicitações DeleteBucket
- Quaisquer solicitações para modificar dados de um objeto existente, metadados definidos pelo usuário ou marcação de objeto S3

Habilitar HTTP para conexões de nó de armazenamento

Por padrão, os aplicativos cliente usam o protocolo de rede HTTPS para qualquer conexão direta com os nós de armazenamento. Opcionalmente, você pode habilitar HTTP para essas conexões, por exemplo, ao testar uma grade que não seja de produção.

Use HTTP para conexões de nós de armazenamento somente se os clientes S3 precisarem fazer conexões HTTP diretamente com os nós de armazenamento. Você não precisa usar esta opção para clientes que usam apenas conexões HTTPS ou para clientes que se conectam ao serviço Load Balancer (porque você pode ["configurar cada ponto de extremidade do balanceador de carga"](#) para usar HTTP ou HTTPS).

Ver ["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.

Selecionar opções

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem permissão de acesso Root.

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Configurações de segurança**.
2. Selecione a aba **Rede e objetos**.
3. Para criptografia de objetos armazenados, use a configuração **Nenhum** (padrão) se não quiser que objetos armazenados sejam criptografados ou selecione **AES-128** ou **AES-256** para criptografar objetos armazenados.
4. Opcionalmente, selecione **Impedir modificação do cliente** se quiser impedir que 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 dimensionamento.

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 o HTTP para uma grade de produção porque as solicitações serão enviadas sem criptografia.

6. Selecione **Salvar**.

Alterar as configurações de segurança da interface

As configurações de segurança da interface permitem que você controle se os usuários serão desconectados caso fiquem inativos por mais tempo do que o especificado e se um rastreamento de pilha será incluído nas respostas de erro da API.

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você tem "[Permissão de acesso root](#)".

Sobre esta tarefa

A página **Configurações de segurança** inclui as configurações de **Tempo limite de inatividade do navegador** e **Rastreamento de pilha da API de gerenciamento**.

Tempo limite de inatividade do navegador

Indica por quanto tempo o navegador de um usuário pode ficar inativo antes que ele seja desconectado. O padrão é 15 minutos.

O tempo limite de inatividade do navegador também é controlado pelo seguinte:

- Um temporizador StorageGRID separado e não configurável, incluído para segurança do sistema. O token de autenticação de cada usuário expira 16 horas após o usuário efetuar 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 o valor do tempo limite do navegador não tenha sido atingido. Para renovar o token, o usuário deve efetuar login novamente.
- Configurações de tempo limite para o provedor de identidade, supondo que o logon único (SSO) esteja habilitado para StorageGRID.

Se o SSO estiver habilitado e o navegador do usuário expirar, o usuário deverá inserir novamente suas credenciais de SSO para acessar o StorageGRID novamente. Ver "[Configurar logon único](#)".

Rastreamento de pilha da API de gerenciamento

Controla se um rastreamento de pilha é retornado nas respostas de erro da API do Grid Manager e do Tenant Manager.

Esta opção está desabilitada por padrão, mas talvez você queira habilitar essa funcionalidade para um ambiente de teste. Em geral, você deve deixar o rastreamento de pilha desabilitado 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 aba **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 15 minutos.
 - c. Para desativar esse recurso, desmarque a caixa de seleção.
 - d. Selecione **Salvar**.

A nova configuração não afeta os usuários que estão conectados no momento. Os usuários devem fazer login novamente ou atualizar seus navegadores para que a nova configuração de tempo limite entre em vigor.

4. Para alterar a configuração do rastreamento de pilha da API de gerenciamento:
 - a. Expanda o acordeão.
 - b. Marque 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 desabilitado em ambientes de produção para evitar revelar detalhes internos do software quando ocorrerem erros de API.

- c. Selecione **Salvar**.

Configurar servidores de gerenciamento de chaves

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

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

O StorageGRID suporta apenas determinados servidores de gerenciamento de chaves. Para obter uma lista de produtos e versões suportados, use o ["Ferramenta de Matriz de Interoperabilidade NetApp \(IMT\)"](#).

Você pode usar um ou mais servidores de gerenciamento de chaves para gerenciar as chaves de criptografia de nós para qualquer nó do dispositivo StorageGRID que tenha a configuração **Criptografia de Nó** ativada durante a instalação. O uso de servidores de gerenciamento de chaves com esses nós de dispositivos 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

possa se comunicar com o KMS.



O StorageGRID não cria nem gerencia as chaves externas usadas para criptografar e descriptografar nós do dispositivo. Se você planeja usar um servidor externo de gerenciamento de chaves para proteger os dados do StorageGRID, você deve 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 precisar de ajuda, consulte a documentação do seu servidor de gerenciamento de chaves ou entre em contato com o suporte técnico.

Configuração do KMS e do dispositivo

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

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

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 de nós para novos nós do dispositivo, com base em seus requisitos.

Configurar o servidor de gerenciamento de chaves (KMS)

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

Etapa	Consulte
Acesse o software KMS e adicione um cliente para StorageGRID a cada KMS ou cluster KMS.	"Configurar o StorageGRID como um cliente no KMS"
Obtenha as informações necessárias para o cliente StorageGRID no KMS.	"Configurar o StorageGRID como um 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 aparelho

A configuração de um nó de dispositivo para uso do KMS inclui as seguintes etapas de alto nível.

1. Durante o estágio de configuração de hardware da instalação do dispositivo, use o StorageGRID Appliance Installer para habilitar a configuração **Criptografia de nó** para o dispositivo.



Não é possível habilitar a configuração **Criptografia de nó** depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não tenham a criptografia de nó habilitada.

2. Execute o instalador do dispositivo StorageGRID . Durante a instalação, uma chave de criptografia de dados aleatória (DEK) é atribuída a cada volume do dispositivo, da seguinte forma:
 - Os DEKs são usados para criptografar os dados em cada volume. Essas chaves são geradas usando a criptografia de disco Linux Unified Key Setup (LUKS) no sistema operacional do dispositivo 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 dispositivo possa se conectar ao KMS.
3. Adicione o nó do dispositivo ao StorageGRID.

Ver "[Habilitar criptografia de nó](#)" para mais detalhes.

Processo de criptografia de gerenciamento de chaves (ocorre automaticamente)

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

1. Quando você instala um dispositivo com criptografia de nó habilitada na grade, o 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 dispositivo receberá a configuração do KMS.
 - Se um KMS ainda não tiver sido configurado para o site, os dados no dispositivo continuarão sendo criptografados pela KEK temporária até que você configure um KMS para o site e o dispositivo receba a configuração do KMS.
2. O dispositivo usa a configuração do 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 os DEKs para os volumes do dispositivo.



Todos os dados existentes antes do nó do dispositivo criptografado se conectar ao KMS configurado são criptografados com uma chave temporária. No entanto, os volumes do dispositivo 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 reconectará ao KMS para solicitar a chave. A chave, que é salva na memória volátil, não sobrevive a uma queda de energia ou a uma reinicialização.

Considerações e requisitos para usar um servidor de gerenciamento de chaves

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

Qual versão do KMIP é suportada?

O StorageGRID suporta o KMIP versão 1.4.

["Especificação do Protocolo de Interoperabilidade de Gerenciamento de Chaves Versão 1.4"](#)

Quais são as considerações sobre a rede?

As configurações do firewall de rede devem permitir que cada nó do dispositivo se comunique por meio da 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 de rede ao KMS ou cluster KMS que você configurou para o site.

Quais versões do TLS são suportadas?

As comunicações entre os nós do dispositivo e o KMS configurado usam conexões TLS seguras. O StorageGRID pode oferecer suporte ao protocolo TLS 1.2 ou TLS 1.3 ao fazer conexões KMIP com um cluster KMS ou KMS, com base no que o KMS oferece suporte e em quais ["Política de TLS e SSH"](#) você está usando.

O StorageGRID negocia o protocolo e a cifra (TLS 1.2) ou conjunto de cifras (TLS 1.3) com o KMS quando faz a conexão. Para ver quais versões de protocolo e cifras/conjuntos de cifras estão disponíveis, revise o `tlsOutbound` seção da política TLS e SSH ativa da grade (**CONFIGURAÇÃO > Segurança Configurações de segurança**).

Quais aparelhos são suportados?

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



Não é possível habilitar a criptografia de nós depois que um dispositivo é adicionado à grade e não é possível usar o gerenciamento de chaves externas para dispositivos que não tenham a criptografia de nós habilitada.

Você pode usar o KMS configurado para dispositivos e nós de dispositivos StorageGRID .

Não é possível usar o KMS configurado para nós baseados em software (não dispositivos), incluindo o seguinte:

- 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 armazenamento de dados ou do disco.

Quando devo configurar servidores de gerenciamento de chaves?

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

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

Quantos servidores de gerenciamento de chaves eu preciso?

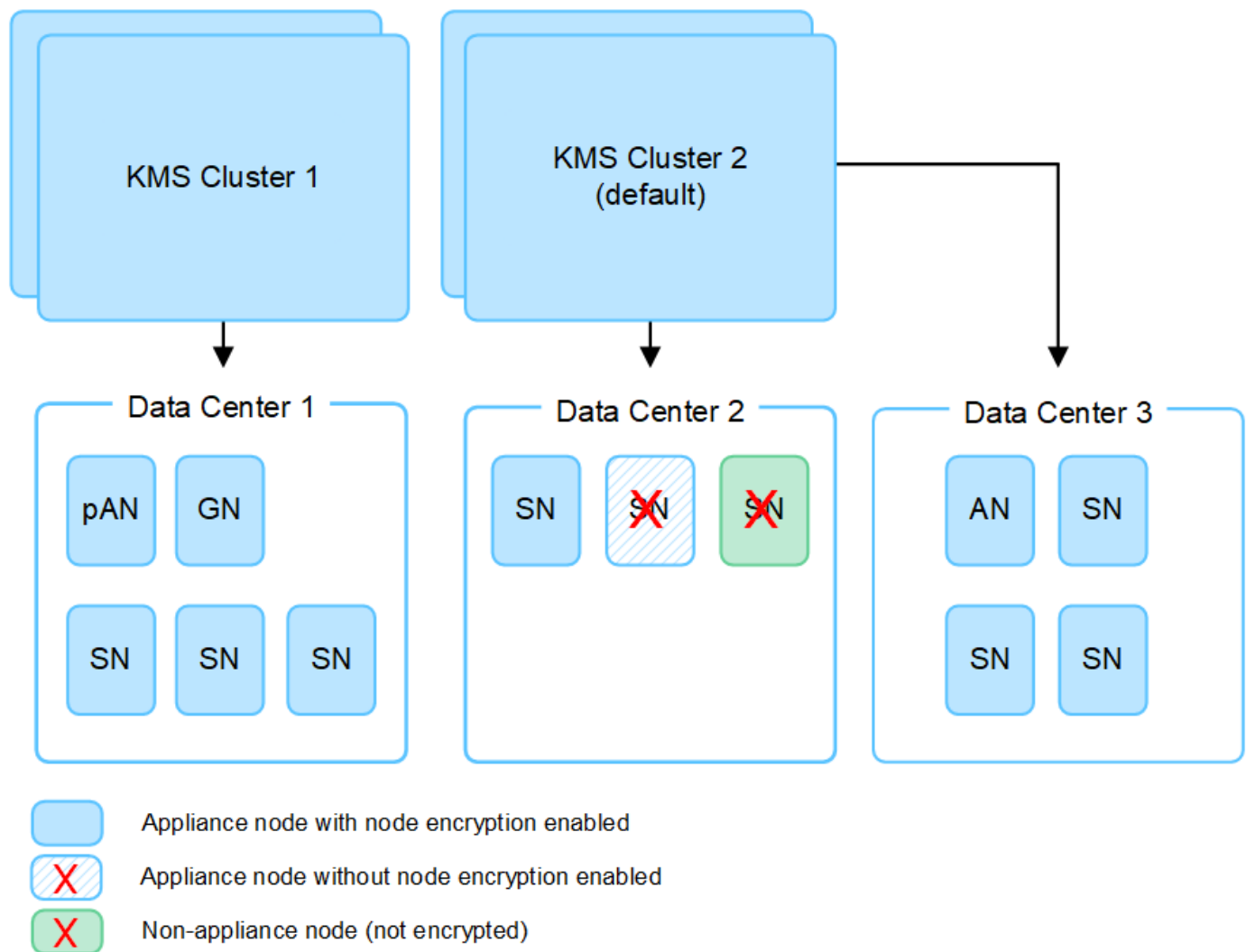
Você pode configurar um ou mais servidores externos de gerenciamento de chaves para fornecer chaves de

criptografia aos nós do dispositivo no seu sistema StorageGRID . Cada KMS fornece uma única chave de criptografia para os nós do dispositivo StorageGRID em um único site ou em um grupo de sites.

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

Por exemplo, suponha que seu sistema StorageGRID tenha três locais de data center. Você pode configurar um cluster KMS para fornecer uma chave para todos os nós do dispositivo no Data Center 1 e um segundo cluster KMS para fornecer uma chave para todos os nós do dispositivo em todos os outros 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 de dispositivo ou para nós de dispositivo que não tenham a configuração **Criptografia de nó** ativada durante a instalação.



O que acontece quando uma chave é girada?

Como prática recomendada de segurança, você deve periodicamente ["gire a chave de criptografia"](#) usado por cada KMS configurado.

Quando a nova versão da chave estiver disponível:

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

Posso reutilizar um nó de dispositivo depois que ele for criptografado?

Se você precisar instalar um dispositivo criptografado em outro sistema StorageGRID , primeiro desative o nó da grade para mover os dados do objeto para outro nó. Em seguida, você pode usar o StorageGRID Appliance Installer para "[limpar a configuração do KMS](#)". Limpar a configuração do KMS desabilita a configuração **Criptografia de nó** e remove a associação entre o nó do dispositivo e a configuração do KMS para o site StorageGRID .



Sem acesso à chave de criptografia do KMS, todos os dados que permanecerem no dispositivo não poderão mais ser acessados e serão bloqueados permanentemente.

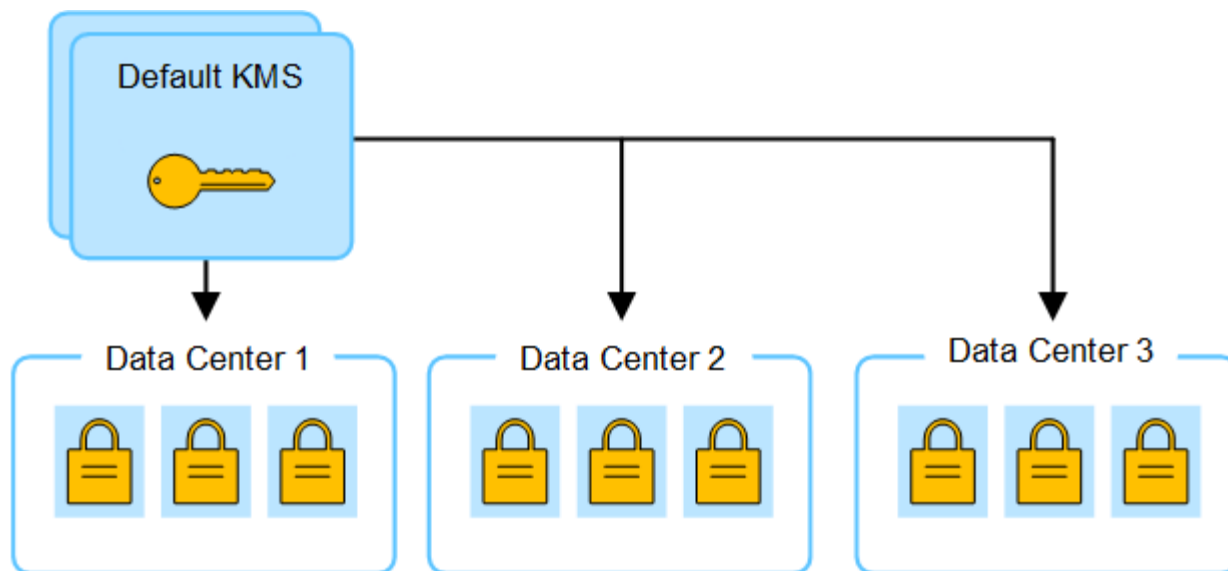
Considerações para alterar o KMS de um site

Cada servidor de gerenciamento de chaves (KMS) ou cluster KMS fornece uma chave de criptografia para todos os nós do dispositivo em um único 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.

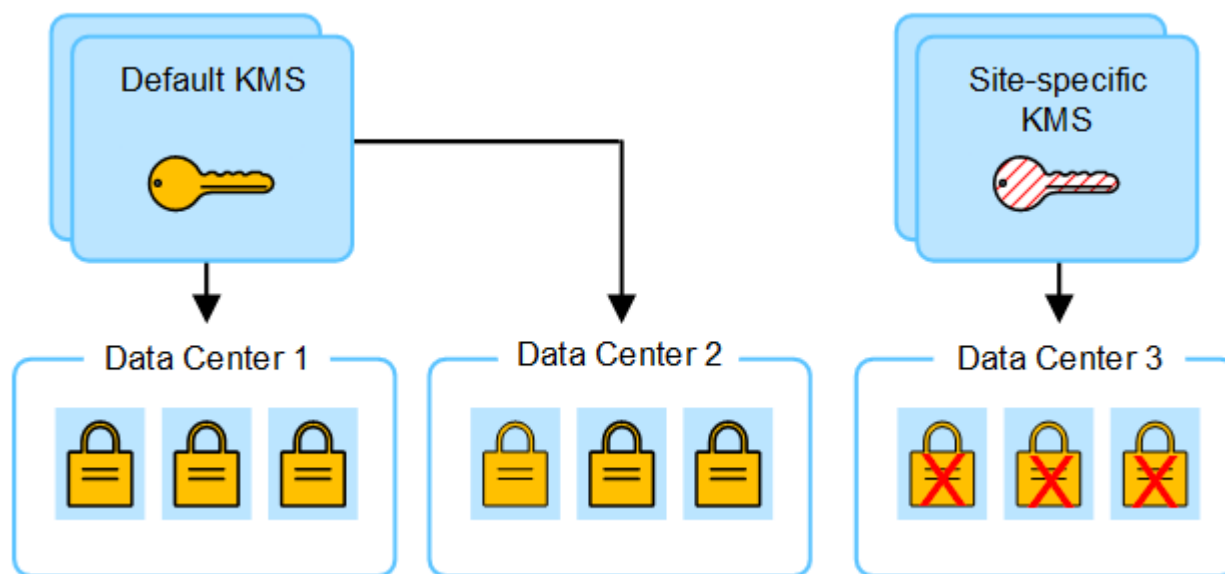
Se você alterar o KMS usado para um site, deverá garantir que os nós do dispositivo criptografados anteriormente naquele site possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, pode ser necessário copiar a versão atual da chave de criptografia do KMS original para o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

Por exemplo:

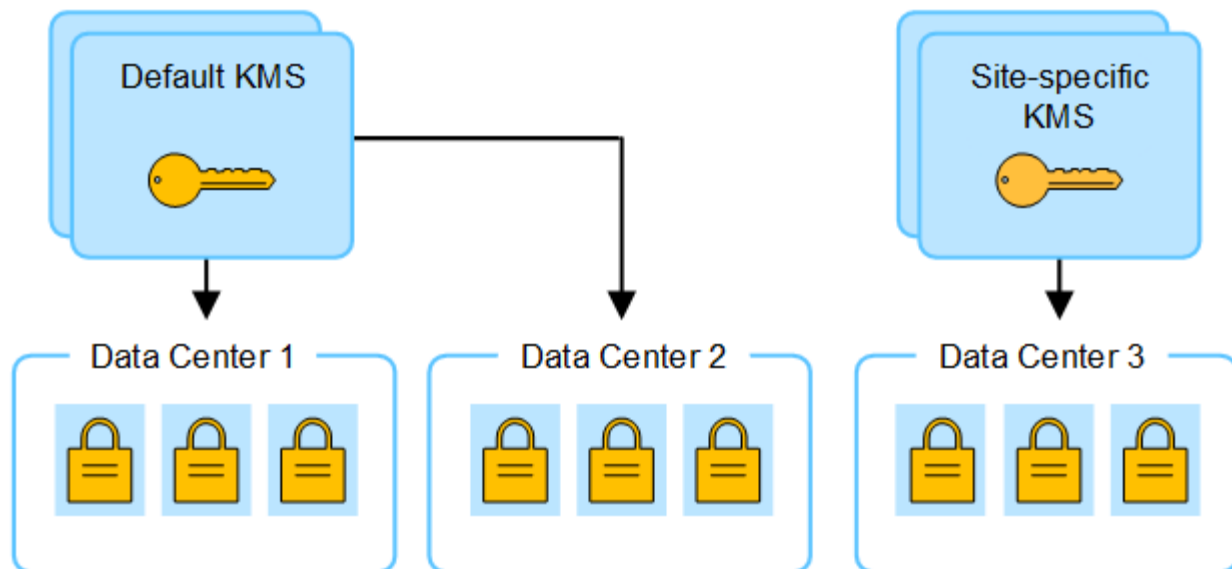
1. Inicialmente, você configura um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós do dispositivo que têm a configuração **Criptografia de nó** ativada se conectam ao KMS e solicitam a chave de criptografia. Esta chave é usada para criptografar os nós do dispositivo em todos os sites. Essa mesma chave também deve ser usada para descriptografar esses aparelhos.



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



4. Para resolver o problema, copie a versão atual da chave de criptografia do KMS padrão para o novo KMS. (Tecnicamente, você copia a chave original para uma nova chave com o mesmo alias. A chave original se torna uma versão anterior da nova chave.) O KMS específico do site agora tem a chave correta para descriptografar os nós do dispositivo no Data Center 3, para que ela possa 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 tem uma ou mais entradas KMS específicas do site e deseja usar uma delas como o 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 tem um KMS padrão e adiciona um novo site em uma expansão. Você não quer usar o KMS padrão para o novo site.	- Se os nós do dispositivo 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. - Usando o Grid Manager, adicione o novo KMS e selecione o site. "Adicionar um servidor de gerenciamento de chaves (KMS)"
Você quer que o KMS de um site use um servidor diferente.	- Se os nós do dispositivo no site 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. - Usando o Grid Manager, edite a configuração do KMS existente e insira o novo nome do host ou endereço IP. "Adicionar um servidor de gerenciamento de chaves (KMS)"

Configurar o StorageGRID como um cliente no KMS

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

StorageGRID.



Estas instruções se aplicam ao Thales CipherTrust Manager e ao Hashicorp Vault. Para obter uma lista de produtos e versões suportados, use o ["Ferramenta de Matriz de Interoperabilidade NetApp \(IMT\)"](#).

Passos

1. No 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 dispositivos StorageGRID em um único site ou em um grupo de sites.

2. Crie uma chave usando um dos dois métodos a seguir:
 - Use 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.

- Faça com que o StorageGRID crie a chave. Você será avisado quando testar e salvar depois ["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 de chave para a chave de criptografia no KMS.

4. Para cada KMS ou cluster KMS, obtenha um certificado de servidor assinado por uma autoridade de certificação (CA) ou um pacote de certificados que contenha cada um dos arquivos de certificado de 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 do Privacy Enhanced Mail (PEM).
- O campo Nome Alternativo do Assunto (SAN) em cada certificado de servidor deve incluir o nome de domínio totalmente qualificado (FQDN) ou endereço IP ao qual o StorageGRID se conectará.



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

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

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

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

Adicionar um servidor de gerenciamento de chaves (KMS)

Use 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 o StorageGRID como um cliente no KMS"](#) , e você terá as informações necessárias para cada KMS ou cluster KMS.
- Você está conectado ao Grid Manager usando um ["navegador da 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 dispositivos criptografados por nó na grade serão criptografados pelo KMS padrão. Se você quiser criar um KMS específico do site mais tarde, primeiro deverá copiar a versão atual da chave de criptografia do KMS padrão para o novo KMS. Ver ["Considerações para alterar o KMS de um site"](#) para mais 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 **Criar**.

A etapa 1 (detalhes do KMS) do assistente Adicionar um servidor de gerenciamento de chaves 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 não criou uma chave usando seu produto KMS, será solicitado que o StorageGRID crie a chave.

Campo	Descrição
Gerencia chaves para	O site 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 gerenciará 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 todos os sites que não tenham um KMS dedicado e a todos os sites que você adicionar em expansões subsequentes. Observação: Um erro de validação ocorrerá quando você salvar a configuração do KMS se você selecionar um site que foi criptografado anteriormente pelo KMS padrão, mas não tiver fornecido 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 para o KMS. Observação: O campo Nome Alternativo do Assunto (SAN) do certificado do servidor deve incluir o FQDN ou endereço IP que você inserir aqui. Caso contrário, o 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 **Continuar**.

Etapa 2: Carregar 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. Na **Etapa 2 (Carregar certificado do servidor)**, navegue até o local do certificado do servidor ou pacote de certificados salvo.
2. Carregue o arquivo do 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 **Continuar**.

Etapa 3: Carregar certificados de cliente

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

Passos

1. Na **Etapa 3 (Carregar certificados do cliente)**, navegue até o local do certificado do cliente.
2. Carregue o arquivo de certificado do cliente.

Os metadados do certificado do cliente são exibidos.

3. Navegue até o local da chave privada do certificado do cliente.
4. Carregue o arquivo da chave privada.
5. Selecione **Testar e salvar**.

Se uma chave não existir, você será solicitado a solicitar que o StorageGRID crie uma.

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



Imediatamente após adicionar um KMS, o status do certificado na página Servidor de Gerenciamento de Chaves 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 quando você selecionar **Testar e salvar**, 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 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 dispositivo com esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós do dispositivo que tenham a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

8. Revise 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.

Gerenciar um KMS

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 Grid Manager usando um ["navegador da 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) no 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 guia Detalhes da configuração lista todos os servidores de gerenciamento de chaves que estão configurados.
 - A guia Nós criptografados lista todos os nós que têm a criptografia de nós habilitada.
2. Para visualizar os detalhes de um KMS específico e executar 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).
Nome do host	O nome de domínio totalmente qualificado ou endereço IP do KMS. Se houver um cluster de dois servidores de gerenciamento de chaves, o nome de domínio totalmente qualificado ou o endereço IP de ambos os servidores serão listados. Se houver mais de dois servidores de gerenciamento de chaves em um cluster, o nome de domínio totalmente qualificado ou o endereço IP do primeiro KMS será listado junto 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 guia na página de detalhes do KMS para visualizar as seguintes informações:

Aba	Campo	Descrição
Detalhes importantes	Nome da chave	O alias da chave para o cliente StorageGRID no KMS.
UID da chave	O identificador exclusivo da versão mais recente da chave.	Última modificação
Data e hora da versão mais recente da chave.	Certificado do servidor	Metadados
Os metadados do certificado, como número de série, data e hora de validade e o PEM do certificado.	Certificado PEM	O conteúdo do arquivo PEM (privacy enhanced mail) do certificado.
Certificado de cliente	Metadados	Os metadados do certificado, como número de série, data e hora de validade e o PEM do certificado.

4. Sempre que exigido pelas práticas de segurança da sua organização, selecione **Girar chave** ou use o software KMS para criar uma nova versão da chave.

Quando a rotação da chave é bem-sucedida, os campos UID da chave e Última modificação são atualizados.



Se você girar a chave de criptografia usando o software KMS, gire-a da última versão usada da chave para uma nova versão da mesma chave. Não gire para uma chave totalmente diferente.

Nunca tente rotacionar uma chave alterando o nome da chave (alias) para o KMS. O StorageGRID exige que todas as versões de chaves usadas anteriormente (bem como quaisquer futuras) sejam acessíveis a partir do KMS com o mesmo alias de chave. Se você alterar o alias da chave de um KMS configurado, o StorageGRID poderá não conseguir descriptografar seus dados.

Gerenciar certificados

Resolva imediatamente quaisquer problemas de certificado de servidor ou cliente. Se possível, substitua os certificados antes que eles expirem.



Você deve resolver quaisquer problemas de certificado 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 Expiração do certificado para cada KMS.
3. Se a expiração do certificado para qualquer KMS for Desconhecida, aguarde até 30 minutos e atualize seu navegador.
4. Se a coluna Expiração do certificado indicar que um certificado expirou ou está próximo da expiração, 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 essas subetapas e selecione **Certificado do cliente** em vez de Certificado do servidor.
5. Quando os alertas **Expiração do certificado da CA KMS**, **Expiração do certificado do cliente KMS** e **Expiração do certificado do servidor KMS** forem acionados, observe a descrição de cada alerta e execute as ações recomendadas.

Pode levar até 30 minutos para o StorageGRID receber 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**, certifique-se de que seu KMS permite obter um certificado de servidor sem exigir um certificado de cliente.

Exibir nós criptografados

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

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Servidor de gerenciamento de chaves**.

A página Servidor de Gerenciamento de Chaves é exibida. A guia Detalhes da configuração mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. No topo da página, selecione a aba **Nós criptografados**.

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

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

Coluna	Descrição
Nome do nó	O nome do nó do dispositivo.
Tipo de nó	O tipo de nó: Armazenamento, Administração ou Gateway.
Site	O nome do site StorageGRID onde o nó está instalado.

Coluna	Descrição
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 dispositivo. Para visualizar um UID de chave inteiro, selecione o texto. Um traço (--) indica que o UID da chave é desconhecido, possivelmente devido a um problema de conexão entre o nó do dispositivo e o KMS.
Status	O status da conexão entre o KMS e o nó do dispositivo. Se o nó estiver conectado, o registro de data e hora será atualizado a cada 30 minutos. Pode levar vários minutos para que o status da conexão seja atualizado após as alterações na configuração do KMS. Observação: Atualize seu navegador para ver os novos valores.

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

Durante as operações normais do KMS, o status será **Conectado ao KMS**. Se um nó for desconectado da rede, o estado da conexão do nó será exibido (Administrativamente inativo ou Desconhecido).

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

- Falha ao carregar a configuração do KMS
- Erro de conectividade do KMS
- Nome da chave de criptografia KMS não encontrado
- Falha na rotação da chave de criptografia do KMS
- A chave KMS falhou ao descriptografar um volume do dispositivo
- O 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 alterar o KMS de um site"](#).

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Permissão de acesso root"](#) .

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Servidor de gerenciamento de chaves**.

A página Servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que deseja editar e selecione **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 Editar um servidor de gerenciamento de chaves.

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.
Gerencia chaves para	Se você estiver editando um KMS específico do site e ainda não tiver um KMS padrão, opcionalmente selecione Sites não gerenciados por outro KMS (KMS padrão). Esta seleção converte um KMS específico do site no KMS padrão, que será aplicado a todos os sites que não têm um KMS dedicado e a quaisquer sites adicionados em uma expansão. Observação: se você estiver editando um KMS específico do site, não poderá selecionar outro site. Se você estiver editando o KMS padrão, não poderá selecionar um site específico.
Porta	A porta que o servidor KMS usa para comunicações 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 para o KMS. Observação: O campo Nome Alternativo do Assunto (SAN) do certificado do servidor deve incluir o FQDN ou endereço IP que você inserir aqui. Caso contrário, o 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 **Continuar**.

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

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

7. Selecione **Continuar**.

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

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

9. Selecione **Testar e salvar**.

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

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

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

11. Se 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 dispositivo com esse KMS. Se houver um problema com a configuração, talvez você não consiga reinicializar os nós do dispositivo que tenham a criptografia de nó ativada no site afetado. Você pode perder o acesso aos seus dados até que os problemas sejam resolvidos.

A configuração do KMS é salva.

12. Revise 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, pode ser necessário remover um servidor de gerenciamento de chaves. Por exemplo, você pode querer remover um KMS específico do site se tiver desativado o site.

Antes de começar

- Você revisou o ["considerações e requisitos para usar um servidor de gerenciamento de chaves"](#) .
- Você está conectado ao Grid Manager usando um ["navegador da 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 dispositivo com criptografia de nó habilitada.
- Você pode remover o KMS padrão se já existir um KMS específico do site para cada site que tenha nós de dispositivo com criptografia de nó habilitada.

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Servidor de gerenciamento de chaves**.

A página Servidor de gerenciamento de chaves é exibida e mostra todos os servidores de gerenciamento de chaves que foram configurados.

2. Selecione o KMS que deseja 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 de um site que não tem nenhum nó de dispositivo com criptografia de nó habilitada.
- Você está removendo o KMS padrão, mas já existe um KMS específico do site para cada site com criptografia de nó.

4. Selecione **Sim**.

A configuração do KMS foi removida.

Gerenciar configurações de proxy

Configurar proxy de armazenamento

Se estiver usando serviços de plataforma ou pools de armazenamento em nuvem, você poderá configurar um proxy não transparente entre os nós de armazenamento e os endpoints externos do S3. Por exemplo, você pode precisar de um proxy não transparente para permitir que mensagens de serviços de plataforma sejam enviadas para endpoints externos, como um endpoint na Internet.



As configurações de proxy de armazenamento configuradas não se aplicam aos pontos de extremidade dos serviços da plataforma Kafka.

Antes de começar

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

Sobre esta tarefa

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

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Configurações de proxy**.
2. Na guia **Armazenamento**, marque a caixa de seleção **Ativar proxy de armazenamento**.
3. Selecione o protocolo para o proxy de armazenamento.
4. Digite o nome do host ou endereço IP do servidor proxy.
5. Opcionalmente, insira a porta usada para conectar ao servidor proxy.

Deixe este campo em branco para usar a porta padrão para o protocolo: 80 para HTTP ou 1080 para SOCKS5.

6. Selecione **Salvar**.

Depois que o proxy de armazenamento for salvo, novos endpoints para serviços de plataforma ou pools de armazenamento em nuvem poderão ser configurados e testados.



As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

7. Verifique as configurações do seu servidor proxy para garantir que as mensagens relacionadas ao serviço de plataforma do StorageGRID não sejam bloqueadas.
8. Se precisar desabilitar um proxy de armazenamento, desmarque a caixa de seleção e selecione **Salvar**.

Configurar as definições de proxy do administrador

Se você enviar pacotes do AutoSupport usando HTTP ou HTTPS, poderá configurar um servidor proxy não transparente entre os nós de administração e o suporte técnico (AutoSupport).

Para obter mais informações sobre o AutoSupport, consulte "[Configurar AutoSupport](#)".

Antes de começar

- Você tem "[permissões de acesso específicas](#)".
- Você está conectado ao Grid Manager usando um "[navegador da 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, Armazenamento é selecionado no menu de guias.

2. Selecione a aba **Admin**.
3. Marque a caixa de seleção **Ativar proxy de administrador**.
4. Digite o nome do host ou 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 quiser proteger a conexão com o proxy do administrador, selecione **Verificar certificado de proxy**. Carregue um pacote de CA para verificar a autenticidade dos certificados SSL apresentados pelo servidor proxy do administrador.



O AutoSupport on Demand, o AutoSupport E-Series por meio do StorageGRID e a determinação do caminho de atualização na página de atualização do StorageGRID não funcionarão se um certificado proxy for verificado.

Depois de carregar o pacote CA, seus metadados aparecem.

- Se você não quiser validar certificados ao se comunicar com o servidor proxy do administrador, selecione **Não verificar certificado proxy**.

8. Selecione **Salvar**.

Depois que o proxy do administrador é salvo, o servidor proxy entre os nós de administração e o suporte técnico é configurado.



As alterações de proxy podem levar até 10 minutos para entrarem em vigor.

9. Se precisar desabilitar o proxy de administrador, desmarque a caixa de seleção **Habilitar proxy de administrador** e selecione **Salvar**.

Firewalls de controle

Controle de acesso em 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 locatários consigam se conectar ao Grid Manager pelo firewall, além de usar outros métodos para controlar o acesso ao sistema.

Se você quiser configurar o firewall interno do StorageGRID, consulte "[Configurar firewall interno](#)".

Porta	Descrição	Se a porta estiver aberta...
443	Porta HTTPS padrão para nós de administração	Navegadores da Web e clientes da API de gerenciamento podem acessar o Grid Manager, a Grid Management API, o Tenant Manager e a Tenant Management API. Observação: a porta 443 também é usada para algum tráfego interno.

Porta	Descrição	Se a porta estiver aberta...
8443	Porta do Grid Manager restrita em nós de administração	• Navegadores da Web e clientes da API de gerenciamento podem acessar o Grid Manager e a Grid Management API usando HTTPS. • Navegadores da Web e clientes da API de gerenciamento não podem acessar o Gerenciador de Tenants ou a API de Gerenciamento de Tenants. • Solicitações de conteúdo interno serão rejeitadas.
9443	Porta restrita do Tenant Manager em nós de administração	• Navegadores da Web e clientes da API de gerenciamento podem acessar o Gerenciador de Tenants e a API de Gerenciamento de Tenants usando HTTPS. • Navegadores da Web e clientes da API de gerenciamento não podem acessar o Grid Manager ou a Grid Management API. • Solicitações de conteúdo interno serão rejeitadas.



O logon 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 logon único.

Informações relacionadas

- ["Sign in no Grid Manager"](#)
- ["Criar conta de inquilino"](#)
- ["Comunicações externas"](#)

Gerenciar controles internos de firewall

O StorageGRID inclui um firewall interno em cada nó que aumenta a segurança da sua grade, permitindo que você controle o acesso da rede ao nó. Use o firewall para impedir o acesso à rede em todas as portas, exceto aquelas necessárias para sua implantação de grade específica. As alterações de configuração feitas na página de controle do Firewall são implantadas em cada nó.

Use as três guias na página de controle do Firewall para personalizar o acesso necessário para sua grade.

- **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 guia Gerenciar acesso externo.
- **Gerenciar acesso externo:** use esta guia para fechar portas que estão abertas por padrão ou reabrir portas fechadas anteriormente.
- **Rede de cliente não confiável:** use esta guia para especificar se um nó confia no tráfego de entrada da rede de cliente.

As configurações nesta guia substituem as configurações na guia Gerenciar acesso externo.

- Um nó com uma rede de cliente não confiável aceitará apenas conexões em portas de ponto de extremidade do balanceador de carga configuradas naquele nó (pontos de extremidade globais, de interface de nó e vinculados ao tipo de nó).
- As portas de ponto de extremidade do balanceador de carga *são as únicas portas abertas* em redes de clientes não confiáveis, independentemente das configurações na guia Gerenciar redes externas.
- Quando confiáveis, todas as portas abertas na guia Gerenciar acesso externo ficam acessíveis, assim como quaisquer pontos de extremidade do balanceador de carga abertos na Rede do Cliente.



As configurações feitas em uma guia podem afetar as alterações de acesso feitas em outra guia. Não deixe de verificar as configurações em todas as abas para garantir que sua rede se comporte da maneira esperada.

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 em firewall externo](#)".

Lista de endereços privilegiados e guias Gerenciar acesso externo

A guia Lista de endereços privilegiados permite que você registre um ou mais endereços IP que têm acesso às portas de rede que estão fechadas. A guia 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 que são acessíveis por nós não pertencentes à grade por padrão). Essas duas guias geralmente podem ser usadas juntas para personalizar o acesso exato à rede que você precisa permitir para sua grade.



Endereços IP privilegiados não têm acesso à porta de rede interna por padrão.

Exemplo 1: Use um host de salto para tarefas de manutenção

Suponha que você queira usar um host de salto (um host com segurança reforçada) para administração de rede. Você pode usar estas etapas gerais:

1. Use a guia Lista de endereços privilegiados para adicionar o endereço IP do host de salto.
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 em 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.

Depois de salvar sua configuração, todas as portas externas no nó de administração em sua grade serão bloqueadas para todos os hosts, exceto o host de salto. Você pode então usar o jump host para executar tarefas de manutenção na sua rede com mais segurança.

Exemplo 2: Bloquear portas sensíveis

Suponha que você queira bloquear portas sensíveis e o serviço nessa porta (por exemplo, SSH na porta 22). Você pode usar as seguintes etapas 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 para acessar o Grid Manager e o Tenant Manager (as portas predefinidas são 443 e 8443). Qualquer usuário conectado em 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.

Depois de salvar sua configuração, a porta 22 e o serviço SSH estarão disponíveis para hosts na lista de endereços privilegiados. Todos os outros hosts terão o acesso ao serviço negado, independentemente da interface de onde a solicitação vier.

Exemplo 3: Desabilitar acesso a serviços não utilizados

No nível da rede, você pode desabilitar alguns serviços que não pretende usar. Por exemplo, para bloquear o tráfego do cliente HTTP S3, você usaria a alternância na guia Gerenciar acesso externo para bloquear a porta 18084.

Guia Redes de clientes não confiáveis

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

Por padrão, a Rede do Cliente em cada nó da grade é *confiável*. Ou seja, por padrão, o 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 sistema StorageGRID especificando que a Rede do Cliente em cada nó seja *não confiável*. Se a rede do cliente de um nó não for confiável, o nó só aceitará conexões de entrada em portas explicitamente configuradas como pontos de extremidade do balanceador de carga. Ver ["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 recuse todo o tráfego de entrada na rede do cliente, exceto solicitações HTTPS S3. Você executaria estas etapas gerais:

1. Do ["Pontos de extremidade do balanceador de carga"](#) página, configure um ponto de extremidade do balanceador de carga para S3 sobre HTTPS na porta 443.
2. Na página de controle do Firewall, selecione Não confiável para especificar que a Rede do Cliente no Nó do Gateway não é confiável.

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

Exemplo 2: O nó de armazenamento envia solicitações de serviços da plataforma S3

Suponha que você queira habilitar o tráfego de serviços de plataforma S3 de saída de um nó de armazenamento, mas deseja impedir qualquer conexão de entrada para esse nó de armazenamento na rede do cliente. 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.

Depois de salvar sua configuração, o Nó de Armazenamento não aceita mais nenhum tráfego de entrada na Rede do Cliente, mas continua permitindo solicitações de saída para destinos de serviços de plataforma configurados.

Exemplo 3: Limitando o acesso ao Grid Manager a uma sub-rede

Suponha que você queira permitir acesso do Grid Manager somente em uma sub-rede específica. Você executaria os seguintes passos:

1. Anexe a rede do cliente dos seus nós de administração à sub-rede.
2. Use a guia Rede de cliente não confiável para configurar a Rede de cliente como não confiável.
3. Ao criar um ponto de extremidade do 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).

Depois de salvar sua configuração, somente hosts na sub-rede especificada poderão acessar o Grid Manager. Todos os outros hosts estão bloqueados.

Configurar firewall interno

Você pode configurar o firewall StorageGRID para controlar o acesso da rede a portas específicas nos seus nós StorageGRID .

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem ["permissões de acesso específicas"](#) .
- Você revisou as informações em ["Gerenciar controles de firewall"](#) e ["Diretrizes de rede"](#) .
- Se você quiser que um nó de administração ou nó de gateway aceite tráfego de entrada somente em pontos de extremidade explicitamente configurados, você terá definido os pontos de extremidade do balanceador de carga.



Ao alterar a configuração da Rede do Cliente, as conexões de cliente existentes podem falhar se os pontos de extremidade do balanceador de carga não tiverem sido configurados.

Sobre esta tarefa

O StorageGRID inclui um firewall interno em cada nó que permite abrir ou fechar algumas portas nos nós da sua grade. Você pode usar as guias de controle do Firewall para abrir ou fechar portas que são abertas por padrão na Rede Grid, Rede de Administração e Rede Cliente. Você também pode criar uma lista de endereços IP privilegiados que podem acessar portas de grade que estão fechadas. Se estiver usando uma Rede Cliente, você poderá especificar se um nó confia no tráfego de entrada da Rede Cliente e poderá configurar o acesso de portas específicas na Rede Cliente.

Limitar o número de portas abertas para endereços IP fora da sua rede apenas para aquelas que são absolutamente necessárias aumenta a segurança da sua rede. Use 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 o uso de 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 em firewall externo"](#) .

Controles de firewall de acesso

Passos

1. Selecione **CONFIGURAÇÃO > Segurança > Controle de firewall**.

As três guias nesta página são descritas em "[Gerenciar controles de firewall](#)".

2. Selecione qualquer aba para configurar os controles do firewall.

Você pode usar essas guias em qualquer ordem. As configurações definidas em uma guia não limitam o que você pode fazer nas outras guias; no entanto, as alterações de configuração feitas em uma guia podem alterar o comportamento das portas configuradas em outras guias.

Lista de endereços privilegiados

Use a guia Lista de endereços privilegiados para conceder aos hosts acesso a portas que estão fechadas por padrão ou fechadas por configurações na guia Gerenciar acesso externo.

Endereços IP e sub-redes privilegiados não têm acesso à rede interna por padrão. Além disso, os pontos de extremidade do balanceador de carga e as portas adicionais abertas na guia Lista de endereços privilegiados podem ser acessados mesmo se bloqueados na guia Gerenciar acesso externo.



As configurações na guia Lista de endereços privilegiados não podem substituir as configurações na guia Rede de clientes não confiáveis.

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 privilegiada.

3. Opcionalmente, selecione ***Permitir que endereços IP privilegiados acessem as portas internas do StorageGRID ***. Ver "[Portas internas do StorageGRID](#)".



Esta opção remove algumas proteções para serviços internos. Deixe-o desabilitado, se possível.

4. Selecione **Salvar**.

Gerenciar acesso externo

Quando uma porta é fechada na guia Gerenciar acesso externo, a porta não pode ser acessada por nenhum endereço IP que não seja da rede, 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 cliente não confiável. Por exemplo, se um nó não for confiável, a porta SSH/22 será bloqueada na Rede do Cliente, mesmo que esteja aberta na guia Gerenciar acesso externo. As configurações na guia Rede de cliente não confiável substituem portas fechadas (como 443, 8443, 9443) na Rede de cliente.

Passos

1. Selecione **Gerenciar acesso externo**. A guia exibe uma tabela com todas as portas externas (portas que são acessíveis por nós não pertencentes à grade por padrão) para os nós na sua grade.
2. Configure as portas que você deseja abrir e fechar usando as seguintes opções:
 - Use o botão de alternância 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 conectados em uma porta bloqueada, incluindo você, perderão o acesso ao Grid Manager, a menos que seus endereços IP tenham sido adicionados à lista de endereços privilegiados.



Use a barra de rolagem no lado direito da tabela para ter certeza de que visualizou todas as portas disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer porta externa inserindo um número de porta. Você pode inserir 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 **Salvar**

Rede de clientes não confiáveis

Se a rede do cliente de um nó não for confiável, o nó aceitará somente tráfego de entrada em portas configuradas como pontos de extremidade do balanceador de carga e, opcionalmente, portas adicionais selecionadas 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 pontos de extremidade do balanceador de carga não tiverem sido configurados.

As alterações de configuração feitas na guia **Rede de cliente não confiável** substituem as configurações na guia **Gerenciar acesso externo**.

Passos

1. Selecione **Rede de cliente não confiável**.
2. Na seção Definir novo nó padrão, especifique qual deve ser a configuração padrão quando novos nós são adicionados à grade em um procedimento de expansão.
 - **Confiável** (padrão): quando um nó é adicionado em uma expansão, sua Rede de Cliente é confiável.
 - **Não confiável**: quando um nó é adicionado em uma expansão, sua Rede de Cliente não é confiável.

Conforme necessário, você pode retornar a esta guia para alterar a configuração de um novo nó específico.



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

3. Use as seguintes opções para selecionar os nós que devem permitir conexões de cliente somente em pontos de extremidade do balanceador de carga explicitamente configurados ou em portas adicionais selecionadas:

- Selecione **Desconfiar dos nós exibidos** para adicionar todos os nós exibidos na tabela à lista Rede de clientes não confiáveis.
- Selecione **Confiar nos nós exibidos** para remover todos os nós exibidos na tabela da lista Rede de clientes não confiáveis.
- Use a alternância ao lado de cada nó para definir a Rede do Cliente como Confiável ou Não Confiável para o nó selecionado.

Por exemplo, você pode selecionar **Desconfiar dos nós exibidos** para adicionar todos os nós à lista Rede de clientes não confiáveis e, em seguida, usar a alternância ao lado de um nó individual para adicionar esse único nó à lista Rede de clientes confiáveis.



Use a barra de rolagem no lado direito da tabela para ter certeza de que visualizou todos os nós disponíveis. Use o campo de pesquisa para encontrar as configurações de qualquer nó inserindo o nome do nó. Você pode inserir um nome parcial. Por exemplo, se você digitar **GW**, todos os nós que têm a string "GW" como parte do nome serão exibidos.

4. Selecione **Salvar**.

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

Gerenciar inquilinos

O que são contas de inquilino?

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 .



Os detalhes do Swift foram removidos desta versão do site de documentação. Ver ["StorageGRID 11.8: Gerenciar locatários"](#) .

Como administrador de grade, você cria e gerencia as contas de locatário que os clientes S3 usam para armazenar e recuperar objetos.

Cada conta de locatário tem grupos federados ou locais, usuários, buckets S3 e objetos.

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 corporativo:** Se você estiver administrando um sistema StorageGRID em um aplicativo corporativo, talvez queira segregar o armazenamento de objetos da grade pelos diferentes departamentos da sua organização. Nesse caso, você pode 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 usar o protocolo de cliente S3, poderá usar buckets e políticas de bucket do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa usar contas de inquilino. Veja as instruções para implementação "[Buckets S3 e políticas de bucket](#)" para mais informações.

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

Para obter mais informações, consulte "[Use uma conta de inquilino](#)".

Como crio uma conta de inquilino?

Use o Grid Manager para criar uma conta de locatário. Ao criar uma conta de locatário, você especifica as seguintes informações:

- Informações básicas, incluindo nome do locatário, tipo de cliente (S3) e cota de armazenamento opcional.
- Permissões para a conta do locatário, como se a conta do locatário pode usar os serviços da plataforma S3, configurar sua própria fonte de identidade, usar o S3 Select ou usar uma conexão de federação de grade.
- O acesso root inicial para o locatário, com base no uso de grupos e usuários locais pelo sistema StorageGRID, federação de identidade ou logon único (SSO).

Além disso, você pode habilitar a configuração de Bloqueio de Objeto S3 para o sistema StorageGRID se as contas de locatário S3 precisarem estar em conformidade com os requisitos regulatórios. Quando o Bloqueio de Objeto S3 está habilitado, todas as contas de locatário S3 podem criar e gerenciar buckets compatíveis.

Para que serve o Tenant Manager?

Depois de criar a conta do locatário, os usuários locatários podem fazer login no Gerenciador de Locatários para executar tarefas como as seguintes:

- Configurar federação de identidade (a menos que a fonte de identidade seja compartilhada com a grade)
- Gerenciar grupos e usuários
- Use a federação de grade para clonagem de conta e replicação entre grades
- Gerenciar chaves de acesso S3
- Criar e gerenciar buckets S3
- Use os serviços da plataforma S3
- Use o S3 Select
- Monitorar o uso do armazenamento



Embora os usuários do tenant do S3 possam criar e gerenciar chaves de acesso e buckets do S3 com o Tenant Manager, eles devem usar um aplicativo cliente do S3 para ingerir e gerenciar objetos. Ver "[Usar API REST do S3](#)" para mais detalhes.

Criar uma conta de inquilino

Você deve criar pelo menos uma conta de locatário para controlar o acesso ao

armazenamento no seu sistema StorageGRID .

As etapas para criar uma conta de locatário variam dependendo se "[federação de identidade](#)" e "[login único](#)" estão configurados e se a conta do Grid Manager que você usa para criar a conta do locatário pertence a um grupo de administradores com permissão de acesso Root.

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)" .
- Você tem o "[Permissão de acesso root ou 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 Root para a conta do locatário a um grupo federado, você terá importado esse grupo federado para o Grid Manager. Você não precisa atribuir nenhuma permissão do Grid Manager a este grupo de administradores. Ver "[Gerenciar grupos de administradores](#)" .
- Se você quiser permitir que um locatário do S3 clone dados da conta e replique objetos de bucket para outra grade usando uma conexão de federação de grade:
 - Você tem "[configurou a conexão da federação de grade](#)" .
 - O status da conexão é **Conectado**.
 - Você tem permissão de acesso Root.
 - Você revisou as considerações para "[gerenciamento de inquilinos permitidos para federação de rede](#)" .
 - Se a conta do locatário usar a fonte de identidade configurada para o Grid Manager, você importou o mesmo grupo federado para o Grid Manager em ambas as grades.

Ao criar o locatário, você selecionará esse grupo para ter a permissão de acesso Root inicial para as contas do locatário de origem e 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 **LOCATÁRIOS**.
2. Selecione **Criar**.

Insira os detalhes

Passos

1. Insira os detalhes do inquilino.

Campo	Descrição
Nome	Um nome para a conta do locatário. Os nomes dos inquilinos 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 inquilino. Se você estiver criando um locatário que usará uma conexão de federação de grade, 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 na Grade 1 também aparecerá para o locatário replicado na Grade 2: "Este locatário foi criado na Grade 1".
Tipo de cliente	O tipo de protocolo de cliente que este locatário usará, S3 ou Swift. Observação: O suporte para aplicativos cliente Swift foi descontinuado e será removido em uma versão futura.
Cota de armazenamento (opcional)	Se você quiser que este locatário tenha uma cota de armazenamento, um valor numérico para a cota e as unidades.

2. Selecione **Continuar**.

Selecionar 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 o CloudMirror. Ver "Gerenciar serviços de plataforma para contas de locatários do S3" .
Use sua própria fonte de identidade	O locatário pode configurar e gerenciar sua própria fonte de identidade para grupos e usuários federados. Esta opção estará desabilitada se você tiver "SSO configurado" para seu sistema StorageGRID .
Permitir seleção S3	O locatário pode emitir solicitações da API S3 SelectObjectContent para filtrar e recuperar dados do objeto. Ver "Gerenciar S3 Select para contas de locatários" . Importante: 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 somente para locatários confiáveis.

2. Opcionalmente, selecione as permissões avançadas que você deseja que este locatário tenha.

Permissão	Se selecionado...
Conexão de federação de rede	O inquilino pode usar uma conexão de federação de rede, que: - Faz com que este locatário e todos os grupos de locatários e usuários adicionados à conta sejam clonados desta grade (a <i>grade de origem</i>) para a outra grade na conexão selecionada (a <i>grade de destino</i>). - Permite que este locatário configure a replicação entre grades entre buckets correspondentes em cada grade. Ver "Gerenciar os inquilinos permitidos para federação de rede" .
Bloqueio de Objeto S3	Permitir que o locatário use recursos específicos do S3 Object Lock: Definir período máximo de retenção define por quanto tempo 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 substituam ou excluam versões de objetos protegidos durante o período de retenção.

3. Selecione **Continuar**.

Definir acesso root e criar locatário

Passos

1. Defina o acesso root para a conta do locatário, com base no uso de federação de identidades pelo seu sistema StorageGRID , logon único (SSO) ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver habilitada	Especifique a senha a ser usada ao fazer login no locatário como usuário root local.
Se a federação de identidade estiver habilitada	a. Selecione um grupo federado existente para ter permissão de acesso Root para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário root local.
Se a federação de identidade e o logon único (SSO) estiverem habilitados	Selecione um grupo federado existente para ter permissão de acesso Root para o locatário. Nenhum usuário local pode fazer login.

2. Selecione **Criar inquilino**.

Uma mensagem de sucesso é exibida e o novo inquilino é listado na página Inquilinos. Para saber como visualizar detalhes do locatário e monitorar a atividade do locatário, consulte ["Monitorar a atividade do inquilino"](#) .



A aplicação das configurações do locatário na grade 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 grade** para o locatário:
- Confirme se um inquilino idêntico foi replicado para a outra grade na conexão. Os inquilinos em ambas as grades terão o mesmo ID de conta de 20 dígitos, nome, descrição, cota e permissões.



Se você vir a mensagem de erro "Locatário criado sem um clone", consulte as instruções em "[Solucionar erros de federação de grade](#)".

- Se você forneceu uma senha de usuário root local ao definir o acesso root, "[alterar a senha do usuário root local](#)" para o inquilino replicado.



Um usuário root local não pode fazer login no Tenant Manager na grade de destino até que a senha seja alterada.

Sign in como inquilino (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. Ver "[Controle de acesso em firewall externo](#)".

Sign in agora

Se você estiver usando...	Faça isso...
Porta 443 e você define uma senha para o usuário root local	- Selecione * Sign in como root*. Ao fazer login, aparecem links para configurar buckets, federação de identidades, grupos e usuários. - Selecione os links para configurar a conta do locatário. Cada link abre a página correspondente no Gerenciador de Inquilinos. Para completar a página, veja a "instruções para usar contas de inquilinos".
Porta 443 e você não definiu uma senha para o usuário root local	Selecione * Sign in* e insira as credenciais de um usuário no grupo federado de acesso Root.

Se você estiver usando...	Faça isso...
Uma porta restrita	1. Selecione Concluir 2. Selecione Restrito na tabela Locatário para saber mais sobre como acessar esta conta de locatário. A URL do Gerenciador de Inquilinos tem este formato: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> ◦ <code>`FQDN_or_Admin_Node_IP`</code> é um nome de domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ <code>`port`</code> é a porta somente para inquilinos ◦ <code>`20-digit-account-id`</code> é o ID de conta exclusivo do inquilino

Sign in mais tarde

Se você estiver usando...	Faça uma dessas...
Porta 443	• No Grid Manager, selecione LOCATÁRIOS e selecione * Sign in* à direita do nome do locatário. • Digite a URL do locatário em um navegador da web: <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> ◦ <code>`FQDN_or_Admin_Node_IP`</code> é um nome de domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ <code>`20-digit-account-id`</code> é o ID de conta exclusivo do inquilino
Uma porta restrita	• No Grid Manager, selecione LOCATÁRIOS 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> ◦ <code>`FQDN_or_Admin_Node_IP`</code> é um nome de domínio totalmente qualificado ou o endereço IP de um nó de administração ◦ <code>`port`</code> é a porta restrita somente para inquilinos ◦ <code>`20-digit-account-id`</code> é o ID de conta exclusivo do inquilino

Configurar o locatário

Siga as instruções em "[Use uma conta de inquilino](#)" para gerenciar grupos de locatários e usuários, chaves de acesso S3, buckets, serviços de plataforma, clone de conta e replicação entre redes.

Editar conta de inquilino

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 grade**, você poderá editar os detalhes do locatário de qualquer grade na conexão. Entretanto, quaisquer alterações feitas em uma grade na conexão não serão copiadas para a outra grade. Se você quiser manter os detalhes do locatário exatamente sincronizados entre as grades, faça as mesmas edições em ambas as grades. Ver "[Gerenciar os inquilinos permitidos para conexão de federação de rede](#)".

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você tem o "[Permissão de acesso root ou contas de locatário](#)".



A aplicação das configurações do locatário na grade pode levar 15 minutos ou mais, dependendo da conectividade da rede, do status do nó e das operações do Cassandra.

Passos

1. Selecione **LOCATÁRIOS**.

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 de locatário que você deseja editar.

Use a caixa de pesquisa para procurar um inquilino por nome ou ID do inquilino.

3. Selecione o inquilino. Você pode fazer qualquer um dos seguintes:
 - Marque a caixa de seleção do locatário e selecione **Ações > Editar**.
 - Selecione o nome do inquilino para exibir a página de detalhes e selecione **Editar**.
4. Opcionalmente, altere os valores destes campos:
 - **Nome**

- **Descrição**
- **Cota de armazenamento**

5. Selecione **Continuar**.

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

- Se você desabilitar os **Serviços da plataforma** para um locatário que já os esteja usando, 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 tiver configurado a replicação do 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 um ponto de extremidade. Ver "[Gerenciar serviços de plataforma para contas de locatários do S3](#)".
- Altere a configuração de **Usar fonte de identidade própria** para determinar se a conta do locatário usará sua própria fonte de identidade ou a fonte de identidade que foi configurada para o Grid Manager.

Se **Usar fonte de identidade própria** for:

- Desativado e selecionado, o locatário já habilitou sua própria fonte de identidade. Um locatário deve desabilitar sua fonte de identidade antes de poder usar a fonte de identidade que foi configurada para o Grid Manager.
- Desabilitado 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. Ver "[Gerenciar S3 Select para contas de locatários](#)".
- Para remover a permissão **Usar conexão de federação de grade**:
 - Selecione a aba **Federação de grade**.
 - Selecione **Remover permissão**.
- Para adicionar a permissão **Usar conexão de federação de grade**:
 - Selecione a aba **Federação de grade**.
 - Marque a caixa de seleção **Usar conexão de federação de grade**.
 - Opcionalmente, selecione **Clonar usuários e grupos locais existentes** para cloná-los na grade remota. Se desejar, você pode interromper a clonagem em andamento ou tentar clonar novamente se alguns usuários ou grupos locais não puderem ser 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 objeto S3 deve ser habilitado na grade antes que você possa usar essas configurações.

- Selecione a aba **S3 Object Lock**.
- Para **Definir período máximo de retenção**, insira um valor e selecione o período de tempo no menu suspenso.
- Para **Permitir modo de conformidade**, marque a caixa de seleção.

Alterar senha do usuário root local do locatário

Pode ser necessário alterar a senha do usuário root local de um locatário se o usuário

root estiver bloqueado na conta.

Antes de começar

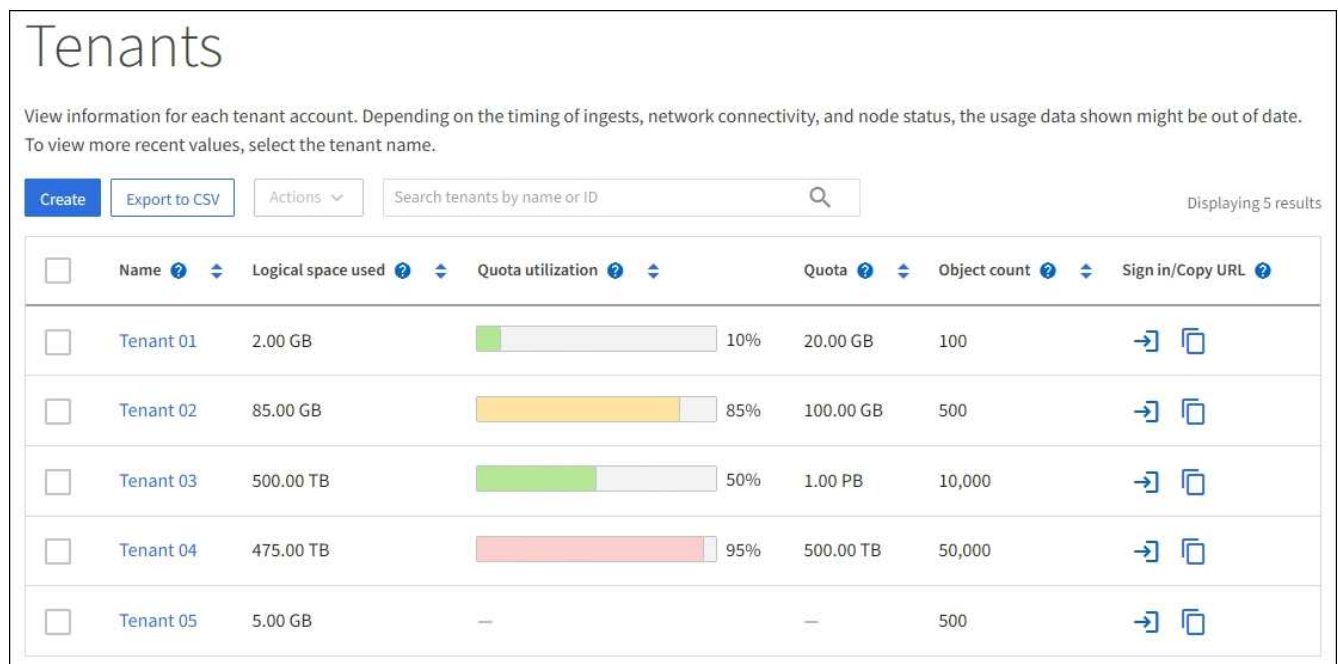
- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem ["permissões de acesso específicas"](#) .

Sobre esta tarefa

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

Passos

1. Selecione **LOCATÁRIOS**.



☐	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 qualquer um dos seguintes:
 - Marque a caixa de seleção do locatário e selecione **Ações > Alterar senha 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 locatário.
4. Selecione **Salvar**.

Excluir conta de inquilino

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

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem ["permissões de acesso específicas"](#) .
- Você removeu todos os buckets e objetos do S3 associados à conta do locatário.

- Se o inquilino tiver permissão para usar uma conexão de federação de rede, você revisou as considerações para ["excluindo um locatário com a permissão Usar conexão de federação de grade"](#) .

Passos

1. Selecione **LOCATÁRIOS**.
2. Localize a conta ou contas de locatário que você deseja excluir.

Use a caixa de pesquisa para procurar um inquilino por nome ou ID do inquilino.
3. Para excluir vários inquilinos, marque as caixas de seleção e selecione **Ações > Excluir**.
4. Para excluir um único locatário, faça um dos seguintes:
 - Marque a caixa de seleção e selecione **Ações > Excluir**.
 - Selecione o nome do inquilino para exibir a página de detalhes e, em seguida, selecione **Ações > Excluir**.
5. Selecione **Sim**.

Gerenciar serviços de plataforma

O que são serviços de plataforma?

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

Se você habilitar serviços de plataforma para contas de locatários do S3, deverá configurar sua grade para que os locatários possam acessar os recursos externos necessários para usar esses serviços.

Replicação do CloudMirror

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

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



A replicação do CloudMirror tem algumas semelhanças e diferenças importantes com o recurso de replicação entre grades. Para saber mais, consulte ["Comparar a replicação entre grades e a replicação do CloudMirror"](#) .



A replicação do CloudMirror não será suportada se o bucket de origem tiver o S3 Object Lock habilitado.

Notificações

Notificações de eventos por bucket são usadas para enviar notificações sobre ações específicas executadas em objetos para um cluster Kafka externo especificado ou Amazon Simple Notification Service.

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



Embora a notificação de eventos possa ser configurada em um bucket com o S3 Object Lock habilitado, os metadados do S3 Object Lock (incluindo Retain Until Date e status de retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

Serviço de integração de pesquisa

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

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



Embora a integração do Elasticsearch possa ser configurada em um bucket com o S3 Object Lock habilitado, os metadados do S3 Object Lock (incluindo Retain Until Date e status de retenção legal) dos objetos não serão incluídos nas mensagens de notificação.

Os serviços de plataforma oferecem aos locatários a capacidade de usar recursos de armazenamento externo, serviços de notificação e serviços de pesquisa ou análise com seus dados. Como o local de destino dos serviços da plataforma normalmente é externo à sua implantação do StorageGRID, você deve decidir se deseja permitir que os locatários usem esses serviços. Se fizer isso, você deverá habilitar o uso dos serviços da plataforma ao criar ou editar contas de locatários. Você também deve configurar sua rede de modo que as mensagens dos serviços de plataforma geradas pelos locatários possam chegar aos seus destinos.

Recomendações para 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 o controle de versão e a replicação do CloudMirror habilitados, você também deverá habilitar o controle de versão do bucket S3 para o endpoint de destino. Isso permite que a replicação do CloudMirror gere versões de objetos semelhantes no ponto de extremidade.
- Você não deve usar mais de 100 locatários ativos com solicitações S3 que exijam replicação, notificações e integração de pesquisa do CloudMirror. Ter mais de 100 locatários ativos pode resultar em desempenho mais lento do cliente S3.
- Solicitações para um endpoint que não podem ser concluídas serão enfileiradas para um máximo de 500.000 solicitações. Esse limite é dividido igualmente entre os inquilinos ativos. Novos inquilinos podem exceder temporariamente esse limite de 500.000 para que os inquilinos recém-criados não sejam penalizados injustamente.

Informações relacionadas

- ["Gerenciar serviços de plataforma"](#)
- ["Configurar as definições de proxy de armazenamento"](#)
- ["Monitorar StorageGRID"](#)

Rede e portas para serviços de plataforma

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

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

Por exemplo, os locatários podem configurar os seguintes tipos de pontos de extremidade 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 bucket S3 hospedado localmente na mesma ou em outra instância do StorageGRID
- Um ponto de extremidade externo, como um ponto de extremidade no Amazon Web Services.

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

Os locatários podem especificar uma porta diferente ao criar ou editar um ponto de extremidade.



Se uma implantação do StorageGRID for usada como destino para 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 implantação do StorageGRID de destino esteja especificada no ponto de extremidade.

Se você usar um servidor proxy não transparente, você também deve [configurar configurações de proxy de armazenamento](#) para permitir que mensagens sejam enviadas para terminais externos, como um terminal na Internet.

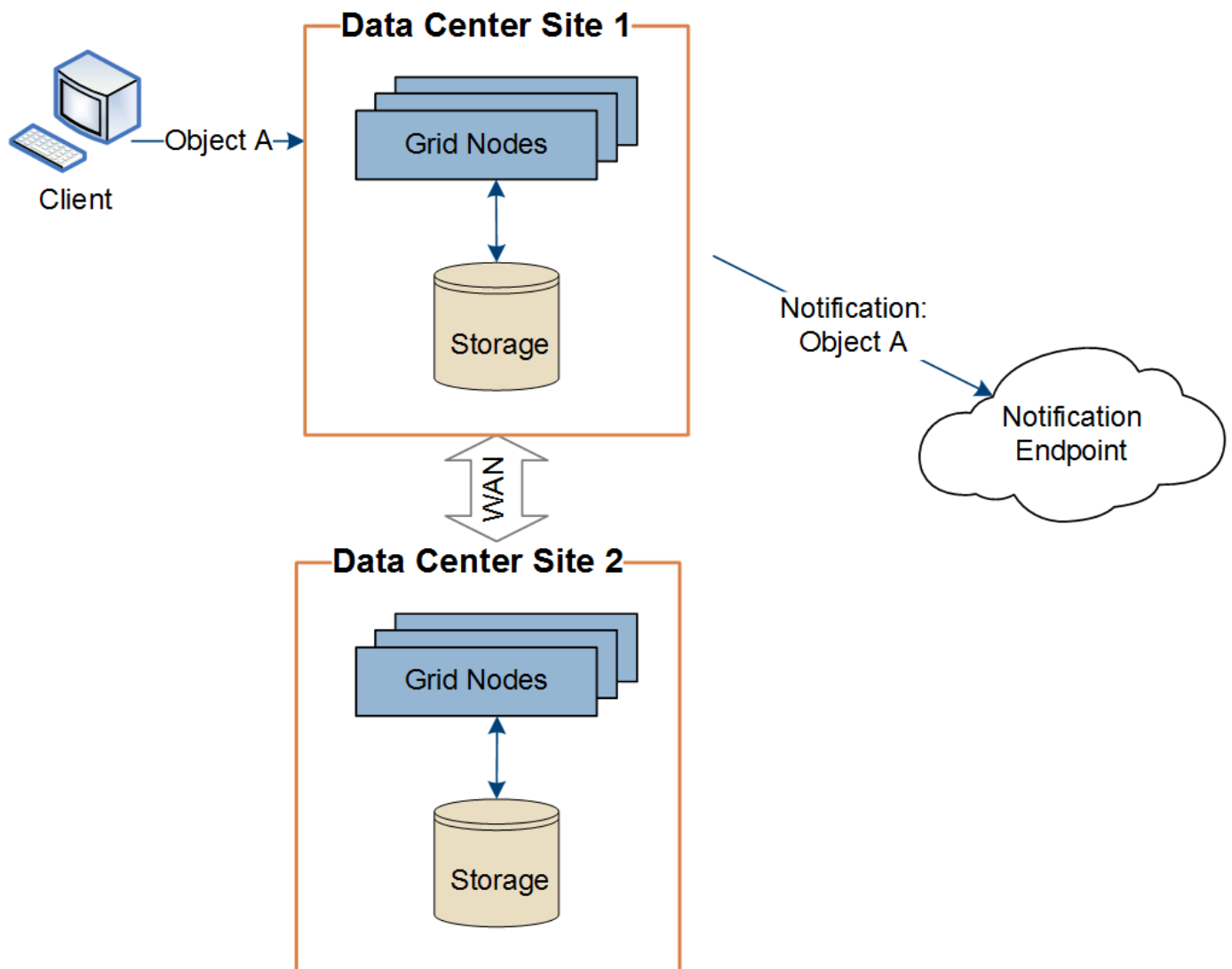
Informações relacionadas

["Use uma conta de inquilino"](#)

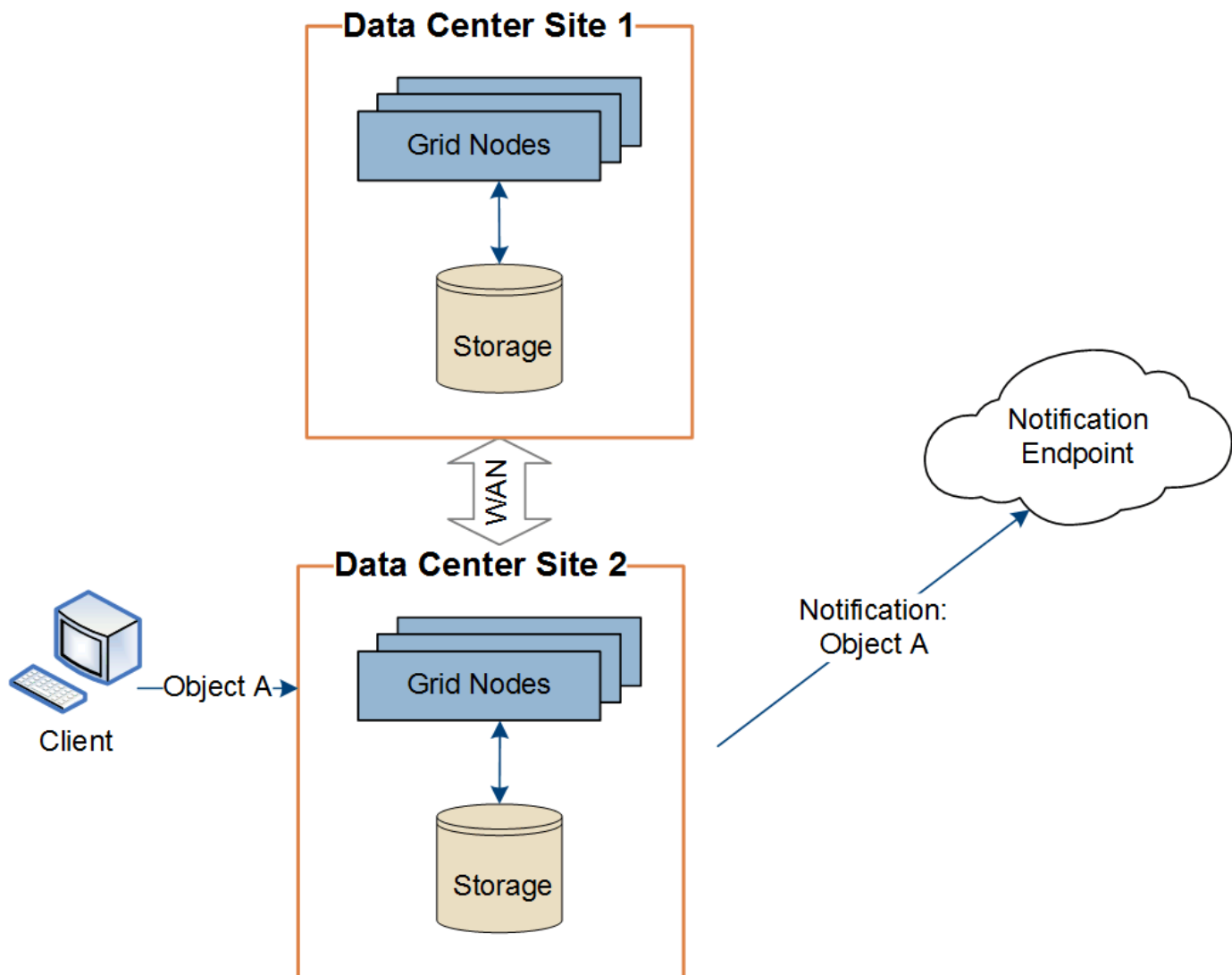
Entrega de mensagens de serviços de plataforma por site

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

Ou seja, se um locatário usar um cliente para executar uma operação de criação de API do S3 em um objeto conectando-se a um nó de gateway no site do data center 1, a notificação sobre essa ação será acionada e enviada do site do data center 1.



Se o cliente posteriormente executar uma operação de exclusão da API S3 no mesmo objeto do Site do Data Center 2, a notificação sobre a ação de exclusão será acionada e enviada do Site do Data Center 2.



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

Solucionar problemas de serviços de plataforma

Os pontos de extremidade usados nos serviços da plataforma são criados e mantidos pelos usuários locatários no Gerenciador de Locatários; no entanto, se um locatário tiver problemas para configurar ou usar os serviços da plataforma, você poderá usar o Gerenciador de Grade para ajudar a resolver o problema.

Problemas com novos endpoints

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

Quando um locatário cria um ponto de extremidade, o sistema StorageGRID valida que o ponto de extremidade existe e que pode ser acessado usando as credenciais especificadas. A conexão com o ponto de

extremidade é validada a partir de um nó em cada site.

Se a validação do ponto de extremidade falhar, uma mensagem de erro explicará o motivo da falha. O usuário locatário deve resolver o problema e tentar criar o endpoint novamente.



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

Problemas com endpoints existentes

Se ocorrer um erro quando o StorageGRID tentar acessar um ponto de extremidade existente, uma mensagem será exibida no painel do Gerenciador de Tenants.



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 Endpoints para revisar a mensagem de erro mais recente para cada endpoint e determinar há quanto tempo o erro ocorreu. A coluna **Último erro** exibe a mensagem de erro mais recente para cada ponto de extremidade e indica há quanto tempo o erro ocorreu. Erros que

incluem o ícone ocorreu 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 de 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 pontos de extremidade do serviço de plataforma, podem ocorrer erros se o 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 bloqueadas.

Determinar se ocorreu um erro

Se algum erro de endpoint tiver ocorrido nos últimos 7 dias, o painel no Gerenciador de Tenants 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 de serviços de plataforma podem causar falhas nas operações do cliente no bucket S3. Por exemplo, as operações do cliente S3 falharão se o serviço interno da Máquina de Estado Replicado (RSM) parar ou se houver muitas mensagens de serviços de plataforma enfileiradas para entrega.

Para verificar o status dos serviços:

1. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
2. Selecione **site > Nó de Armazenamento > SSM > Serviços**.

Erros de endpoint recuperáveis e irre recuperáveis

Após a criação dos endpoints, erros de solicitação de serviço de plataforma podem ocorrer por vários motivos. Alguns erros podem ser recuperados com 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 pode ser entregue.

Se o StorageGRID encontrar um erro recuperável, a solicitação de serviço da plataforma será repetida até ser bem-sucedida.

Outros erros são irre recuperáveis. Por exemplo, um erro irre recuperável ocorre se o ponto de extremidade for excluído.

Se o StorageGRID encontrar um erro de endpoint irre recuperável:

- No Grid Manager, acesse **Suporte > Ferramentas > Métricas > Grafana > Visão geral dos serviços de plataforma** para visualizar detalhes do erro.
- No Gerenciador de Tenants, acesse **ARMAZENAMENTO (S3) > Pontos de extremidade dos serviços de plataforma** para visualizar os detalhes do erro.
- Verifique o `/var/local/log/bycast-err.log` para erros relacionados. Os nós de armazenamento que têm o serviço ADC contêm este arquivo de log.

As mensagens dos serviços da plataforma não podem ser entregues

Se o destino encontrar um problema que o impeça de aceitar mensagens de serviços de plataforma, a operação do cliente no bucket será bem-sucedida, mas a mensagem de serviços de plataforma não será entregue. Por exemplo, esse erro pode ocorrer se as credenciais forem atualizadas no destino de forma que o

StorageGRID não consiga mais se autenticar no serviço de destino.

Verifique se há alertas relacionados.

Desempenho mais lento para solicitações de serviço de plataforma

O software StorageGRID pode limitar as solicitações S3 recebidas para um bucket se a taxa na qual as solicitações estão sendo enviadas exceder a taxa na qual o ponto de extremidade de destino pode receber as solicitações. A limitação só ocorre quando há um acúmulo de solicitações aguardando para serem enviadas ao ponto de extremidade de destino.

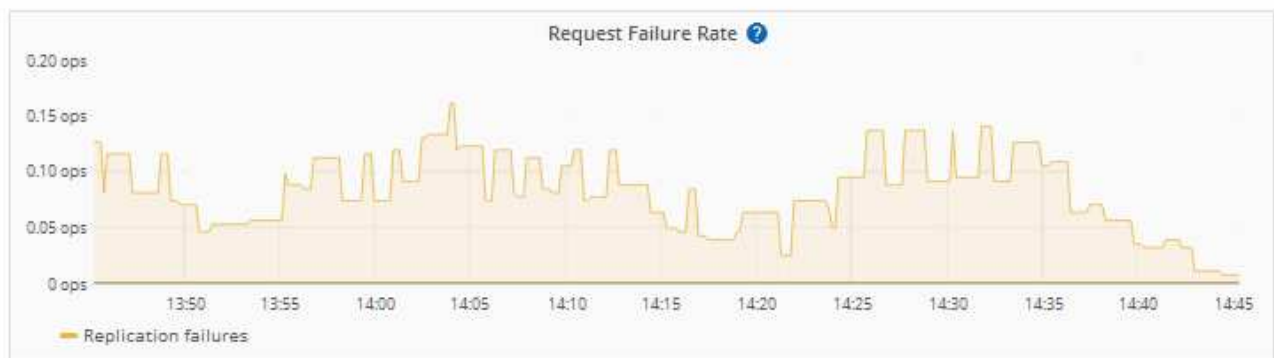
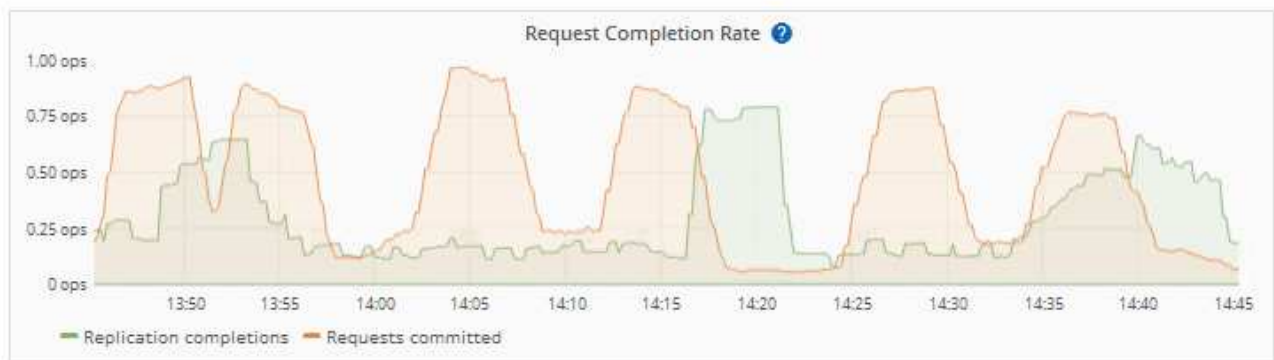
O único efeito visível é que as solicitações S3 recebidas levarão mais tempo para serem executadas. Se você começar a detectar um desempenho significativamente mais lento, reduza a taxa de ingestão ou use um ponto de extremidade com maior capacidade. Se o acúmulo de solicitações continuar a crescer, as operações do cliente S3 (como solicitações PUT) acabarão falhando.

As solicitações do CloudMirror têm maior probabilidade de serem afetadas pelo desempenho do ponto de extremidade de destino porque essas solicitações geralmente envolvem mais transferência de dados do que as solicitações de integração de pesquisa ou notificação de eventos.

Falha nas solicitações de serviço da plataforma

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

1. Selecione **NODES**.
2. Selecione **síte > Serviços de plataforma**.
3. Veja o gráfico de taxas de erros de solicitação.

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

Alerta de serviços de plataforma indisponíveis

O alerta **Serviços de plataforma indisponíveis** indica que nenhuma operação de serviço de plataforma pode ser executada em um site porque poucos nós de armazenamento com o serviço RSM estão em execução ou disponíveis.

O serviço RSM garante que as solicitações de serviço da plataforma sejam enviadas aos seus respectivos terminais.

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



Se mais de um nó de armazenamento que contém o serviço RSM falhar em um site, você perderá todas as solicitações de serviço de plataforma pendentes para esse site.

Orientações adicionais para solução de problemas de endpoints de serviços de plataforma

Para obter informações adicionais, consulte [Use uma conta de locatário](#) > [Solucionar problemas de endpoints de serviços de plataforma](#).

Informações relacionadas

["Solucionar problemas do sistema StorageGRID"](#)

Gerenciar S3 Select para contas de locatários

Você pode permitir que determinados locatários 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 precisar implantar um banco de dados e recursos associados para habilitar pesquisas. Também reduz o custo e a latência da recuperação de dados.

O que é o S3 Select?

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

Considerações e requisitos para usar o S3 Select

Requisitos de administração da rede

O administrador da rede deve conceder aos locatários a capacidade de seleção do S3. Selecione **Permitir seleção S3** quando ["criando um inquilino"](#) ou ["editando um inquilino"](#).

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 compactação em colunas usando GZIP ou Snappy. O S3 Select não oferece suporte à compactação de objetos inteiros para objetos Parquet.
 - O S3 Select não suporta saída Parquet. Você deve especificar o formato de saída como CSV ou JSON.
 - O tamanho máximo do grupo de linhas descompactado é 512 MB.
 - Você deve usar os tipos de dados especificados no esquema do objeto.
 - Você não pode usar os tipos lógicos INTERVAL, JSON, LIST, TIME ou UUID.

Requisitos de endpoint

A solicitação `SelectObjectContent` deve ser enviada para um ["Ponto de extremidade do balanceador de carga"](#)

[StorageGRID](#) .

Os nós de administração e gateway usados pelo endpoint devem ser um dos seguintes:

- Um nó de dispositivo de serviços
- Um nó de software baseado em VMware
- Um nó bare metal executando um kernel com cgroup v2 habilitado

Considerações gerais

As consultas não podem ser enviadas diretamente para os nós de armazenamento.



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 somente para locatários confiáveis.

Veja o "[instruções para usar o S3 Select](#)" .

Para visualizar "[Gráficos Grafana](#)" para operações S3 Select ao longo do tempo, selecione **SUPORTE > Ferramentas > Métricas** no Grid Manager.

Configurar conexões do cliente

Configurar conexões do cliente S3

Como administrador de grade, você gerencia as opções de configuração que controlam como os aplicativos cliente S3 se conectam ao seu sistema StorageGRID para armazenar e recuperar dados.



Os detalhes do Swift foram removidos desta versão do site de documentação. Ver "[StorageGRID 11.8: Configurar conexões de cliente S3 e Swift](#)" .

Tarefas de configuração

1. Execute tarefas de 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 identidade
- SSO

1. Use o StorageGRID para obter os valores que o aplicativo precisa para se conectar à grade. Você pode usar o assistente de configuração do S3 ou configurar cada entidade do StorageGRID manualmente. +

Use o assistente de configuração do S3

Siga as etapas do assistente de configuração do S3.

Configurar manualmente

1. Criar grupo de alta disponibilidade
2. Criar ponto de extremidade do balanceador de carga
3. Criar conta de inquilino
4. Criar bucket e chaves de acesso
5. Configurar regra e política do ILM

1. Use o aplicativo S3 para concluir a conexão com o StorageGRID. Crie entradas DNS para associar endereços IP a quaisquer nomes de domínio que você planeja usar.

Conforme necessário, execute configurações adicionais do aplicativo.

2. Execute tarefas contínuas no aplicativo e no StorageGRID para gerenciar e monitorar o armazenamento de objetos ao longo do tempo.

Informações necessárias para anexar o StorageGRID a um aplicativo cliente

Antes de poder anexar o StorageGRID a um aplicativo cliente S3, você deve executar etapas de configuração no StorageGRID e obter determinado valor.

Quais valores eu preciso?

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 de extremidade do balanceador de carga	Aplicação do cliente
Certificado SSL	StorageGRID > Ponto de extremidade do balanceador de carga	Aplicação do cliente
Nome do servidor (FQDN)	StorageGRID > Ponto de extremidade do balanceador de carga	• Aplicação do cliente • Entrada DNS
ID da chave de acesso S3 e chave de acesso secreta	StorageGRID > Locatário e bucket	Aplicação do cliente
Nome do balde/recipiente	StorageGRID > Locatário e bucket	Aplicação do cliente

Como obtenho esses valores?

Dependendo de suas necessidades, você pode fazer o seguinte para obter as informações necessárias:

- *Use o "[Assistente de configuração do S3](#)" *. O assistente de configuração do 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 nas etapas necessárias e ajuda a garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID .



Se você estiver configurando um aplicativo S3, é recomendável usar o assistente de configuração do S3, a menos que você saiba que tem requisitos especiais ou que sua implementação exija personalização significativa.

- *Use o "[Assistente de configuração do FabricPool](#)" *. Semelhante ao assistente de configuração do S3, o assistente de configuração do FabricPool ajuda você a configurar rapidamente os valores necessários e gera um arquivo que você pode usar ao configurar uma camada de nuvem do FabricPool no ONTAP.



Se você planeja usar o StorageGRID como o sistema de armazenamento de objetos para uma camada de nuvem do FabricPool , é recomendável usar o assistente de configuração do FabricPool , a menos que você saiba que tem requisitos especiais ou que sua implementação exija personalização significativa.

- **Configurar itens manualmente.** Se você estiver se conectando a um aplicativo S3 e preferir não usar o assistente de configuração do S3, poderá obter os valores necessários executando a configuração manualmente. Siga estes passos:
 - a. Configure o grupo de alta disponibilidade (HA) que você deseja usar para o aplicativo S3. Ver "[Configurar grupos de alta disponibilidade](#)" .
 - b. Crie o ponto de extremidade do balanceador de carga que o aplicativo S3 usará. Ver "[Configurar pontos de extremidade do balanceador de carga](#)" .

- c. Crie a conta de locatário que o aplicativo S3 usará. Ver "[Criar uma conta de inquilino](#)".
- d. Para um locatário S3, entre 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. Ver "[Crie suas próprias chaves de acesso](#)".
- e. Crie um ou mais buckets S3 na conta do locatário. Para S3, veja "[Criar bucket S3](#)".
- f. Para adicionar instruções de posicionamento específicas para os objetos pertencentes ao novo locatário ou bucket/contêiner, crie uma nova regra do ILM e ative uma nova política do ILM para usar essa regra. Ver "[Criar regra ILM](#)" e "[Criar política de ILM](#)".

Segurança para clientes S3

As contas de locatário do StorageGRID usam aplicativos cliente S3 para salvar dados de objetos no StorageGRID. Você deve revisar as medidas de segurança implementadas para aplicativos clientes.

Resumo

A lista a seguir resume como a segurança é implementada para a API REST do S3:

Segurança de 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 o StorageGRID fornece segurança para aplicativos clientes

Os aplicativos cliente S3 podem se conectar ao serviço Load Balancer em nós de gateway ou nós de administração ou diretamente aos nós de armazenamento.

- Os clientes que se conectam ao serviço Load Balancer podem usar HTTPS ou HTTP, dependendo de como você "[configurar o ponto de extremidade do balanceador de carga](#)".

HTTPS fornece comunicação segura e criptografada por TLS e é recomendado. Você deve anexar um certificado de segurança ao ponto de extremidade.

O HTTP fornece comunicação menos segura e não criptografada e deve ser usado somente para grades de teste ou que não sejam de produção.

- Clientes que se conectam aos nós de armazenamento também podem usar HTTPS ou HTTP.

HTTPS é o padrão e é recomendado.

O HTTP fornece comunicação menos segura e não criptografada, mas pode ser opcionalmente "[habilitado](#)" para grades de não produção ou de teste.

- As comunicações entre o StorageGRID e o cliente são criptografadas usando TLS.
- As comunicações entre o serviço do balanceador de carga e os nós de armazenamento na grade são criptografadas, independentemente de o ponto de extremidade do balanceador de carga estar configurado para aceitar conexões HTTP ou HTTPS.
- Os clientes devem fornecer "[Cabeçalhos de autenticação HTTP](#)" para StorageGRID para executar operações da API REST.

Certificados de segurança e aplicativos cliente

Em todos os casos, os aplicativos clientes podem fazer conexões TLS usando um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado gerado pelo sistema StorageGRID :

- Quando os aplicativos cliente se conectam ao serviço do Load Balancer, eles usam o certificado que foi configurado para o ponto de extremidade do balanceador de carga. Cada ponto de extremidade do balanceador de carga tem seu próprio certificado, um certificado de servidor personalizado carregado pelo administrador da grade ou um certificado que o administrador da grade gerou no StorageGRID ao configurar o ponto de extremidade.

Ver "[Considerações para balanceamento de carga](#)" .

- Quando aplicativos cliente se conectam diretamente a um nó de armazenamento, eles usam os certificados de servidor gerados pelo sistema que foram gerados para nós de armazenamento quando o sistema StorageGRID foi instalado (que são assinados pela autoridade de certificação do sistema) ou um único certificado de servidor personalizado fornecido para a grade por um administrador de grade. Ver "[adicionar um certificado de API S3 personalizado](#)" .

Os clientes devem ser configurados para confiar na autoridade de certificação que assinou qualquer certificado que eles usam para estabelecer conexões TLS.

Algoritmos de hash e criptografia suportados para bibliotecas TLS

O sistema StorageGRID oferece suporte a um conjunto de conjuntos de cifras que os aplicativos clientes podem usar ao estabelecer uma sessão TLS. Para configurar cifras, vá para **CONFIGURAÇÃO > Segurança > Configurações de segurança** e selecione **Políticas TLS e SSH**.

Versões suportadas do TLS

O 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 configuração do S3

Usar o assistente de configuração do S3: considerações e requisitos

Você pode usar o assistente de configuração do S3 para configurar o StorageGRID como o sistema de armazenamento de objetos para um aplicativo S3.

Quando usar o assistente de configuração do S3

O assistente de configuração do S3 orienta você em cada etapa da configuração do StorageGRID para uso com um aplicativo S3. Como parte da conclusão do assistente, você baixa arquivos que podem ser usados para inserir valores no aplicativo S3. Use o assistente para configurar seu sistema mais rapidamente e

garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID .

Se você tem o "[Permissão de acesso root](#)" , você pode concluir o assistente de configuração do S3 ao começar a usar o StorageGRID Grid Manager ou pode acessar e concluir o assistente 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 se você concluiu estes pré-requisitos.

Obter endereços IP e configurar interfaces VLAN

Se você configurar um grupo de alta disponibilidade (HA), saberá a quais nós o aplicativo S3 se conectará e qual rede StorageGRID será usada. Você também sabe quais valores inserir para o CIDR de 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. Ver "[Configurar interfaces VLAN](#)" .

Configurar federação de identidade e SSO

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 root para a conta de locatário que o aplicativo S3 usará. Ver "[Usar federação de identidade](#)" e "[Configurar logon único](#)" .

Obter e configurar nomes de domínio

Você sabe qual nome de domínio totalmente qualificado (FQDN) usar para StorageGRID. As entradas do servidor de nomes de domínio (DNS) mapearão esse FQDN para os endereços IP virtuais (VIP) do grupo HA que você criar usando o assistente.

Se você planeja usar solicitações de estilo de hospedagem virtual S3, você deve ter "[nomes de domínio de endpoint S3 configurados](#)" . É recomendável usar solicitações de estilo de hospedagem virtual.

Revisar os requisitos do balanceador de carga e do certificado de segurança

Se você planeja usar o balanceador de carga StorageGRID , revise as considerações gerais para balanceamento de carga. Você tem os certificados que irá enviar ou os valores necessários para gerar um certificado.

Se você planeja usar um ponto de extremidade de balanceador de carga externo (de terceiros), você tem o nome de domínio totalmente qualificado (FQDN), a porta e o certificado para esse balanceador de carga.

Configurar quaisquer conexões de federação de grade

Se você quiser permitir que o locatário do S3 clone dados da conta e replique objetos de bucket para outra grade usando uma conexão de federação de grade, confirme o seguinte antes de iniciar o assistente:

- Você tem "[configurou a conexão da federação de grade](#)" .
- O status da conexão é **Conectado**.
- Você tem permissão de acesso Root.

Acesse e conclua o assistente de configuração do S3

Você pode usar o assistente de configuração do S3 para configurar o StorageGRID para uso com um aplicativo S3. O assistente de configuração fornece os valores que o aplicativo precisa para acessar um bucket do StorageGRID e salvar objetos.

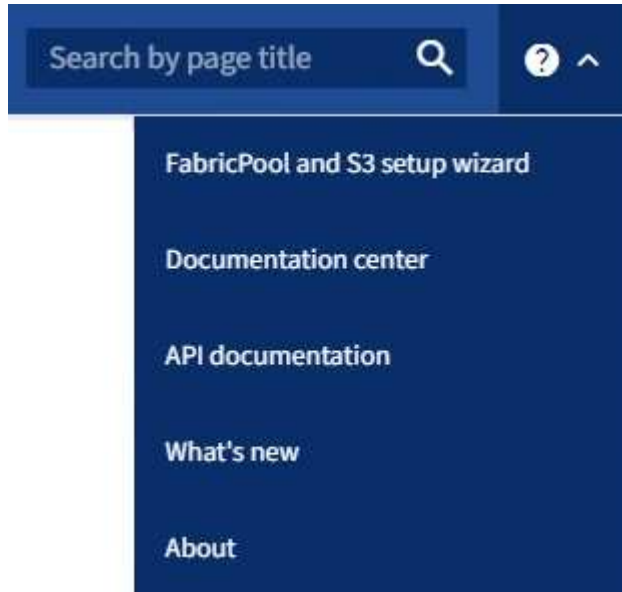
Antes de começar

- Você tem o ["Permissão de acesso root"](#) .
- Você revisou o ["considerações e requisitos"](#) para usar o assistente.

Acesse o assistente

Passos

1. Sign in no Grid Manager usando um ["navegador da web compatível"](#) .
2. Se o banner * Assistente de configuração do FabricPool e do S3* 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 * Assistente de configuração do FabricPool e S3*.



3. Na seção do aplicativo S3 da página do assistente de configuração do FabricPool e do S3, selecione **Configurar agora**.

Etapa 1 de 6: Configurar grupo HA

Um grupo HA é uma coleção de nós que contêm o serviço StorageGRID Load Balancer. Um grupo HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo 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 HA. Selecione **Ignorar esta etapa** e vá para [Etapa 2 de 6: Configurar o ponto de extremidade do balanceador de carga](#) .
2. Para usar o balanceador de carga StorageGRID , você pode criar um novo grupo de HA ou usar um grupo de HA existente.

Criar grupo HA

- Para criar um novo grupo HA, selecione **Criar grupo HA**.
- Para a 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.

- Para a etapa **Adicionar interfaces**, selecione as interfaces de nó que deseja usar neste grupo de HA.

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 pode selecionar apenas uma interface para cada nó.

- Para a etapa **Priorizar interfaces**, determine a interface primária e quaisquer interfaces de backup para este grupo de HA.

Arraste as linhas para alterar os valores na coluna **Ordem de prioridade**.

A primeira interface na 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 IP virtuais (VIP) serão movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de backup e assim por diante. Quando as falhas são resolvidas, os endereços VIP retornam para a interface de maior prioridade disponível.

- Para a etapa **Inserir endereços IP**, preencha os seguintes campos.

Campo	Descrição
CIDR de 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 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 depois selecione **Concluir** para retornar ao assistente de configuração 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 ponto de extremidade do balanceador de carga

O StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de aplicativos clientes. O balanceamento de carga maximiza a velocidade e a capacidade de conexão entre vários nós de armazenamento.

Você pode usar o serviço StorageGRID Load Balancer, que existe em todos os nós de gateway e administração, ou pode se conectar a um balanceador de carga externo (de terceiros). É recomendado usar o balanceador de carga StorageGRID .

Para obter detalhes sobre esta tarefa, consulte "[Considerações para balanceamento de carga](#)".

Para usar o serviço StorageGRID Load Balancer, selecione a guia * StorageGRID load balancer* e crie ou selecione o ponto de extremidade do balanceador de carga que deseja usar. Para usar um balanceador de carga externo, selecione a aba **Balanceador de carga externo** e forneça detalhes sobre o sistema que você já configurou.

Criar ponto final

Passos

1. Para criar um ponto de extremidade do balanceador de carga, selecione **Criar ponto de extremidade**.
2. Para a etapa **Inserir detalhes do ponto de extremidade**, preencha os seguintes campos.

Campo	Descrição
Nome	Um nome descritivo para o ponto de extremidade.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo assume como padrão 10433 para o primeiro ponto de extremidade criado, mas você pode inserir qualquer porta externa não utilizada. Se você digitar 80 ou 443, o ponto de extremidade será configurado somente em nós de gateway, porque essas portas são reservadas em nós de administração. Observação: Portas usadas por outros serviços de rede não são permitidas. Veja o "Referência de porta de rede".
Tipo de cliente	Deve ser S3 .
Protocolo de rede	Selecione HTTPS. Observação: a comunicação com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada.

3. Para a etapa **Selecionar modo de vinculação**, especifique o modo de vinculação. O modo de vinculação controla como o ponto de extremidade é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

Modo	Descrição
Global (padrão)	Os clientes podem acessar o ponto de extremidade usando o endereço IP de qualquer nó de gateway ou nó de administração, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração Global (padrão), a menos que você precise restringir a acessibilidade deste ponto de extremidade.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este ponto de extremidade. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.

Modo	Descrição
Interfaces de nó	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar este ponto de extremidade.
Tipo de nó	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó de administração ou o endereço IP (ou FQDN correspondente) de qualquer nó de gateway para acessar esse ponto de extremidade.

4. Para a etapa de acesso do locatário, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os inquilinos (padrão)	Todas as contas de locatários podem usar esse endpoint para acessar seus buckets.
Permitir inquilinos selecionados	Somente as contas de locatários selecionadas podem usar este ponto de extremidade para acessar seus buckets.
Bloquear inquilinos selecionados	As contas de locatários selecionadas não podem usar este ponto de extremidade para acessar seus buckets. Todos os outros inquilinos podem usar este ponto de extremidade.

5. Para a etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Carregar certificado (recomendado)	Use esta opção para carregar um certificado de servidor assinado pela CA, uma chave privada de certificado e um pacote de CA opcional.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Ver " Configurar pontos de extremidade do balanceador de carga " para obter detalhes sobre o que inserir.
Usar certificado StorageGRID S3	Use esta opção somente se você já tiver carregado ou gerado uma versão personalizada do certificado global StorageGRID . Ver " Configurar certificados da API S3 " para mais detalhes.

6. Selecione **Concluir** para retornar ao assistente de configuração do S3.

7. Selecione **Continuar** para ir para a etapa do locatário e do bucket.



Alterações em um certificado de ponto de extremidade podem levar até 15 minutos para serem aplicadas a todos os nós.

Usar ponto de extremidade do balanceador de carga existente

Passos

1. Para usar um ponto de extremidade existente, selecione seu nome em **Selecionar um ponto de extremidade do balanceador de carga**.
2. Selecione **Continuar** para ir para a etapa do locatário e do bucket.

Usar balanceador de carga externo

Passos

1. Para usar um balanceador de carga externo, preencha os seguintes campos.

Campo	Descrição
FQDN	O nome de 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 do locatário e do 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 tem seus próprios usuários, chaves de acesso, buckets, objetos e um conjunto específico de recursos.

Um bucket é um contêiner usado para armazenar objetos e metadados de objetos de um locatário. Embora os locatários possam ter muitos buckets, o assistente ajuda você a criar um locatário e um bucket da maneira mais rápida e fácil. Se precisar adicionar buckets ou definir opções posteriormente, você pode usar o Gerenciador de Tenants.

Para obter detalhes sobre esta tarefa, consulte ["Criar conta de inquilino"](#) e ["Criar bucket S3"](#).

Passos

1. Insira um nome para a conta do locatário.

Os nomes dos inquilinos não precisam ser exclusivos. Quando a conta do locatário é criada, ela recebe um ID de conta numérico exclusivo.

2. Defina o acesso root para a conta do locatário, com base no uso do seu sistema StorageGRID ["federação de identidade"](#), ["logon único \(SSO\)"](#), ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver habilitada	Especifique a senha a ser usada ao fazer login no locatário como usuário root local.

Opção	Faça isso
Se a federação de identidade estiver habilitada	a. Selecione um grupo federado existente para ter " Permissão de acesso root " para o inquilino. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário root local.
Se a federação de identidade e o logon único (SSO) estiverem habilitados	Selecione um grupo federado existente para ter " Permissão de acesso root " para o inquilino. Nenhum usuário local pode fazer login.

- Se você quiser que o assistente crie o ID da chave de acesso e a chave de acesso secreta para o usuário root, selecione **Criar chave de acesso S3 do usuário root automaticamente**.

Selecione esta opção se o único usuário do locatário for o usuário root. Se outros usuários usarem este locatário, "[usar o Gerenciador de Inquilinos](#)" para configurar chaves e permissões.

- Se você quiser criar um bucket para este locatário agora, selecione **Criar bucket para este locatário**.



Se o S3 Object Lock estiver habilitado para a grade, o bucket criado nesta etapa não terá o S3 Object Lock habilitado. Se você precisar usar um bucket do S3 Object Lock para este aplicativo S3, não selecione criar um bucket agora. Em vez disso, use o Tenant Manager para "[crie o balde](#)" mais tarde.

- Insira o nome do bucket que o aplicativo S3 usará. Por exemplo, `s3-bucket`.

Não é possível alterar o nome do bucket após 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 acabou de configurar.

Passos

- Se você selecionou **Criar chave de acesso S3 de usuário root automaticamente**, faça um ou ambos os procedimentos a seguir:
 - Selecione **Baixar chaves de acesso** para baixar um `.csv` arquivo contendo o nome da conta do locatário, o ID da chave de acesso e a chave de acesso secreta.
 - Selecione o ícone de cópia () 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 `.txt` arquivo contendo as configurações para o endpoint do balanceador de carga, locatário, bucket e usuário root.
- Salve essas informações em um local seguro.



Não feche esta página até ter copiado ambas as chaves de acesso. As chaves não estarão disponíveis depois que 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. Se solicitado, marque 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: Revise a regra e a política do ILM para o S3

As regras de gerenciamento do ciclo de vida das informações (ILM) controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos no seu sistema StorageGRID . A política ILM incluída no StorageGRID faz duas cópias replicadas de todos os objetos. Esta política estará em vigor até que você ative pelo menos uma nova política.

Passos

1. Revise as informações fornecidas na página.
2. Se você quiser adicionar instruções específicas para os objetos pertencentes ao novo locatário ou bucket, crie uma nova regra e uma nova política. Ver "[Criar regra ILM](#)" e "[Usar políticas de ILM](#)".
3. Selecione **Eu revisei estas etapas e entendi o que preciso fazer**.
4. Marque a caixa de seleção para indicar que você entende o que fazer em seguida.
5. Selecione **Continuar** para ir para **Resumo**.

Etapa 6 de 6: Resumo da revisão

Passos

1. Revise o resumo.
2. Anote os detalhes nas próximas etapas, que descrevem a configuração adicional que pode ser necessária antes de se conectar ao cliente S3. Por exemplo, selecionar * Sign in como root* leva você ao Gerenciador de locatários, onde você pode adicionar usuários locatários, criar buckets adicionais e atualizar as configurações de buckets.
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 HA

O que são grupos de alta disponibilidade (HA)?

Grupos de alta disponibilidade (HA) fornecem conexões de dados de alta disponibilidade para clientes S3 e conexões de alta disponibilidade 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 nós de gateway, nós de administração ou ambos fornecem conexões de dados de alta disponibilidade para clientes S3.
- Grupos de HA que incluem apenas nós de administração fornecem conexões de alta disponibilidade ao Grid Manager e ao Tenant Manager.
- Um grupo HA que inclui apenas dispositivos de serviços e nós de software baseados em VMware pode fornecer conexões de alta disponibilidade para ["Locatários do S3 que usam o S3 Select"](#) . Grupos HA são recomendados ao usar o S3 Select, mas não são obrigatórios.

Como criar um grupo HA?

1. Selecione uma interface de rede para um ou mais nós de administração ou nós de gateway. Você pode usar uma interface de rede de grade (eth0), uma interface de rede de cliente (eth2), uma interface de VLAN ou uma interface de acesso que você adicionou ao nó.



Não é possível 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 determina a ordem de prioridade para qualquer interface de backup.
4. Você atribui de um a 10 endereços IP virtuais (VIP) ao grupo. Os aplicativos clientes podem usar qualquer um desses endereços VIP para se conectar ao StorageGRID.

Para obter instruções, consulte ["Configurar grupos de alta disponibilidade"](#) .

O que 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 interface "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.

Exibir o status atual do grupo HA de um nó

Para ver se um nó está atribuído a um grupo HA e determinar seu status atual, selecione **NODES > node**.

Se a guia **Visão geral** incluir uma entrada para **grupos de HA**, o nó será atribuído aos grupos de HA listados. O valor após o nome do grupo é o status atual do nó no grupo HA:

- **Ativo:** O grupo HA está atualmente hospedado neste nó.
- **Backup:** O grupo HA não está usando este nó no momento; esta é uma interface de backup.
- **Interrompido:** 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 Admin e uma interface de backup para o grupo de clientes FabricPool .

DC1-ADM1 (Primary Admin Node) [🔗](#)

Overview
Hardware
Network
Storage
Load balancer
Tasks

Node information [?](#)

Name:	DC1-ADM1
Type:	Primary Admin Node
ID:	ce00d9c8-8a79-4742-bdef-c9c658db5315
Connection state:	🟢 Connected
Software version:	11.6.0 (build 20211207.1804.614bc17)
HA groups:	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 movidos para a primeira interface de backup disponível na ordem de prioridade. Se essa interface falhar, os endereços VIP serão movidos 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 clientes sofram pouco impacto e possam contar com comportamentos normais de repetição para

continuar a operação.

Quando a falha é resolvida e uma interface de prioridade mais alta fica disponível novamente, os endereços VIP são movidos automaticamente para a interface de prioridade mais alta disponível.

Como os grupos HA são usados?

Você pode usar grupos de alta disponibilidade (HA) para fornecer conexões de alta disponibilidade ao StorageGRID para dados de objetos e para uso administrativo.

- Um grupo HA pode fornecer conexões administrativas de alta disponibilidade ao Grid Manager ou ao Tenant Manager.
- Um grupo HA pode fornecer conexões de dados de alta disponibilidade para clientes S3.
- Um grupo HA que contém apenas uma interface permite que você forneça muitos endereços VIP e defina explicitamente endereços IPv6.

Um grupo HA pode fornecer alta disponibilidade somente 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 necessários.

- **Nós de administração:** inclua o serviço Load Balancer e habilite o acesso ao Grid Manager ou ao Tenant Manager.
- **Nós de gateway:** inclui o serviço Load Balancer.

Objetivo do grupo HA	Adicionar nós deste tipo ao grupo HA
Acesso ao Grid Manager	• Nó de administração primário (Primário) • Nós administrativos não primários Observação: O nó de administração principal deve ser a interface primária. Alguns procedimentos de manutenção só podem ser executados no nó de administração principal.
Acesso somente ao Gerenciador de Inquilinos	• Nós administrativos primários ou não primários
Acesso do cliente S3 — serviço de balanceador de carga	• Nós de administração • Nós de gateway
Acesso de cliente S3 para "Seleção S3"	• Aparelhos de serviços • Nós de software baseados em VMware Observação: grupos HA são recomendados ao usar o S3 Select, mas não são obrigatórios.

Limitações do uso de grupos HA 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 o failover, você será

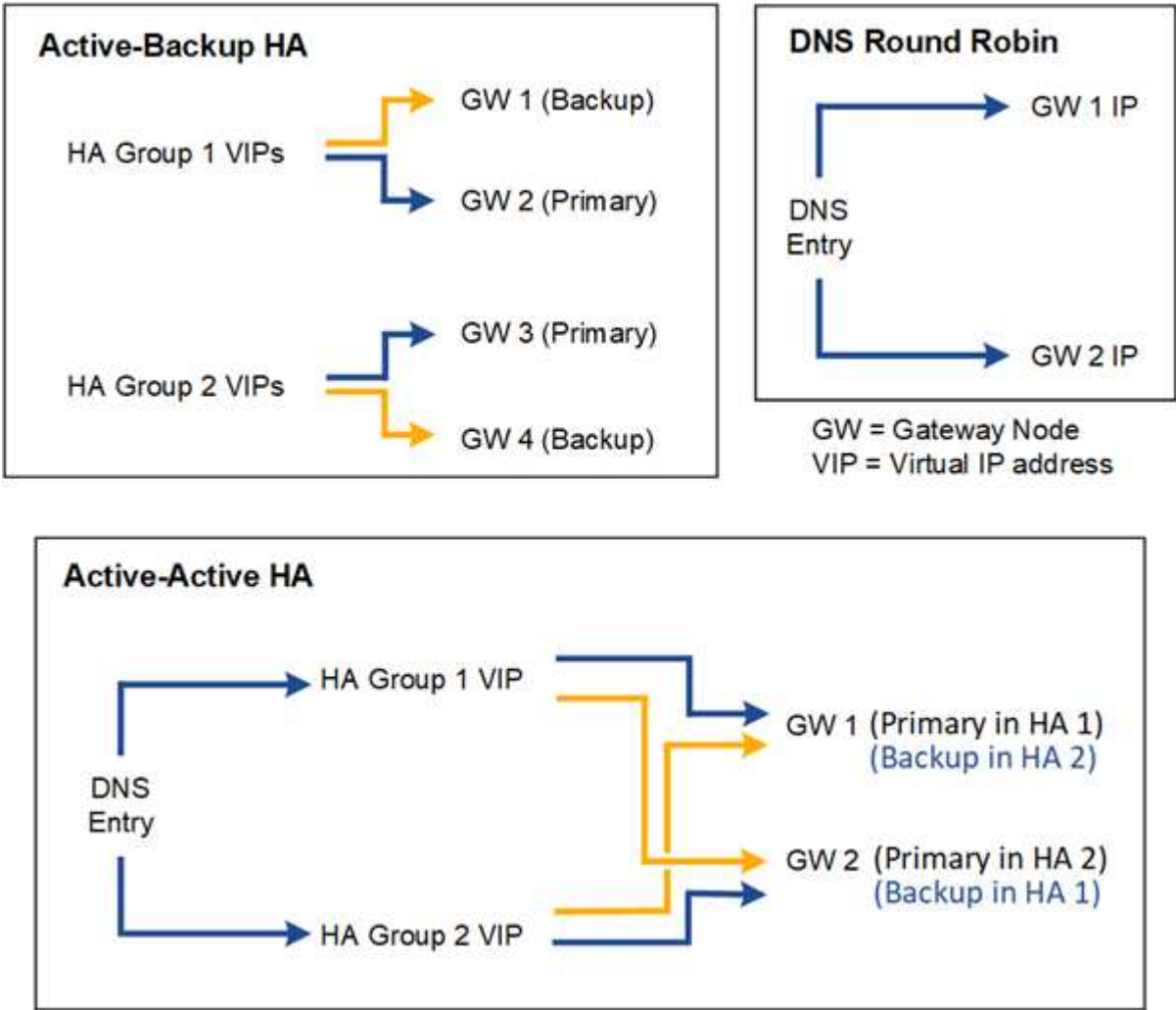
desconectado e deverá fazer login novamente para retomar sua tarefa.

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

Opções de configuração para grupos HA

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

Nos diagramas, o azul indica a interface primária no grupo HA e o amarelo indica a interface de backup no grupo HA.



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

Configuração	Vantagens	Desvantagens
HA de backup ativo	- Gerenciado pelo StorageGRID sem dependências externas. - Failover rápido.	Somente um nó em um grupo HA está ativo. Pelo menos um nó por grupo HA ficará ocioso.

Configuração	Vantagens	Desvantagens
DNS Round Robin	• Aumento do rendimento agregado. • Nenhum host ocioso.	• Failover lento, que pode depender do comportamento do cliente. • Requer configuração de hardware fora do StorageGRID. • Precisa de uma verificação de integridade implementada pelo cliente.
HA ativo-ativo	• O tráfego é distribuído entre vários grupos de HA. • Alto rendimento agregado que pode ser dimensionado com o número de grupos HA. • Failover rápido.	• Mais complexo de configurar. • Requer configuração de hardware fora do StorageGRID. • Precisa de uma verificação de integridade implementada pelo cliente.

Configurar grupos de alta disponibilidade

Você pode configurar grupos de alta disponibilidade (HA) para fornecer acesso de alta disponibilidade aos serviços em nós de administração ou nós de gateway.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da 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. Ver ["Configurar interfaces VLAN"](#) .
- Se você planeja usar uma interface de acesso para um nó em um grupo de HA, você criou a interface:
 - **Red Hat Enterprise Linux (antes de instalar o nó):** ["Criar arquivos de configuração de nó"](#)
 - **Ubuntu ou Debian (antes de instalar o nó):** ["Criar arquivos de configuração de nó"](#)
 - **Linux (após instalar o nó):** ["Linux: Adicionar interfaces de tronco ou acesso a um nó"](#)
 - **VMware (após instalar o nó):** ["VMware: Adicionar interfaces de tronco ou acesso a um nó"](#)

Criar um grupo de alta disponibilidade

Ao criar um grupo de alta disponibilidade, você seleciona uma ou mais interfaces e as organiza em ordem de prioridade. Em seguida, você atribui um ou mais endereços VIP ao grupo.

Uma interface deve ser para um nó de gateway ou um nó de administração para ser incluído em um grupo de HA. Um grupo HA só pode usar uma interface para cada nó; no entanto, outras interfaces para o mesmo nó podem ser usadas em outros grupos HA.

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Grupos de alta disponibilidade**.
2. Selecione **Criar**.

Insira detalhes para o grupo HA

Passos

1. Forneça um nome exclusivo para o grupo HA.
2. Opcionalmente, insira uma descrição para o grupo HA.
3. Selecione **Continuar**.

Adicionar interfaces ao grupo HA

Passos

1. Selecione uma ou mais interfaces para adicionar a este grupo 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



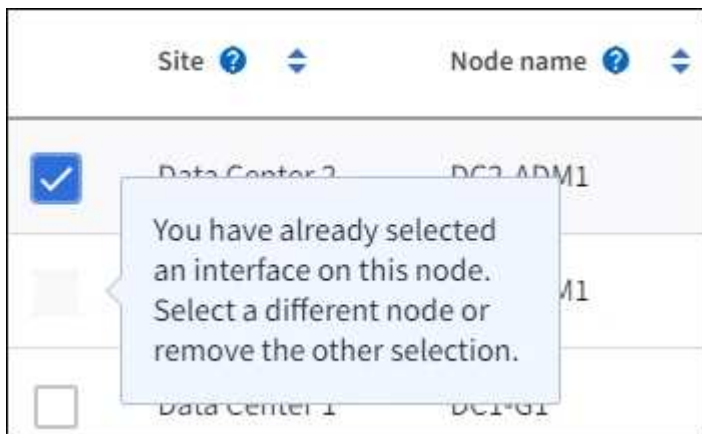
Após criar uma interface VLAN, aguarde até 5 minutos para que a nova interface apareça na tabela.

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 HA dos serviços do nó administrativo, que incluem o Grid Manager e o Tenant Manager, selecione interfaces somente nos nós administrativos.
- Se o grupo HA for para proteção HA do tráfego do cliente S3, selecione interfaces em nós de administração, nós de gateway ou ambos.
- Se você selecionar interfaces em diferentes tipos de nós, uma nota informativa será exibida. Lembre-se de que, se ocorrer um failover, os serviços fornecidos pelo nó ativo anteriormente podem não estar disponíveis no nó recém-ativo. Por exemplo, um nó de gateway de backup não pode fornecer proteção de alta disponibilidade dos serviços do nó de administração. Da mesma forma, um nó administrativo

de backup não pode executar todos os procedimentos de manutenção que o nó administrativo principal pode fornecer.

- Se você não puder selecionar uma interface, sua caixa de seleção estará desabilitada. A dica de ferramenta fornece mais informações.



- Não é possível selecionar uma interface se o valor da sub-rede ou do gateway estiver em conflito com outra interface selecionada.
- Você não pode selecionar uma interface configurada se ela não tiver um endereço IP estático.

2. Selecione **Continuar**.

Determinar a ordem de prioridade

Se o grupo HA incluir mais de uma interface, você poderá determinar qual é a interface primária e quais são as interfaces de backup (failover). Se a interface primária falhar, os endereços VIP serão movidos para a interface de maior prioridade disponível. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de maior prioridade disponível, 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 na 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 deverá selecionar uma interface no nó de administração principal para ser a interface primária. Alguns procedimentos de manutenção só podem ser executados no nó de administração principal.

2. Selecione **Continuar**.

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 do S3 acessar esses endereços VIP 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 esse 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 esse grupo de HA para balanceamento de carga, crie um ponto de extremidade do balanceador de carga para determinar a porta e o protocolo de rede e anexar quaisquer certificados necessários. Ver "[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, talvez seja 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. Marque a caixa de seleção do grupo HA que você deseja editar.
3. Faça um dos seguintes procedimentos, com base no que você deseja atualizar:
 - Selecione **Ações > Editar endereço IP virtual** para adicionar ou remover endereços VIP.
 - Selecione **Ações > Editar grupo HA** para atualizar o nome ou a descrição do grupo, adicionar ou remover interfaces, alterar a ordem de prioridade ou adicionar ou remover endereços VIP.
4. Se você selecionou **Editar endereço IP virtual**:
 - a. Atualize os endereços IP virtuais 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, marque ou desmarque as caixas de seleção para adicionar ou remover interfaces.



Se o grupo HA fornecer acesso ao Grid Manager, você deverá selecionar uma interface no nó de administração principal para ser a interface primária. Alguns procedimentos de manutenção só podem ser executados a partir do nó de administração principal

- c. Opcionalmente, arraste as linhas para alterar a ordem de prioridade da interface primária e de quaisquer interfaces de backup para este grupo de HA.
- d. Opcionalmente, atualize os endereços IP virtuais.
- e. Selecione **Salvar** e depois **Concluir**.

Remover um grupo de alta disponibilidade

Você pode remover um ou mais grupos de alta disponibilidade (HA) por vez.



Não é possível remover um grupo de HA se ele estiver vinculado a um ponto de extremidade do balanceador de carga. Para excluir um grupo de HA, você deve removê-lo de todos os pontos de extremidade do balanceador de carga que o utilizam.

Para evitar interrupções no cliente, atualize todos os aplicativos cliente S3 afetados antes de remover um grupo de 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. Revise a coluna **Pontos de extremidade do balanceador de carga** para cada grupo de HA que você deseja remover. Se algum ponto de extremidade do balanceador de carga estiver listado:
 - a. Vá para **CONFIGURAÇÃO > Rede > Pontos de extremidade do balanceador de carga**.
 - b. Marque a caixa de seleção do ponto de extremidade.
 - c. Selecione **Ações > Editar modo de vinculação de ponto de extremidade**.
 - d. Atualize o modo de vinculação para remover o grupo HA.
 - e. Selecione **Salvar alterações**.
3. Se nenhum ponto de extremidade do balanceador de carga estiver listado, marque a caixa de seleção de cada grupo de HA que você deseja remover.
4. Selecione **Ações > Remover grupo HA**.
5. Revise a mensagem e selecione **Excluir grupo HA** para confirmar sua seleção.

Todos os grupos de HA selecionados serão removidos. Um banner de sucesso verde aparece na página Grupos de alta disponibilidade.

Gerenciar balanceamento de carga

Considerações para balanceamento de carga

Você pode usar o balanceamento de carga para lidar com 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, o StorageGRID usa 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 distribuindo a carga de trabalho entre vários nós de armazenamento.

O serviço StorageGRID Load Balancer é instalado em todos os nós de administração e todos os nós de gateway e fornece balanceamento de carga da Camada 7. Ele executa o encerramento de solicitações de clientes pelo protocolo TLS (Transport Layer Security), inspeciona as solicitações e estabelece novas conexões seguras com os nós de armazenamento.

O serviço Load Balancer 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 Load Balancer encaminha mais solicitações para nós de armazenamento com maior disponibilidade de CPU.



Embora o serviço StorageGRID Load Balancer seja o mecanismo de balanceamento de carga recomendado, talvez você queira integrar um balanceador de carga de terceiros. Para obter informações, entre em contato com seu representante de conta NetApp ou consulte ["TR-4626: balanceadores de carga globais e de terceiros do StorageGRID"](#).

Quanto nós de balanceamento de carga eu preciso?

Como prática recomendada geral, cada site no seu sistema StorageGRID deve incluir dois ou mais nós com o serviço Load Balancer. Por exemplo, um site pode incluir dois nós de gateway ou um nó de administração e um nó de gateway. Certifique-se de que haja infraestrutura de rede, hardware ou virtualização adequada para cada nó de balanceamento de carga, esteja você usando dispositivos de serviços, nós bare metal ou nós baseados em máquina virtual (VM).

O que é um ponto de extremidade do balanceador de carga?

Um ponto de extremidade do balanceador de carga define a porta e o protocolo de rede (HTTPS ou HTTP) que as solicitações de entrada e saída do aplicativo cliente usarão para acessar os nós que contêm o serviço do balanceador de carga. O ponto de extremidade também define o tipo de cliente (S3), o modo de vinculação e, opcionalmente, uma lista de locatários permitidos ou bloqueados.

Para criar um ponto de extremidade do balanceador de carga, selecione **CONFIGURAÇÃO > Rede > Pontos de extremidade do balanceador de carga** ou conclua o assistente de configuração do FabricPool e do S3. Para instruções:

- ["Configurar pontos de extremidade do balanceador de carga"](#)
- ["Use o assistente de configuração do S3"](#)
- ["Use o assistente de configuração do FabricPool"](#)

Considerações para o porto

A porta para um ponto de extremidade do balanceador de carga é definida como 10433 para o primeiro ponto de extremidade criado, mas você pode especificar qualquer porta externa não utilizada entre 1 e 65535. Se você usar a porta 80 ou 443, o ponto de extremidade usará o serviço Load Balancer somente nos nós de gateway. Essas portas são reservadas em nós de administração. Se você usar a mesma porta para mais de um ponto de extremidade, deverá especificar um modo de vinculação diferente para cada ponto de extremidade.

Portas usadas por outros serviços de rede não são permitidas. Veja o ["Referência de porta de rede"](#).

Considerações sobre o protocolo de rede

Na maioria dos casos, as conexões entre aplicativos cliente e o StorageGRID devem usar criptografia TLS (Transport Layer Security). A conexão ao StorageGRID sem criptografia TLS é suportada, mas não recomendada, especialmente em ambientes de produção. Ao selecionar o protocolo de rede para o ponto de extremidade do balanceador de carga StorageGRID, você deve selecionar **HTTPS**.

Considerações sobre certificados de ponto de extremidade do balanceador de carga

Se você selecionar **HTTPS** como o 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 upload de um certificado assinado (recomendado).** Este certificado pode ser assinado por uma autoridade de certificação (CA) pública ou privada. Usar um certificado de servidor CA publicamente confiável para proteger a conexão é a melhor prática. Ao contrário dos certificados gerados, os certificados assinados por uma CA podem ser rotacionados sem interrupções, o que pode ajudar a evitar problemas de expiração.

Você deve obter os seguintes arquivos antes de criar o ponto de extremidade do balanceador de carga:

- O arquivo de certificado do servidor personalizado.
 - O arquivo de chave privada do certificado do servidor personalizado.
 - Opcionalmente, um pacote de CA dos certificados de cada autoridade certificadora emissora intermediária.
- **Gerar um certificado autoassinado.**
 - **Use o certificado global StorageGRID S3.** Você deve carregar ou gerar uma versão personalizada deste certificado antes de poder selecioná-lo para o ponto de extremidade do balanceador de carga. Ver ["Configurar certificados da API S3"](#).

Quais valores eu preciso?

Para criar o certificado, você deve saber todos os nomes de domínio e endereços IP que os aplicativos cliente S3 usarão para acessar o ponto de extremidade.

A entrada **Subject DN** (Distinguished Name) do 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 do 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 de estilo de hospedagem virtual S3, o certificado também deve incluir uma entrada **Nome Alternativo** para cada ["Nome de domínio do ponto de extremidade S3"](#) que você configurou, incluindo quaisquer nomes curinga. Por exemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```



Se você usar curingas para nomes de domínio, revise o ["Diretrizes de proteção 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 o StorageGRID expirar, o aplicativo poderá perder temporariamente o acesso ao StorageGRID.

Para evitar problemas de expiração de certificado, siga estas práticas recomendadas:

- Monitore cuidadosamente todos os alertas que avisam sobre a aproximação das datas de expiração do certificado, como os alertas **Expiração do certificado de ponto de extremidade do balanceador de carga** e **Expiração do certificado do servidor global para a API S3**.
- Mantenha sempre as versões do certificado do StorageGRID e do aplicativo S3 sincronizadas. Se você substituir ou renovar o certificado usado para um ponto de extremidade do balanceador de carga, deverá substituir ou renovar o certificado equivalente usado pelo aplicativo S3.
- Use um certificado de CA assinado publicamente. Se você usar um certificado assinado por uma CA, poderá substituir certificados prestes a expirar sem interrupções.
- Se você gerou um certificado StorageGRID autoassinado e esse certificado estiver prestes a expirar, você deverá substituí-lo manualmente no StorageGRID e no aplicativo S3 antes que o certificado existente expire.

Considerações sobre o modo de ligação

O modo de vinculação permite controlar quais endereços IP podem ser usados para acessar um ponto de extremidade do balanceador de carga. Se um ponto de extremidade usar um modo de vinculação, os aplicativos clientes só poderão acessar o ponto de extremidade se usarem um endereço IP permitido ou seu nome de domínio totalmente qualificado (FQDN) correspondente. Aplicativos clientes que usam qualquer outro endereço IP ou FQDN não conseguem acessar o endpoint.

Você pode especificar qualquer um dos seguintes modos de vinculação:

- **Global (padrão):** Os aplicativos cliente podem acessar o ponto de extremidade usando o endereço IP de qualquer nó de gateway ou nó de administração, o endereço IP virtual (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 ponto de extremidade.
- **IPs virtuais de grupos HA.** Os aplicativos cliente devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA.
- **Interfaces de nó.** Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas.
- **Tipo de nó.** Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó de administração ou o endereço IP (ou FQDN correspondente) de qualquer nó de gateway.

Considerações sobre acesso de inquilinos

O acesso do locatário é um recurso de segurança opcional que permite controlar quais contas de locatário do StorageGRID podem usar um ponto de extremidade do balanceador de carga para acessar seus buckets. Você pode permitir que todos os locatários acessem um ponto de extremidade (padrão) ou pode especificar uma lista de locatários permitidos ou bloqueados para cada ponto de extremidade.

Você pode usar esse recurso para fornecer melhor isolamento de segurança entre locatários e seus endpoints. Por exemplo, você pode usar esse recurso para garantir que os materiais ultrassecretos ou altamente confidenciais de propriedade de um inquilino permaneçam completamente inacessíveis a outros inquilinos.



Para fins de controle de acesso, o locatário é determinado a partir das chaves de acesso usadas na solicitação do cliente. Se nenhuma chave de acesso for fornecida como parte da solicitação (como no caso de acesso anônimo), o proprietário do bucket será usado para determinar o locatário.

Exemplo de acesso do inquilino

Para entender como esse recurso de segurança funciona, considere o seguinte exemplo:

1. Você criou dois pontos de extremidade do balanceador de carga, como segue:
 - Ponto de extremidade **público**: usa a porta 10443 e permite acesso a todos os locatários.
 - Ponto de extremidade **Top Secret**: usa a porta 10444 e permite acesso somente ao locatário **Top Secret**. Todos os outros inquilinos estão bloqueados de acessar este ponto de extremidade.
2. O `top-secret.pdf` está em um balde de propriedade do inquilino **ultrassecreto**.

Para acessar o `top-secret.pdf`, um usuário no locatário **Top secret** pode emitir uma solicitação GET para `https://w.x.y.z:10444/top-secret.pdf`. Como esse locatário tem permissão para usar o ponto de extremidade 10444, o usuário pode acessar o objeto. Entretanto, se um usuário pertencente a qualquer outro locatário emitir a mesma solicitação para o mesmo URL, ele 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 nó de administração e nó de gateway opera de forma independente ao encaminhar o tráfego S3 para os nós de armazenamento. Por meio de um processo de ponderação, o serviço Load Balancer encaminha mais solicitações para nós de armazenamento com maior disponibilidade de CPU. As informações de carga da CPU do nó são atualizadas a cada poucos minutos, mas a ponderação pode ser atualizada com mais frequência. Todos os nós de armazenamento recebem um valor mínimo de peso base, mesmo que um nó relate 100% de utilização ou não relate sua utilização.

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

Configurar pontos de extremidade do balanceador de carga

Os pontos de extremidade do balanceador de carga determinam as portas e os protocolos de rede que os clientes S3 podem usar ao se conectar ao balanceador de carga StorageGRID nos nós de gateway e de administração. Você também pode usar endpoints para acessar o Grid Manager, o Tenant Manager ou ambos.



Os detalhes do Swift foram removidos desta versão do site de documentação. Ver "[Configurar conexões de cliente S3 e Swift](#)".

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você tem o "[Permissão de acesso root](#)".
- Você revisou o "[considerações para balanceamento de carga](#)".
- Se você remapeou anteriormente uma porta que pretende usar para o ponto de extremidade do balanceador de carga, você tem "[removeu o remapeamento da porta](#)".

- Você criou todos os grupos de alta disponibilidade (HA) que planeja usar. Grupos HA são recomendados, mas não obrigatórios. Ver "[Gerenciar grupos de alta disponibilidade](#)".
- Se o ponto de extremidade do balanceador de carga for usado por "[Inquilinos S3 para S3 Select](#)", ele não deve usar os endereços IP ou FQDNs de nenhum nó bare-metal. Somente dispositivos de serviços e nós de software baseados em VMware são permitidos para os pontos de extremidade do balanceador de carga usados para o S3 Select.
- Você configurou todas as interfaces VLAN que planeja usar. Ver "[Configurar interfaces VLAN](#)".
- Se estiver criando um ponto de extremidade HTTPS (recomendado), você terá as informações para o certificado do servidor.



Alterações em um certificado de ponto de extremidade podem levar até 15 minutos para serem aplicadas a todos os nós.

- Para carregar um certificado, você precisa do certificado do servidor, da chave privada do certificado e, opcionalmente, de um pacote de CA.
- Para gerar um certificado, você precisa de todos os nomes de domínio e endereços IP que os clientes S3 usarão para acessar o ponto de extremidade. Você também deve conhecer o assunto (Nome Distinto).
- Se você quiser usar o certificado StorageGRID S3 API (que também pode ser usado para conexões diretas com nós de armazenamento), você já substituiu o certificado padrão por um certificado personalizado assinado por uma autoridade de certificação externa. Ver "[Configurar certificados da API S3](#)".

Criar um ponto de extremidade do balanceador de carga

Cada ponto de extremidade do balanceador de carga do cliente S3 especifica uma porta, um tipo de cliente (S3) e um protocolo de rede (HTTP ou HTTPS). Os pontos de extremidade do balanceador de carga da interface de gerenciamento especificam uma porta, um tipo de interface e uma rede de cliente não confiável.

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Pontos de extremidade do balanceador de carga**.
2. Para criar um ponto de extremidade para um cliente S3 ou Swift, selecione a guia **Cliente S3 ou Swift**.
3. Para criar um ponto de extremidade para acesso ao Grid Manager, ao Tenant Manager ou a ambos, selecione a guia **Interface de gerenciamento**.
4. Selecione **Criar**.

Insira os detalhes do ponto de extremidade

Passos

1. Selecione as instruções apropriadas para inserir detalhes sobre o tipo de ponto de extremidade que você deseja criar.

Cliente S3 ou Swift

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página Endpoints do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo assume como padrão 10433 para o primeiro ponto de extremidade criado, mas você pode inserir qualquer porta externa não utilizada de 1 a 65535. Se você digitar 80 ou 8443, o ponto de extremidade será configurado somente em nós de gateway, a menos que você tenha liberado a porta 8443. Em seguida, você pode usar a porta 8443 como um ponto de extremidade S3, e a porta será configurada nos nós de gateway e de administração.
Tipo de cliente	O tipo de aplicativo cliente que usará este ponto de extremidade, S3 ou Swift .
Protocolo de rede	O protocolo de rede que os clientes usarão ao se conectar a este ponto de extremidade. • Selecione HTTPS para comunicação segura e criptografada por TLS (recomendado). Você deve anexar um certificado de segurança antes de salvar o endpoint. • Selecione HTTP para comunicação menos segura e não criptografada. Use HTTP somente para uma grade não produtiva.

Interface de gerenciamento

Campo	Descrição
Nome	Um nome descritivo para o endpoint, que aparecerá na tabela na página Endpoints do balanceador de carga.
Porta	A porta StorageGRID que você deseja usar para acessar o Grid Manager, o Tenant Manager ou ambos. • Gerente de grade: 8443 • Gerente de inquilinos: 9443 • Gerente de Rede e Gerente de Inquilino: 443 Observação: Você pode usar essas portas predefinidas ou outras portas disponíveis.
Tipo de interface	Selecione o botão de opção para a interface StorageGRID que você acessará usando este ponto de extremidade.

Campo	Descrição
Rede de clientes não confiáveis	Selecione Sim se este ponto de extremidade deve ser acessível a redes de clientes não confiáveis. Caso contrário, selecione Não. Quando você seleciona Sim, a porta é aberta em todas as redes de clientes não confiáveis. Observação: você só pode configurar uma porta para ser aberta ou fechada para redes de clientes não confiáveis ao criar o ponto de extremidade do balanceador de carga.

1. Selecione **Continuar**.

Selecione um modo de encadernação

Passos

1. Selecione um modo de vinculação para o ponto de extremidade para controlar como o ponto de extremidade é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

Alguns modos de vinculação estão disponíveis para terminais de cliente ou terminais de interface de gerenciamento. Todos os modos para ambos os tipos de endpoint estão listados aqui.

Modo	Descrição
Global (padrão para endpoints do cliente)	Os clientes podem acessar o ponto de extremidade usando o endereço IP de qualquer nó de gateway ou nó de administração, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração Global, a menos que você precise restringir a acessibilidade deste ponto de extremidade.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este ponto de extremidade. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nó	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar este ponto de extremidade.
Tipo de nó (somente terminais do cliente)	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó de administração ou o endereço IP (ou FQDN correspondente) de qualquer nó de gateway para acessar esse ponto de extremidade.

Modo	Descrição
Todos os nós de administração (padrão para terminais de interface de gerenciamento)	Os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó de administração para acessar este ponto de extremidade.

Se mais de um ponto de extremidade usar a mesma porta, o StorageGRID usará esta ordem de prioridade para decidir qual ponto de extremidade usar: **IPs virtuais de grupos de HA** > **Interfaces de nó** > **Tipo de nó** > **Global**.

Se você estiver criando pontos de extremidade de interface de gerenciamento, somente nós de administração serão permitidos.

2. Se você selecionou **IPs virtuais de grupos de HA**, selecione um ou mais grupos HA.

Se você estiver criando endpoints de interface de gerenciamento, selecione VIPs associados somente a nós de administração.

3. Se você selecionou **Interfaces de nó**, selecione uma ou mais interfaces de nó para cada nó de administração ou nó de gateway que deseja associar a este ponto de extremidade.
4. Se você selecionou **Tipo de nó**, selecione Nós de administração, que inclui o Nó de administração primário e quaisquer Nós de administração não primários, ou Nós de gateway.

Controlar o acesso do inquilino



Um ponto de extremidade da interface de gerenciamento pode controlar o acesso do locatário somente quando o ponto de extremidade tem [tipo de interface do Gerenciador de Inquilinos](#).

Passos

1. Para a etapa **Acesso do locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os inquilinos (padrão)	Todas as contas de locatários podem usar esse 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 ponto de extremidade do balanceador de carga para permitir ou bloquear contas específicas.
Permitir inquilinos selecionados	Somente as contas de locatários selecionadas podem usar este ponto de extremidade para acessar seus buckets.
Bloquear inquilinos selecionados	As contas de locatários selecionadas não podem usar este ponto de extremidade para acessar seus buckets. Todos os outros inquilinos podem usar este ponto de extremidade.

2. Se você estiver criando um ponto de extremidade **HTTP**, não precisará anexar um certificado. Selecione

Criar para adicionar o novo ponto de extremidade do balanceador de carga. Então vá para [Depois que você terminar](#) . Caso contrário, selecione **Continuar** para anexar o certificado.

Anexar certificado

Passos

1. Se você estiver criando um ponto de extremidade **HTTPS**, selecione o tipo de certificado de segurança que deseja anexar ao ponto de extremidade.

O certificado protege as conexões entre clientes S3 e o serviço Load Balancer no nó de administração ou nos nós de gateway.

- **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.
- **Use o certificado StorageGRID S3.** Selecione esta opção se quiser usar o certificado global da API S3, que também pode ser usado para conexões diretas com nós de armazenamento.

Você não pode selecionar esta opção a menos que tenha substituído o certificado padrão da API S3, que é assinado pela CA da grade, por um certificado personalizado assinado por uma autoridade de certificação externa. Ver "[Configurar certificados da API S3](#)".

- **Usar certificado de interface de gerenciamento.** Selecione esta opção se quiser usar o certificado da interface de gerenciamento global, que também pode ser usado para conexões diretas com nós de administração.
2. Se você não estiver usando o certificado StorageGRID S3, carregue ou gere o certificado.

Carregar certificado

a. Selecione **Carregar certificado**.

b. Carregue os arquivos de certificado do servidor necessários:

- **Certificado do servidor:** O arquivo de certificado do servidor personalizado na codificação PEM.
- **Chave privada do certificado:** O arquivo de chave privada do certificado do servidor personalizado(`.key`).



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

- **Pacote CA:** Um único arquivo opcional contendo os certificados de cada autoridade certificadora intermediária emissora (CA). O arquivo deve conter cada um dos arquivos de certificado 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 será exibido em sua própria guia.

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

Especifique o nome do arquivo do certificado e o local do 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 e colá-lo em outro lugar.

d. Selecione **Criar**. + O ponto de extremidade do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 ou a interface de gerenciamento e o ponto de extremidade.

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 a serem incluídos no certificado. Use um * como curinga para representar vários nomes de domínio.
IP	Um ou mais endereços IP a serem incluídos no certificado.
Assunto (opcional)	Assunto X.509 ou nome distinto (DN) do proprietário do certificado. Se nenhum valor for inserido neste campo, o certificado gerado usará o primeiro nome de domínio ou endereço IP como o nome comum do assunto (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. Observação: 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 ver os metadados do certificado gerado.

- Selecione **Baixar certificado** para salvar o arquivo de certificado.

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

Por exemplo: `storagegrid_certificate.pem`

- Selecione **Copiar certificado PEM** para copiar o conteúdo do certificado e colá-lo em outro lugar.

e. Selecione **Criar**.

O ponto de extremidade do balanceador de carga é criado. O certificado personalizado é usado para todas as novas conexões subsequentes entre clientes S3 ou a interface de gerenciamento e este ponto de extremidade.

Depois que você terminar

Passos

1. Se você usar um DNS, certifique-se de que o DNS inclua um registro para associar o nome de domínio totalmente qualificado (FQDN) do StorageGRID a cada endereço IP que os clientes usarão para fazer conexões.

O endereço IP inserido no registro DNS depende se você está usando um grupo HA de nós de balanceamento de carga:

- Se você tiver configurado um grupo HA, os clientes se conectarão aos endereços IP virtuais desse grupo HA.
- Se você não estiver usando um grupo HA, os clientes se conectarão ao serviço StorageGRID Load Balancer usando o endereço IP de um nó de gateway ou nó de administrador.

Você também deve garantir que o registro DNS faça referência a todos os nomes de domínio de endpoint necessários, incluindo quaisquer nomes curinga.

2. Forneça aos clientes S3 as informações necessárias para se conectar ao ponto de extremidade:

- Número da porta
- Nome de domínio totalmente qualificado ou endereço IP
- Quaisquer detalhes do certificado necessários

Visualizar e editar pontos de extremidade do balanceador de carga

Você pode visualizar detalhes dos pontos de extremidade do balanceador de carga existentes, incluindo os metadados do certificado para um ponto de extremidade protegido. Você pode alterar determinadas configurações de um ponto de extremidade.

- Para visualizar informações básicas de todos os pontos de extremidade do balanceador de carga, revise as tabelas na página Pontos de extremidade do balanceador de carga.
- Para visualizar todos os detalhes sobre um ponto de extremidade específico, incluindo metadados do certificado, selecione o nome do ponto de extremidade na tabela. As informações mostradas 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 Endpoints do balanceador de carga.



Se você perder o acesso ao Grid Manager ao editar a porta de um ponto de extremidade da interface de gerenciamento, atualize o URL e a porta para recuperar o acesso.



Depois de editar um ponto de extremidade, pode ser necessário esperar até 15 minutos para que suas alterações sejam aplicadas a todos os nós.

Tarefa	Menu de ações	Página de detalhes
Editar nome do ponto de extremidade	a. Marque a caixa de seleção do ponto de extremidade. b. Selecione Ações > Editar nome do ponto de extremidade. c. Digite o novo nome. d. Selecione Salvar.	a. Selecione o nome do ponto de extremidade para exibir os detalhes. b. Selecione o ícone de edição  . c. Digite o novo nome. d. Selecione Salvar.
Editar porta do ponto de extremidade	a. Marque a caixa de seleção do ponto de extremidade. b. Selecione Ações > Editar porta do ponto de extremidade c. Digite um número de porta válido. d. Selecione Salvar.	<i>n / D</i>
Editar modo de vinculação de ponto de extremidade	a. Marque a caixa de seleção do ponto de extremidade. b. Selecione Ações > Editar modo de vinculação de ponto de extremidade. c. Atualize o modo de vinculação conforme necessário. d. Selecione Salvar alterações.	a. Selecione o nome do ponto de extremidade para exibir os detalhes. b. Selecione Editar modo de vinculação. c. Atualize o modo de vinculação conforme necessário. d. Selecione Salvar alterações.
Editar certificado de ponto de extremidade	a. Marque a caixa de seleção do ponto de extremidade. b. Selecione Ações > Editar certificado de ponto de extremidade. c. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3, conforme necessário. d. Selecione Salvar alterações.	a. Selecione o nome do ponto de extremidade para exibir os detalhes. b. Selecione a aba Certificado. c. Selecione Editar certificado. d. Carregue ou gere um novo certificado personalizado ou comece a usar o certificado global S3, conforme necessário. e. Selecione Salvar alterações.

Tarefa	Menu de ações	Página de detalhes
Editar acesso do locatário	a. Marque a caixa de seleção do ponto de extremidade. b. Selecione Ações > Editar acesso do locatário . c. Escolha uma opção de acesso diferente, selecione ou remova inquilinos da lista ou faça as duas coisas. d. Selecione Salvar alterações .	a. Selecione o nome do ponto de extremidade para exibir os detalhes. b. Selecione a aba Acesso do locatário . c. Selecione Editar acesso do locatário . d. Escolha uma opção de acesso diferente, selecione ou remova inquilinos da lista ou faça as duas coisas. e. Selecione Salvar alterações .

Remover pontos de extremidade do balanceador de carga

Você pode remover um ou mais endpoints usando o menu **Ações** ou pode remover um único endpoint da página de detalhes.



Para evitar interrupções no cliente, atualize todos os aplicativos cliente S3 afetados antes de remover um ponto de extremidade do balanceador de carga. Atualize cada cliente para se conectar usando uma porta atribuída a outro ponto de extremidade do balanceador de carga. Não se esqueça de atualizar também todas as informações necessárias do certificado.



Se você perder o acesso ao Grid Manager ao remover um ponto de extremidade da interface de gerenciamento, atualize o URL.

- Para remover um ou mais pontos de extremidade:
 - Na página Balanceador de carga, marque a caixa de seleção de cada endpoint que deseja remover.
 - Selecione **Ações > Remover**.
 - Selecione **OK**.
- Para remover um ponto de extremidade da página de detalhes:
 - Na página Balanceador de carga, selecione o nome do endpoint.
 - Selecione **Remover** na página de detalhes.
 - Selecione **OK**.

Configurar nomes de domínio de endpoint S3

Para dar suporte a solicitações de 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 do S3 se conectam.



Não há suporte para o uso de um endereço IP para um nome de domínio de ponto de extremidade. Versões futuras impedirão essa configuração.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem ["permissões de acesso específicas"](#) .
- Você confirmou que uma atualização de rede não está em andamento.



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

Sobre esta tarefa

Para permitir que os clientes usem nomes de domínio de ponto de extremidade S3, você deve fazer tudo o seguinte:

- Use o Grid Manager para adicionar os nomes de domínio do endpoint S3 ao sistema StorageGRID .
- Assegurar que o ["certificado que o cliente usa para conexões HTTPS com o StorageGRID"](#) é assinado para todos os nomes de domínio que o cliente requer.

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

- Configure o servidor DNS usado pelo cliente. Inclua registros DNS para os endereços IP que os clientes usam para fazer conexões e garanta que os registros façam referência a todos os nomes de domínio de ponto de extremidade S3 necessários, incluindo quaisquer nomes curinga.



Os clientes podem se conectar ao StorageGRID usando o endereço IP de um nó de gateway, um nó de administração ou um nó de armazenamento, ou conectando-se ao endereço IP virtual de um grupo de alta disponibilidade. Você deve entender como os aplicativos clientes se conectam à grade para incluir os endereços IP corretos nos registros DNS.

Clientes que usam conexões HTTPS (recomendado) para a grade podem usar qualquer um destes certificados:

- Clientes que se conectam a um ponto de extremidade do balanceador de carga podem usar um certificado personalizado para esse ponto de extremidade. Cada ponto de extremidade do balanceador de carga pode ser configurado para reconhecer diferentes nomes de domínio de ponto de extremidade S3.
- Os clientes que se conectam a um ponto de extremidade do balanceador de carga ou diretamente a um nó de armazenamento podem personalizar o certificado global da API do S3 para incluir todos os nomes de domínio de ponto de extremidade do S3 necessários.



Se você não adicionar nomes de domínio de ponto de extremidade S3 e a lista estiver vazia, o suporte para solicitações de estilo de hospedagem virtual S3 será desabilitado.

Adicionar um nome de domínio de ponto de extremidade S3

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Nomes de domínio de ponto de extremidade S3**.
2. Digite o nome do 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 do servidor usados pelos clientes correspondam aos nomes de domínio do ponto de extremidade S3 necessários.
 - Se os clientes se conectarem a um ponto de extremidade do balanceador de carga que usa seu próprio certificado, ["atualizar o certificado associado ao ponto de extremidade"](#) .
 - Se os clientes se conectarem a um ponto de extremidade do balanceador de carga que usa o certificado global da API S3 ou diretamente aos nós de armazenamento, ["atualizar o certificado global da API S3"](#) .
5. Adicione os registros DNS necessários para garantir que as solicitações de nome de domínio do endpoint possam ser resolvidas.

Resultado

Agora, quando os clientes usam o ponto de extremidade `bucket.s3.company.com` , o servidor DNS resolve para o ponto de extremidade correto e o certificado autentica o ponto de extremidade conforme o esperado.

Renomear um nome de domínio de ponto de extremidade S3

Se você alterar um nome usado pelos aplicativos S3, as solicitações no estilo de hospedagem virtual falharão.

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Nomes de domínio de ponto de extremidade S3**.
2. Selecione o campo de nome de domínio que deseja editar e faça as alterações necessárias.
3. Selecione **Salvar**.
4. Selecione **Sim** para confirmar sua alteração.

Excluir um nome de domínio de ponto de extremidade S3

Se você remover um nome usado por aplicativos S3, as solicitações no estilo de hospedagem virtual falharão.

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Nomes de domínio de ponto de extremidade S3**.
2. Selecione o ícone de exclusão  ao lado do nome do domínio.
3. Selecione **Sim** para confirmar a exclusão.

Informações relacionadas

- ["Usar API REST do S3"](#)
- ["Ver endereços IP"](#)
- ["Configurar grupos de alta disponibilidade"](#)

Resumo: Endereços IP e portas para conexões de clientes

Para armazenar ou recuperar objetos, os aplicativos cliente S3 se conectam ao serviço Load Balancer, que está incluído em todos os nós de administração e nós de gateway, ou ao serviço Local Distribution Router (LDR), que está incluído em todos os nós de armazenamento.

Os aplicativos cliente podem se conectar ao StorageGRID usando o endereço IP de um nó de 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 de alta disponibilidade que usam endereços IP virtuais (VIP). Se você quiser se conectar ao StorageGRID usando um nome de 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 do balanceador de carga e grupos de alta disponibilidade (HA), consulte [Onde encontrar endereços IP](#) para localizar esses valores no Grid Manager.

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 ponto de extremidade do balanceador de carga
Nó de administração	Balanceador de carga	Endereço IP do nó de administração	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de gateway	Balanceador de carga	Endereço IP do nó de gateway	Porta atribuída ao ponto de extremidade do balanceador de carga
Nó de armazenamento	LDR	Endereço IP do nó de armazenamento	Portas S3 padrão: • HTTPS: 18082 • HTTP: 18084

URLs de exemplo

Para conectar um aplicativo cliente ao ponto de extremidade 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 ponto de extremidade do balanceador de carga for 10443, um aplicativo poderá usar a seguinte URL para se conectar ao StorageGRID:

```
https://192.0.2.5:10443
```

Onde encontrar endereços IP

1. Sign in no Grid Manager usando um ["navegador da web compatível"](#).
2. Para encontrar o endereço IP de um nó de grade:
 - a. Selecione **NODES**.
 - b. Selecione o nó de administração, nó de gateway ou nó de armazenamento ao qual você deseja se conectar.
 - c. Selecione a aba **Visão geral**.

- d. Na seção Informações do nó, observe os endereços IP do nó.
- e. Selecione **Mostrar mais** para visualizar endereços IPv6 e mapeamentos de interface.

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

- **eth0**: Rede de grade
- **eth1**: Rede de administração (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 mostrado 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 ponto de extremidade do Load Balancer:
 - a. Selecione **CONFIGURAÇÃO > Rede > Pontos de extremidade do balanceador de carga**.
 - b. Anote o número da porta do ponto de extremidade que você deseja usar.



Se o número da porta for 80 ou 443, o ponto de extremidade será configurado somente em nós de gateway, porque essas portas são reservadas em nós de administração. Todas as outras portas são configuradas nos nós de gateway e nos nós de administração.

- c. Selecione o nome do ponto de extremidade na tabela.
 - d. Confirme se o **Tipo de cliente** (S3) corresponde ao aplicativo cliente que usará o ponto de extremidade.

Gerenciar redes e conexões

Configurar as configurações de rede

Você pode configurar várias configurações de rede no Grid Manager para ajustar a operação do seu sistema StorageGRID .

Configurar interfaces VLAN

Você pode "[criar interfaces de LAN virtual \(VLAN\)](#)" para isolar e particionar o tráfego para segurança, flexibilidade e desempenho. Cada interface VLAN está associada a uma ou mais interfaces pai em nós de administração e nós de gateway. Você pode usar interfaces VLAN em grupos de HA e em pontos de extremidade do balanceador de carga para segregar o tráfego de cliente ou administrador por aplicativo ou locatário.

Políticas de classificação de tráfego

Você pode usar "[políticas de classificação de tráfego](#)" para identificar e manipular diferentes tipos de tráfego de rede, incluindo tráfego relacionado a buckets específicos, locatários, sub-redes de clientes ou pontos de extremidade do balanceador de carga. Essas políticas podem ajudar a limitar e monitorar o tráfego.

Diretrizes para redes StorageGRID

Você pode usar o Grid Manager para configurar e gerenciar redes e conexões do StorageGRID .

Ver "[Configurar conexões do cliente S3](#)" para aprender como conectar clientes S3.

Redes StorageGRID padrão

Por padrão, o StorageGRID oferece suporte a três interfaces de rede por nó de grade, permitindo que você configure a rede para cada nó de grade individual para atender aos seus requisitos de segurança e acesso.

Para obter mais informações sobre topologia de rede, consulte "[Diretrizes de rede](#)".

Rede de grade

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

Rede de administração

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

Rede de clientes

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

Diretrizes

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

Rede	Nome da interface
Grade	eth0
Administrador (opcional)	eth1
Cliente (opcional)	eth2

- Se o nó estiver conectado a um dispositivo StorageGRID , portas específicas serão usadas para cada rede. Para mais detalhes, consulte as instruções de instalação do seu aparelho.
- A rota padrão é gerada automaticamente, por nó. Se eth2 estiver habilitado, então 0.0.0.0/0 usa a Rede

do Cliente em eth2. Se eth2 não estiver habilitado, então 0.0.0.0/0 usa a Grid Network em eth0.

- A Rede do Cliente não se torna operacional até que o nó da rede se junte à rede
- A rede de administração pode ser configurada durante a implantação do nó da grade para permitir acesso à interface do usuário de instalação antes que a grade esteja totalmente instalada.

Interfaces opcionais

Opcionalmente, você pode adicionar interfaces extras a um nó. Por exemplo, você pode querer adicionar uma interface de tronco a um nó de administração ou gateway, para que possa 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 acesso, consulte o seguinte:

- **VMware (após instalar o nó):** ["VMware: Adicionar interfaces de tronco ou acesso a um nó"](#)
 - **Red Hat Enterprise Linux (antes de instalar o nó):** ["Criar arquivos de configuração de nó"](#)
 - **Ubuntu ou Debian (antes de instalar o nó):** ["Criar arquivos de configuração de nó"](#)
 - **RHEL, Ubuntu ou Debian (após instalar o nó):** ["Linux: Adicionar interfaces de tronco ou acesso a um nó"](#)

Ver endereços IP

Você pode visualizar o endereço IP de cada nó de grade no seu sistema StorageGRID. Você pode então usar esse endereço IP para efetuar login no nó da grade na linha de comando e executar vários procedimentos de manutenção.

Antes de começar

Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).

Sobre esta tarefa

Para obter informações sobre como alterar endereços IP, consulte ["Configurar endereços IP"](#).

Passos

1. Selecione **NÓS > nó da grade > Visão geral**.
2. Selecione **Mostrar mais** à direita do título Endereços IP.

Os endereços IP para esse nó de grade são 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

Você pode criar interfaces de LAN virtual (VLAN) em nós de administração e nós de gateway e usá-las em grupos de HA e pontos de extremidade do balanceador de carga para isolar e particionar o tráfego para segurança, flexibilidade e desempenho. Os nós selecionados no grupo HA podem usar as interfaces VLAN para compartilhar até 10 endereços IP virtuais, de modo que, se um nó cair, outro nó assume o tráfego de e para os endereços IP virtuais.

Considerações para interfaces VLAN

- Você cria uma interface VLAN inserindo uma ID de VLAN e escolhendo uma interface pai em um ou mais nós.

- Uma interface pai deve ser configurada como uma interface de tronco no switch.
- Uma interface pai pode ser a Rede de Grade (eth0), a Rede do Cliente (eth2) ou uma interface de tronco adicional para a VM ou host bare-metal (por exemplo, ens256).
- Para cada interface VLAN, você pode selecionar apenas uma interface pai para um determinado nó. Por exemplo, você não pode usar a interface de rede de grade e a interface de rede do cliente no mesmo nó de gateway que a interface pai para a mesma VLAN.
- Se a interface VLAN for para tráfego do nó de administração, o que inclui tráfego relacionado ao Grid Manager e ao Tenant Manager, selecione interfaces somente nos nós de administração.
- Se a interface VLAN for para tráfego de cliente S3, selecione interfaces em Nós de administração ou Nós de gateway.
- Se você precisar adicionar interfaces de tronco, veja o seguinte para obter detalhes:
 - **VMware (após instalar o nó):** ["VMware: Adicionar interfaces de tronco ou acesso a um nó"](#)
 - **RHEL (antes de instalar o nó):** ["Criar arquivos de configuração de nó"](#)
 - **Ubuntu ou Debian (antes de instalar o nó):** ["Criar arquivos de configuração de nó"](#)
 - **RHEL, Ubuntu ou Debian (após instalar o nó):** ["Linux: Adicionar interfaces de tronco ou acesso a um nó"](#)

Criar uma interface VLAN

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Permissão de acesso root"](#) .
- Uma interface de tronco foi configurada na rede e anexada à VM ou ao nó Linux. Você sabe o nome da interface do tronco.
- Você sabe o ID da VLAN que está configurando.

Sobre esta tarefa

O administrador da rede pode ter configurado uma ou mais interfaces de tronco e uma ou mais VLANs para segregar o tráfego do cliente ou do 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 do FabricPool e a VLAN 200 para um aplicativo de arquivamento.

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

Acesse o assistente

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Interfaces VLAN**.
2. Selecione **Criar**.

Insira detalhes para as interfaces VLAN

Passos

1. Especifique o ID da VLAN na sua rede. Você pode inserir qualquer valor entre 1 e 4094.

Os IDs de VLAN não precisam ser exclusivos. Por exemplo, você pode usar a ID de VLAN 200 para

tráfego de administrador em um site e a mesma ID de VLAN para tráfego de cliente em outro site. Você pode criar interfaces VLAN separadas com diferentes conjuntos de interfaces pai em cada site. No entanto, duas interfaces 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 será exibida.

2. Opcionalmente, insira uma breve descrição para a interface VLAN.
3. Selecione **Continuar**.

Escolha as interfaces dos pais

A tabela lista as interfaces disponíveis para todos os nós de administração e nós de gateway em cada site da sua grade. As interfaces de rede de administração (eth1) não podem ser usadas como interfaces pai e não são exibidas.

Passos

1. Selecione uma ou mais interfaces pai para anexar esta VLAN.

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

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 **Continuar**.

Confirme as configurações

Passos

1. Revise a configuração e faça as alterações necessárias.
 - Se precisar alterar o ID ou a descrição da VLAN, selecione **Inserir detalhes da VLAN** na parte superior da página.
 - Se precisar alterar uma interface pai, selecione **Escolher interfaces pai** na parte superior da página ou selecione **Anterior**.

- Se você precisar remover uma interface pai, selecione a lixeira  .

2. Selecione **Salvar**.

3. Aguarde até 5 minutos para que a nova interface apareça como uma seleção na página Grupos de alta disponibilidade e seja listada na tabela **Interfaces de rede** do nó (**NÓS > nó da interface pai > Rede**).

Editar uma interface VLAN

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

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

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

Observe o seguinte:

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

Por exemplo, suponha que a VLAN 200 esteja anexada 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 poderá remover a interface pai não utilizada para o nó B, mas não poderá remover a interface pai usada para o nó A.

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Interfaces VLAN**.
2. Marque 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**.

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

4. Opcionalmente, marque ou desmarque as caixas de seleção para adicionar interfaces pai ou remover interfaces não utilizadas. Em seguida, selecione **Continuar**.
5. Revise a configuração e faça 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 deve remover a interface VLAN do grupo HA antes de poder removê-la.

Para evitar interrupções no tráfego de clientes, considere fazer uma das seguintes ações:

- Adicione uma nova interface VLAN ao grupo HA antes de remover esta interface VLAN.
- Crie um novo grupo HA que não use esta interface VLAN.
- Se a interface VLAN que você deseja remover for a interface ativa no momento, 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. Marque a caixa de seleção de cada interface VLAN que você deseja remover. Em seguida, selecione **Ações > Excluir**.
3. Selecione **Sim** para confirmar sua seleção.

Todas as interfaces VLAN selecionadas serão removidas. Um banner verde de sucesso aparece na página de interfaces de VLAN.

Gerenciar políticas de classificação de tráfego

O que são políticas de classificação de tráfego?

As políticas de classificação de tráfego permitem identificar e monitorar diferentes tipos de tráfego de rede. Essas políticas podem ajudar a limitar e monitorar o tráfego para melhorar suas ofertas de qualidade de serviço (QoS).

As políticas de classificação de tráfego são aplicadas aos endpoints no serviço StorageGRID Load Balancer para nós de gateway e nós de administração. Para criar políticas de classificação de tráfego, você já deve ter criado pontos de extremidade do balanceador de carga.

Regras de correspondência

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:

- Baldes
- Sub-rede
- Inquilino
- Pontos de extremidade do balanceador de carga

O StorageGRID monitora o tráfego que corresponde a qualquer regra dentro da política de acordo com os objetivos da regra. Qualquer tráfego que corresponda a qualquer regra de uma política é tratado por essa política. Por outro lado, você pode definir regras para corresponder a todo o tráfego, exceto uma entidade especificada.

Limitação de tráfego

Opcionalmente, você pode adicionar os seguintes tipos de limite a uma política:

- Largura de banda agregada
- Largura de banda por solicitação
- Solicitações simultâneas
- Taxa de solicitação

Os valores limite são aplicados por 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 especificados.



Você pode criar políticas para limitar a largura de banda agregada ou para limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Limites agregados de largura de banda podem impor um impacto menor adicional no desempenho do tráfego não limitado.

Para limites de largura de banda agregados ou por solicitação, as solicitações entram ou saem na taxa que você definir. O StorageGRID só pode impor uma velocidade, portanto, a correspondência de política mais específica, por tipo de correspondente, é a que é imposta. A largura de banda consumida pela solicitação não é contabilizada em outras políticas de correspondência menos específicas que contêm políticas agregadas de limite de largura de banda. 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 excedem 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 esperados.

Use políticas de classificação de tráfego com SLAs

Você pode usar políticas de classificação de tráfego em conjunto com limites de capacidade e proteção de dados para 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 de SLA.

Nível de serviço	Capacidade	Proteção de Dados	Desempenho máximo permitido	Custo
Ouro	1 PB de armazenamento permitido	3 cópias da regra ILM	25 K solicitações/seg Largura de banda de 5 GB/seg (40 Gbps)	\$\$\$ por mês
Prata	250 TB de armazenamento permitido	2 cópias da regra ILM	10 K solicitações/seg Largura de banda de 1,25 GB/seg (10 Gbps)	\$\$ por mês
Bronze	100 TB de armazenamento permitido	2 cópias da regra ILM	5 K solicitações/seg Largura de banda de 1 GB/seg (8 Gbps)	\$ por mês

Criar políticas de classificação de tráfego

Você pode criar políticas de classificação de tráfego se quiser monitorar e, opcionalmente, limitar o tráfego de rede por bucket, regex de bucket, CIDR, ponto de

extremidade do balanceador de carga ou locatário. 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 Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Permissão de acesso root"](#) .
- Você criou todos os pontos de extremidade do balanceador de carga que deseja corresponder.
- Você criou todos os inquilinos que deseja corresponder.

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Classificação de tráfego**.
2. Selecione **Criar**.
3. Insira um nome e uma descrição (opcional) para a política e selecione **Continuar**.

Por exemplo, descreva a que esta política de classificação de tráfego se aplica e o que ela limitará.

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, regex de bucket, CIDR, ponto de extremidade do balanceador de carga e locatário.
Valor da partida	Insira o valor que corresponde ao Tipo selecionado. • Bucket: insira um ou mais nomes de bucket. • Expressão regular de bucket: insira uma ou mais expressões regulares usadas para corresponder a um conjunto de nomes de bucket. A expressão regular não está ancorada. Use a âncora ^ para corresponder ao início do nome do bucket e use a âncora \$ para corresponder ao final do nome. A correspondência de expressões regulares oferece suporte a um subconjunto da sintaxe PCRE (expressão regular compatível com Perl). • CIDR: insira uma ou mais sub-redes IPv4, em notação CIDR, que correspondam à sub-rede desejada. • Ponto de extremidade do balanceador de carga: selecione um nome de 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" . • Locatário: a correspondência de locatários usa 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 locatário.

Campo	Descrição
Correspondência inversa	Se você quiser corresponder todo o tráfego de rede <i>exceto</i> o tráfego consistente com o Tipo e o Valor de correspondência recém-definidos, marque a caixa de seleção Correspondência inversa. Caso contrário, deixe a caixa de seleção desmarcada. Por exemplo, se você quiser que esta política se aplique a todos os endpoints do balanceador de carga, exceto um, especifique o endpoint do balanceador de carga a ser excluído e selecione Correspondência inversa. Para uma política que contém vários correspondentes, onde pelo menos um é um correspondente inverso, tome cuidado para não criar uma política que corresponda a todas as solicitações.

- Opcionalmente, selecione **Adicionar um limite** e selecione os seguintes detalhes para adicionar um ou mais limites para controlar o tráfego de rede correspondido por uma regra.



O StorageGRID coleta métricas mesmo se você não adicionar nenhum limite, para que você possa entender as tendências de tráfego.

Campo	Descrição
Tipo	O tipo de limite que você deseja aplicar ao tráfego de rede correspondido pela regra. Por exemplo, você pode limitar a largura de banda ou a taxa de solicitação. Observação: você pode criar políticas para limitar a largura de banda agregada ou para limitar a largura de banda por solicitação. No entanto, o StorageGRID não pode limitar ambos os tipos de largura de banda ao mesmo tempo. Quando a largura de banda agregada está em uso, a largura de banda por solicitação não está disponível. Por outro lado, quando a largura de banda por solicitação está em uso, a largura de banda agregada não está disponível. Limites agregados de largura de banda podem impor um impacto menor 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 que tenham limites de largura de banda. O StorageGRID implementa as "melhores" correspondências para limites de largura de banda na seguinte ordem: • Endereço IP exato (máscara /32) • Nome exato do bucket • Expressão regular de balde • Inquilino • Ponto final • Correspondências CIDR não exatas (não /32) • Correspondências inversas
Aplica-se a	Se esse limite se aplica a solicitações de leitura do cliente (GET ou HEAD) ou solicitações de gravação (PUT, POST ou DELETE).
Valor	O valor ao qual o tráfego de rede será limitado, com base na Unidade selecionada. Por exemplo, insira 10 e selecione MiB/s para evitar que o tráfego de rede correspondido por esta regra exceda 10 MiB/s. Observação: Dependendo da configuração das unidades, as unidades disponíveis serão binárias (por exemplo, GiB) ou decimais (por exemplo, GB). Para alterar a configuração das unidades, selecione o menu suspenso do usuário no canto superior direito do Grid Manager e selecione Preferências do usuário.
Unidade	A unidade que descreve o valor inserido.

Por exemplo, se você quiser criar um limite de largura de banda de 40 GB/s para uma camada de SLA, crie dois limites de largura de banda agregados: GET/HEAD a 40 GB/s e PUT/POST/DELETE a 40 GB/s.

6. Selecione **Continuar**.

7. Leia e revise a política de classificação de tráfego. Use o botão **Anterior** para voltar e fazer as alterações necessárias. Quando estiver satisfeito com a política, selecione **Salvar e continuar**.

O tráfego do cliente S3 agora é tratado de acordo com a política de classificação de tráfego.

Depois que você terminar

"[Exibir métricas de tráfego de rede](#)" para verificar se as políticas estão aplicando os limites de tráfego esperados.

Editar política de classificação de tráfego

Você pode editar uma política de classificação de tráfego para alterar seu nome ou descrição, ou para criar, editar ou excluir quaisquer regras ou limites para a política.

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você tem o "[Permissão de acesso root](#)".

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Classificação de tráfego**.

A página Políticas de classificação de tráfego é exibida e as políticas existentes são listadas em uma tabela.

2. Edite a política usando o menu Ações ou a página de detalhes. Ver "[criar políticas de classificação de tráfego](#)" para o que inserir.

Menu de ações

- a. Marque 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 política.

3. Para a etapa Inserir nome da política, edite opcionalmente o nome ou a descrição da política e selecione **Continuar**.
4. Para a 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. Para a etapa Definir limites, opcionalmente adicione, edite ou exclua um limite e selecione **Continuar**.
6. Revise a política atualizada e selecione **Salvar e continuar**.

As alterações feitas na política são salvas e o tráfego de rede agora é tratado de acordo com as políticas de classificação de tráfego. Você pode visualizar gráficos de trânsito e verificar se as políticas estão aplicando os limites de tráfego esperados.

Excluir uma política de classificação de tráfego

Você pode excluir uma política de classificação de tráfego se não precisar mais dela. Certifique-se de excluir a política correta porque uma política não pode ser recuperada quando excluída.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Permissão de acesso root"](#) .

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Classificação de tráfego**.

A página Políticas de classificação de tráfego é exibida 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. Marque 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 deseja excluir a política.

A política foi excluída.

Exibir métricas de tráfego de rede

Você pode monitorar o tráfego de rede visualizando os gráficos disponíveis na página Políticas de classificação de tráfego.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Permissão de acesso root ou contas de locatário"](#) .

Sobre esta tarefa

Para qualquer política de classificação de tráfego existente, você pode visualizar métricas do serviço do 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 precisa ajustar a política.

Mesmo que não haja limites definidos para uma política de classificação de tráfego, as métricas são coletadas e os gráficos fornecem informações úteis para entender as tendências de tráfego.

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Classificação de tráfego**.

A página 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 as métricas.

3. Selecione a aba **Métricas**.

Os gráficos da política de classificação de tráfego são exibidos. Os gráficos exibem métricas somente para o tráfego que corresponde à política selecionada.

Os gráficos a seguir estão incluídos na página.

- Taxa de solicitação: este gráfico fornece a quantidade de largura de banda correspondente a esta política manipulada por todos os balanceadores de carga. Os dados recebidos incluem cabeçalhos de solicitação para todas as solicitações e tamanho dos dados do corpo para respostas que têm dados do corpo. Enviado inclui cabeçalhos de resposta para todas as solicitações e tamanho dos dados do corpo da resposta para solicitações que incluem dados do corpo na resposta.



Quando as solicitações são concluídas, este gráfico mostra apenas o uso da largura de banda. Para solicitações de objetos lentos ou grandes, a largura de banda instantânea real pode ser diferente dos valores relatados neste gráfico.

- Taxa de resposta de erro: Este gráfico fornece uma taxa aproximada na qual solicitações que correspondem a esta política estão retornando erros (código de status HTTP ≥ 400) aos clientes.
 - Duração média da solicitação (sem erro): Este gráfico fornece uma duração média de solicitações bem-sucedidas que correspondem a esta política.
 - Uso de largura de banda da política: este gráfico fornece a quantidade de largura de banda correspondente a esta política manipulada por todos os balanceadores de carga. Os dados recebidos incluem cabeçalhos de solicitação para todas as solicitações e tamanho dos dados do corpo para respostas que têm dados do corpo. Enviado inclui cabeçalhos de resposta para todas as solicitações e tamanho dos dados do corpo da resposta para solicitações que incluem dados do corpo na resposta.
4. Posicione o cursor sobre um gráfico de linhas para ver um pop-up de valores em uma parte específica do gráfico.
5. Selecione **Painel do Grafana** logo abaixo do título Métricas para visualizar todos os gráficos de uma política. Além dos quatro gráficos da aba **Métricas**, você pode visualizar mais dois gráficos:
- Taxa de solicitação de gravação por tamanho do objeto: a taxa de solicitações PUT/POST/DELETE que correspondem a esta política. O posicionamento em uma célula individual mostra taxas por segundo. As taxas mostradas na visualização instantânea são truncadas para contagens inteiras e podem reportar 0 quando há solicitações diferentes de zero no bucket.
 - Taxa de solicitação de leitura por tamanho do objeto: a taxa de solicitações GET/HEAD que correspondem a esta política. O posicionamento em uma célula individual mostra taxas por segundo. As taxas mostradas na visualização instantânea são truncadas para contagens inteiras e podem reportar 0 quando há solicitações 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 um 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 seu ID. Os IDs de política são listados na página Políticas de classificação de tráfego.

7. Analise os gráficos para determinar com que frequência a política está limitando o tráfego e se você precisa ajustá-la.

Cifras suportadas para conexões TLS de saída

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

Versões suportadas do TLS

O StorageGRID oferece suporte a TLS 1.2 e TLS 1.3 para conexões com sistemas externos usados para federação de identidades e pools de armazenamento em nuvem.

As cifras TLS suportadas para uso com sistemas externos foram selecionadas para garantir compatibilidade com uma variedade de sistemas externos. A lista é maior que a lista de cifras suportadas para uso com aplicativos cliente S3. Para configurar cifras, vá para **CONFIGURAÇÃO > Segurança > Configurações de segurança** e selecione **Políticas TLS e SSH**.



Opções de configuração de 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 NetApp se tiver solicitações específicas sobre essas configurações.

Benefícios de conexões HTTP ativas, ociosas e simultâneas

A maneira 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 inativas abertas

Você deve manter as conexões HTTP abertas mesmo quando os aplicativos clientes estiverem ociosos para permitir que os aplicativos clientes realizem transações subsequentes na conexão aberta. Com base nas medições do sistema e na experiência de integração, você deve manter uma conexão HTTP inativa aberta por no máximo 10 minutos. O StorageGRID pode fechar automaticamente uma conexão HTTP que seja mantida 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 executar uma transação HTTP até o momento em que o sistema StorageGRID pode executar a transação

A latência reduzida é a principal vantagem, especialmente pelo 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 várias classes de condições de falha que interrompem a conectividade entre o aplicativo cliente e o sistema StorageGRID

Determinar por quanto tempo manter uma conexão ociosa aberta é uma compensação entre os benefícios do início lento associado à conexão existente e a alocação ideal da conexão aos recursos internos do sistema.

Benefícios das conexões HTTP ativas

Para conexões diretas com nós de armazenamento, 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 que uma conexão deve ser mantida aberta é uma compensação entre os benefícios da persistência da conexão e a alocação ideal da conexão aos recursos internos do sistema.

Para conexões de clientes com nós de armazenamento, limitar 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 não ser mais ideal, pois os requisitos de balanceamento de carga mudam. O sistema executa seu melhor balanceamento de carga quando os aplicativos clientes estabelecem uma conexão HTTP separada para cada transação, mas isso anula os ganhos muito mais valiosos associados às conexões persistentes.

- Permite que aplicativos clientes direcionem transações HTTP para serviços LDR que tenham espaço disponível.
- Permite iniciar procedimentos de manutenção.

Alguns procedimentos de manutenção começam somente depois que todas as conexões HTTP em andamento são concluídas.

Para conexões de clientes com o serviço Load Balancer, limitar a duração das conexões abertas pode ser útil para permitir que alguns procedimentos de manutenção sejam iniciados imediatamente. Se a duração das conexões do cliente não for limitada, poderá 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 uma variedade de fatores.

Conexões HTTP simultâneas fornecem os seguintes benefícios:

- Latência reduzida

As transações podem começar imediatamente em vez de esperar que outras transações sejam concluídas.

- Aumento da produtividade

O sistema StorageGRID pode executar transações paralelas e aumentar o rendimento agregado de transações.

Os aplicativos clientes devem estabelecer várias conexões HTTP. Quando um aplicativo cliente precisa executar 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 tem um pico de rendimento diferente para transações e conexões simultâneas antes que o desempenho comece a cair. O pico de rendimento depende de fatores como recursos de computação, recursos de rede, recursos de armazenamento e links WAN. O número de servidores e serviços e o número de aplicativos que o sistema StorageGRID suporta também são fatores.

Os sistemas StorageGRID geralmente oferecem suporte a vários aplicativos clientes. Você deve ter isso em mente ao determinar o número máximo de conexões simultâneas usadas por um aplicativo cliente. Se o aplicativo cliente consistir em várias entidades de software, cada uma estabelecendo conexões com o sistema StorageGRID, você deverá somar todas as conexões entre as entidades. Pode ser necessário ajustar o número máximo de conexões simultâneas nas seguintes situações:

- A topologia do sistema StorageGRID afeta o número máximo de transações e conexões simultâneas que o sistema pode suportar.
- Os aplicativos clientes que interagem com o sistema StorageGRID por meio de uma rede com largura de banda limitada podem ter que reduzir o grau de simultaneidade 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 simultaneidade para evitar exceder os limites do sistema.

Separação de pools de conexão HTTP para operações de leitura e gravação

Você pode usar pools separados de conexões HTTP para operações de leitura e gravação e controlar a quantidade de um pool a ser usada para cada uma. Pools separados de conexões HTTP permitem que você controle melhor as transações e equilibre as cargas.

Os aplicativos cliente podem criar cargas que são dominantes em recuperação (leitura) ou dominantes em armazenamento (gravação). Com pools separados de conexões HTTP para transações de leitura e gravação, você pode ajustar quanto de cada pool será dedicado para transações de leitura ou gravação.

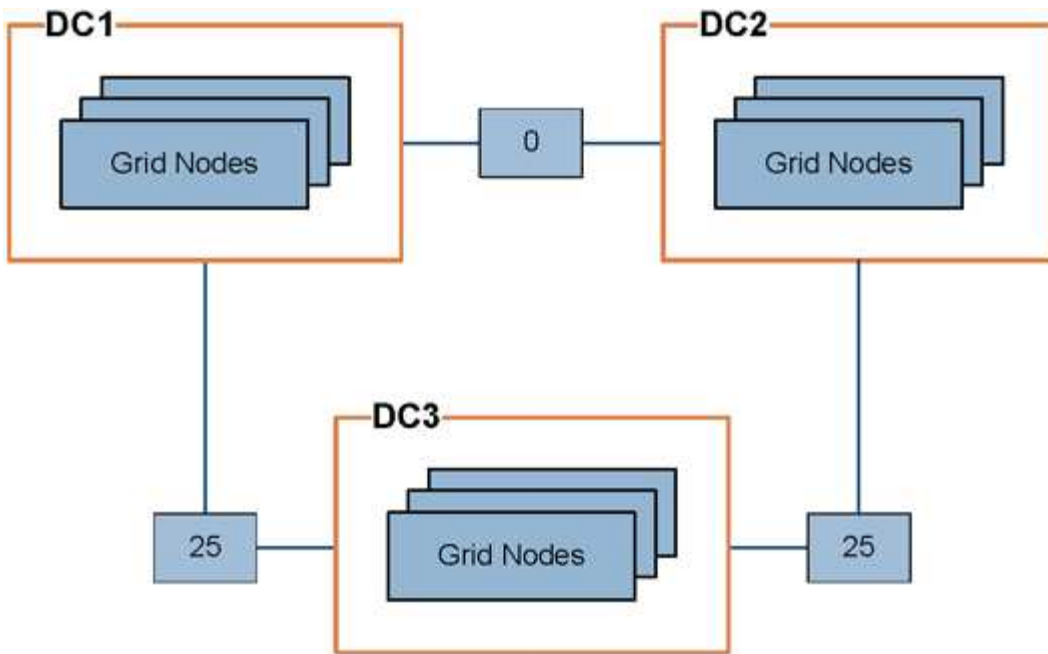
Gerenciar custos de link

Os custos de link 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 dos links para refletir a latência entre os sites.

O que são custos de link?

- Os custos de link são usados para priorizar qual cópia de objeto é usada para atender às recuperações de objetos.
- Os custos de link são usados pela API de gerenciamento de grade e pela API de gerenciamento de locatários para determinar quais serviços internos do StorageGRID usar.
- Os custos de link são usados pelo serviço Load Balancer em nós de administração e nós de gateway para direcionar conexões de clientes. Ver "[Considerações para balanceamento de carga](#)".

O diagrama mostra uma grade de três sites que tem custos de link configurados entre sites:



- O serviço Load Balancer nos nós de administração e nos nós de gateway distribui igualmente as conexões do cliente para todos os nós de armazenamento no mesmo site do data center e para quaisquer sites do data center com um custo de link de 0.

No exemplo, um nó de gateway no site do data center 1 (DC1) distribui igualmente conexões de clientes para nós de armazenamento no DC1 e para nós de armazenamento no DC2. Um nó de gateway no DC3 envia conexões de cliente somente para nós de armazenamento no DC3.

- Ao recuperar um objeto que existe como várias cópias replicadas, o StorageGRID recupera a cópia no data center que tem o menor custo de link.

No exemplo, se um aplicativo cliente no DC2 recupera um objeto armazenado tanto no DC1 quanto no DC3, o objeto é 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 link são números relativos arbitrários, sem unidade de medida específica. Por exemplo, um custo de link de 50 é usado com menos preferência do que um custo de link de 25. A tabela mostra os custos de link comumente usados.

Link	Custo do link	Notas
Entre locais de data center físico	25 (padrão)	Data centers conectados por um link WAN.
Entre sites de data center lógicos no mesmo local físico	0	Data centers lógicos no mesmo prédio físico ou campus conectados por uma LAN.

Atualizar custos de link

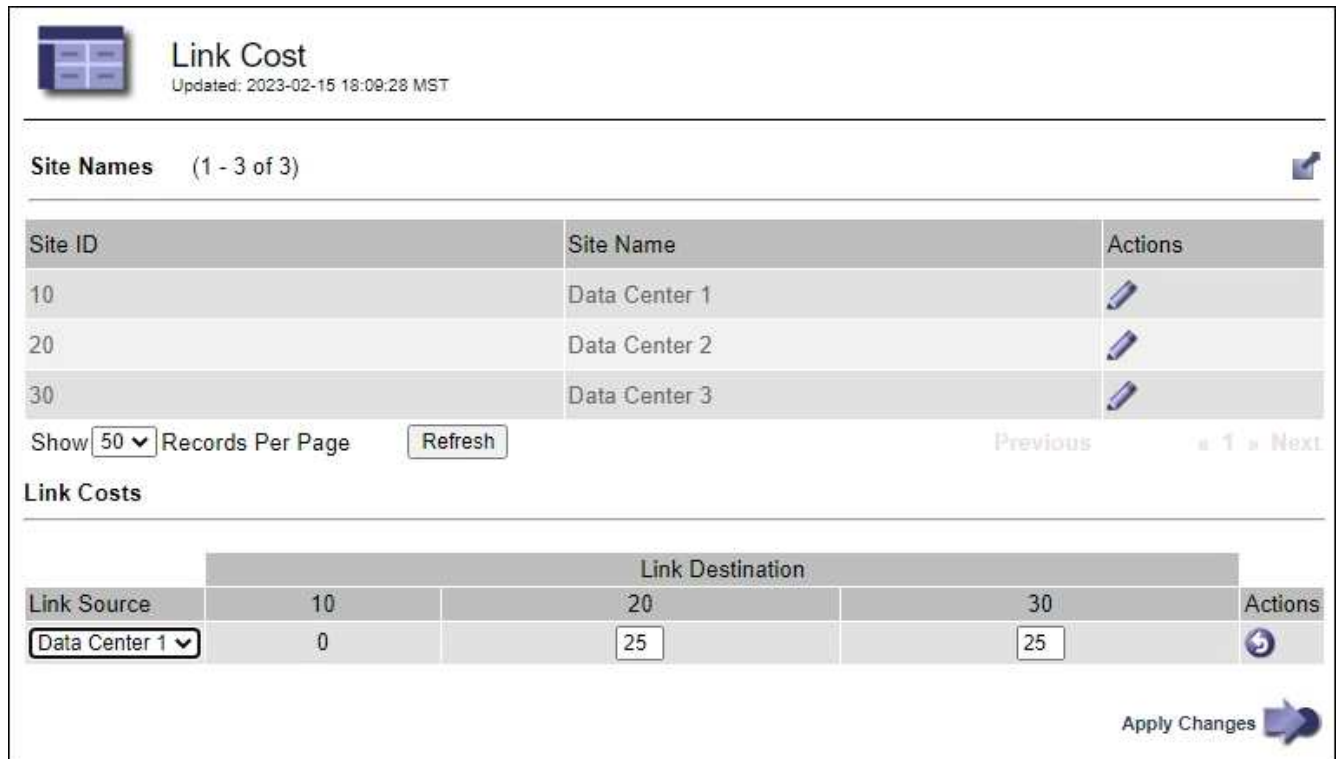
Você pode atualizar os custos de link entre sites de data center para refletir a latência entre sites.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Permissão de configuração da página de topologia de grade"](#) .

Passos

1. Selecione **SUPORTE > Outro > Custo do link**.



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**.

Você não pode alterar o custo do link se a origem for a mesma que o destino.

Para cancelar as alterações, selecione **Reverter**.

3. Selecione **Aplicar alterações**.

Usar AutoSupport

O que é AutoSupport?

O recurso AutoSupport permite que o StorageGRID envie pacotes de integridade e status ao suporte técnico da NetApp .

Usar o AutoSupport pode acelerar significativamente a determinação e a resolução de problemas. O suporte técnico também pode monitorar as necessidades de armazenamento do seu sistema e ajudar você a determinar se precisa adicionar novos nós ou sites. Opcionalmente, você pode configurar os pacotes do AutoSupport para serem enviados para um destino adicional.

O StorageGRID tem dois tipos de AutoSupport:

- * StorageGRID AutoSupport* relata problemas de software StorageGRID . Ativado por padrão quando você instala o StorageGRID pela primeira vez. Você pode ["alterar a configuração padrão do AutoSupport"](#) se necessário.



Se o StorageGRID AutoSupport não estiver habilitado, uma mensagem será exibida no painel do Grid Manager. 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 navegador seja limpo, mesmo que o AutoSupport permaneça desativado.

- * O AutoSupport de hardware do dispositivo* relata problemas no dispositivo StorageGRID . Você deve ["configurar o AutoSupport de hardware em cada dispositivo"](#) .

O que é Active IQ?

O Active IQ é um consultor digital baseado em nuvem que aproveita a análise preditiva e a sabedoria da comunidade da base instalada da NetApp. Suas avaliações contínuas de risco, alertas preditivos, orientação prescritiva e ações automatizadas ajudam a prevenir problemas antes que eles ocorram, resultando em melhor integridade do sistema e maior disponibilidade do sistema.

Se quiser usar os painéis e a funcionalidade do Active IQ no site de suporte da NetApp , você deve habilitar o AutoSupport.

["Documentação do Digital Advisor Active IQ"](#)

Informações incluídas no pacote AutoSupport

Um pacote AutoSupport contém os seguintes arquivos e detalhes.

Nome do arquivo	Campos	Descrição
AUTOSUPPORT-HISTORY.XML	Número de sequência do AutoSupport + Destino para este AutoSupport + Status da entrega + Tentativas de entrega + Assunto do AutoSupport + URI de entrega + Último erro + Nome do arquivo PUT do AutoSupport + Hora da geração + Tamanho compactado do AutoSupport + Tamanho descompactado do AutoSupport + Tempo total de coleta (ms)	Arquivo de histórico do AutoSupport .
AUTOSUPPORT.XML	Nó + Protocolo para contato com o suporte + URL de suporte para HTTP/HTTPS + Endereço de suporte + Estado do AutoSupport OnDemand + URL do servidor do AutoSupport OnDemand + Intervalo de pesquisa do AutoSupport OnDemand	Arquivo de status do AutoSupport . Fornece detalhes do protocolo usado, URL e endereço de suporte técnico, intervalo de pesquisa e OnDemand AutoSupport , se ativado ou desativado.

Nome do arquivo	Campos	Descrição
BUCKETS.XML	ID do bucket + ID da conta + Versão da compilação + Configuração de restrição de local + Conformidade habilitada + Configuração de conformidade + Bloqueio de objeto S3 habilitado + Configuração de bloqueio de objeto S3 + Configuração de consistência + CORS habilitado + Configuração do CORS + Hora do último acesso habilitada + Política habilitada + Configuração da política + Notificações habilitadas + Configuração de notificações + Cloud Mirror habilitado + Configuração do Cloud Mirror + Pesquisa habilitada + Configuração de pesquisa + Marcação de bucket habilitada + Configuração de marcação de bucket + Configuração de controle de versão	Fornece detalhes de configuração e estatísticas no nível do bucket. Exemplos de configurações de bucket incluem serviços de plataforma, conformidade e consistência de bucket.
CONFIGURAÇÕES DE GRADE.XML	ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Arquivo de informações de configuração de toda a rede. Contém informações sobre certificados de grade, espaço reservado de metadados, definições de configuração de toda a grade (conformidade, bloqueio de objeto S3, compactação de objeto, alertas, syslog e configuração de ILM), detalhes do perfil de codificação de eliminação, nome DNS e " Nome da NMS ".
ESPECIFICAÇÃO DE GRADE.XML	Especificações de grade, XML bruto	Usado para configurar e implantar o StorageGRID. Contém especificações de grade, IP do servidor NTP, 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 de tarefas de grade (procedimentos de manutenção). Fornece detalhes das tarefas ativas, encerradas, concluídas, com falha e pendentes da grade.

Nome do arquivo	Campos	Descrição
GRADE.JSON	Grade + Revisão + Versão do Software + Descrição + Licença + Senhas + DNS + NTP + Sites + Nós	Informações da grade.
ILM-CONFIGURAÇÃO.XML	ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Lista de atributos para configurações de 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 taxas de avaliação de ILM para cada nó e métricas de toda a grade.
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 armazenamento, comportamento de ingestão, filtros, regras e descrição.
LOG.TGZ	<i>n / D</i>	Arquivo de log para download. Contém <code>broadcast-err.log</code> e <code>servermanager.log</code> de cada nó.
MANIFESTO.XML	Ordem de coleta + Nome do arquivo de conteúdo do AutoSupport para esses dados + Descrição deste item de dados + Número de bytes coletados + Tempo gasto na coleta + Status deste item de dados + Descrição do erro + Tipo de conteúdo do AutoSupport para esses dados +	Contém metadados do AutoSupport e breves descrições de todos os arquivos do AutoSupport .
NMS-ENTIDADES.XML	Índice de atributo + OID da entidade + ID do nó + ID do modelo do dispositivo + Versão do modelo do dispositivo + Nome da entidade	Entidades de grupo e de serviço no " Árvore NMS ". Fornece detalhes da topologia da grade. O nó pode ser determinado com base nos serviços em execução no nó.

Nome do arquivo	Campos	Descrição
OBJETOS-STATUS.XML	Nó + Caminho do serviço + ID do atributo + Nome do atributo + Valor + Índice + ID da tabela + Nome da tabela	Status do objeto, incluindo status de verificação em segundo plano, transferência ativa, taxa de transferência, transferências totais, taxa de exclusão, fragmentos corrompidos, objetos perdidos, objetos ausentes, tentativa de reparo, taxa de verificação, período estimado de verificação e status de conclusão do reparo.
STATUS-DO-SERVIDOR.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 armazenamento, número de série do chassi do dispositivo de armazenamento, contagem de unidades com falha do controlador de armazenamento, 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.
STATUS-DO-SERVIÇO.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 do Reaper do banco de dados, duração do reparo do segmento, duração do trabalho de reparo, reinicializações automáticas do trabalho e encerramento automático do trabalho.
ARMAZENAMENTO-GRADES.XML	ID do nível de armazenamento + Nome do nível de armazenamento + ID do nó de armazenamento + Caminho do nó de armazenamento	Arquivo de definições de nível de armazenamento para cada nó de armazenamento.
RESUMO-ATRIBUTOS.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 do sistema de alto nível que resumem as informações de uso do StorageGRID . Fornece detalhes como nome da grade, nomes dos sites, número de nós de armazenamento por grade e por site, tipo de licença, capacidade e uso da licença, termos de suporte de software e detalhes das operações do S3.

Nome do arquivo	Campos	Descrição
ALERTAS-DO-SISTEMA.XML	Nome + Gravidade + Nome do nó + Status do alerta + Nome do site + Hora de acionamento 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 .
AGENTES DO USUÁRIO.XML	Agente do usuário + Número de dias + Total de solicitações HTTP + Total de bytes ingeridos + Total de bytes recuperados + Solicitações PUT + Solicitações GET + Solicitações DELETE + Solicitações HEAD + Solicitações POST + Solicitações OPTIONS + Tempo médio de solicitação (ms) + Tempo médio de solicitação PUT (ms) + Tempo médio de solicitação GET (ms) + Tempo médio de solicitação DELETE (ms) + Tempo médio de solicitação HEAD (ms) + Tempo médio de solicitação POST (ms) + Tempo médio de solicitação OPTIONS (ms)	Estatísticas baseadas nos agentes de usuários do aplicativo. Por exemplo, o número de operações PUT/GET/DELETE/HEAD por agente de usuário e o tamanho total de 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 +	Dados do cabeçalho do AutoSupport .

Configurar AutoSupport

Por padrão, o recurso StorageGRID AutoSupport é habilitado quando você instala o StorageGRID pela primeira vez. No entanto, você deve configurar o AutoSupport de hardware em cada dispositivo. Conforme necessário, você pode alterar a configuração do AutoSupport .

Se você quiser alterar a configuração do StorageGRID AutoSupport, faça suas alterações somente no nó de administração principal. Você deve [configurar hardware AutoSupport](#) em cada aparelho.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Permissão de acesso root"](#) .
- Se você usar HTTPS para enviar pacotes de AutoSupport , você forneceu acesso de saída à Internet para o nó de administração principal, diretamente ou ["usando um servidor proxy"](#) (conexões de entrada não são necessárias).
- Se HTTP for selecionado na página StorageGRID AutoSupport , você terá ["configurou um servidor proxy"](#) para encaminhar pacotes do AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitarão pacotes enviados via HTTP.
- Se você usar SMTP como protocolo para pacotes AutoSupport , você terá configurado um servidor de e-mail SMTP.

Sobre esta tarefa

Você pode usar qualquer combinação das seguintes opções para enviar pacotes do AutoSupport ao suporte técnico:

- **Semanal:** Envie automaticamente pacotes de AutoSupport uma vez por semana. Configuração padrão: Ativado.
- **Acionado por evento:** envie automaticamente pacotes de AutoSupport a cada hora ou quando ocorrerem eventos significativos do sistema. Configuração padrão: Ativado.
- **Sob demanda:** permita 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 protocolo de transmissão HTTPS AutoSupport). Configuração padrão: Desativado.
- **Acionado pelo usuário:** envie manualmente pacotes do AutoSupport a qualquer momento.

Especifique o protocolo para pacotes AutoSupport

Você pode usar qualquer um dos seguintes protocolos para enviar pacotes do AutoSupport :

- **HTTPS:** Esta é a configuração padrão e recomendada para novas instalações. Este protocolo usa a porta 443. Se você quiser [habilitar o recurso AutoSupport on Demand](#) , você deve usar HTTPS.
- **HTTP:** Se você selecionar HTTP, deverá configurar um servidor proxy para encaminhar pacotes do AutoSupport como HTTPS. Os servidores AutoSupport da NetApp rejeitam pacotes enviados via HTTP. Este protocolo usa a porta 80.
- **SMTP:** Use esta opção se quiser que os pacotes do AutoSupport sejam enviados por e-mail.

O protocolo definido é usado para enviar todos os tipos de pacotes do AutoSupport .

Passos

1. Selecione **SUPORTE > Ferramentas > * AutoSupport* > Configurações**.
2. Selecione o protocolo que você deseja usar para enviar pacotes do AutoSupport .
3. Se você selecionou **HTTPS**, selecione 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 do AutoSupport seja segura. O certificado de suporte da 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 por eventos são enviados usando o protocolo selecionado.

Desativar o AutoSupport semanal

Por padrão, o sistema StorageGRID é configurado para enviar um pacote AutoSupport ao suporte técnico uma vez por semana.

Para determinar quando o pacote semanal de AutoSupport será enviado, vá para a aba * AutoSupport* > **Resultados**. Na seção * AutoSupport semanal*, observe 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 AutoSupport semanal**.
3. Selecione **Salvar**.

Desabilitar AutoSupport acionado por evento

Por padrão, o sistema StorageGRID é configurado para enviar um pacote AutoSupport ao suporte técnico a cada hora.

Você pode desabilitar o AutoSupport acionado por evento a qualquer momento.

Passos

1. Selecione **SUPORTE > Ferramentas > * AutoSupport* > Configurações**.
2. Desmarque a caixa de seleção **Habilitar AutoSupport Acionado por Evento**.
3. Selecione **Salvar**.

Habilitar AutoSupport sob Demanda

O AutoSupport on Demand pode ajudar a resolver problemas nos quais o suporte técnico está trabalhando ativamente.

Por padrão, o AutoSupport on Demand está desativado. Habilitar esse recurso permite que o suporte técnico solicite que seu sistema StorageGRID envie pacotes do AutoSupport automaticamente. O suporte técnico também pode definir o intervalo de tempo de pesquisa para consultas do AutoSupport on Demand.

O suporte técnico não pode ativar ou desativar o AutoSupport on Demand.

Passos

1. Selecione **SUPORTE > Ferramentas > * AutoSupport* > Configurações**.
2. Selecione **HTTPS** para o protocolo.
3. Marque a caixa de seleção **Ativar AutoSupport semanal**.
4. Marque a caixa de seleção **Ativar AutoSupport sob demanda**.
5. Selecione **Salvar**.

O AutoSupport on Demand está habilitado e o suporte técnico pode enviar solicitações do AutoSupport on Demand para o StorageGRID.

Desativar verificações de atualizações de software

Por padrão, o StorageGRID entra em contato com a NetApp para determinar se há atualizações de software disponíveis para o seu sistema. Se um hotfix ou uma nova versão do StorageGRID estiver disponível, a nova versão será exibida na página de atualização do StorageGRID .

Conforme necessário, você pode opcionalmente desabilitar a verificação de atualizações de software. Por exemplo, se o seu sistema não tiver acesso WAN, você deve desabilitar 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 de AutoSupport

Quando você habilita o AutoSupport, os pacotes de saúde e status são enviados ao 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](#) .



Você não pode usar o protocolo SMTP para enviar pacotes do AutoSupport para um destino adicional.

Passos

1. Selecione **SUPORTE > Ferramentas > * AutoSupport* > Configurações**.
2. Selecione **Ativar destino de AutoSupport adicional**.
3. Especifique o seguinte:

Nome do host

O nome do host do servidor 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

Se um certificado TLS é usado para proteger a conexão com o destino adicional.

- Selecione **Verificar certificado** para usar a validação do certificado.
- Selecione **Não verificar certificado** para enviar seus pacotes do AutoSupport 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 o local do certificado da CA.
- b. Carregue o arquivo do certificado da CA.

Os metadados do certificado da CA são exibidos.

5. Selecione **Salvar**.

Todos os pacotes futuros do AutoSupport semanais, acionados por eventos e acionados pelo usuário serão enviados para o destino adicional.

Configurar AutoSupport para aparelhos

O AutoSupport para dispositivos relata problemas de hardware do StorageGRID , e o StorageGRID AutoSupport relata problemas de software do StorageGRID , com uma exceção: para o SGF6112, o StorageGRID AutoSupport relata problemas de hardware e software. Você deve configurar o AutoSupport em cada dispositivo, exceto o SGF6112, que não requer configuração adicional. O AutoSupport é implementado de forma diferente para dispositivos de serviços e dispositivos de armazenamento.

Use o SANtricity para habilitar o AutoSupport para cada dispositivo de armazenamento. Você pode configurar o SANtricity AutoSupport durante a configuração inicial do dispositivo ou após a instalação do dispositivo:

- Para aparelhos SG6000 e SG5700, "[configurar AutoSupport no SANtricity System Manager](#)"

Os pacotes AutoSupport dos dispositivos E-Series podem ser incluídos no StorageGRID AutoSupport se você configurar a entrega do AutoSupport por proxy em "[Gerente do Sistema SANtricity](#)".

O StorageGRID AutoSupport não relata problemas de hardware, como falhas no DIMM ou na placa de interface do host (HIC). No entanto, algumas falhas de componentes podem desencadear "[alertas de hardware](#)". Para dispositivos StorageGRID com um controlador de gerenciamento de placa base (BMC), você pode configurar interceptações de e-mail e SNMP para relatar falhas de hardware:

- "[Configurar notificações por e-mail para alertas do BMC](#)"
- "[Configurar definições SNMP para BMC](#)"

Informações relacionadas

["Suporte NetApp"](#)

Acionar manualmente um pacote AutoSupport

Para auxiliar o suporte técnico na solução de problemas com seu sistema StorageGRID , você pode acionar manualmente o envio de um pacote AutoSupport .

Antes de começar

- Você deve estar conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você deve ter acesso Root ou permissão para Outra configuração de grade.

Passos

1. Selecione **SUPORTE > Ferramentas > * AutoSupport***.
2. Na guia **Ações**, selecione **Enviar AutoSupport acionado pelo usuário**.

O StorageGRID tenta enviar um pacote de AutoSupport para o site de suporte da NetApp . Se a tentativa for bem-sucedida, os valores **Resultado mais recente** e **Última hora bem-sucedida** na guia **Resultados** serão atualizados. Se houver um problema, o valor **Resultado mais recente** será atualizado para "Falha" e o StorageGRID não tentará enviar o pacote AutoSupport novamente.



Após enviar um pacote de AutoSupport acionado pelo usuário, atualize a página de AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

Solucionar problemas de pacotes AutoSupport

Se uma tentativa de enviar um pacote AutoSupport falhar, o sistema StorageGRID tomará ações diferentes dependendo do tipo de pacote AutoSupport . Você pode verificar o status dos pacotes do AutoSupport selecionando **SUPPORT > Tools > * AutoSupport* > Results**.

Quando o pacote AutoSupport falha ao enviar, "Falha" aparece na guia **Resultados** da página * AutoSupport*.



Se você configurou um servidor proxy para encaminhar pacotes do AutoSupport para o NetApp, você deve ["verifique se as configurações do servidor proxy estão corretas"](#) .

Falha no pacote AutoSupport semanal

Se um pacote semanal do AutoSupport não for enviado, o sistema StorageGRID tomará as seguintes ações:

1. Atualiza o atributo Resultado Mais Recente para Tentando Novamente.
2. Tenta reenviar o pacote AutoSupport 15 vezes a cada quatro minutos durante uma hora.
3. Após uma hora de falhas de envio, atualiza o atributo Resultado Mais Recente para Falha.
4. Tenta enviar um pacote AutoSupport novamente no próximo horário agendado.
5. Mantém o cronograma regular do AutoSupport se o pacote falhar porque o serviço NMS não está disponível e se um pacote for enviado antes de sete dias.
6. Quando o serviço NMS estiver disponível novamente, envie um pacote AutoSupport imediatamente se um pacote não tiver sido enviado por sete dias ou mais.

Falha do pacote AutoSupport acionada pelo usuário ou por evento

Se um pacote AutoSupport acionado pelo usuário ou por evento não for enviado, o sistema StorageGRID executará as seguintes ações:

1. Exibe uma mensagem de erro se o erro for conhecido. Por exemplo, se um usuário selecionar o protocolo SMTP sem fornecer as configurações 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 tente enviar o pacote novamente.
3. Registra o erro em `nms.log` .

Se ocorrer uma falha e o SMTP for o protocolo selecionado, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se o seu servidor de e-mail está em execução (**SUPORTE > Alarmes (antigos) > 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 SMTP for o protocolo selecionado, verifique se o servidor de e-mail do sistema StorageGRID está configurado corretamente e se 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.

Enviar pacotes E-Series AutoSupport por meio do StorageGRID

Você pode enviar pacotes do E-Series SANtricity System Manager AutoSupport para o suporte técnico por meio de um nó de administração do StorageGRID em vez da porta de gerenciamento do dispositivo de armazenamento.

Ver ["AutoSupport de hardware da série E"](#) para obter mais informações sobre como usar o AutoSupport com dispositivos da Série E.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Permissão de acesso root ou de administrador do dispositivo de armazenamento"](#) .
- Você configurou o SANtricity AutoSupport:
 - Para aparelhos SG6000 e SG5700, ["configurar AutoSupport no SANtricity System Manager"](#)



Você deve ter o firmware SANtricity 8.70 ou superior para acessar o SANtricity System Manager usando o Grid Manager.

Sobre esta tarefa

Os pacotes AutoSupport da Série E contêm detalhes do hardware de armazenamento 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 do AutoSupport por meio de um nó de administração do StorageGRID sem usar a porta de gerenciamento do dispositivo. Os pacotes AutoSupport transmitidos desta forma são enviados pelo ["nó de administração do remetente preferencial"](#) , e eles usam qualquer ["configurações de proxy do administrador"](#) que foram configurados no Grid Manager.

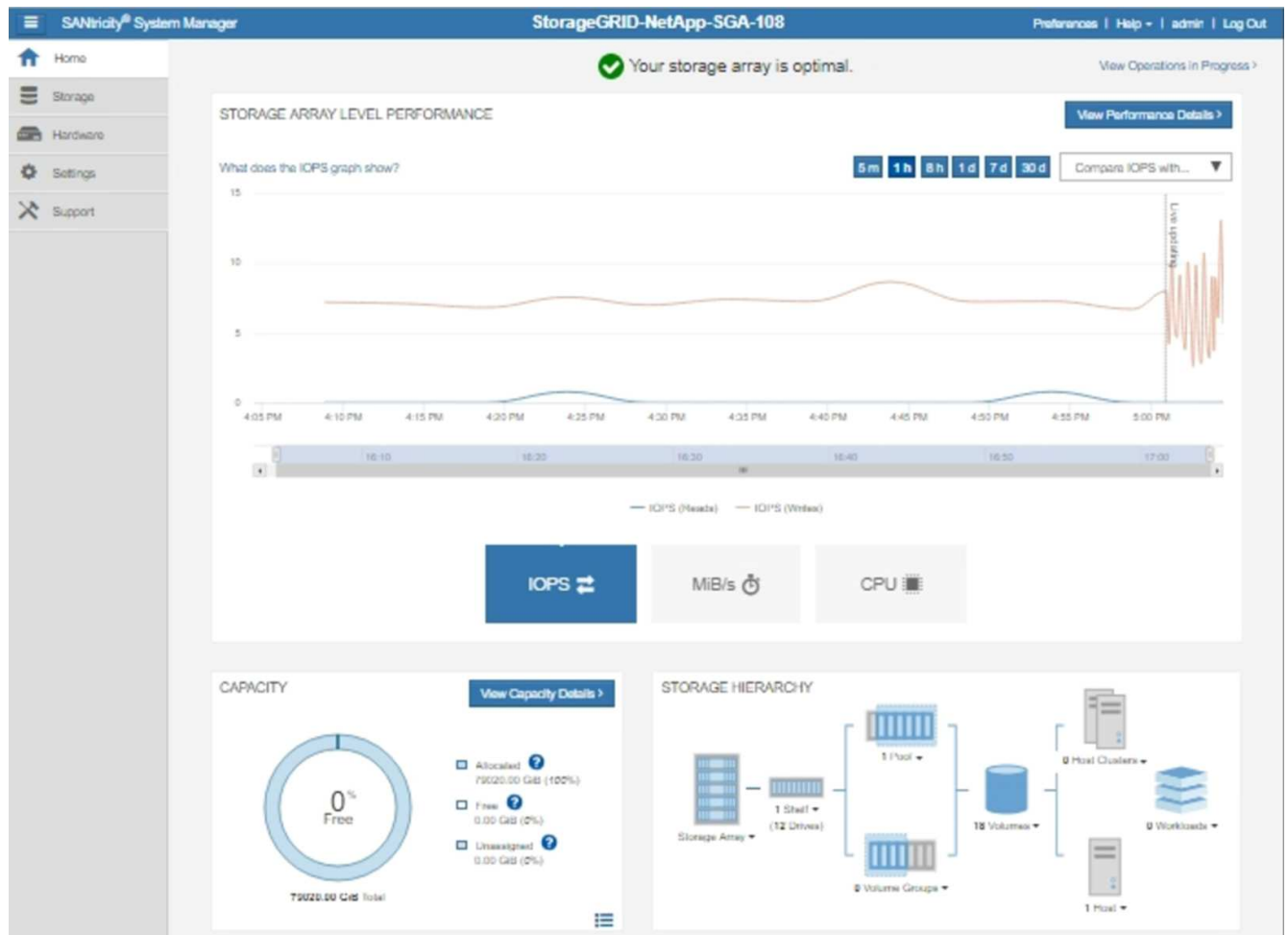


Este procedimento serve apenas para configurar um servidor proxy StorageGRID para pacotes E-Series AutoSupport . Para obter detalhes adicionais sobre a configuração do E-Series AutoSupport , consulte o ["Documentação do NetApp E-Series e SANtricity"](#) .

Passos

1. No Grid Manager, selecione **NODES**.
2. Na lista de nós à esquerda, selecione o nó do dispositivo de armazenamento que você deseja configurar.
3. Selecione * SANtricity System Manager*.

A página inicial do SANtricity System Manager é exibida.



4. Seleccione **SUPORTE** > **Centro 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 método de entrega do AutoSupport*.

A página Configurar método de entrega do AutoSupport é exibida.

Configure AutoSupport Delivery Method [X]

Select AutoSupport dispatch delivery method...

☒ **HTTPS**

☐ HTTP

☐ Email

HTTPS delivery settings [Show destination address](#)

Connect to support team...

☐ Directly ?

☒ **via Proxy server** ?

Host address ?

tunnel-host

Port number ?

10225

☐ My proxy server requires authentication

☐ via Proxy auto-configuration script (PAC) ?

Save **Test Configuration** Cancel

6. Selecione **HTTPS** como método de entrega.



O certificado que habilita HTTPS está pré-instalado.

7. Selecione **via servidor proxy**.

8. Digitar `tunnel-host` para o **Endereço do host**.

`tunnel-host` é o endereço especial para usar um nó de administração para enviar pacotes do E-Series AutoSupport .

9. Digitar `10225` para o **Número da porta**.

`10225` é o número da porta no servidor proxy 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 correto, uma mensagem em um banner verde aparecerá: "Sua configuração do AutoSupport foi

verificada".

Se o teste falhar, uma mensagem de erro aparecerá em um banner vermelho. Verifique as configurações de DNS e rede do StorageGRID , certifique-se de que "[nó de administração do remetente preferencial](#)" você pode se conectar ao site de suporte da NetApp e tentar o teste novamente.

11. Selecione **Salvar**.

A configuração é salva e uma mensagem de confirmação é exibida: "O método de entrega do AutoSupport foi configurado."

Gerenciar nós de armazenamento

Gerenciar nós de armazenamento

Os nós de armazenamento fornecem capacidade e serviços de armazenamento em disco. O gerenciamento de nós de armazenamento envolve o seguinte:

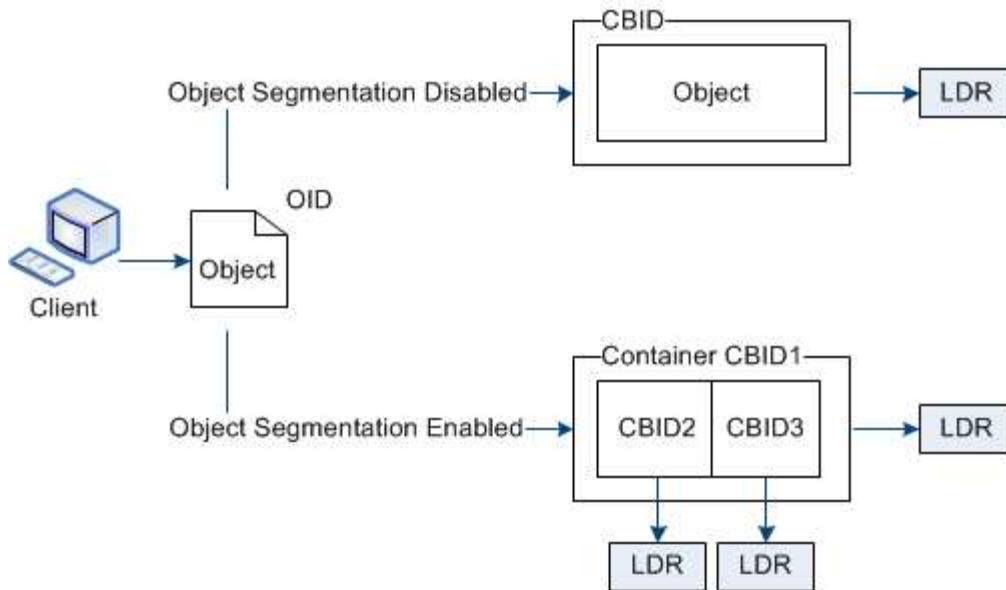
- Gerenciando opções de armazenamento
- Entendendo o que são marcas d'água de volume de armazenamento e como você pode usar substituições de marca d'água para controlar quando os nós de armazenamento se tornam somente leitura
- Monitoramento e gerenciamento do espaço usado para metadados de objetos
- Configurando configurações globais para objetos armazenados
- Aplicando as configurações do nó de armazenamento
- Gerenciando nós de armazenamento completos

Usar opções de armazenamento

O que é segmentação de objetos?

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 multipart do S3 também cria objetos segmentados, com um objeto representando cada parte.

Quando um objeto é ingerido no sistema StorageGRID , o serviço LDR divide o objeto em segmentos e cria um contêiner de 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.

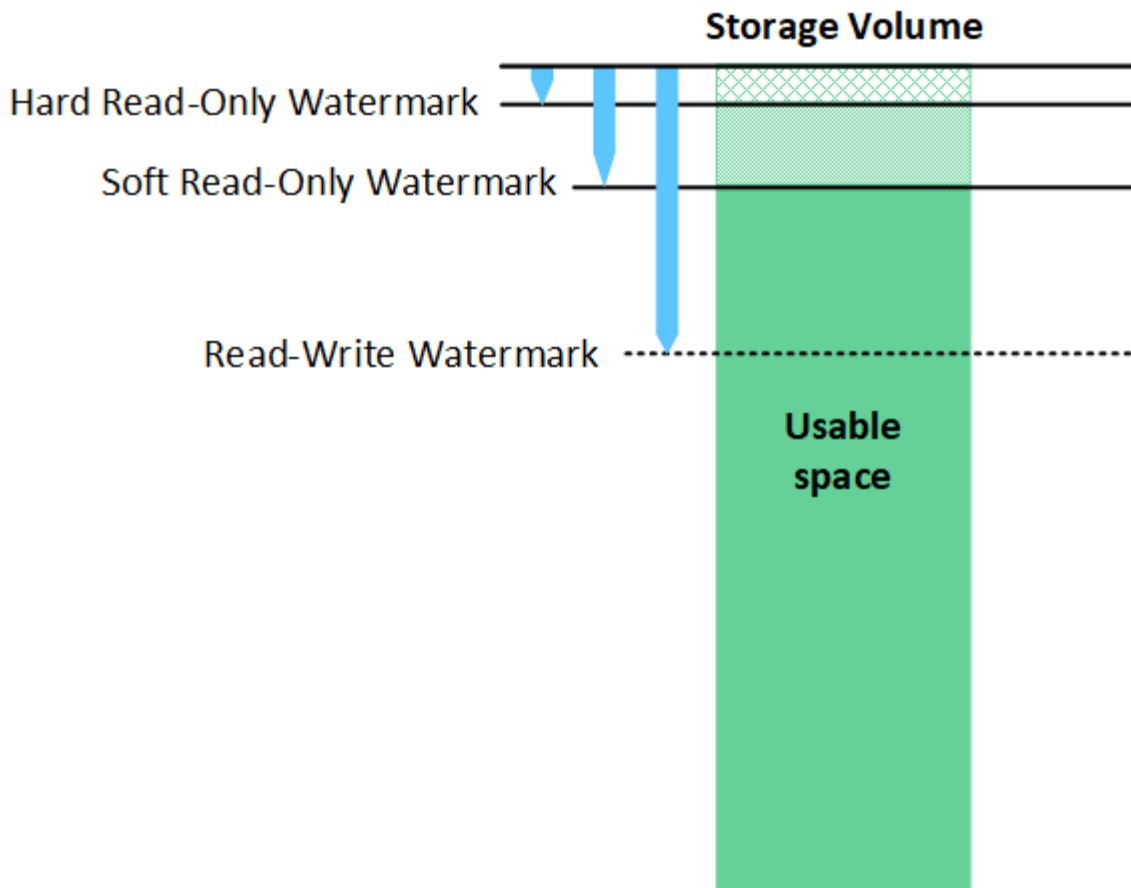
O contêiner e os segmentos não são necessariamente armazenados no mesmo nó de armazenamento. O contêiner e os segmentos podem ser armazenados em qualquer nó de armazenamento dentro do pool de armazenamento especificado na regra ILM.

Cada segmento é tratado pelo sistema StorageGRID de forma independente e contribui para a contagem de atributos, como Objetos Gerenciados e Objetos Armazenados. Por exemplo, se um objeto armazenado no sistema StorageGRID for dividido em dois segmentos, o valor dos Objetos Gerenciados aumentará em três após a conclusão da ingestão, da seguinte forma:

`segment container + segment 1 + segment 2 = three stored objects`

O que são marcas d'água de volume de armazenamento?

O StorageGRID usa 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 de ficarem com espaço criticamente baixo e para permitir que os nós de armazenamento que foram transferidos para um estado somente leitura se tornem leitura-gravação novamente.



As marcas d'água do volume de armazenamento se aplicam somente ao espaço usado para dados de objetos replicados e codificados para eliminação. Para saber mais sobre o espaço reservado para metadados de objetos no volume 0, acesse "[Gerenciar armazenamento de metadados de objetos](#)".

O que é a marca d'água suave somente leitura?

A **marca d'água de somente leitura do volume de armazenamento** é a primeira marca d'água a indicar que o espaço utilizável de um Nó de Armazenamento para dados de objeto está ficando cheio.

Se cada volume em um nó de armazenamento tiver menos espaço livre do que a marca d'água somente leitura do volume, o nó de armazenamento fará a transição para o *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 nó de armazenamento tenha uma marca d'água somente leitura de 10 GB. Assim que cada volume tiver menos de 10 GB de espaço livre, o nó de armazenamento passará para o modo somente leitura suave.

O que é a marca d'água somente leitura?

A **marca d'água de somente leitura do volume de armazenamento** é a próxima marca d'água para indicar que o espaço utilizável de um nó para dados de objeto está ficando cheio.

Se o espaço livre em um volume for menor que a marca d'água de somente leitura desse volume, as gravações no volume falharão. No entanto, as gravações em outros volumes podem continuar até que o espaço livre nesses volumes seja menor que suas marcas d'água de somente leitura.

Por exemplo, suponha que cada volume em um nó de armazenamento tenha uma marca d'água somente leitura de 5 GB. Assim que cada volume tiver menos de 5 GB de espaço livre, o nó de armazenamento não aceitará mais nenhuma solicitação de gravação.

A marca d'água somente leitura rígida é sempre menor que a marca d'água somente leitura flexível.

O que é a marca d'água de leitura e gravação?

A **marca d'água de leitura/gravação do volume de armazenamento** se aplica somente aos nós de armazenamento que fizeram a transição para o modo somente leitura. Ele determina quando o nó pode se tornar leitura-gravação novamente. Quando o espaço livre em qualquer volume de armazenamento em um nó de armazenamento for maior que a marca d'água de leitura e gravação desse volume, o nó retornará automaticamente ao estado de leitura e gravação.

Por exemplo, suponha que o nó de armazenamento tenha passado para o modo somente leitura. Suponha também que cada volume tenha uma marca d'água de leitura e gravação de 30 GB. Assim que o espaço livre para qualquer volume aumenta para 30 GB, o nó se torna novamente de leitura e gravação.

A marca d'água de leitura e gravação é sempre maior que a marca d'água somente leitura suave e a marca d'água somente leitura forte.

Exibir marcas d'água do volume de armazenamento

Você pode visualizar as configurações atuais da marca d'água e os valores otimizados do sistema. Se marcas d'água otimizadas não estiverem sendo usadas, você pode determinar se pode ou deve ajustar as configurações.

Antes de começar

- Você concluiu a atualização para o StorageGRID 11.6 ou superior.
- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).

Ver configurações atuais de marca d'água

Você pode visualizar as configurações atuais da marca d'água de armazenamento no Grid Manager.

Passos

1. Selecione **SUPORTE > Outros > Marcas d'água de armazenamento**.
2. Na página Marcas d'água de armazenamento, marque 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 armazenamento em cada nó de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

Esta é a configuração padrão e recomendada. Não atualize esses valores. Opcionalmente, você pode [Exibir marcas d'água de armazenamento otimizadas](#).

- Se a caixa de seleção Usar valores otimizados estiver desmarcada, marcas d'água personalizadas (não otimizadas) serão usadas. Não é recomendado usar configurações de marca d'água personalizadas. Use as instruções para ["solução de problemas de alertas de substituição de marca d'água somente leitura"](#) para determinar se você pode ou deve ajustar as configurações.

Ao especificar configurações de marca d'água personalizadas, você deve inserir valores maiores que

Ver marcas d'água de armazenamento otimizadas

O StorageGRID usa duas métricas do Prometheus para mostrar os valores otimizados que ele calculou para a marca d'água somente leitura do volume de armazenamento. Você pode visualizar os valores mínimos e máximos otimizados para cada nó de armazenamento na sua grade.

1. Selecione **SUORTE > Ferramentas > Métricas**.
2. Na seção Prometheus, selecione o link para acessar a interface do usuário do Prometheus.
3. Para ver a marca d'água mínima recomendada 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 somente leitura para todos os volumes de armazenamento em cada nó de armazenamento. Se esse valor for maior que a configuração personalizada para a marca d'água somente leitura do volume de armazenamento, o alerta **Substituição de marca d'água somente leitura baixa** será acionado para o Nó de Armazenamento.

4. Para ver a marca d'água máxima recomendada para 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 somente leitura para todos os volumes de armazenamento em cada nó de armazenamento.

Gerenciar armazenamento de metadados de objetos

A capacidade de metadados de objetos de um sistema StorageGRID controla o número máximo de objetos que podem ser armazenados nesse sistema. Para garantir que seu sistema StorageGRID tenha espaço adequado para armazenar novos objetos, você deve entender onde e como o StorageGRID armazena metadados de objetos.

O que são metadados de objeto?

Metadados de objeto são quaisquer informações que descrevem um objeto. O StorageGRID usa metadados de objetos para rastrear os locais de todos os objetos na grade e gerenciar o ciclo de vida de cada objeto ao longo do tempo.

Para um objeto no StorageGRID, os metadados do objeto incluem os seguintes tipos de informações:

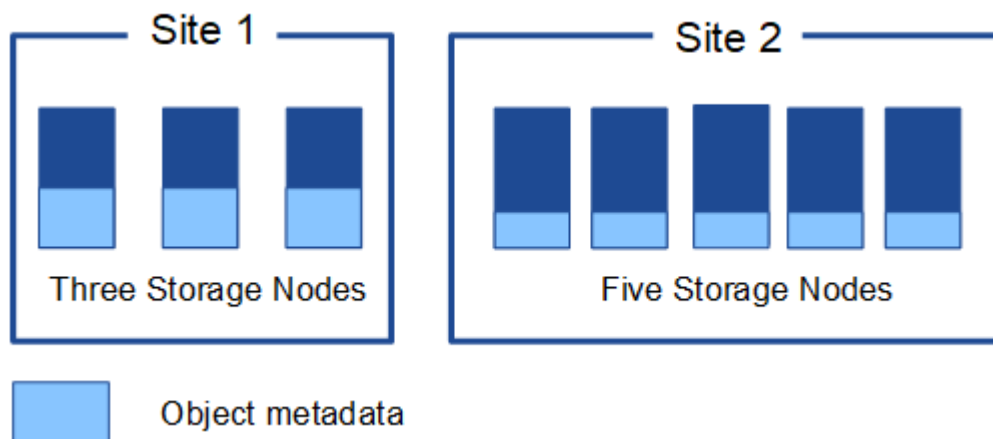
- Metadados do sistema, incluindo um ID exclusivo para cada objeto (UUID), o nome do objeto, o nome do bucket do S3, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e a hora em que o objeto foi criado pela primeira vez e a data e a hora em que o objeto foi modificado pela última 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 codificadas por eliminação, o local de armazenamento atual de cada fragmento.

- Para cópias de objetos em um pool de armazenamento em nuvem, o local do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
- Para objetos segmentados e objetos multipartes, identificadores de segmento e tamanhos de dados.

Como os metadados do objeto são armazenados?

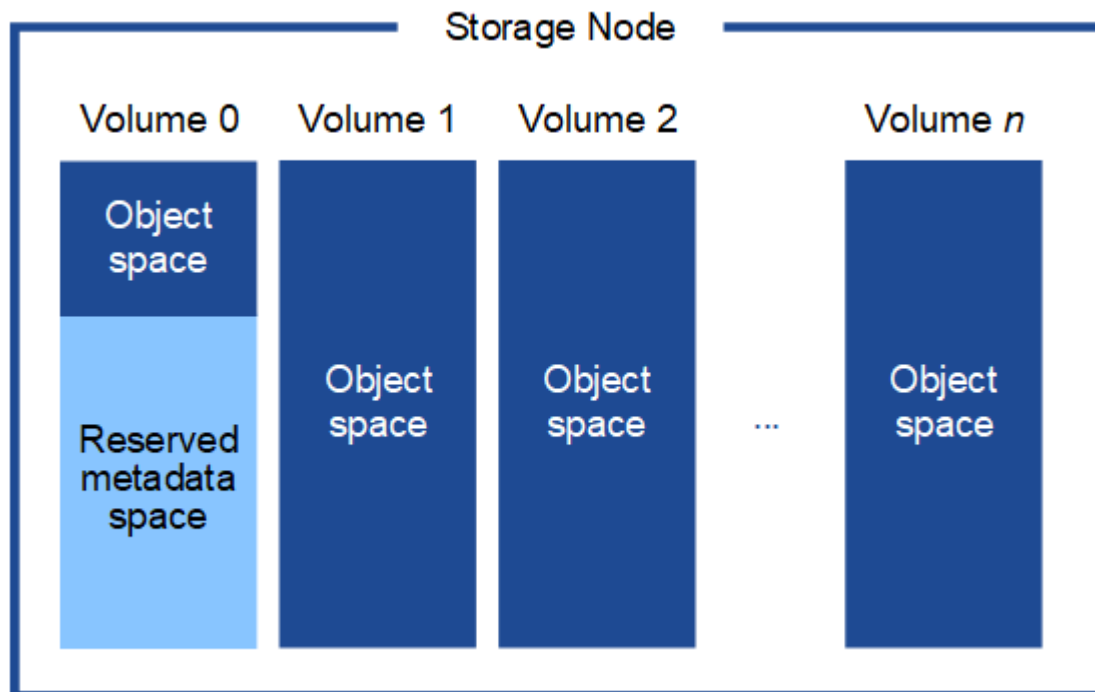
O StorageGRID mantém metadados de objetos em um banco de dados Cassandra, que é armazenado independentemente dos dados do objeto. Para fornecer redundância e proteger os metadados do objeto contra perdas, o StorageGRID armazena três cópias dos metadados para todos os objetos no sistema em cada site.

Esta figura representa os nós de armazenamento em dois locais. Cada site tem a mesma quantidade de metadados de objeto, e os metadados de cada site são subdivididos entre todos os nós de armazenamento naquele site.



Onde os metadados do objeto são armazenados?

Esta figura representa os volumes de armazenamento de um único nó de armazenamento.



Conforme mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de armazenamento 0 de cada nó de armazenamento. Ele usa o espaço reservado para armazenar metadados de objetos e executar operações essenciais do banco de dados. Qualquer espaço restante no volume de armazenamento 0 e todos os outros volumes de armazenamento no Nó de Armazenamento são usados exclusivamente para dados de objeto (cópias replicadas e fragmentos codificados para eliminação).

A quantidade de espaço reservada para metadados de objetos em um nó de armazenamento específico depende de vários fatores, descritos abaixo.

Configuração de espaço reservado de 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 nó de armazenamento. Conforme mostrado na tabela, o valor padrão desta configuração é baseado em:

- A versão do software que você estava usando quando instalou o StorageGRID inicialmente.
- A quantidade de RAM em cada nó de armazenamento.

Versão usada para instalação inicial do StorageGRID	Quantidade de RAM nos nós de armazenamento	Configuração padrão de espaço reservado de metadados
11,5 a 11,9	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 site	4 TB (4.000 GB)
	Menos de 128 GB em qualquer nó de armazenamento em cada site	3 TB (3.000 GB)
11.0 ou anterior	Qualquer quantia	2 TB (2.000 GB)

Exibir configuração de espaço reservado de metadados

Siga estas etapas para visualizar a configuração de espaço reservado de metadados para 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 de metadados deve ser de pelo menos 100 GB e não mais que 1 PB.

A configuração padrão para uma nova instalação do StorageGRID 11.6 ou superior, na qual cada nó de armazenamento tem 128 GB ou mais de RAM, é 8.000 GB (8 TB).

Espaço real reservado para metadados

Em contraste com a configuração de espaço reservado de metadados em todo o sistema, o *espaço reservado real* para metadados de objeto é determinado para cada nó de armazenamento. Para qualquer nó de armazenamento, o espaço reservado real para metadados depende do tamanho do volume 0 para o nó e da configuração de espaço reservado de metadados em todo o sistema.

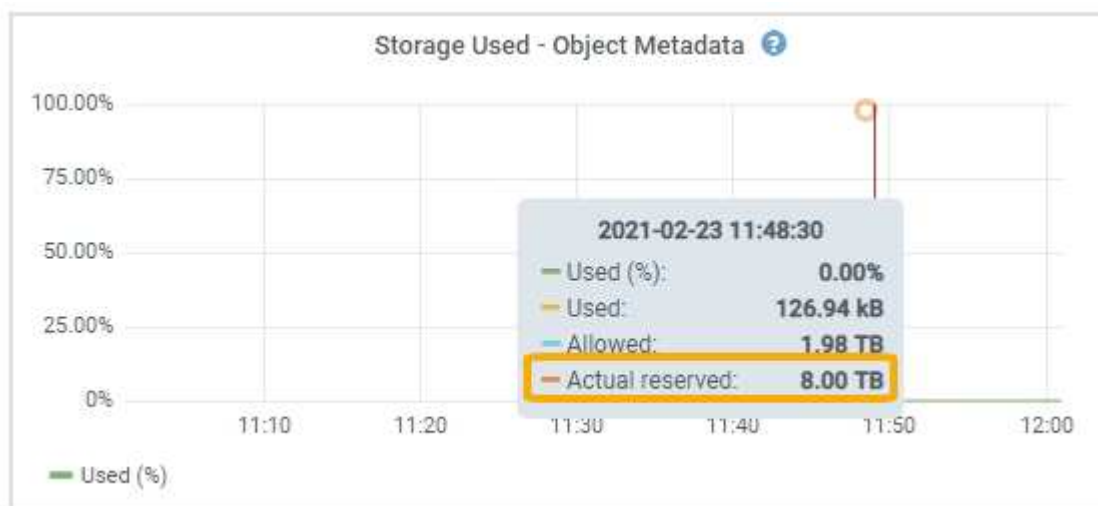
Tamanho do volume 0 para o nó	Espaço real reservado para metadados
Menos de 500 GB (uso não produtivo)	10% do volume 0
500 GB ou mais + ou + Nós de armazenamento somente de metadados	O menor desses valores: • Volume 0 • Configuração de espaço reservado de metadados Observação: somente um rangedb é necessário para nós de armazenamento somente de metadados.

Ver espaço reservado real para metadados

Siga estas etapas para visualizar o espaço real reservado para metadados em um nó de armazenamento específico.

Passos

1. No Grid Manager, selecione **NODES > Storage Node**.
2. Selecione a aba **Armazenamento**.
3. Posicione o cursor sobre o gráfico Armazenamento usado - Metadados do objeto e localize o valor **Realmente reservado**.



Na captura de tela, o valor **Realmente reservado** é 8 TB. Esta captura de tela é de um grande nó de armazenamento em uma nova instalação do StorageGRID 11.6. Como a configuração de espaço reservado de metadados em todo o sistema é menor que o volume 0 para este nó de armazenamento, o espaço reservado real para este nó é igual à configuração de espaço reservado de metadados.

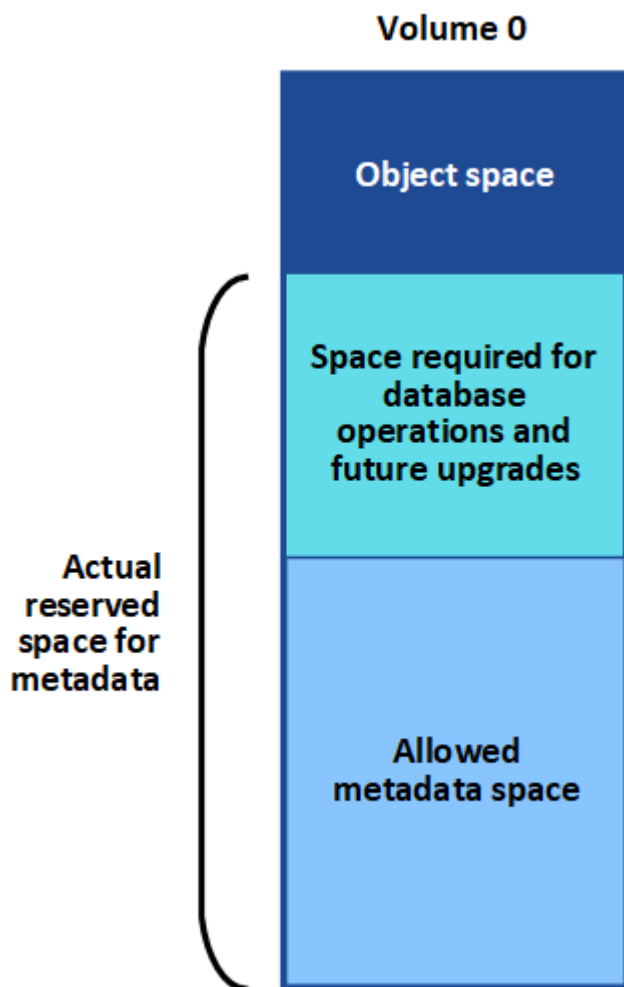
Exemplo de espaço de metadados reservado real

Suponha que você instale um novo sistema StorageGRID usando a versão 11.7 ou posterior. Para este exemplo, suponha que cada nó de armazenamento tenha mais de 128 GB de RAM e que o volume 0 do nó de armazenamento 1 (SN1) seja de 6 TB. Com base nestes 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 nó de armazenamento tiver mais de 128 GB de RAM.)
- O espaço real reservado para metadados para SN1 é de 6 TB. (O volume inteiro é reservado porque o volume 0 é menor que a configuração **Espaço reservado de metadados**.)

Espaço de metadados permitido

O espaço real reservado de cada nó de armazenamento para metadados é subdividido no espaço disponível para metadados de objetos (o *espaço de metadados permitido*) e no espaço necessário para operações essenciais do banco de dados (como compactação e reparo) e futuras atualizações de hardware e software. O espaço de metadados permitido controla a capacidade geral do objeto.



A tabela a seguir mostra como o StorageGRID calcula o **espaço de metadados permitido** para diferentes nós de armazenamento, com base na quantidade de memória do nó e no espaço real reservado para metadados.

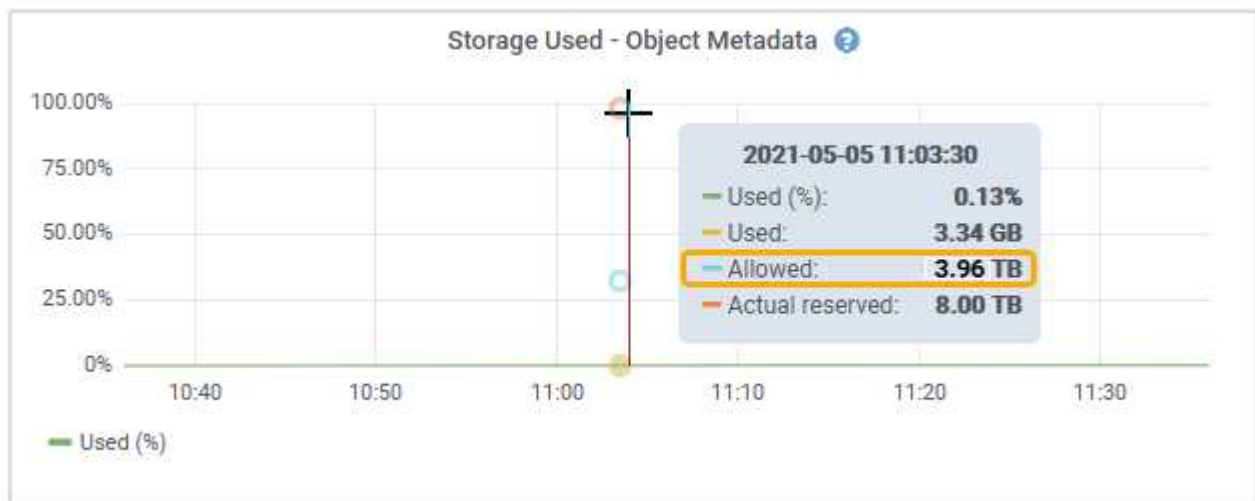
		Quantidade de memória no nó de armazenamento	
	< 128 GB	>= 128 GB	Espaço reservado real para metadados
≤ 4 TB	60% do espaço real reservado para metadados, até um máximo de 1,32 TB	60% do espaço real reservado para metadados, até um máximo de 1,98 TB	4 TB

Exibir espaço de metadados permitido

Siga estas etapas para visualizar o espaço de metadados permitido para um nó de armazenamento.

Passos

1. No Grid Manager, selecione **NODES**.
2. Selecione o nó de armazenamento.
3. Selecione a aba **Armazenamento**.
4. Posicione o cursor sobre o gráfico Armazenamento usado - metadados do objeto e localize o valor **Permitido**.



Na captura de tela, o valor **Permitido** é 3,96 TB, que é o valor máximo para um Nó de Armazenamento cujo espaço real reservado para metadados é maior que 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 sistema StorageGRID usando a versão 11.6. Para este exemplo, suponha que

cada nó de armazenamento tenha mais de 128 GB de RAM e que o volume 0 do nó de armazenamento 1 (SN1) seja de 6 TB. Com base nestes valores:

- O **espaço reservado de metadados** em todo o sistema está definido como 8 TB. (Este é o valor padrão para StorageGRID 11.6 ou superior quando cada nó de armazenamento tem mais de 128 GB de RAM.)
- O espaço real reservado para metadados para SN1 é de 6 TB. (O volume inteiro é reservado porque o volume 0 é menor que a configuração **Espaço reservado de metadados**.)
- O espaço permitido para metadados no SN1 é de 3 TB, com base no cálculo mostrado na [tabela para espaço permitido para metadados](#) : (Espaço reservado real para metadados – 1 TB) × 60%, até um máximo de 3,96 TB.

Como nós de armazenamento de tamanhos diferentes afetam a capacidade do objeto

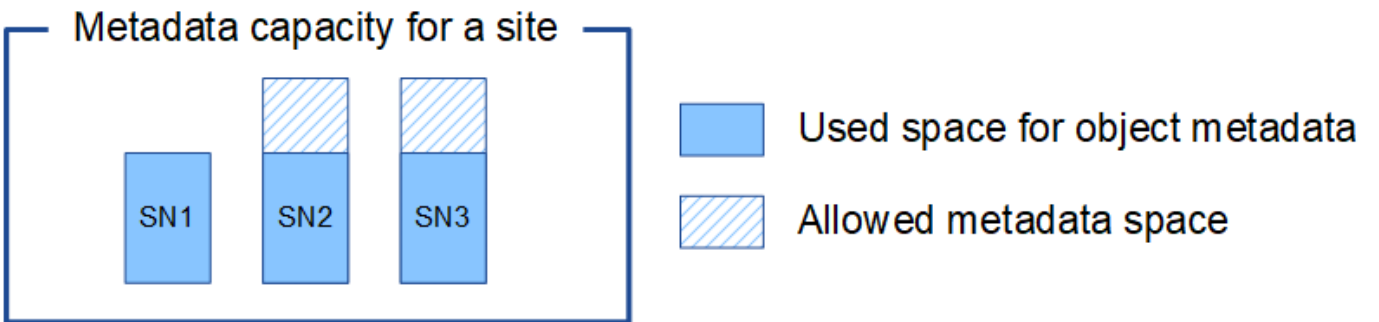
Conforme descrito acima, o StorageGRID distribui uniformemente os metadados dos objetos entre os nós de armazenamento em cada site. Por esse motivo, se um site contiver nós de armazenamento de tamanhos diferentes, o menor nó no site determinará a capacidade de metadados do site.

Considere o seguinte exemplo:

- Você tem uma grade de site único contendo três nós de armazenamento de tamanhos diferentes.
- A configuração **Espaço reservado para metadados** é 4 TB.
- Os nós de armazenamento têm os seguintes valores para o espaço de metadados reservado real e o espaço de metadados permitido.

Nó de armazenamento	Tamanho do volume 0	Espaço de metadados reservado real	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 do objeto são distribuídos uniformemente entre os nós de armazenamento em um site, cada nó neste exemplo pode conter 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 objeto para um sistema StorageGRID em cada site, a capacidade geral de metadados de um sistema StorageGRID é determinada pela capacidade de metadados de objeto do menor site.

E como a capacidade de metadados do objeto controla a contagem máxima de objetos, quando um nó fica sem capacidade de metadados, a grade fica efetivamente cheia.

Informações relacionadas

- Para saber como monitorar a capacidade de metadados do objeto para cada nó de armazenamento, consulte as instruções para ["Monitoramento StorageGRID"](#) .
- Para aumentar a capacidade de metadados de objetos do seu sistema, ["expandir uma grade"](#) adicionando novos nós de armazenamento.

Aumentar a configuração do Espaço Reservado de Metadados

Você poderá aumentar a configuração do sistema Espaço Reservado de 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 da web compatível"](#) .
- Você tem o ["Permissão de acesso root ou permissões de configuração da página de topologia de grade e outras configurações de grade"](#) .



A página de topologia de grade foi descontinuada e será removida em uma versão futura.

Sobre esta tarefa

Você pode aumentar manualmente a configuração de Espaço Reservado de Metadados em todo o sistema para até 8 TB.

Você só poderá aumentar o valor da configuração Espaço Reservado de Metadados em todo o sistema se ambas as afirmações forem verdadeiras:

- Os nós de armazenamento em qualquer local do seu sistema têm 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.

Esteja ciente de que se você aumentar essa configuração, você reduzirá simultaneamente o espaço disponível para armazenamento de objetos no volume de armazenamento 0 de todos os Nós de Armazenamento. Por esse motivo, você pode preferir definir o Espaço Reservado de Metadados para um valor menor que 8 TB, com base nos requisitos esperados de metadados do objeto.



Em geral, é melhor usar um valor mais alto em vez de um valor mais baixo. Se a configuração do Espaço Reservado de Metadados for muito grande, você poderá diminuí-la mais tarde. Por outro lado, se você aumentar o valor posteriormente, o sistema poderá precisar mover dados do objeto para liberar espaço.

Para obter uma explicação detalhada de como a configuração do Espaço Reservado de Metadados afeta o espaço permitido para armazenamento de metadados de objetos em um nó de armazenamento específico, consulte ["Gerenciar armazenamento de metadados de objetos"](#) .

Passos

1. Determine a configuração atual do Espaço Reservado de Metadados.
 - a. Selecione **CONFIGURAÇÃO > Sistema > Opções de armazenamento**.

- b. Na seção Marcas d'água de armazenamento, observe o valor de **Espaço reservado para metadados**.
2. Certifique-se de ter espaço disponível suficiente no volume de armazenamento 0 de cada nó de armazenamento para aumentar esse valor.
 - a. Selecione **NODES**.
 - b. Selecione o primeiro nó de armazenamento na grade.
 - c. Selecione a aba Armazenamento.
 - d. Na seção Volumes, localize a entrada **/var/local/rangedb/0**.
 - e. Confirme se 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 de Metadados.

Por exemplo, se a configuração do Espaço Reservado de Metadados for atualmente 4 TB e você quiser aumentá-la para 6 TB, o valor Disponível deverá ser 2 TB ou maior.
 - f. Repita essas etapas para todos os nós de armazenamento.
 - Se um ou mais nós de armazenamento não tiverem espaço disponível suficiente, o valor do espaço reservado de metadados não poderá ser aumentado. Não continue com este procedimento.
 - Se cada nó de armazenamento tiver espaço disponível suficiente no volume 0, vá para a próxima etapa.
3. Certifique-se de ter pelo menos 128 GB de RAM em cada nó de armazenamento.
 - a. Selecione **NODES**.
 - b. Selecione o primeiro nó de armazenamento na grade.
 - c. Selecione a aba **Hardware**.
 - d. Passe o cursor sobre o gráfico de uso de memória. Certifique-se de que a **Memória Total** seja de pelo menos 128 GB.
 - e. Repita essas etapas para todos os nós de armazenamento.
 - Se um ou mais nós de armazenamento não tiverem memória total disponível suficiente, o valor do espaço reservado de metadados não poderá ser aumentado. Não continue 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 do Espaço Reservado de Metadados.
 - a. Selecione **CONFIGURAÇÃO > Sistema > Opções de armazenamento**.
 - b. Selecione a aba Configuração.
 - c. Na seção Marcas d'água de armazenamento, selecione **Espaço reservado para metadados**.
 - d. Digite o novo valor.

Por exemplo, para inserir 8 TB, que é o valor máximo suportado, insira **8000000000000** (8, seguido de 12 zeros)

Storage Options

Overview

Configuration



Configure Storage Options

Updated: 2021-12-10 13:48:23 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1000000000

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0
Storage Volume Soft Read-Only Watermark Override	0
Storage Volume Hard Read-Only Watermark Override	0
Metadata Reserved Space	800000000000

Apply Changes

a. Selecione **Aplicar alterações**.

Compactar objetos armazenados

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 Grid Manager usando um "[navegador da web compatível](#)".
- Você tem "[permissões de acesso específicas](#)".

Sobre esta tarefa

Por padrão, a compactação de objetos está desabilitada. Se você habilitar a compactação, o StorageGRID tentará compactar cada objeto ao salvá-lo, usando compactação 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 dimensionamento.

Antes de habilitar a compactação de objetos, esteja ciente do seguinte:

- Você não deve selecionar **Compactar objetos armazenados** a menos que saiba que os dados armazenados são compactáveis.
- Aplicativos que salvam objetos no StorageGRID podem compactar objetos antes de salvá-los. Se um aplicativo cliente já tiver compactado um objeto antes de salvá-lo no StorageGRID, selecionar esta opção não reduzirá ainda mais o tamanho do objeto.
- Não selecione **Compactar objetos armazenados** se estiver usando o NetApp FabricPool com StorageGRID.
- Se **Compactar objetos armazenados** for selecionado, os aplicativos cliente S3 deverão evitar executar

operações `GetObject` que especifiquem um intervalo de bytes a serem retornados. Essas operações de "leitura de intervalo" são ineficientes porque o StorageGRID precisa descompactar efetivamente 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 os intervalos forem lidos de objetos compactados, as solicitações do cliente poderão 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 > Compactação de objetos**.
2. Marque a caixa de seleção **Compactar objetos armazenados**.
3. Selecione **Salvar**.

Gerenciar nós de armazenamento completos

À medida que os nós de armazenamento atingem a capacidade, você deve expandir o sistema StorageGRID por meio da adição de novo armazenamento. Há três opções disponíveis: adicionar volumes de armazenamento, adicionar prateleiras de expansão de armazenamento e adicionar nós de armazenamento.

Adicionar volumes de armazenamento

Cada nó de armazenamento suporta um número máximo de volumes de armazenamento. O máximo definido varia de acordo com a plataforma. Se um nó de armazenamento contiver menos do que o número máximo de volumes de armazenamento, você poderá adicionar volumes para aumentar sua capacidade. Veja as instruções para ["expandindo um sistema StorageGRID"](#).

Adicionar prateleiras de expansão de armazenamento

Alguns nós de armazenamento do dispositivo StorageGRID, como o SG6060 ou o SG6160, podem suportar prateleiras de armazenamento adicionais. Se você tiver dispositivos StorageGRID com recursos de expansão que ainda não foram expandidos para a capacidade máxima, você pode adicionar prateleiras de armazenamento para aumentar a capacidade. Veja as instruções para ["expandindo um sistema StorageGRID"](#).

Adicionar nós de armazenamento

Você pode aumentar a capacidade de armazenamento adicionando nós de armazenamento. É preciso considerar cuidadosamente as regras de ILM atualmente ativas e os requisitos de capacidade ao adicionar armazenamento. Veja as instruções para ["expandindo um sistema StorageGRID"](#).

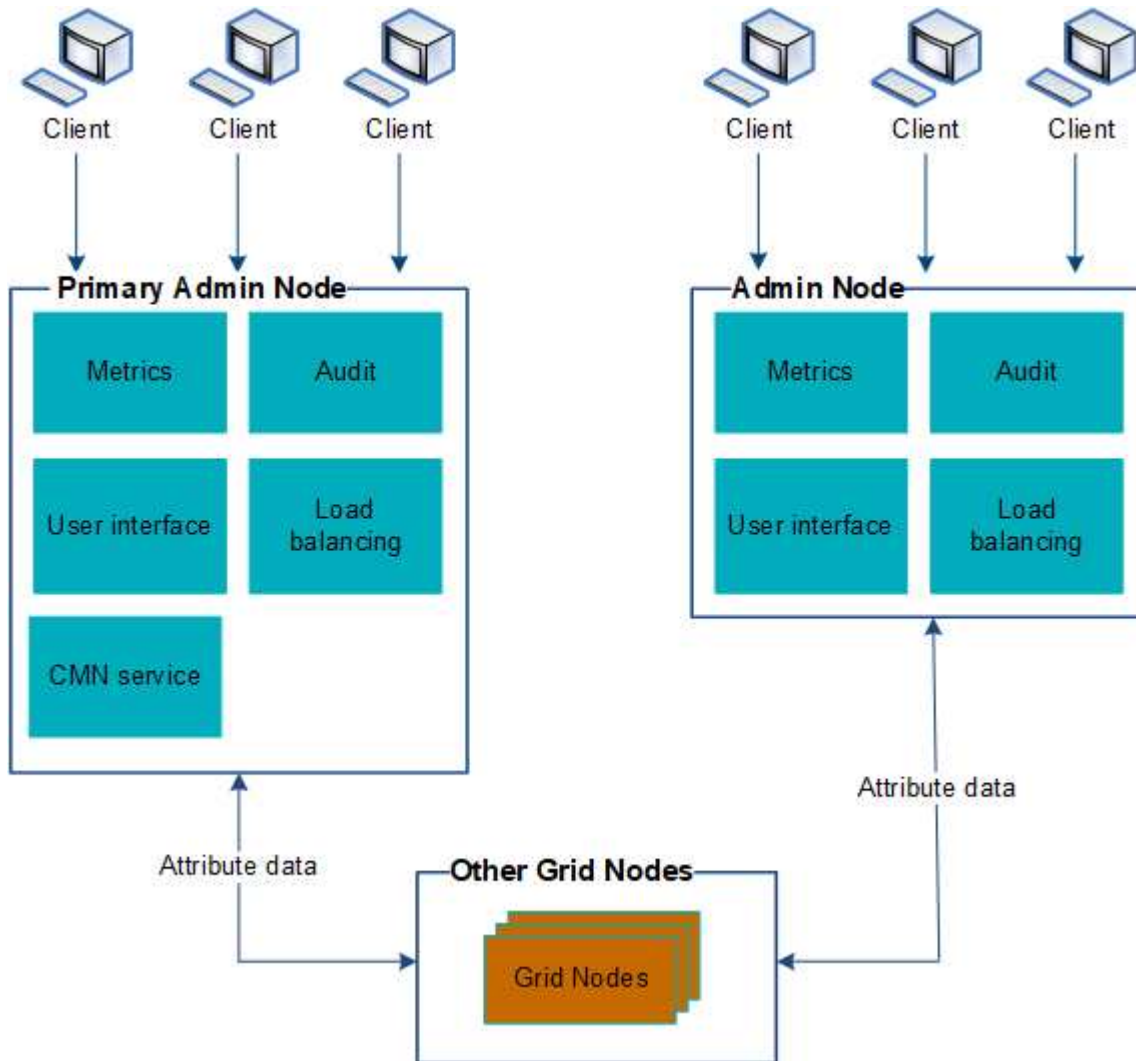
Gerenciar nós de administração

Use vários nós de administração

Um sistema StorageGRID pode incluir vários nós de administração para permitir que você monitore e configure continuamente seu sistema StorageGRID, mesmo se um nó

de administração falhar.

Se um nó de administração ficar indisponível, o processamento de atributos continuará, os alertas ainda serão acionados e as notificações por e-mail e os pacotes de AutoSupport ainda serão enviados. No entanto, ter vários nós de administração não fornece proteção contra failover, exceto para notificações e pacotes de AutoSupport .



Há duas opções para continuar a visualizar e configurar o sistema StorageGRID se um nó de administração falhar:

- Os clientes da Web podem se reconectar a qualquer outro nó de administração disponível.
- Se um administrador do sistema tiver configurado um grupo de alta disponibilidade de nós de administração, os clientes da Web poderão continuar acessando o Grid Manager ou o Tenant Manager usando o endereço IP virtual do grupo HA. Ver "[Gerenciar grupos de alta disponibilidade](#)".



Ao usar um grupo HA, o acesso é interrompido se o nó de administração ativo falhar. Os usuários devem efetuar login novamente depois que o endereço IP virtual do grupo HA falhar para outro nó de administração no grupo.

Algumas tarefas de manutenção só podem ser executadas usando o nó de administração principal. Se o nó de administração primário falhar, ele deverá ser recuperado antes que o sistema StorageGRID esteja

totalmente funcional novamente.

Identifique o nó de administração principal

O nó administrativo primário fornece mais funcionalidades do que os nós administrativos não primários. Por exemplo, alguns procedimentos de manutenção devem ser executados 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 Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem ["permissões de acesso específicas"](#) .

Passos

1. Selecione **NODES**.
2. Digite **primário** na caixa de pesquisa.

Nos resultados da pesquisa, identifique o nó com "Nó de administração principal" exibido na coluna Tipo. Um nó de administração primário deve ser listado.

Ver status de notificação e filas

O serviço do Sistema de Gerenciamento de Rede (NMS) nos Nós de Administração envia notificações ao servidor de e-mail. Você pode visualizar o status atual do serviço NMS e o tamanho da fila de notificações na página Interface Engine.

Para acessar a página Interface Engine, selecione **SUPORTE > Ferramentas > Topologia de grade**. Em seguida, selecione **site > Admin Node > NMS > Interface Engine**.

Overview Alarms Reports Configuration

Main

Overview: NMS (170-176) - Interface Engine
Updated: 2009-03-09 10:12:17 PDT

NMS Interface Engine Status:	Connected	
Connected Services:	15	

E-mail Notification Events

E-mail Notifications Status:	No Errors	
E-mail Notifications Queued:	0	

Database Connection Pool

Maximum Supported Capacity:	100	
Remaining Capacity:	95 %	
Active Connections:	5	

As notificações são processadas pela fila de notificações por e-mail e enviadas ao servidor de e-mail uma após a outra na ordem em que são acionadas. Se houver um problema (por exemplo, um erro de conexão de rede) e o servidor de e-mail não estiver disponível quando for feita a tentativa de enviar a notificação, uma tentativa de reenviar a notificação ao servidor de e-mail continuará por um período de 60 segundos. Se a

notificação não for enviada ao servidor de e-mail após 60 segundos, ela será descartada da fila de notificações e será feita uma tentativa de enviar a próxima notificação na fila.

Gerenciar objetos com ILM

Gerenciar objetos com ILM

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 de 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 entender seus requisitos operacionais, a topologia do seu sistema StorageGRID, suas necessidades de proteção de objetos e os tipos de armazenamento disponíveis. Em seguida, você deve determinar como deseja que diferentes tipos de objetos sejam copiados, distribuídos e armazenados.

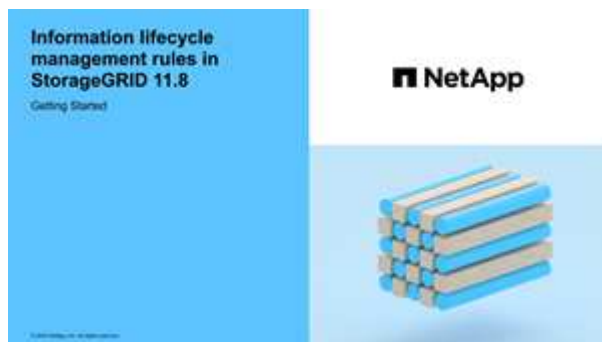
Use estas instruções para:

- Saiba mais sobre o StorageGRID ILM, incluindo ["como o ILM opera ao longo da vida de um objeto"](#).
- Aprenda a configurar ["pools de armazenamento"](#), ["Pools de armazenamento em nuvem"](#), e ["Regras do ILM"](#).
- Aprenda como ["criar, simular e ativar uma política de ILM"](#) que protegerá dados de objetos em um ou mais sites.
- Aprenda como ["gerenciar objetos com S3 Object Lock"](#), o que ajuda a garantir que objetos em buckets S3 específicos não sejam excluídos ou substituídos por um período de tempo especificado.

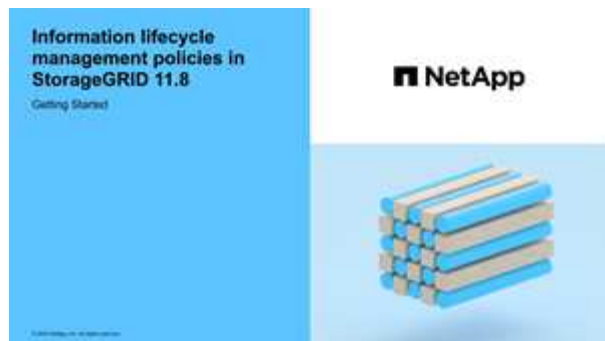
Saber mais

Para saber mais, assista a estes vídeos:

- ["Vídeo: Visão geral das regras do ILM"](#).



- ["Vídeo: Visão geral das políticas do ILM"](#)



ILM e ciclo de vida do objeto

Como o ILM opera ao longo da vida de um objeto

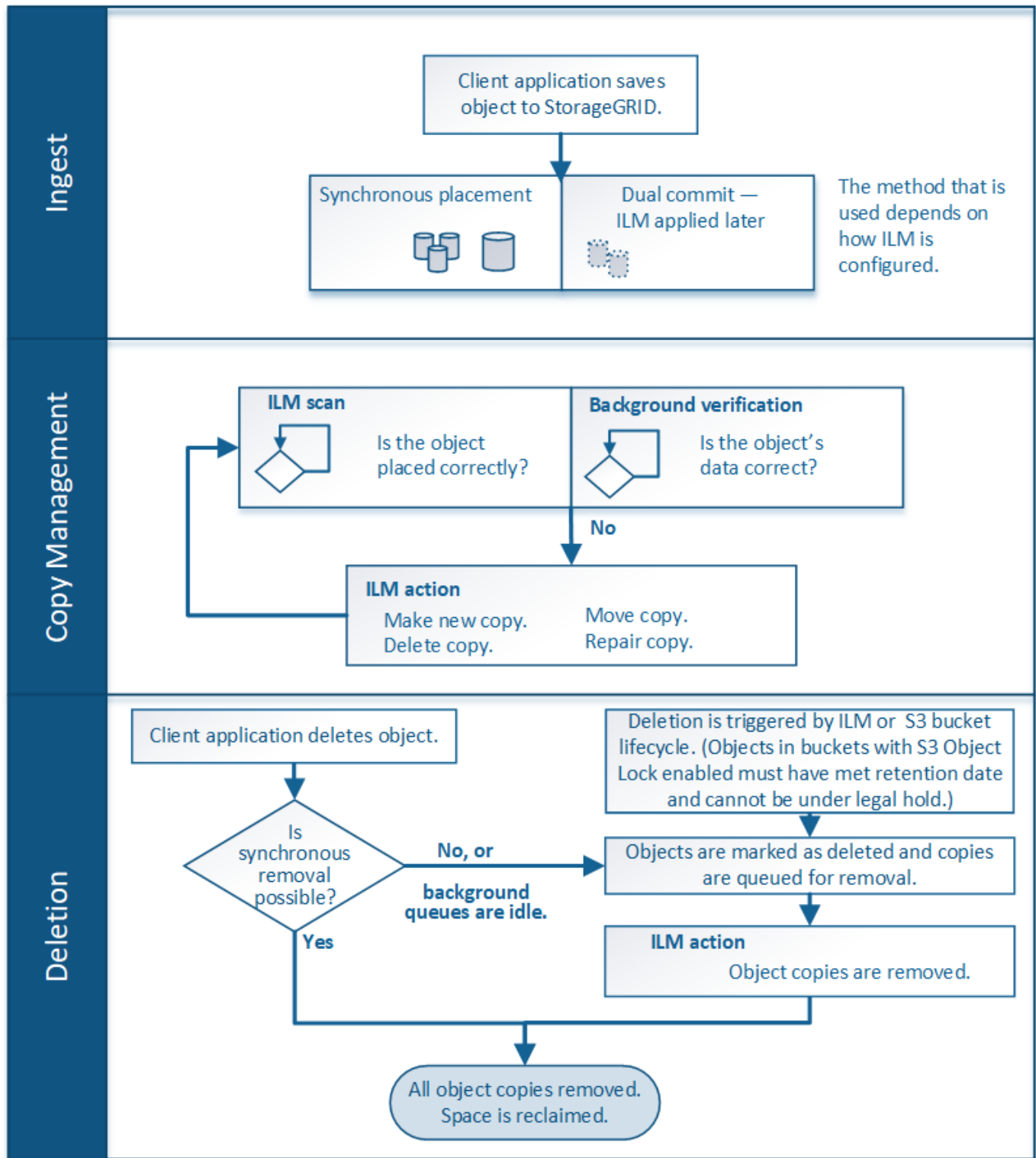
Entender como o StorageGRID usa o ILM para gerenciar objetos durante cada estágio de sua vida útil pode ajudar você a criar uma política mais eficaz.

- **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" ao cliente. Os dados do objeto são protegidos durante a ingestão, aplicando instruções do ILM imediatamente (posicionamento síncrono) ou criando cópias provisórias e aplicando o ILM posteriormente (confirmação dupla), dependendo de como os requisitos do ILM foram especificados.
- **Gerenciamento de cópias:** Depois de criar o número e o tipo de cópias de objetos especificados nas instruções de posicionamento do ILM, o StorageGRID gerencia os locais dos objetos e os protege contra perdas.
 - **Varredura e avaliação do ILM:** O StorageGRID varre continuamente a lista de objetos armazenados na grade e verifica se as cópias atuais atendem aos requisitos do ILM. Quando diferentes tipos, números ou locais de cópias de objetos são necessários, o StorageGRID cria, exclui ou move cópias conforme necessário.
 - **Verificação em segundo plano:** O StorageGRID realiza continuamente a verificação em segundo plano para verificar a integridade dos dados do objeto. Se um problema for encontrado, o StorageGRID cria automaticamente uma nova cópia do objeto ou um fragmento de objeto codificado para eliminação de substituição em um local que atenda aos requisitos atuais do ILM. Ver "[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 por um cliente, ou como resultado de uma exclusão por ILM ou exclusão causada pela expiração do ciclo de vida de um bucket do S3.



Objetos em um bucket que tenha o S3 Object Lock ativado não podem ser excluídos se estiverem sob retenção legal ou se uma data de retenção tiver sido especificada, mas ainda não tiver sido atingida.

O diagrama resume como o ILM opera durante todo o ciclo de vida de um objeto.



Como os objetos são ingeridos

Opções de ingestão

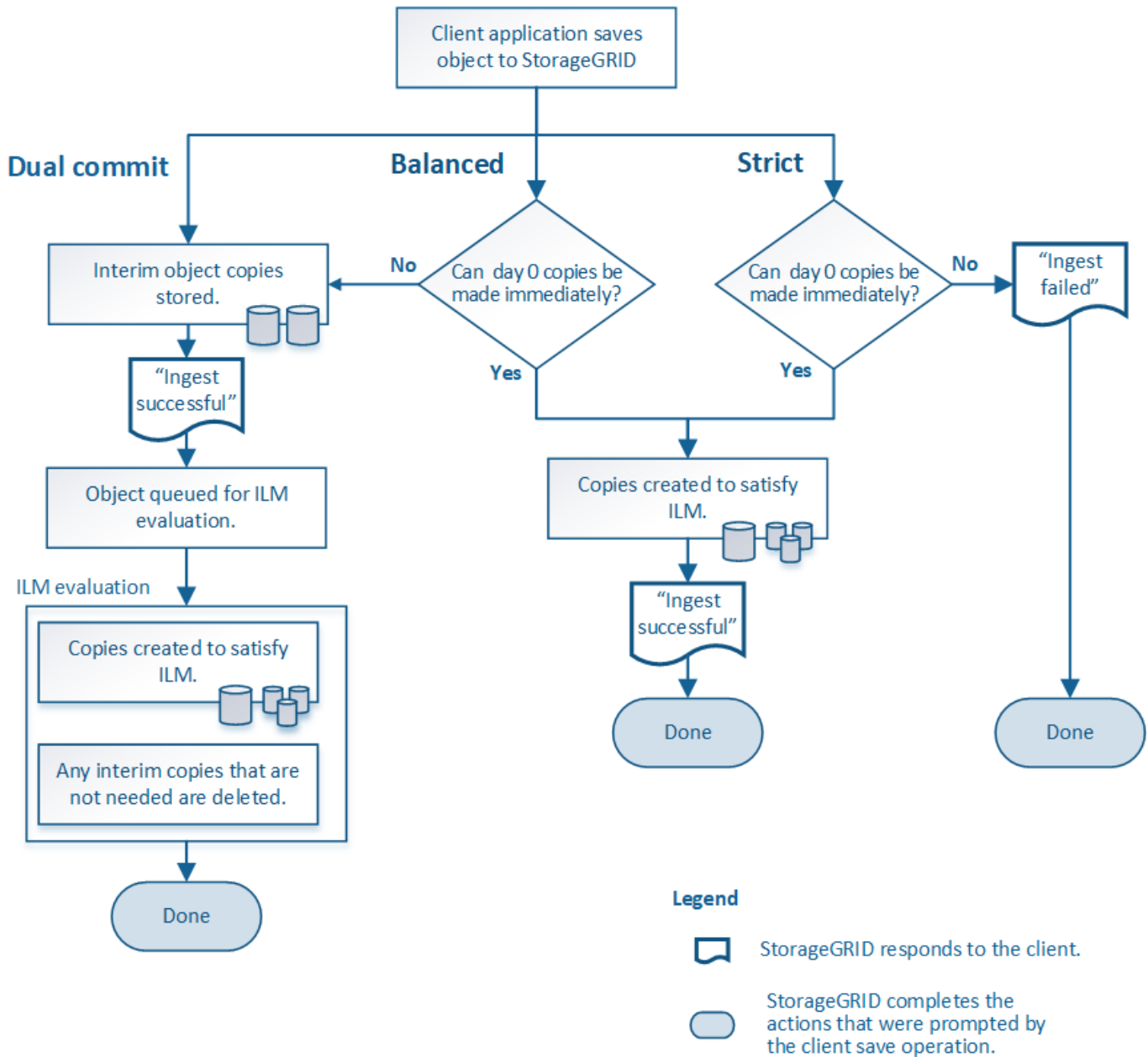
Ao criar uma regra de ILM, você especifica uma das três opções para proteger objetos na ingestão: Confirmação dupla, Estrita ou Balanceada.

Dependendo da sua escolha, o StorageGRID faz cópias provisórias e enfileira os objetos para avaliação

posterior do ILM, ou usa posicionamento síncrono e faz cópias imediatamente para atender aos requisitos do ILM.

Fluxograma de 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 ingestão.



Comprometimento duplo

Quando você seleciona a opção Dual commit, o StorageGRID imediatamente faz cópias provisórias do objeto em dois nós de armazenamento diferentes e retorna uma mensagem de "ingestão bem-sucedida" ao cliente. O objeto é enfileirado para avaliação do ILM, e cópias que atendem às instruções de posicionamento da regra são feitas posteriormente. Se a política ILM não puder ser processada imediatamente após a confirmação dupla, a proteção contra perda de site poderá levar algum tempo para ser alcançada.

Use a opção Dual commit em qualquer um destes casos:

- Você está usando regras de ILM multisite e a latência de ingestão do cliente é sua principal consideração. Ao usar o Dual Commit, você deve garantir que sua grade possa executar o trabalho adicional de criar e remover cópias de dual-commit se elas não satisfizerem o ILM. Especificamente:
 - A carga na rede deve ser baixa o suficiente para evitar um acúmulo de ILM.
 - A grade deve ter recursos de hardware excedentes (IOPS, CPU, memória, largura de banda de rede e assim por diante).
- Você está usando regras ILM multisite e a conexão WAN entre os sites geralmente tem alta latência ou largura de banda limitada. Nesse cenário, usar a opção Dual commit pode ajudar a evitar tempos limite do cliente. Antes de escolher a opção Dual commit, você deve testar o aplicativo cliente com cargas de trabalho realistas.

Equilibrado (padrão)

Quando você seleciona a opção Balanceado, o StorageGRID também usa o posicionamento síncrono na ingestão e faz imediatamente todas as cópias especificadas nas instruções de posicionamento da regra. Em contraste com a opção Strict, se o StorageGRID não puder fazer todas as cópias imediatamente, ele usará o Dual commit. Se a política de ILM usar posicionamentos em vários sites e a proteção imediata contra perda de site não puder ser alcançada, o alerta **posicionamento de ILM inalcançável** será acionado.

Use a opção Balanceado para obter a melhor combinação de proteção de dados, desempenho da grade e sucesso de ingestão. Balanceado é a opção padrão no assistente Criar regra ILM.

Estrito

Quando você seleciona a opção Estrito, o StorageGRID usa o posicionamento síncrono na ingestão e faz imediatamente todas as cópias de objetos especificadas nas instruções de posicionamento da regra. A ingestão falha se o StorageGRID não puder criar todas as cópias, por exemplo, porque um local de armazenamento necessário está temporariamente indisponível. O cliente deve tentar a operação novamente.

Use a opção Estrito se você tiver um requisito operacional ou regulatório para armazenar objetos imediatamente apenas nos locais descritos na regra ILM. Por exemplo, para atender a um requisito regulatório, talvez seja necessário usar a opção Estrita e um filtro avançado Restrição de Localização para garantir que objetos nunca sejam armazenados em determinados data centers.

Ver ["Exemplo 5: regras e política do ILM para comportamento de ingestão estrita"](#) .

Vantagens, desvantagens e limitações das opções de ingestão

Entender as vantagens e desvantagens de cada uma das três opções para proteger dados na ingestão (balanceado, estrito ou confirmação dupla) pode ajudar você a decidir qual selecionar para uma regra de ILM.

Para uma visão geral das opções de ingestão, consulte ["Opções de ingestão"](#) .

Vantagens das opções Balanceada e Estrita

Quando comparado ao Dual commit, que cria cópias provisórias durante a ingestão, as duas opções de posicionamento síncrono podem fornecer as seguintes vantagens:

- **Melhor segurança de dados:** os dados do objeto são imediatamente protegidos, 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 armazenamento. O commit duplo só pode proteger contra a perda de uma única cópia local.

- **Operação de grade mais eficiente:** Cada objeto é processado apenas uma vez, à medida que é ingerido. Como o sistema StorageGRID não precisa rastrear ou excluir cópias provisórias, há menos carga de processamento e menos espaço no banco de dados é consumido.
- **(Balanceado) Recomendado:** A opção Balanceada fornece eficiência ideal de ILM. É recomendável usar a opção Balanceada, a menos que o comportamento de ingestão Estrito seja necessário ou a grade atenda a todos os critérios para usar o Dual commit.
- **(Estrita) Certeza sobre localizações de objetos:** A opção Estrita garante que os objetos sejam armazenados imediatamente de acordo com as instruções de posicionamento na regra ILM.

Desvantagens das opções Balanceada e Estrita

Quando comparado ao Dual commit, as opções Balanced e Strict têm algumas desvantagens:

- **Ingestões de clientes mais longas:** As latências de ingestão de clientes podem ser maiores. Quando você usa as opções Balanceado ou Estrito, uma mensagem de "ingestão bem-sucedida" não é retornada ao cliente até que todos os fragmentos codificados para eliminação ou cópias replicadas sejam criados e armazenados. No entanto, os dados do objeto provavelmente chegarão ao seu posicionamento final muito mais rápido.
- **(Rigoroso) Taxas mais altas de falha de ingestão:** Com a opção Rigoroso, a ingestão falha sempre que o StorageGRID não consegue fazer imediatamente todas as cópias especificadas na regra ILM. Você poderá observar altas taxas de falha de ingestão se um local de armazenamento necessário estiver temporariamente offline ou se problemas de rede causarem atrasos na cópia de objetos entre sites.
- **(Rigoroso) Os posicionamentos de upload multipartes do S3 podem não ser como esperado em algumas circunstâncias:** Com o Rigoroso, você espera que os objetos sejam posicionados conforme descrito pela regra do ILM ou que a ingestão falhe. No entanto, com um upload multiparte do S3, o ILM é avaliado para cada parte do objeto à medida que ele é ingerido e para o objeto como um todo quando o upload multiparte é concluído. Nas seguintes circunstâncias, isso pode resultar em posicionamentos diferentes do esperado:
 - **Se o ILM for alterado enquanto um upload multiparte do S3 estiver em andamento:** como cada parte é colocada de acordo com a regra que está ativa quando a parte é ingerida, algumas partes do objeto podem não atender aos requisitos atuais do ILM quando o upload multiparte for concluído. Nesses casos, a ingestão do objeto não falha. Em vez disso, qualquer peça que não seja colocada corretamente é colocada na fila 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 peça, o StorageGRID filtra pelo tamanho da peça, 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 de 10 GB ou maiores sejam armazenados no DC1, enquanto todos os objetos menores sejam armazenados no DC2, na ingestão, cada parte de 1 GB de um upload multiparte de 10 partes será armazenada no DC2. Quando o ILM é avaliado para o objeto, todas as partes do objeto são movidas para DC1.
- **(Rigoroso) A ingestão não falha quando tags de objeto ou metadados são atualizados e novos posicionamentos obrigatórios não podem ser feitos:** Com o Rigoroso, você espera que os objetos sejam posicionados conforme descrito pela regra ILM ou que a ingestão falhe. No entanto, quando você atualiza metadados ou tags para um objeto que já está armazenado na grade, o objeto não é reingerido. Isso significa que quaisquer alterações no posicionamento do objeto acionadas pela atualização não são feitas imediatamente. 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 Balanceado e Estrito

As opções Balanceado ou Estrito não podem ser usadas para regras ILM que tenham qualquer uma destas instruções de posicionamento:

- Colocação em um pool de armazenamento em nuvem no dia 0.
- Posicionamentos em um pool de armazenamento em nuvem quando a regra tem um horário de criação definido pelo usuário como seu horário de referência.

Essas restrições existem porque o StorageGRID não pode fazer cópias sincronizadas para um pool de armazenamento em nuvem, e um horário de criação definido pelo usuário pode ser resolvido para o presente.

Como as regras e a consistência do ILM interagem para afetar a proteção de dados

Tanto sua regra ILM quanto sua escolha de consistência afetam como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, o comportamento de ingestão selecionado para uma regra ILM afeta o posicionamento inicial de cópias de objetos, enquanto a consistência usada quando um objeto é armazenado afeta o posicionamento inicial de metadados de objetos. Como o StorageGRID requer acesso aos dados e metadados de um objeto para atender às solicitações do cliente, selecionar níveis correspondentes de proteção para consistência e comportamento de ingestão pode fornecer melhor proteção inicial de dados e respostas mais previsíveis do sistema.

Aqui está um breve resumo dos valores de consistência disponíveis no StorageGRID:

- **Todos:** Todos os nós recebem metadados do objeto imediatamente ou a solicitação falhará.
- **Strong-global:** Os metadados do objeto são imediatamente distribuídos a todos os sites. Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
- **Strong-site:** Os metadados do objeto são imediatamente distribuídos para outros nós no site. Garante consistência de leitura após gravação para todas as solicitações de clientes em um site.
- **Leitura após nova gravação:** fornece 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:** Fornece consistência eventual para novos objetos e atualizações de objetos. Para buckets S3, use somente quando necessário (por exemplo, para um bucket que contém valores de log que raramente são lidos ou para operações HEAD ou GET em chaves que não existem). Não suportado para buckets do S3 FabricPool .



Antes de selecionar um valor de consistência, ["leia a descrição completa de consistência"](#) . Você deve entender os benefícios e limitações antes de alterar o valor padrão.

Exemplo de como a consistência e as regras do ILM podem interagir

Suponha que você tenha uma grade de dois sites com a seguinte regra ILM e a seguinte consistência:

- **Regra do ILM:** Crie duas cópias de objetos, uma no site local e outra em um site remoto. Use o comportamento de ingestão estrito.
- **consistência:** Forte-global (os metadados do objeto são imediatamente distribuídos para todos os sites).

Quando um cliente armazena um objeto na grade, o StorageGRID faz cópias do objeto e distribui metadados para ambos os sites antes de retornar o sucesso ao cliente.

O objeto é totalmente protegido contra perda no momento da ingestão bem-sucedida da mensagem. Por exemplo, se o site local for perdido logo após a ingestão, cópias dos dados do objeto e dos metadados do objeto ainda existirão no site remoto. O objeto é totalmente recuperável.

Se, em vez disso, você usasse a mesma regra de ILM e a consistência de site forte, o cliente poderia receber uma mensagem de sucesso depois que os dados do objeto fossem replicados para o site remoto, 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 site local for perdido logo após a ingestão, os metadados do objeto serão perdidos. O objeto não pode ser recuperado.

A inter-relação entre consistência e regras de ILM pode ser complexa. Entre em contato com a NetApp se precisar de assistência.

Informações relacionadas

["Exemplo 5: regras e política do ILM para comportamento de ingestão estrita"](#)

Como os objetos são armazenados (replicação ou codificação de eliminação)

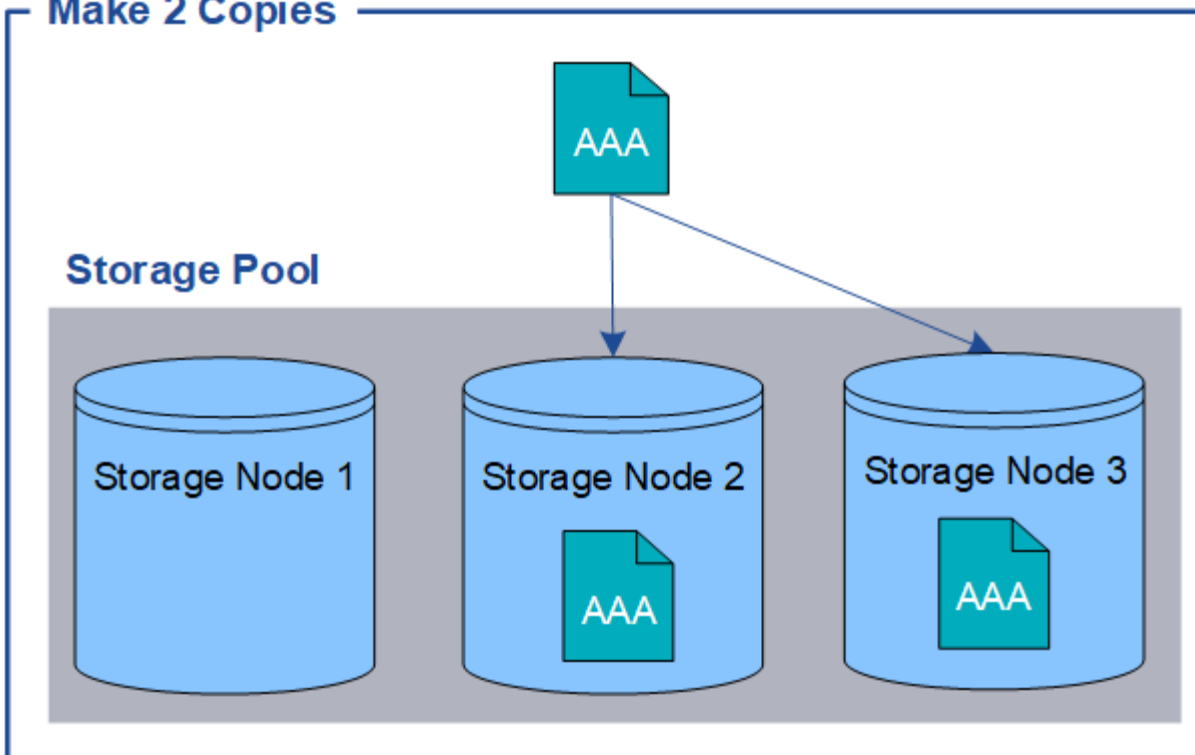
O que é replicação?

A replicação é um dos dois métodos usados pelo StorageGRID para armazenar dados de objetos (a codificação de eliminação é o outro método). Quando os objetos correspondem a uma regra do ILM que usa replicação, o sistema cria cópias exatas dos dados do objeto e armazena as cópias nos nós de armazenamento.

Ao configurar uma regra do ILM para criar cópias replicadas, você especifica quantas cópias devem ser criadas, onde elas devem ser colocadas e por quanto tempo elas 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 armazenamento que contém três nós de armazenamento.

Make 2 Copies



Quando o StorageGRID corresponde objetos a essa regra, ele cria duas cópias do objeto, colocando cada cópia em um nó de armazenamento diferente no pool de armazenamento. As duas cópias podem ser colocadas em quaisquer dois dos três nós de armazenamento disponíveis. Neste caso, a regra colocou cópias de objetos nos Nós de Armazenamento 2 e 3. Como há duas cópias, o objeto pode ser recuperado se algum dos nós no pool de armazenamento falhar.



O StorageGRID pode armazenar apenas uma cópia replicada de um objeto em qualquer nó de armazenamento. Se sua grade incluir três nós de armazenamento e você criar uma regra ILM de 4 cópias, apenas três cópias serão feitas — uma cópia para cada nó de armazenamento. 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 armazenamento"](#)
- ["Habilitar proteção contra perda de site usando replicação e codificação de eliminação"](#)

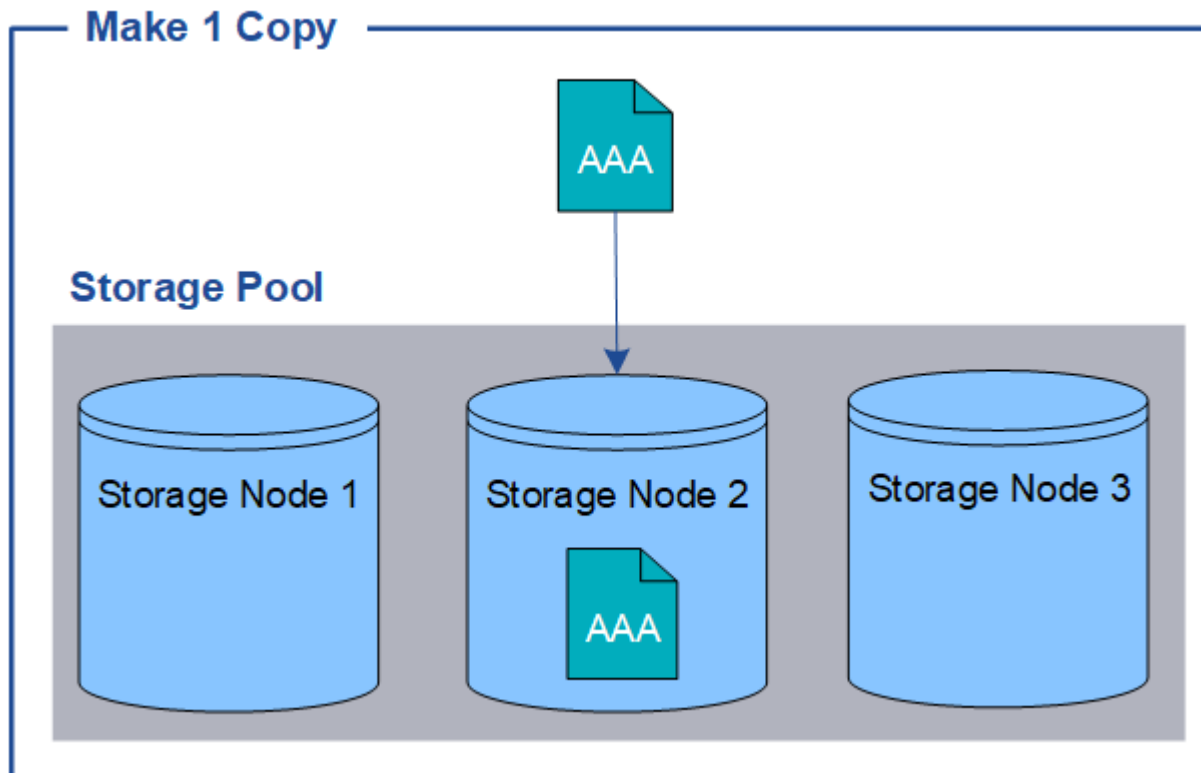
Por que você não deve usar replicação de cópia única

Ao criar uma regra de ILM para criar cópias replicadas, você deve sempre especificar pelo menos duas cópias para qualquer período de tempo nas instruções de posicionamento.

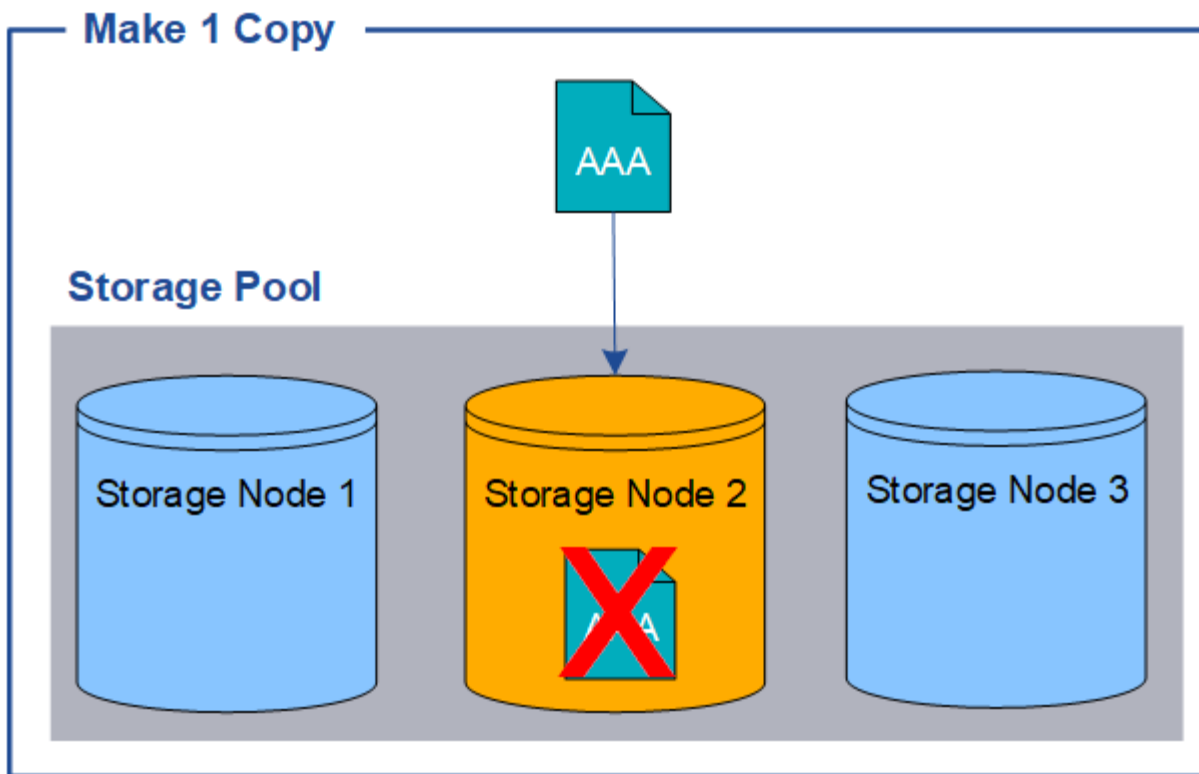


Não use uma regra de ILM que crie apenas uma cópia replicada para qualquer período de tempo. Se existir apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

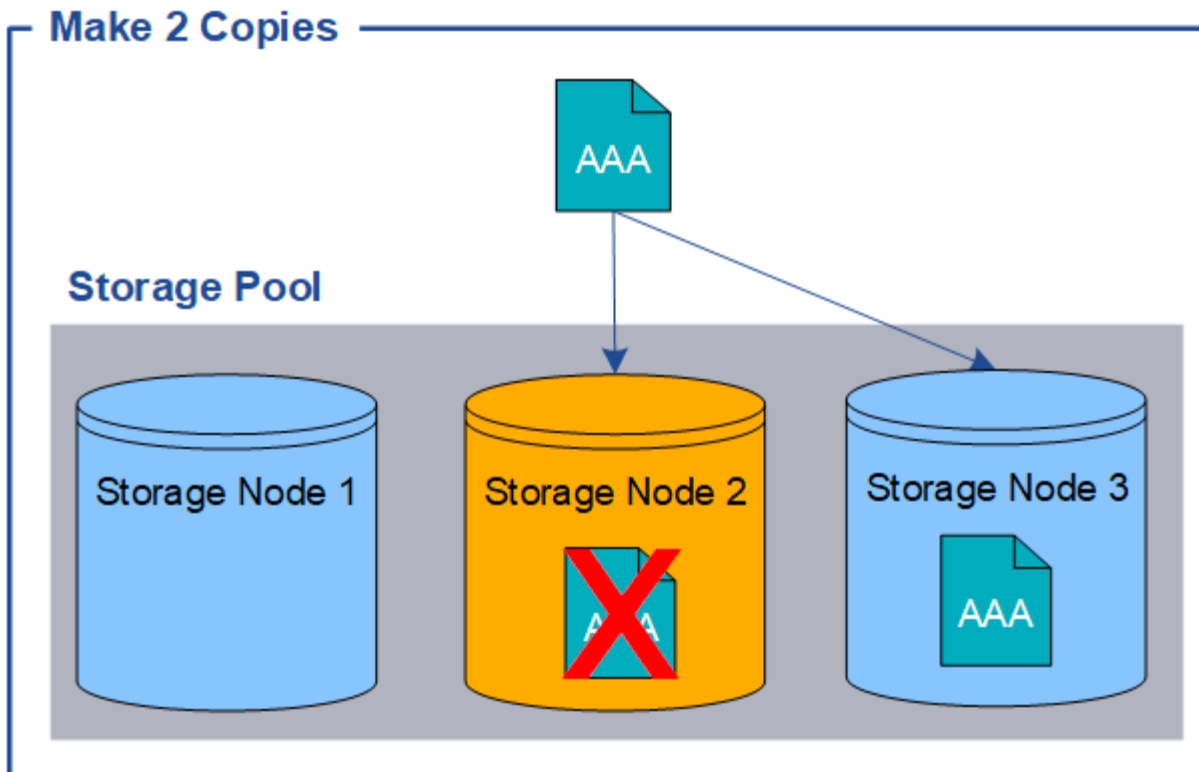
No exemplo a seguir, a regra Make 1 Copy ILM especifica que uma cópia replicada de um objeto seja colocada em um pool de armazenamento que contém três nós de armazenamento. Quando um objeto que corresponde a essa regra é ingerido, o StorageGRID coloca uma única cópia em apenas um nó de armazenamento.



Quando uma regra de ILM cria apenas uma cópia replicada de um objeto, o objeto se torna inacessível quando o Nó de Armazenamento não está disponível. Neste exemplo, você perderá temporariamente o acesso ao objeto AAA sempre que o Nó de Armazenamento 2 estiver offline, como durante uma atualização ou outro procedimento de manutenção. Você perderá o objeto AAA completamente se o Nó de Armazenamento 2 falhar.



Para evitar a perda de dados do objeto, você deve sempre fazer pelo menos duas cópias de todos os objetos que deseja proteger com replicação. Se houver duas ou mais cópias, você ainda poderá acessar o objeto se um nó de armazenamento falhar ou ficar offline.



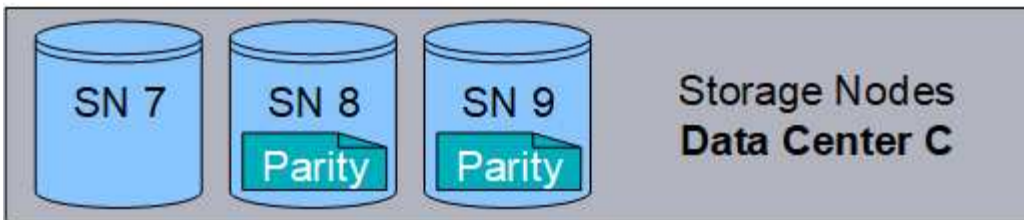
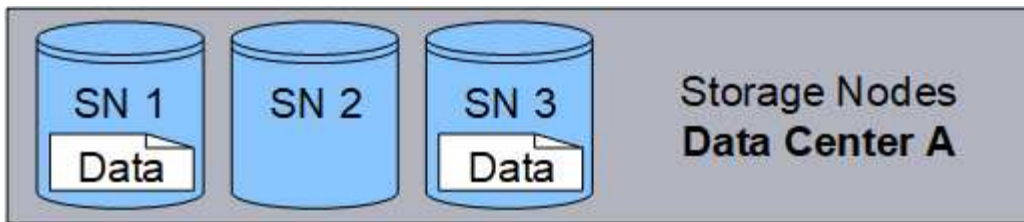
O que é codificação de eliminação?

A codificação de eliminação é um dos dois métodos que o StorageGRID usa para armazenar dados de objetos (a replicação é o outro método). Quando objetos correspondem a uma regra ILM que usa codificação de eliminação, esses objetos são divididos em fragmentos de dados, fragmentos de paridade adicionais são computados e cada fragmento é armazenado em um nó de armazenamento diferente.

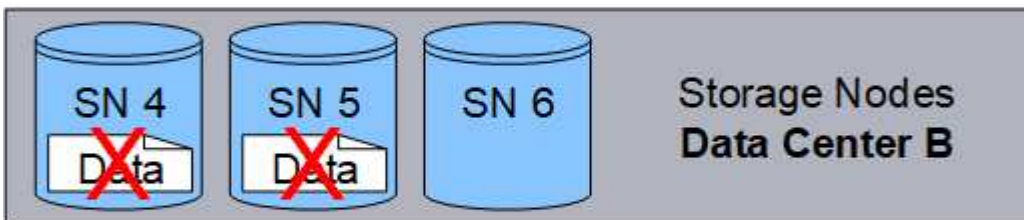
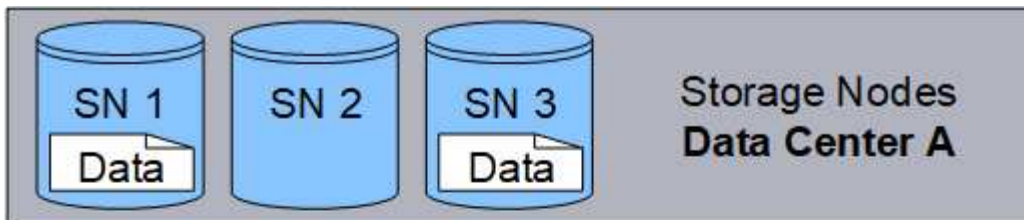
Quando um objeto é acessado, ele é remontado usando os fragmentos armazenados. Se um dado ou um fragmento de paridade for corrompido ou perdido, o algoritmo de codificação de eliminação pode recriar esse fragmento usando um subconjunto dos dados e fragmentos de paridade restantes.

À medida que você cria regras de ILM, o StorageGRID cria perfis de codificação de eliminação que dão suporte a essas regras. Você pode visualizar uma lista de perfis de codificação de eliminação, ["renomear um perfil de codificação de eliminação"](#), ou ["desativar um perfil de codificação de eliminação se ele não estiver sendo usado atualmente em nenhuma regra do ILM"](#).

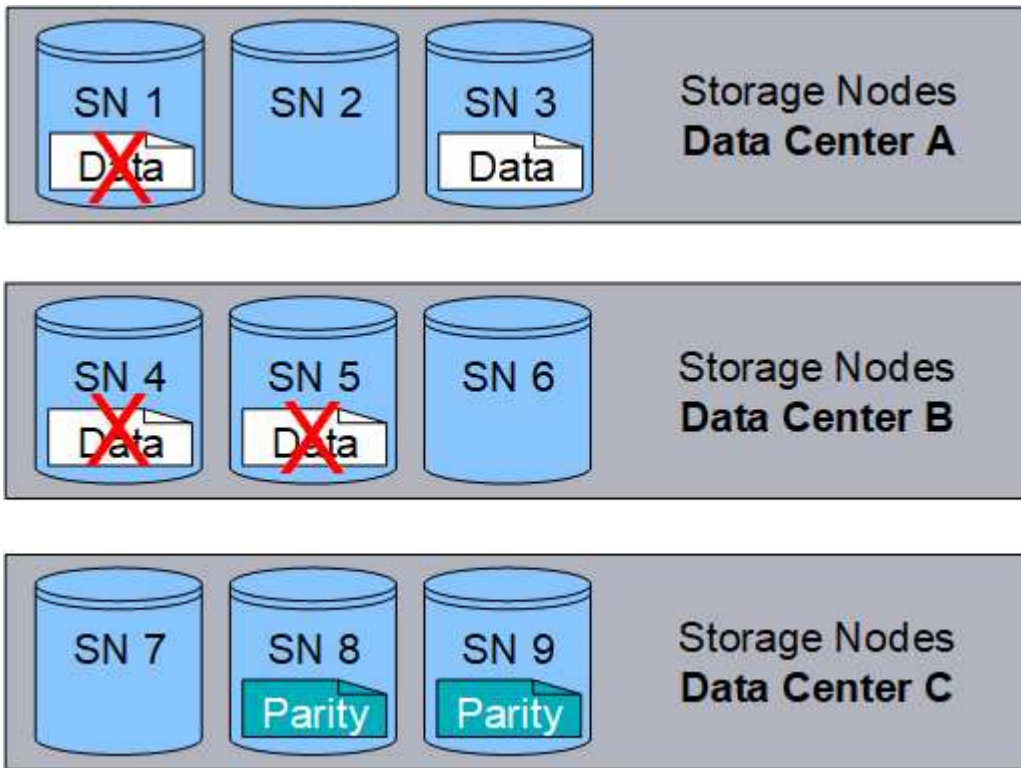
O exemplo a seguir ilustra o uso de um algoritmo de codificação de eliminação nos dados de um objeto. Neste exemplo, a regra ILM usa um esquema de codificação de eliminação 4+2. Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados do objeto. Cada um dos seis fragmentos é armazenado em um nó diferente em três locais do data center para fornecer proteção de dados em caso de falhas de nó ou perda de local.



O esquema de codificação de apagamento 4+2 pode ser configurado de várias maneiras. Por exemplo, você pode configurar um pool de armazenamento de site único que contenha seis nós de armazenamento. Para "proteção contra perda de site", você pode usar um pool de armazenamento contendo três sites com três nós de armazenamento em cada site. Um objeto pode ser recuperado desde que quatro dos seis fragmentos (dados ou paridade) permaneçam disponíveis. Até dois fragmentos podem ser perdidos sem perda dos dados do objeto. Se um local 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 armazenamento"](#)
- ["O que são esquemas de codificação de apagamento"](#)
- ["Renomear um perfil de codificação de eliminação"](#)
- ["Desativar um perfil de codificação de eliminação"](#)

O que são esquemas de codificação de apagamento?

Os esquemas de codificação de eliminação 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 eliminação disponível. O StorageGRID cria automaticamente esquemas de codificação de eliminação com base em quantos nós de armazenamento e sites compõem o pool de armazenamento que você planeja usar.

Proteção de dados

O sistema StorageGRID usa o algoritmo de codificação de eliminação Reed-Solomon. O algoritmo divide um objeto em k fragmentos de dados e m fragmentos de paridade.

O $k + m = n$ fragmentos estão espalhados por n Nós de armazenamento para fornecer proteção de dados da seguinte forma:

- Para recuperar ou reparar um objeto, k fragmentos são necessários.
- Um objeto pode sustentar até m fragmentos perdidos ou corrompidos. Quanto maior o valor de m , maior

será a tolerância a falhas.

A melhor proteção de dados é fornecida pelo esquema de codificação de eliminação com a maior tolerância a falhas de nó ou volume dentro de um pool de armazenamento.

Despesas gerais de armazenamento

A sobrecarga de armazenamento de um esquema de codificação de eliminação é calculada dividindo o número de fragmentos de paridade(m) pelo número de fragmentos de dados(k). Você pode usar a sobrecarga de armazenamento para calcular quanto espaço em disco cada objeto codificado por eliminação 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 armazenamento), o objeto consumirá 15 MB de armazenamento em grade. Se você armazenar o mesmo objeto de 10 MB usando o esquema 6+2 (que tem 33% de sobrecarga de armazenamento), 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 que menos nós sejam adicionados em um ["expansão quando mais armazenamento é necessário"](#)

Diretrizes para pools de armazenamento

Ao selecionar o pool de armazenamento a ser usado para uma regra que criará uma cópia codificada para eliminação, use as seguintes diretrizes para pools de armazenamento:

- O pool de armazenamento deve incluir três ou mais sites, ou exatamente um site.



Não é possível usar a codificação de eliminação se o pool de armazenamento incluir dois sites.

- [Esquemas de codificação de apagamento para pools de armazenamento contendo três ou mais sites](#)
- [Esquemas de codificação de eliminação para pools de armazenamento de um site](#)
- Não use um pool de armazenamento que inclua o site Todos os Sites.
- O pool de armazenamento deve incluir pelo menos $k+m + 1$ Nós de armazenamento que podem armazenar dados de objetos.



Os nós de armazenamento podem ser configurados durante a instalação para conter apenas metadados de objetos e não 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 pendências de ILM se um nó de armazenamento necessário estiver temporariamente indisponível.

Esquemas de codificação de apagamento para pools de armazenamento contendo três ou mais sites

A tabela a seguir descreve os esquemas de codificação de eliminação atualmente suportados pelo StorageGRID para pools de armazenamento que incluem três ou mais sites. Todos esses esquemas oferecem proteção contra perda de local. Um site pode ser perdido, e o objeto ainda estará acessível.

Para esquemas de codificação de eliminação que fornecem proteção contra perda de site, o número recomendado de nós de armazenamento no pool de armazenamento 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 nós de armazenamento em cada site	Número total recomendado de nós de armazenamento	Proteção contra perda de site?	Despesas gerais de armazenamento
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%



O StorageGRID requer no mínimo três nós de armazenamento por site. Para usar o esquema 7+5, cada site requer um mínimo de quatro nós de armazenamento. É recomendável usar cinco nós de armazenamento por site.

Ao selecionar um esquema de codificação de eliminação que forneça proteção ao site, equilibre a importância relativa dos seguintes fatores:

- **Número de fragmentos:** O desempenho e a flexibilidade de expansão geralmente são melhores quando o número total de fragmentos é menor.
- **Tolerância a falhas:** A tolerância a falhas é aumentada ao ter mais segmentos de paridade (ou seja, quando m tem um valor mais alto.)
- **Tráfego de rede:** Ao se recuperar de falhas, usar um esquema com mais fragmentos (ou seja, um total maior para $k+m$) cria mais tráfego de rede.
- **Sobrecarga de armazenamento:** Esquemas com sobrecarga maior exigem mais espaço de armazenamento por objeto.

Por exemplo, ao decidir entre um esquema 4+2 e um esquema 6+3 (ambos com 50% de sobrecarga de armazenamento), selecione o esquema 6+3 se for necessária tolerância a falhas adicional. Selecione o esquema 4+2 se os recursos de rede forem limitados. Se todos os outros fatores forem iguais, selecione 4+2 porque ele tem um número total de fragmentos menor.



Se 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 eliminação para pools de armazenamento de um site

Um pool de armazenamento de um site suporta todos os esquemas de codificação de eliminação definidos para três ou mais sites, desde que o site tenha nós de armazenamento suficientes.

O número mínimo de nós de armazenamento necessários é $k+m$, mas um pool de armazenamento com $k+m+1$ Nós de armazenamento são recomendados. Por exemplo, o esquema de codificação de eliminação 2+1 requer um pool de armazenamento com no mínimo três nós de armazenamento, mas quatro nós de armazenamento são recomendados.

Esquema de codificação de apagamento ($k+m$)	Número mínimo de nós de armazenamento	Número recomendado de nós de armazenamento	Despesas gerais de armazenamento
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

Antes de decidir se deve usar replicação ou codificação de eliminação para proteger dados de objetos contra perda, você deve entender as vantagens, desvantagens e os requisitos da codificação de eliminação.

Vantagens da codificação de apagamento

Quando comparado à replicação, a codificação de eliminação oferece maior confiabilidade, disponibilidade e

eficiência de armazenamento.

- **Confiabilidade:** A confiabilidade é medida em termos de tolerância a falhas, ou seja, o número de falhas simultâneas que podem ser sustentadas sem perda de dados. Com a replicação, várias cópias idênticas são armazenadas em diferentes nós e entre sites. Com a codificação de eliminação, um objeto é codificado em dados e fragmentos de paridade e distribuído entre muitos nós e sites. Essa dispersão fornece proteção contra falhas no local e no nó. Quando comparado à replicação, a codificação de eliminação proporciona maior confiabilidade com custos de armazenamento comparáveis.
- **Disponibilidade:** Disponibilidade pode ser definida como a capacidade de recuperar objetos se os Nós de Armazenamento falharem ou se tornarem inacessíveis. Quando comparado à replicação, a codificação de eliminação proporciona maior disponibilidade a custos de armazenamento comparáveis.
- **Eficiência de armazenamento:** Para níveis semelhantes de disponibilidade e confiabilidade, objetos protegidos por codificação de eliminação consomem menos espaço em disco do que os mesmos objetos se protegidos por replicação. Por exemplo, um objeto de 10 MB replicado em dois sites consome 20 MB de espaço em disco (duas cópias), enquanto um objeto codificado por eliminação em três sites com um esquema de codificação por eliminação 6+3 consome apenas 15 MB de espaço em disco.



O espaço em disco para objetos codificados para eliminação é calculado como o tamanho do objeto mais a sobrecarga de armazenamento. A porcentagem de sobrecarga de armazenamento é o número de fragmentos de paridade dividido pelo número de fragmentos de dados.

Desvantagens da codificação de apagamento

Quando comparado à replicação, a codificação de eliminação tem as seguintes desvantagens:

- Recomenda-se um número maior de nós de armazenamento e sites, dependendo do esquema de codificação de eliminação. Por outro lado, se você replicar dados de objeto, precisará apenas de um nó de armazenamento para cada cópia. Ver ["Esquemas de codificação de apagamento para pools de armazenamento contendo três ou mais sites"](#) e ["Esquemas de codificação de eliminação para pools de armazenamento de um site"](#).
- Aumento de custo e complexidade das expansões de armazenamento. Para expandir uma implantação que usa replicação, adicione capacidade de armazenamento em cada local onde as cópias de objetos são feitas. Para expandir uma implantação que usa codificação de eliminação, você deve considerar o esquema de codificação de eliminação em uso e o quão cheios os nós de armazenamento existentes estão. Por exemplo, se você esperar até que os nós existentes estejam 100% cheios, você deve adicionar pelo menos $k+m$ Nós de armazenamento, mas se você expandir quando os nós existentes estiverem 70% cheios, você pode adicionar dois nós por site e ainda maximizar a capacidade de armazenamento utilizável. Para obter mais informações, consulte ["Adicionar capacidade de armazenamento para objetos codificados por eliminação"](#).
- Há latências de recuperação maiores quando você usa codificação de eliminação em sites distribuídos geograficamente. Os fragmentos de objeto de um objeto codificado por eliminação e distribuído em sites remotos demoram mais para serem recuperados por meio de conexões WAN do que um objeto replicado e disponível localmente (o mesmo site ao qual o cliente se conecta).
- Ao usar codificação de eliminação em sites distribuídos geograficamente, 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.
- Quando você usa codificação de eliminação em vários sites, a taxa de transferência máxima de objetos diminui drasticamente à medida que a latência da rede entre os sites aumenta. Essa diminuição se deve à diminuição correspondente na taxa de transferência da rede TCP, que afeta a rapidez com que o sistema StorageGRID pode armazenar e recuperar fragmentos de objetos.

- Maior uso de recursos de computação.

Quando usar codificação de apagamento

A codificação de apagamento é mais adequada para os seguintes requisitos:

- Objetos com tamanho maior que 1 MB.



A codificação de eliminação é mais adequada para objetos maiores que 1 MB. Não use codificação de eliminação para objetos menores que 200 KB para evitar a sobrecarga de gerenciamento de fragmentos muito pequenos codificados por eliminação.

- Armazenamento a longo prazo ou a frio para conteúdo recuperado com pouca frequência.
- Alta disponibilidade e confiabilidade de dados.
- Proteção contra falhas completas de sites e nós.
- Eficiência de armazenamento.
- Implantações de site único que exigem proteção de dados eficiente com apenas uma única cópia codificada para eliminação, em vez de várias cópias replicadas.
- Implantações em vários sites onde a latência entre sites é inferior a 100 ms.

Como a retenção de objetos é determinada

O StorageGRID fornece opções para administradores de grade e usuários individuais de locatários para especificar por quanto tempo os objetos serão armazenados. Em geral, quaisquer instruções de retenção fornecidas por um usuário locatário têm precedência sobre as instruções de retenção fornecidas pelo administrador da grade.

Como os usuários locatários controlam a retenção de objetos

Os usuários locatários podem usar estes métodos para controlar por quanto tempo seus objetos são armazenados no StorageGRID:

- Se a configuração global do Bloqueio de Objeto S3 estiver habilitada para a grade, os usuários do locatário S3 poderão criar buckets com o Bloqueio de Objeto S3 habilitado e, em seguida, selecionar um **Período de retenção padrão** para cada bucket.
- Se a configuração global de Bloqueio de Objeto do S3 estiver habilitada para a grade, os usuários do locatário do S3 poderão criar buckets com o Bloqueio de Objeto do S3 habilitado e, em seguida, usar a API REST do S3 para especificar as configurações de retenção até a data e retenção legal para cada versão de objeto adicionada a esse bucket.
 - Uma versão de objeto que está sob retenção legal não pode ser excluída por nenhum método.
 - Antes que a data de retenção de uma versão do objeto seja atingida, essa versão não pode ser excluída por nenhum método.
 - Objetos em buckets com o S3 Object Lock habilitado são retidos pelo ILM "para sempre". No entanto, após atingir a data de retenção, uma versão do objeto pode ser excluída por uma solicitação do cliente ou pela expiração do ciclo de vida do bucket. Ver ["Gerenciar objetos com o S3 Object Lock"](#).
- Os usuários do locatário do S3 podem adicionar uma configuração de ciclo de vida aos seus buckets que especifica uma ação de expiração. Se houver um ciclo de vida de bucket, o StorageGRID armazenará um objeto até que a data ou o número de dias especificado na ação Expiração sejam atingidos, a menos que

o cliente exclua o objeto primeiro. Ver "[Criar configuração do ciclo de vida do S3](#)".

- Um cliente S3 pode emitir uma solicitação de exclusão de objeto. O StorageGRID sempre prioriza as solicitações de exclusão do cliente em relação ao ciclo de vida do bucket S3 ou ILM ao determinar se um objeto deve ser excluído ou mantido.

Como os administradores de grade controlam a retenção de objetos

Os administradores de grade podem usar estes métodos para controlar a retenção de objetos:

- Defina um período máximo de retenção do bloqueio de objeto S3 para cada locatário. Em seguida, os usuários locatários 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 (data de retenção do objeto).
- Crie instruções de posicionamento do ILM para controlar por quanto tempo os objetos são armazenados. Quando objetos são correspondidos por uma regra ILM, o StorageGRID armazena esses objetos até que o último período de tempo na regra ILM tenha decorrido. Os objetos são retidos indefinidamente se "para sempre" for especificado nas 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 para eliminação) são armazenadas e onde as cópias estão localizadas (nós de armazenamento ou pools de armazenamento em nuvem).

Como o ciclo de vida do bucket S3 e o ILM interagem

Quando um ciclo de vida de bucket do S3 é configurado, as ações de expiração do ciclo de vida substituem a política do ILM para objetos que correspondem ao filtro do ciclo de vida. Como resultado, um objeto pode ser retido na grade mesmo depois que quaisquer instruções do ILM para posicioná-lo tenham expirado.

Exemplos de retenção de objetos

Para entender melhor as interações entre o bloqueio de objeto do S3, as configurações do 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 que o ILM

ILM

Armazene duas cópias por 1 ano (365 dias)

Ciclo de vida do bucket

Expira objetos em 2 anos (730 dias)

Resultado

O StorageGRID armazena o objeto por 730 dias. O StorageGRID usa as configurações do ciclo de vida do bucket para determinar se um objeto deve ser excluído ou mantido.



Se o ciclo de vida do bucket especificar que os objetos devem ser mantidos por mais tempo do que o especificado pelo ILM, o StorageGRID continuará a usar 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 armazenadas no StorageGRID dos dias 366 a 730.

Exemplo 2: o ciclo de vida do bucket S3 expira 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

O StorageGRID exclui ambas as cópias do objeto após o dia 365.

Exemplo 3: A exclusão do cliente substitui o ciclo de vida do bucket e o ILM

ILM

Armazene duas cópias nos nós de armazenamento "para sempre"

Ciclo de vida do bucket

Expira objetos em 2 anos (730 dias)

Solicitação de exclusão de cliente

Emitido no dia 400

Resultado

O StorageGRID exclui ambas as cópias do objeto no dia 400 em resposta à solicitação de exclusão do cliente.

Exemplo 4: O bloqueio de objeto S3 substitui a solicitação de exclusão do cliente

Bloqueio de Objeto S3

A data de retenção para uma versão de objeto é 31/03/2026. Uma retenção legal não está em vigor.

Regra ILM compatível

Armazene duas cópias nos nós de armazenamento "para sempre"

Solicitação de exclusão de cliente

Emitido em 31/03/2024

Resultado

O StorageGRID não excluirá a versão do objeto porque a data de retenção ainda está a 2 anos de distância.

Como os objetos são excluídos

O StorageGRID pode excluir objetos em resposta direta a uma solicitação do cliente ou automaticamente como resultado da expiração do ciclo de vida de um bucket do S3 ou dos requisitos da política do ILM. Entender as diferentes maneiras pelas quais objetos podem ser excluídos e como o StorageGRID lida com solicitações de exclusão pode ajudar você a gerenciar objetos de forma mais eficaz.

O StorageGRID pode usar um dos dois métodos para excluir objetos:

- Exclusão síncrona: quando o 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 as cópias serem removidas.
- Os objetos são enfileirados para exclusão: quando o StorageGRID recebe uma solicitação de exclusão, o objeto é enfileirado para exclusão e o cliente é informado imediatamente que a exclusão foi bem-sucedida. Cópias de objetos são removidas posteriormente pelo processamento ILM em segundo plano.

Ao excluir objetos, o StorageGRID usa o método que otimiza o desempenho da exclusão, minimiza possíveis atrasos de exclusão e libera espaço mais rapidamente.

A tabela resume quando o StorageGRID usa cada método.

Método de execução da exclusão	Quando usado
Os objetos são colocados na fila para exclusão	Quando qualquer 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 do S3 foi atingido. ◦ O último período de tempo especificado em uma regra ILM expirou. Observação: Objetos em um bucket que tenha o Bloqueio de Objeto S3 habilitado não podem ser excluídos se estiverem sob retenção legal ou se uma data de retenção tiver sido especificada, mas ainda não tiver sido atingida. • Um cliente S3 solicita 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 a serem processados.

Quando clientes S3 fazem solicitações de exclusão, o StorageGRID começa adicionando objetos à fila de exclusão. Em seguida, ele alterna para executar a exclusão síncrona. Garantir que a fila de exclusão em segundo plano tenha objetos para processar permite que o StorageGRID processe exclusões de forma mais eficiente, especialmente para clientes de baixa simultaneidade, ao mesmo tempo que ajuda a evitar atrasos na exclusão de clientes.

Tempo necessário para excluir objetos

A maneira como o StorageGRID exclui objetos pode afetar o desempenho do sistema:

- Quando o StorageGRID executa uma exclusão síncrona, pode levar até 30 segundos para o StorageGRID retornar 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 o StorageGRID enfileira objetos para exclusão.

- Se você estiver monitorando de perto o desempenho da exclusão durante uma exclusão em massa, poderá notar que a taxa de exclusão parece ficar lenta depois que um certo número de objetos é excluído. Essa alteração ocorre quando o StorageGRID muda de enfileiramento de objetos para exclusão para execução de exclusão síncrona. A aparente redução na taxa de exclusão não significa que as cópias de objetos estão 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 objetos em vez de excluí-los usando ILM ou outros métodos. Em geral, o espaço é liberado mais rapidamente quando a exclusão é realizada pelos clientes porque 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 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 cópias de objetos são enfileiradas para remoção (para exclusões de clientes e outros métodos).

Como objetos versionados do S3 são excluídos

Quando o controle de versão está habilitado para um bucket do S3, o StorageGRID segue o comportamento do Amazon S3 ao responder a solicitações de exclusão, independentemente de essas solicitações virem de um cliente S3, da expiração do ciclo de vida de um bucket do S3 ou dos requisitos da política do ILM.

Quando os objetos são versionados, as solicitações de exclusão de objetos não excluem a versão atual do objeto e não liberam espaço. Em vez disso, uma solicitação de exclusão de objeto cria um marcador de exclusão de zero byte 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.

Mesmo que o objeto não tenha sido removido, o StorageGRID se comporta como se a versão atual do objeto não estivesse mais disponível. Solicitações para esse objeto retornam 404 Not Found. Entretanto, como os dados do objeto não atual não foram removidos, as solicitações que especificam uma versão não atual do objeto podem ser bem-sucedidas.

Para liberar espaço ao excluir objetos versionados ou para remover marcadores de exclusão, use um dos seguintes:

- **Solicitação do cliente S3:** especifique o ID da versão do objeto na solicitação DELETE Object do S3 (DELETE /object?versionId=ID). Tenha em mente que esta solicitação remove apenas cópias de objetos para a versão especificada (as outras versões ainda estão ocupando espaço).
- **Ciclo de vida do bucket:** Use o `NoncurrentVersionExpiration` ação na configuração do ciclo de vida do bucket. Quando o número de `NoncurrentDays` especificado é atingido, o StorageGRID remove permanentemente todas as cópias de versões de objetos não atuais. Essas versões de objetos não podem ser recuperadas.

O `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` especifica que o StorageGRID remove as versões mais antigas quando o valor `NoncurrentDays` tiver decorrido. O `NewerNoncurrentVersions` O limite substitui as regras do ciclo de vida fornecidas pelo ILM, o que significa que um objeto não atual com uma versão dentro do

NewerNoncurrentVersions o limite é mantido se o ILM solicitar sua exclusão.

Para remover marcadores de exclusão de objetos expirados, use o `Expiration` ação com uma das seguintes tags: `ExpiredObjectDeleteMarker` , `Days` , ou `Date` .

- **ILM:** ["Clonar uma política ativa"](#) e adicionar duas regras ILM à nova política:
 - Primeira regra: use "Horário não atual" como o horário 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 de objetos (em buckets do S3 com controle de versão habilitado)?"
 - Segunda regra: use **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** para corresponder aos marcadores de exclusão atuais. Os marcadores de exclusão são removidos somente quando um **período de tempo** de **dias** tiver passado e o criador de exclusão atual tiver expirado (não há versões não atuais).

- **Excluir objetos no bucket:** Use o gerenciador de inquilinos para ["excluir todas as versões do objeto"](#) , incluindo marcadores de exclusão, de um bucket.

Quando um objeto versionado é excluído, o StorageGRID cria um marcador de exclusão de zero byte como a versão atual do objeto. Todos os objetos e marcadores de exclusão devem ser removidos antes que um bucket versionado possa ser excluído.

- Os marcadores de exclusão criados no StorageGRID 11.7 ou anterior só podem ser removidos por meio de solicitações do cliente S3; eles não são removidos pelo ILM, pelas regras do ciclo de vida do bucket ou por objetos de exclusão em operações de bucket.
- Os marcadores de exclusão de um bucket criado no StorageGRID 11.8 ou posterior podem ser removidos por ILM, regras de ciclo de vida do bucket, objetos de exclusão em operações de bucket ou uma exclusão explícita do cliente S3.

Informações relacionadas

- ["Usar API REST do S3"](#)
- ["Exemplo 4: regras e políticas do ILM para objetos versionados do S3"](#)

Criar e atribuir níveis de armazenamento

Os níveis de armazenamento identificam o tipo de armazenamento usado por um nó de armazenamento. Você pode criar níveis de armazenamento se quiser que as regras do ILM coloquem determinados objetos em determinados nós de armazenamento.

Antes de começar

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

Sobre esta tarefa

Quando você instala o StorageGRID pela primeira vez, o nível de armazenamento **Padrão** é atribuído automaticamente a cada Nó de Armazenamento no seu sistema. Conforme necessário, você pode definir opcionalmente níveis de armazenamento personalizados e atribuí-los a diferentes nós de armazenamento.

O uso de níveis de armazenamento personalizados permite que você crie pools de armazenamento ILM que contêm apenas um tipo específico de nó de armazenamento. Por exemplo, você pode querer que determinados objetos sejam armazenados em seus nós de armazenamento mais rápidos, como os dispositivos de armazenamento all-flash StorageGRID .



Os nós de armazenamento podem ser configurados durante a instalação para conter apenas metadados de objetos e não dados de objetos. Nós de armazenamento somente de metadados não podem receber uma classificação de armazenamento. Para obter mais informações, consulte ["Tipos de nós de armazenamento"](#) .

Se o grau de armazenamento não for uma preocupação (por exemplo, todos os nós de armazenamento forem idênticos), você pode pular este procedimento e usar a seleção **inclui todos os graus de armazenamento** para o grau de armazenamento quando você ["criar pools de armazenamento"](#) . Usar essa seleção garante que o pool de armazenamento incluirá todos os nós de armazenamento no site, independentemente do seu nível de armazenamento.



Não crie mais níveis de armazenamento do que o necessário. Por exemplo, não crie um nível de armazenamento para cada nó de armazenamento. Em vez disso, atribua cada grau de armazenamento a dois ou mais nós. Os níveis de armazenamento atribuídos a apenas um nó podem causar atrasos no ILM se esse nó ficar indisponível.

Passos

1. Selecione **ILM > Níveis de armazenamento**.
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 você precisar modificar um rótulo salvo, selecione **Editar*** e selecione ***Aplicar alterações**.



Você não pode excluir notas de armazenamento.

3. Atribuir novos níveis de armazenamento aos nós de armazenamento:

a. Localize o nó de armazenamento na lista LDR e selecione seu ícone ***Editar*** .

b. Selecione o nível de armazenamento apropriado 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 uma classificação de armazenamento a um determinado nó de armazenamento apenas uma vez. Um nó de armazenamento recuperado de uma falha mantém o grau de armazenamento atribuído anteriormente. Não altere esta atribuição depois que a política ILM for ativada. Se a atribuição for alterada, os dados serão armazenados com base no novo grau de armazenamento.

a. Selecione **Aplicar alterações**.

Use pools de armazenamento

O que é um pool de armazenamento?

Um pool de armazenamento é um agrupamento lógico de nós de armazenamento.

Quando você instala o StorageGRID, um pool de armazenamento por site é criado automaticamente. Você pode configurar pools de armazenamento adicionais conforme necessário para suas necessidades de armazenamento.



Os nós de armazenamento podem ser configurados durante a instalação para conter dados de objetos e metadados de objetos, ou apenas metadados de objetos. Nós de armazenamento somente de metadados não podem ser usados em pools de armazenamento. Para obter mais informações, consulte "[Tipos de nós de armazenamento](#)".

Os pools de armazenamento têm dois atributos:

- **Grau de armazenamento:** Para nós de armazenamento, o desempenho relativo do armazenamento de suporte.
- **Local:** O data center onde os objetos serão armazenados.

Pools de armazenamento são usados em regras de ILM para determinar onde os dados do objeto são armazenados e o tipo de armazenamento usado. Ao configurar regras de ILM para replicação, você seleciona um ou mais pools de armazenamento.

Diretrizes para criação de pools de armazenamento

Configure e use pools de armazenamento para proteger contra perda de dados distribuindo dados entre vários sites. Cópias replicadas e cópias codificadas para eliminação exigem configurações de pool de armazenamento diferentes.

Ver ["Exemplos de ativação da proteção contra perda de site usando replicação e codificação de eliminação"](#) .

Diretrizes para todos os pools de armazenamento

- Mantenha as configurações do pool de armazenamento o mais simples possível. Não crie mais pools de armazenamento do que o necessário.
- Crie pools de armazenamento com o maior número possível de nós. Cada pool de armazenamento deve conter dois ou mais nós. Um pool de armazenamento com nós insuficientes pode causar atrasos no ILM se um nó ficar indisponível.
- Evite criar ou usar pools de armazenamento que se sobreponham (contenham um ou mais nós iguais). Se os pools de armazenamento se sobrepuserem, mais de uma cópia dos dados do objeto poderá ser salva no mesmo nó.
- Em geral, não use o pool de armazenamento All Storage Nodes (StorageGRID 11.6 e anteriores) ou 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 desejado.

Diretrizes para pools de armazenamento usados para cópias replicadas

- Para proteção contra perda de site usando ["replicação"](#) , especifique um ou mais pools de armazenamento específicos do site no ["instruções de posicionamento para cada regra ILM"](#) .

Um pool de armazenamento é criado automaticamente para cada site durante a instalação do StorageGRID .

Usar um pool de armazenamento para cada site garante que cópias de objetos replicadas 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 armazenamento que contenha somente o novo site. Então, ["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 armazenamento, o sistema distribuirá as cópias para equilibrar o uso do disco entre os pools.
- Se os pools de armazenamento se sobrepuserem (contiverem os mesmos nós de armazenamento), 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 nós de armazenamento.

Diretrizes para pools de armazenamento usados para cópias codificadas por eliminação

- Para proteção contra perda de site usando ["codificação de apagamento"](#) , crie pools de armazenamento que consistam em pelo menos três sites. Se um pool de armazenamento incluir apenas dois sites, você não poderá usá-lo para codificação de eliminação. Não há esquemas de codificação de eliminação disponíveis para um pool de armazenamento com dois sites.
- O número de nós de armazenamento e sites contidos no pool de armazenamento determinam quais ["esquemas de codificação de apagamento"](#) estão disponíveis.

- Se possível, um pool de armazenamento deve incluir mais do que o número mínimo de nós de armazenamento necessários para o esquema de codificação de eliminação selecionado. Por exemplo, se você usar um esquema de codificação de eliminação 6+3, deverá ter pelo menos nove nós de armazenamento. No entanto, é recomendável ter pelo menos um nó de armazenamento adicional por site.
- Distribua os nós de armazenamento entre os sites da maneira mais uniforme possível. Por exemplo, para dar suporte a um esquema de codificação de eliminação 6+3, configure um pool de armazenamento que inclua pelo menos três nós de armazenamento em três sites.
- Se você tiver requisitos de alta taxa de transferência, não é recomendável usar um pool de armazenamento que inclua vários sites se a latência da rede entre os sites for maior que 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 diminuição na taxa de transferência da rede TCP.

A redução na taxa de transferência afeta as taxas máximas alcançáveis de ingestão e recuperação de objetos (quando Balanceado ou Estrito são selecionados como comportamento de ingestão) ou pode levar a pendências na fila do ILM (quando Confirmação dupla é selecionado como comportamento de ingestão). Ver "[Comportamento de ingestão de regras do ILM](#)".



Se sua grade incluir apenas um site, você não poderá usar o pool de armazenamento. Todos os nós de armazenamento (StorageGRID 11.6 e anteriores) ou o site Todos os sites em um perfil de codificação de eliminação. Esse comportamento evita que o perfil se torne inválido se um segundo site for adicionado.

Habilitar proteção contra perda de site

Se a sua implantação do StorageGRID incluir mais de um site, você poderá usar a replicação e a codificação de eliminação com pools de armazenamento configurados adequadamente para habilitar a proteção contra perda de site.

A replicação e a codificação de eliminação exigem diferentes configurações de pool de armazenamento:

- Para usar a replicação para proteção contra perda de site, use os pools de armazenamento específicos do site que são criados automaticamente durante a instalação do StorageGRID. Em seguida, crie regras ILM com "[instruções de posicionamento](#)" que especificam vários pools de armazenamento para que uma cópia de cada objeto seja colocada em cada site.
- Para usar a codificação de eliminação para proteção contra perda de site, "[criar pools de armazenamento que consistem em vários sites](#)". Em seguida, crie regras de ILM que usem um pool de armazenamento composto por vários sites e qualquer esquema de codificação de eliminação 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](#)".

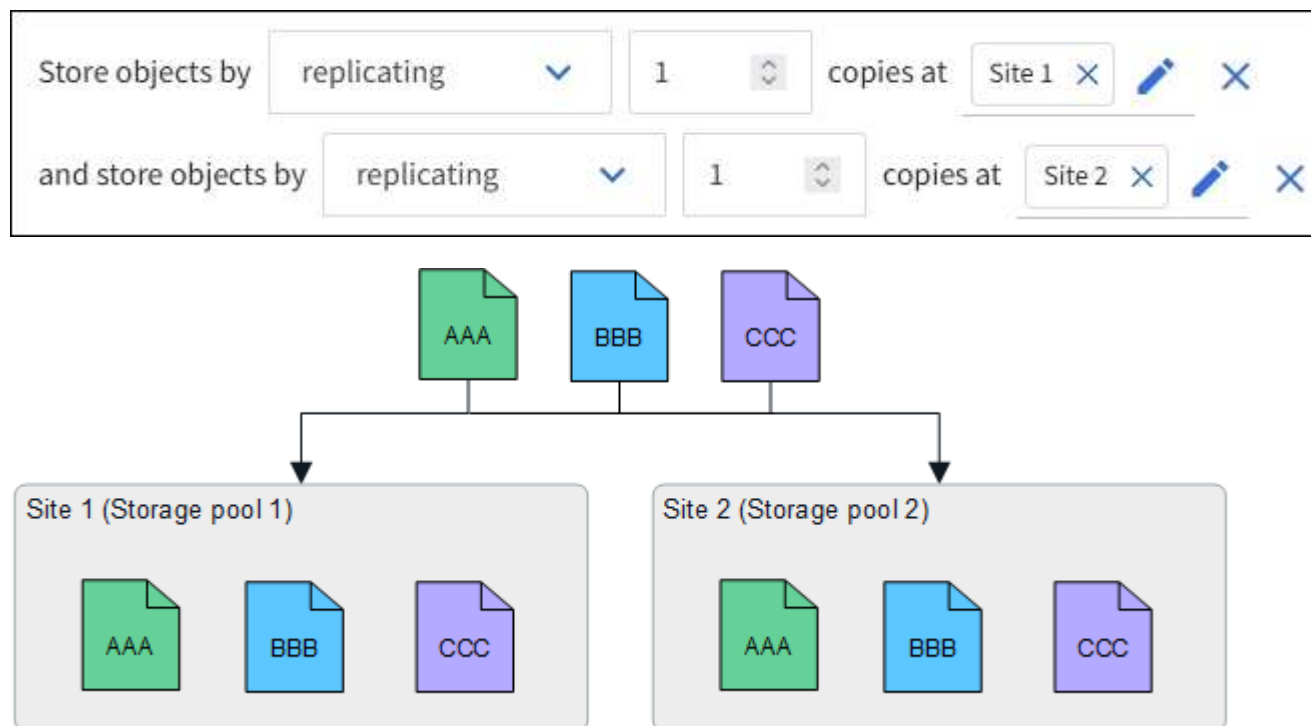
Exemplo de replicação

Por padrão, um pool de armazenamento é criado para cada site durante a instalação do StorageGRID. Ter pools de armazenamento que consistem em apenas um site permite que você configure regras de ILM que usam replicação para proteção contra perda de site. Neste exemplo:

- O pool de armazenamento 1 contém o Site 1
- O pool de armazenamento 2 contém o Site 2
- A regra ILM contém dois posicionamentos:

- Armazene objetos replicando 1 cópia no Site 1
- Armazene objetos replicando 1 cópia no Site 2

Posicionamentos de regras do ILM:



Se um site for perdido, cópias dos objetos estarão disponíveis no outro site.

Exemplo de codificação de apagamento

Ter pools de armazenamento que consistem em mais de um site por pool de armazenamento permite que você configure regras de ILM que usam codificação de eliminação para proteção contra perda de site. Neste exemplo:

- O pool de armazenamento 1 contém os sites 1 a 3
- A regra ILM contém um posicionamento: Armazenar objetos por codificação de eliminação usando um esquema EC 4+2 no pool de armazenamento 1, que contém três sites

Posicionamentos de regras do ILM:



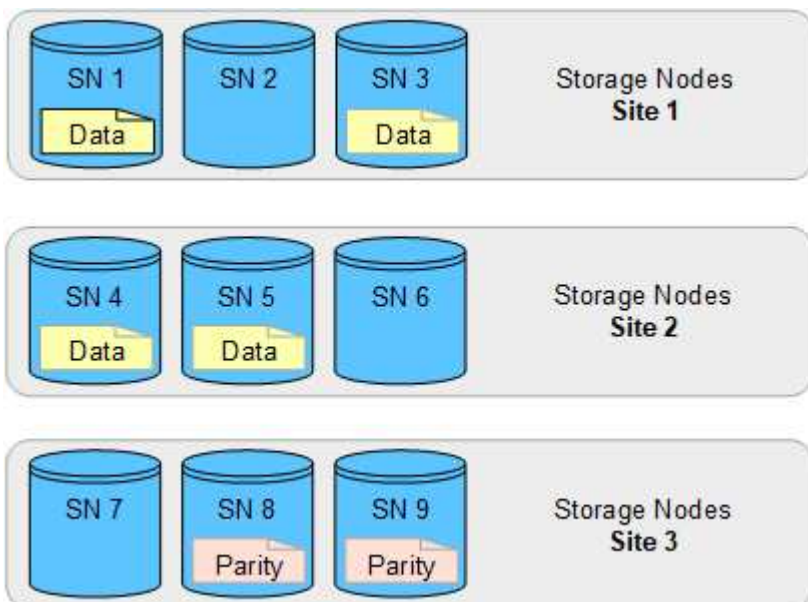
Neste exemplo:

- A regra ILM usa um esquema de codificação de apagamento 4+2.
- Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados do objeto.
- Cada um dos seis fragmentos é armazenado em um nó diferente em três locais do data center para fornecer proteção de dados em caso de falhas de nó ou perda de local.

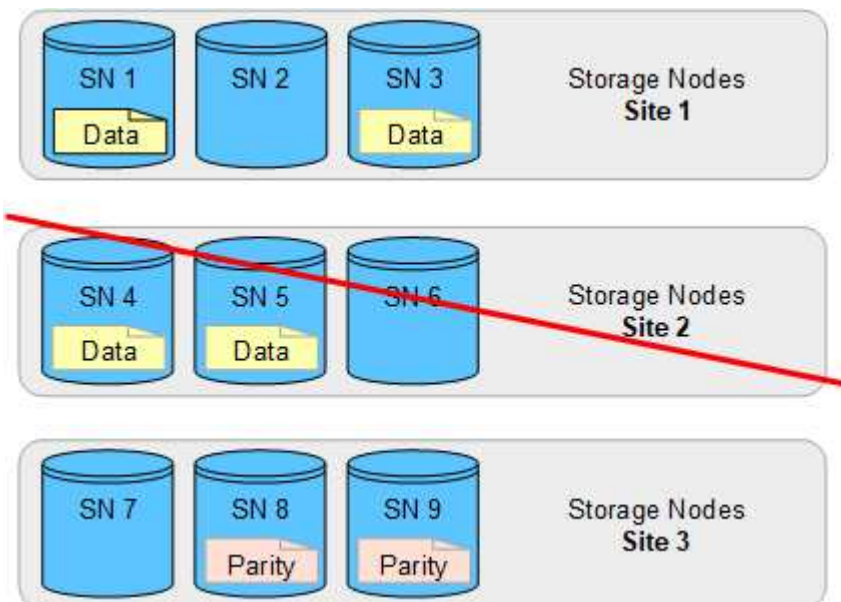


A codificação de eliminação é permitida em pools de armazenamento que contêm qualquer número de sites *exceto* dois sites.

Regra ILM usando esquema de codificação de apagamento 4+2:



Se um site for perdido, os dados ainda poderão ser recuperados:



Criar um pool de armazenamento

Crie pools de armazenamento para determinar onde o sistema StorageGRID armazena dados de objetos e o tipo de armazenamento usado. Cada pool de armazenamento inclui um ou mais sites e um ou mais níveis de armazenamento.



Quando você instala o StorageGRID 11.9 em uma nova grade, pools de armazenamento são criados automaticamente para cada site. No entanto, se você instalou inicialmente o StorageGRID 11.6 ou anterior, os pools de armazenamento não serão criados automaticamente para cada site.

Se você deseja criar pools de armazenamento em nuvem para armazenar dados de objetos fora do seu sistema StorageGRID, consulte o ["informações sobre o uso de pools de armazenamento em nuvem"](#).

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).
- Você revisou as diretrizes para criar pools de armazenamento.

Sobre esta tarefa

Os pools de armazenamento determinam onde os dados do objeto são armazenados. O número de pools de armazenamento necessários depende do número de sites na sua grade e dos tipos de cópias que você deseja: replicadas ou codificadas para eliminação.

- Para replicação e codificação de eliminação de site único, crie um pool de armazenamento para cada site. Por exemplo, se você quiser armazenar cópias de objetos replicadas em três sites, crie três pools de armazenamento.
- Para codificação de eliminação em três ou mais sites, crie um pool de armazenamento que inclua uma entrada para cada site. Por exemplo, se você quiser apagar objetos de código em três sites, crie um pool de armazenamento.



Não inclua o site Todos os sites em um pool de armazenamento que será usado em um perfil de codificação de eliminação. Em vez disso, adicione uma entrada separada ao pool de armazenamento para cada site que armazenará dados codificados para eliminação. Ver esta [etapa](#) por exemplo.

- Se você tiver mais de um nível de armazenamento, não crie um pool de armazenamento que inclua diferentes níveis de armazenamento em um único local. Veja o ["Diretrizes para criação de pools de armazenamento"](#).

Passos

1. Selecione **ILM > Pools de armazenamento**.

A guia Pools de armazenamento lista todos os pools de armazenamento definidos.



Para novas instalações do StorageGRID 11.6 ou anterior, o pool de armazenamento Todos os nós de armazenamento é atualizado automaticamente sempre que você adiciona novos sites de data center. Não use esse pool em regras de ILM.

2. Para criar um novo pool de armazenamento, selecione **Criar**.
3. Insira um nome exclusivo para o pool de armazenamento. Use um nome que seja fácil de identificar ao configurar perfis de codificação de eliminação e regras de ILM.
4. Na lista suspensa **Site**, selecione um site para este pool de armazenamento.

Quando você seleciona um site, o número de nós de armazenamento na tabela é atualizado automaticamente.

Em geral, não use o site Todos os Sites em nenhum pool de armazenamento. As regras do ILM que usam um pool de armazenamento Todos os Sites colocam objetos em qualquer site disponível, dando a você menos controle sobre o posicionamento dos objetos. Além disso, um pool de armazenamento de Todos os Sites usa os Nós de Armazenamento em um novo site imediatamente, o que pode não ser o comportamento esperado.

5. Na lista suspensa **Grau de armazenamento**, selecione o tipo de armazenamento que será usado se uma regra de ILM usar esse pool de armazenamento.

O grau de armazenamento, *inclui todos os graus de armazenamento*, inclui todos os nós de armazenamento no local selecionado. Se você criou níveis de armazenamento adicionais para os Nós de Armazenamento na sua grade, eles serão listados no menu suspenso.

6. Se você quiser usar o pool de armazenamento em um perfil de codificação de eliminação de vários sites, selecione **Adicionar mais nós** para adicionar uma entrada para cada site ao pool de armazenamento.



Você será avisado se adicionar mais de uma entrada com diferentes níveis de armazenamento para um site.

Para remover uma entrada, selecione o ícone de exclusão .

7. Quando estiver satisfeito com suas seleções, selecione **Salvar**.

O novo pool de armazenamento é adicionado à lista.

Ver detalhes do pool de armazenamento

Você pode visualizar os detalhes de um pool de armazenamento para determinar onde ele é usado e ver quais nós e níveis de armazenamento estão incluídos.

Antes de começar

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

Passos

1. Selecione **ILM > Pools de armazenamento**.

A tabela Pools de armazenamento inclui as seguintes informações para cada pool de armazenamento que inclui nós de armazenamento:

- **Nome:** O nome de exibição exclusivo do pool de armazenamento.
- **Contagem de nós:** O número de nós no pool de armazenamento.
- **Uso de armazenamento:** a porcentagem do espaço total utilizável que foi usada para dados de objeto neste nó. Este valor não inclui metadados do objeto.
- **Capacidade total:** O tamanho do pool de armazenamento, que é igual à quantidade total de espaço utilizável para dados de objeto para todos os nós no pool de armazenamento.
- **Uso do ILM:** como o pool de armazenamento está sendo usado atualmente. Um pool de armazenamento pode não estar sendo utilizado ou pode estar sendo usado em uma ou mais regras de ILM, perfis de codificação de eliminação ou ambos.

2. Para visualizar detalhes de um pool de armazenamento específico, selecione seu nome.

A página de detalhes do pool de armazenamento é exibida.

3. Veja a aba **Nós** para saber mais sobre os Nós de Armazenamento incluídos no pool de armazenamento.

A tabela inclui as seguintes informações para cada nó:

- Nome do nó
- Nome do site
- Grau de armazenamento
- Uso de armazenamento: a porcentagem do espaço total utilizável para dados de objeto que foi usada para o nó de armazenamento.



O mesmo valor de uso de armazenamento (%) também é mostrado no gráfico Armazenamento usado - Dados do objeto para cada nó de armazenamento (selecione **NÓS > Nó de armazenamento > Armazenamento**).

4. Veja a aba **Uso do ILM** para determinar se o pool de armazenamento está sendo usado atualmente em alguma regra do ILM ou perfil de codificação de eliminação.
5. Opcionalmente, acesse a **página de regras do ILM** para saber mais e gerenciar quaisquer regras que usem o pool de armazenamento.

Veja o "[instruções para trabalhar com regras ILM](#)".

Editar pool de armazenamento

Você pode editar um pool de armazenamento para alterar seu nome ou atualizar sites e níveis de armazenamento.

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você tem "[permissões de acesso específicas](#)".
- Você revisou o "[diretrizes para criação de pools de armazenamento](#)".
- Se você planeja editar um pool de armazenamento usado por uma regra na política ILM ativa, você deve considerar 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 armazenamento usado na política de ILM ativa, esteja ciente de que os nós de armazenamento 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 de ILM depois de salvar o pool de armazenamento editado.

Passos

1. Selecione **ILM > Pools de armazenamento**.
2. Marque a caixa de seleção do pool de armazenamento que você deseja editar.

Não é possível editar o pool de armazenamento Todos os nós de armazenamento (StorageGRID 11.6 e anteriores).

3. Selecione **Editar**.
4. Conforme necessário, altere o nome do pool de armazenamento.
5. Conforme necessário, selecione outros locais e níveis de armazenamento.

Você não poderá alterar o site ou o nível de armazenamento se o pool de armazenamento for usado em um perfil de codificação de eliminação e a alteração fizer com que o esquema de codificação de eliminação se torne inválido. Por exemplo, se um pool de armazenamento usado em um perfil de codificação de eliminação atualmente inclui um nível de armazenamento com apenas um site, você não poderá usar um nível de armazenamento com dois sites porque a alteração tornaria o esquema de codificação de eliminação inválido.



Adicionar ou remover sites de um pool de armazenamento existente não moverá nenhum dado codificado para eliminação existente. Se quiser mover os dados existentes do site, você deverá criar um novo pool de armazenamento e um perfil 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 armazenamento usado na política de ILM ativa, ative uma nova política de ILM para forçar o StorageGRID a usar o novo site ou nível de armazenamento. Por exemplo, clone sua política de ILM existente e depois ative o clone. Ver ["Trabalhar com regras e políticas do ILM"](#).

Remover um pool de armazenamento

Você pode remover um pool de armazenamento que não está sendo usado.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem o ["permissões de acesso necessárias"](#).

Passos

1. Selecione **ILM > Pools de armazenamento**.
2. Observe a coluna de uso do ILM na tabela para determinar se você pode remover o pool de armazenamento.

Não é possível remover um pool de armazenamento se ele estiver sendo usado em uma regra de ILM ou em um perfil de codificação de eliminação. Conforme necessário, selecione **nome do pool de armazenamento > uso do ILM** para determinar onde o pool de armazenamento é usado.

3. Se o pool de armazenamento que você deseja remover não estiver sendo usado, marque a caixa de seleção.
4. Selecione **Remover**.
5. Selecione **OK**.

Use pools de armazenamento em nuvem

O que é um pool de armazenamento em nuvem?

Um pool de armazenamento 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 um armazenamento em nuvem de menor custo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou a camada de acesso Archive no armazenamento de Blobs do Microsoft Azure. Ou você pode querer manter um backup em nuvem dos objetos StorageGRID para melhorar a recuperação de desastres.

Da perspectiva do ILM, um pool de armazenamento em nuvem é semelhante a um pool de armazenamento. Para armazenar objetos em qualquer local, selecione o pool ao criar as instruções de posicionamento para uma regra ILM. No entanto, enquanto os pools de armazenamento consistem em nós de armazenamento dentro do sistema StorageGRID , um pool de armazenamento em nuvem consiste em um bucket externo (S3) ou contêiner (armazenamento de Blobs do Azure).

A tabela compara pools de armazenamento com pools de armazenamento em nuvem e mostra as semelhanças e diferenças de alto nível.

	Pool de armazenamento	Pool de armazenamento em nuvem
Como é criado?	Usando a opção ILM > Pools de armazenamento no Grid Manager.	Usando a opção ILM > Pools de armazenamento > Pools de armazenamento em nuvem no Grid Manager. Você deve configurar o bucket ou contêiner externo antes de criar o Cloud Storage Pool.
Quantas piscinas você pode criar?	Ilimitado.	Até 10.

	Pool de armazenamento	Pool de armazenamento em nuvem
Onde os objetos são armazenados?	Em um ou mais nós de armazenamento dentro do StorageGRID.	Em um bucket do Amazon S3, contêiner de armazenamento de Blobs do Azure ou Google Cloud externo ao sistema StorageGRID . Se o Cloud Storage Pool for um bucket do Amazon S3: • Opcionalmente, você pode configurar um ciclo de vida de bucket para fazer a transição de objetos para armazenamento de baixo custo e longo prazo, como o Amazon S3 Glacier ou o S3 Glacier Deep Archive. O sistema de armazenamento externo deve oferecer suporte à classe de armazenamento Glacier e à API S3 RestoreObject. • Você pode criar pools de armazenamento em nuvem para uso com o AWS Commercial Cloud Services (C2S), que oferece suporte à AWS Secret Region. Se o Cloud Storage Pool for um contêiner de armazenamento de Blobs do Azure, o StorageGRID fará a transição do objeto para a camada de Arquivo. Observação: Em geral, não configure o gerenciamento do ciclo de vida do armazenamento de Blobs do Azure para o contêiner usado para um Pool de Armazenamento em Nuvem. 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 de ILM nas políticas de ILM ativas.	Uma regra de ILM nas políticas de ILM ativas.
Qual método de proteção de dados é usado?	Codificação de replicação ou eliminação.	Replicação.
Quantas cópias de cada objeto são permitidas?	Múltiplo.	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 armazenamento em nuvem ao mesmo tempo.
Quais são as vantagens?	Os objetos são rapidamente acessíveis a qualquer momento.	Armazenamento de baixo custo. Observação: os dados do FabricPool não podem ser hierarquizados em pools de armazenamento em nuvem.

Ciclo de vida de um objeto de pool de armazenamento em nuvem

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 armazenamento em nuvem

As etapas descrevem os estágios do ciclo de vida de um objeto armazenado em um pool de armazenamento em nuvem do S3.



"Glacier" refere-se à classe de armazenamento Glacier e à classe de armazenamento Glacier Deep Archive, com uma exceção: a classe de armazenamento Glacier Deep Archive não oferece suporte à camada de restauração Expedited. Somente a recuperação em massa ou padrão é suportada.



O Google Cloud Platform (GCP) oferece suporte à recuperação de objetos de armazenamento de longo prazo sem exigir uma operação de restauração POST.

1. Objeto armazenado no StorageGRID

Para iniciar o ciclo de vida, um aplicativo cliente armazena um objeto no StorageGRID.

2. Objeto movido para o S3 Cloud Storage Pool

- Quando o objeto é correspondido por uma regra do ILM que usa um S3 Cloud Storage Pool como seu local de posicionamento, o 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 transferido para o armazenamento Glacier.

3. Objeto transferido para Glacier (estado não recuperável)

- Opcionalmente, o objeto pode ser transferido para o armazenamento Glacier. Por exemplo, o bucket S3 externo pode usar a configuração do ciclo de vida para fazer a transição de um objeto para o armazenamento Glacier imediatamente ou após alguns dias.



Se quiser fazer a transição de objetos, você deve criar uma configuração de ciclo de vida para o bucket S3 externo e usar uma solução de armazenamento que implemente a classe de armazenamento Glacier e suporte a API S3 RestoreObject.

- Durante a transição, o aplicativo cliente pode usar uma solicitação S3 HeadObject para monitorar o status do objeto.

4. Objeto restaurado do armazenamento Glacier

Se um objeto tiver sido transferido para o armazenamento Glacier, o aplicativo cliente poderá emitir uma solicitação S3 RestoreObject para restaurar uma cópia recuperável para o S3 Cloud Storage Pool. A solicitação especifica por quantos dias a cópia deve ficar disponível no Cloud Storage Pool e o nível de acesso a dados a ser usado para a operação de restauração (Acelerado, Padrão ou em Massa). Quando a data de expiração da cópia recuperável for atingida, a cópia será automaticamente retornada ao estado não recuperável.



Se uma ou mais cópias do objeto também existirem em nós de armazenamento dentro do StorageGRID, não há necessidade de 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 é restaurado, o aplicativo cliente pode emitir uma solicitação GetObject para recuperar o objeto restaurado.

Azure: Ciclo de vida de um objeto de pool de armazenamento em nuvem

As etapas descrevem os estágios do ciclo de vida de um objeto armazenado em um Pool de Armazenamento em Nuvem do Azure.

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 armazenamento em nuvem do Azure

Quando o objeto é correspondido por uma regra de ILM que usa um Pool de Armazenamento em Nuvem do Azure como seu local de posicionamento, o StorageGRID move o objeto para o contêiner de armazenamento de Blobs do Azure externo especificado pelo Pool de Armazenamento em Nuvem.

3. Objeto transferido para o nível de arquivo (estado não recuperável)

Imediatamente após mover o objeto para o Pool de Armazenamento em Nuvem do Azure, o StorageGRID faz a transição automática do objeto para a camada de Arquivo de Armazenamento de Blobs do Azure.

4. Objeto restaurado do nível de arquivo

Se um objeto tiver sido transferido para a camada de arquivamento, o aplicativo cliente poderá emitir uma solicitação S3 RestoreObject para restaurar uma cópia recuperável para o pool de armazenamento em nuvem do Azure.

Quando o StorageGRID recebe o RestoreObject, ele temporariamente faz a transição do objeto para a camada Cool do armazenamento de Blobs do Azure. Assim que a data de expiração na solicitação RestoreObject for atingida, o StorageGRID fará a transição do objeto de volta para a camada de arquivamento.



Se uma ou mais cópias do objeto também existirem em nós de armazenamento dentro do StorageGRID, não haverá necessidade de restaurar o objeto da camada de acesso de arquivamento 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 no Pool de Armazenamento em Nuvem do Azure, o aplicativo cliente poderá emitir uma solicitação GetObject para recuperar o objeto restaurado.

Informações relacionadas

["Usar API REST do S3"](#)

Quando usar pools de armazenamento em nuvem

Usando pools de armazenamento em nuvem, você pode fazer backup ou hierarquizar dados em um local externo. Além disso, você pode fazer backup ou hierarquizar dados 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 poderão ser usados para atender às solicitações do cliente. No entanto, talvez seja necessário emitir uma solicitação S3 RestoreObject para acessar a cópia do objeto de backup no Cloud Storage Pool.

Os dados do objeto em um Cloud Storage Pool também podem ser usados para recuperar dados perdidos do StorageGRID devido a uma falha no volume de armazenamento ou no nó de armazenamento. Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID restaurará temporariamente o objeto e criará uma nova cópia no nó de armazenamento recuperado.

Para implementar uma solução de backup:

1. Crie um único pool de armazenamento em nuvem.
2. Configure uma regra de ILM que armazene simultaneamente cópias de objetos em nós de armazenamento (como cópias replicadas ou codificadas para eliminação) e uma única cópia de objeto no pool de armazenamento em nuvem.
3. Adicione a regra à sua política de ILM. Em seguida, simule e ative a política.

Dados em camadas do StorageGRID para 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 manter, mas espera acessá-los raramente, ou nunca. Você pode usar um pool de armazenamento em nuvem para hierarquizar os objetos em armazenamentos de menor custo e liberar espaço no StorageGRID.

Para implementar uma solução em camadas:

1. Crie um único pool de armazenamento em nuvem.
2. Configure uma regra de ILM que mova objetos raramente usados dos nós de armazenamento para o pool de armazenamento em nuvem.
3. Adicione a regra à sua política de ILM. Em seguida, simule e ative a política.

Manter vários endpoints de nuvem

Você pode configurar vários pontos de extremidade do Cloud Storage Pool se quiser hierarquizar ou fazer backup de dados de objetos em mais de uma nuvem. Os filtros nas suas regras do ILM permitem que você especifique quais objetos são armazenados em cada pool do Cloud Storage. Por exemplo, você pode querer armazenar objetos de alguns locatários ou buckets no Amazon S3 Glacier e objetos de outros locatários ou buckets no armazenamento de Blobs do Azure. Ou você pode querer mover dados entre o Amazon S3 Glacier e o armazenamento de Blobs do Azure.



Ao usar vários pontos de extremidade do Cloud Storage Pool, lembre-se de que um objeto pode ser armazenado em apenas um Cloud Storage Pool por vez.

Para implementar vários endpoints de nuvem:

1. Crie até 10 pools de armazenamento em nuvem.
2. Configure regras de ILM para armazenar os dados de objeto apropriados no momento apropriado em cada pool de armazenamento em nuvem. Por exemplo, armazene objetos do bucket A no Cloud Storage Pool A e armazene objetos do bucket B no Cloud Storage Pool B. Ou armazene objetos no Cloud Storage Pool A por um determinado período e depois mova-os para o Cloud Storage Pool B.
3. Adicione as regras à sua política de ILM. Em seguida, simule e ative a política.

Considerações sobre pools de armazenamento em nuvem

Se você planeja usar um Cloud Storage Pool para mover objetos para fora do sistema StorageGRID , revise as considerações para configurar e usar Cloud Storage Pools.

Considerações gerais

- Em geral, o armazenamento de arquivo em nuvem, como o Amazon S3 Glacier ou o armazenamento de Blobs do Azure, é um local barato para armazenar dados de objetos. No entanto, os custos para recuperar dados do armazenamento de arquivos em nuvem são relativamente altos. Para atingir o menor custo geral, você deve considerar quando e com que frequência acessará os objetos no Cloud Storage Pool. O uso de um pool de armazenamento em nuvem é recomendado apenas para conteúdo que você espera acessar com pouca frequência.
- O uso de Cloud Storage Pools com FabricPool não é suportado 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 pools de armazenamento em nuvem.
- Se o bucket S3 de destino para um pool de armazenamento em nuvem tiver o bloqueio de objeto S3 habilitado, a tentativa de configurar a replicação do bucket (PutBucketReplication) falhará com um erro AccessDenied.
- As seguintes combinações de plataforma, autenticação e protocolo com bloqueio de objeto S3 não são suportadas para pools de armazenamento em nuvem:
 - **Plataformas:** Google Cloud Platform e Azure
 - **Tipos de autenticação:** Funções do IAM em qualquer lugar e acesso anônimo
 - **Protocolo:** HTTP

Considerações sobre as portas usadas para pools de armazenamento em nuvem

Para garantir que as regras do ILM possam mover objetos de e para o Pool de Armazenamento em Nuvem especificado, você deve configurar a rede ou redes que contêm os Nós de Armazenamento do seu sistema. Você deve garantir que as seguintes portas possam se comunicar com o Cloud Storage Pool.

Por padrão, os pools de armazenamento em nuvem 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 pool de armazenamento em nuvem.

Se você usar um servidor proxy não transparente, você também deve [configurar um proxy de armazenamento](#) para permitir que mensagens sejam enviadas para terminais externos, como um terminal na Internet.

Considerações sobre custos

O acesso ao armazenamento 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 você espera mover entre o StorageGRID e a nuvem usando o Cloud Storage Pool.

Quando o StorageGRID se conecta ao ponto de extremidade externo do Cloud Storage Pool, ele emite várias solicitações para monitorar a conectividade e garantir que possa executar as operações necessárias. Embora alguns custos adicionais sejam associados a essas solicitações, o custo de monitoramento de um pool de armazenamento em nuvem deve ser apenas uma pequena fração do custo geral de armazenamento de objetos no S3 ou no Azure.

Custos mais significativos podem ser incorridos se você precisar mover objetos de um ponto de extremidade externo do Cloud Storage Pool de volta para o StorageGRID. Os objetos podem ser movidos de volta para o StorageGRID em qualquer um destes casos:

- A única cópia do objeto está em um pool de armazenamento em nuvem e você decide armazená-lo no StorageGRID. Nesse caso, você reconfigura suas regras e políticas de ILM. Quando ocorre a avaliação do ILM, o StorageGRID emite várias solicitações para recuperar o objeto do Cloud Storage Pool. O StorageGRID então cria o número especificado de cópias replicadas ou codificadas para eliminação localmente. Depois que o objeto é movido de volta para StorageGRID, a cópia no Cloud Storage Pool é excluída.
- Objetos são perdidos devido à falha do nó de armazenamento. Se a única cópia restante de um objeto estiver em um pool de armazenamento em nuvem, o StorageGRID restaurará temporariamente o objeto e criará uma nova cópia no nó de armazenamento recuperado.



Quando objetos são movidos de volta para o StorageGRID de um Cloud Storage Pool, o StorageGRID emite várias solicitações ao ponto de extremidade 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 prazo e dos custos associados.

S3: Permissões necessárias para o bucket do Cloud Storage Pool

As políticas para o bucket S3 externo usado para um Cloud Storage Pool devem conceder permissão ao StorageGRID para mover um objeto para o bucket, obter o status de um objeto, restaurar um objeto do armazenamento Glacier quando necessário e muito mais. O ideal é que o StorageGRID tenha acesso de controle total ao bucket(`s3:*`); no entanto, se isso não for possível, a política de 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 o StorageGRID e o bucket S3 externo especificado no Cloud Storage Pool é controlada pelas regras do ILM e pelas políticas ativas do ILM no StorageGRID. Em contraste, a transição de objetos do bucket S3 externo especificado no Cloud Storage Pool para o Amazon S3 Glacier ou S3 Glacier Deep Archive (ou para uma solução de armazenamento que implementa a classe de armazenamento Glacier) é controlada pela configuração do ciclo de vida desse bucket.

Se você quiser fazer a transição de objetos do Cloud Storage Pool, crie a configuração de ciclo de vida apropriada no bucket externo do S3 e use uma solução de armazenamento que implemente a classe de armazenamento Glacier e ofereça suporte à API RestoreObject do S3.

Por exemplo, suponha que você queira que todos os objetos movidos do StorageGRID para o Cloud Storage Pool sejam transferidos para o armazenamento Amazon S3 Glacier imediatamente. Você criaria uma configuração de ciclo de vida no bucket S3 externo que especifica uma única ação (**Transição**) da seguinte maneira:

```
<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 de bucket para o Amazon S3 Glacier no dia em que eles 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. Ações de expiração fazem com que o sistema de armazenamento externo exclua objetos expirados. Se você tentar acessar um objeto expirado do StorageGRID posteriormente, o objeto excluído não será encontrado.

Se você deseja transferir 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 Expedited nível 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 Quente ou Frio. Ao criar uma conta de armazenamento para uso com um pool de armazenamento em nuvem, você deve usar o nível Hot como nível padrão. Embora o StorageGRID defina imediatamente o nível como Arquivar ao mover objetos para o Cloud Storage Pool, usar uma configuração padrão de Quente garante que você não será cobrado por uma taxa de exclusão antecipada para objetos removidos do nível Frio antes do

mínimo de 30 dias.

Azure: Gerenciamento de ciclo de vida não suportado

Não use o gerenciamento do ciclo de vida do armazenamento de Blobs do Azure para o contêiner usado com um Pool de Armazenamento em Nuvem. As operações do ciclo de vida podem interferir nas operações do Cloud Storage Pool.

Informações relacionadas

["Criar um pool de armazenamento em nuvem"](#)

Comparar pools de armazenamento em nuvem e replicação do CloudMirror

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 armazenamento em nuvem	Serviço de replicação CloudMirror
Qual é o objetivo principal?	Atua como um alvo de arquivo. 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 no local, 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 armazenamento, usando o Grid Manager ou a Grid Management API. Pode ser selecionado como o local de posicionamento em uma regra ILM. Enquanto um pool de armazenamento consiste em um grupo de nós de armazenamento, um pool de armazenamento em nuvem é definido usando um ponto de extremidade remoto do S3 ou do Azure (endereço IP, credenciais e assim por diante).	Um usuário locatário "configura a replicação do CloudMirror" definindo um ponto de extremidade do CloudMirror (endereço IP, credenciais e assim por diante) usando o Tenant Manager ou a API do S3. Após a configuração do ponto de extremidade do CloudMirror, qualquer bucket pertencente a essa conta de locatário pode ser configurado para apontar para o ponto de extremidade do CloudMirror.
Quem é responsável por configurá-lo?	Normalmente, um administrador de rede	Normalmente, um usuário locatário
Qual é o destino?	- Qualquer infraestrutura S3 compatível (incluindo Amazon S3) - Camada de arquivo de Blobs do Azure - Plataforma de nuvem do Google (GCP)	- Qualquer infraestrutura S3 compatível (incluindo Amazon S3) - Plataforma de nuvem do Google (GCP)

	Pool de armazenamento em nuvem	Serviço de replicação CloudMirror
O que faz com que os objetos sejam movidos para o destino?	Uma ou mais regras de ILM nas políticas de ILM ativas. As regras do ILM definem quais objetos o 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 do CloudMirror. Objetos que existiam no bucket de origem antes do bucket ser configurado com o endpoint do 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 pool de armazenamento em nuvem. Se a única cópia de um objeto tiver sido transferida para armazenamento de arquivo, 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 do 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 .
Você pode ler diretamente do destino?	Não. Os objetos movidos para um pool de armazenamento em nuvem são gerenciados pelo StorageGRID. As solicitações de leitura devem ser direcionadas ao StorageGRID (e o StorageGRID será responsável pela recuperação do Cloud Storage Pool).	Sim, porque a cópia espelhada é uma cópia independente.
O que acontece se um objeto for excluído da fonte?	O objeto também é excluído do Cloud Storage Pool.	A ação de exclusão não é replicada. Um objeto excluído não existe mais no bucket StorageGRID , mas continua existindo no bucket de destino. Da mesma forma, objetos no bucket de destino podem ser excluídos sem afetar a origem.
Como acessar objetos após um desastre (sistema StorageGRID não operacional)?	Nós StorageGRID com falha devem ser recuperados. Durante esse processo, cópias de objetos replicados podem ser restauradas usando as cópias no Cloud Storage Pool.	As cópias de objetos no destino do CloudMirror são independentes do StorageGRID, portanto, podem ser acessadas diretamente antes que os nós do StorageGRID sejam recuperados.

Criar um pool de armazenamento em nuvem

Um pool de armazenamento em nuvem especifica um único bucket externo do Amazon S3 ou outro provedor compatível com S3 ou um contêiner de armazenamento de Blobs do Azure.

Ao criar um Pool de Armazenamento em Nuvem, você especifica o nome e o local do bucket ou contêiner externo que o StorageGRID usará para armazenar objetos, o tipo de provedor de nuvem (Amazon S3/GCP ou armazenamento de Blobs do Azure) e as informações que o StorageGRID precisa para acessar o bucket ou contêiner externo.

O 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 Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["permissões de acesso necessárias"](#) .
- Você revisou o ["considerações para pools de armazenamento em nuvem"](#) .
- O bucket ou contêiner externo referenciado pelo Cloud Storage Pool já existe e você tem o [informações do ponto de extremidade do serviço](#) .
- Para acessar o balde ou contêiner, você tem o [informações da conta para o tipo de autenticação](#) você escolherá.

Passos

1. Selecione **ILM > Pools de armazenamento > Pools de armazenamento em nuvem**.
2. Selecione **Criar** e insira as seguintes informações:

Campo	Descrição
Nome do pool de armazenamento em nuvem	Um nome que descreve brevemente o Cloud Storage Pool e sua finalidade. Use um nome que seja fácil de identificar ao configurar regras de ILM.
Tipo de provedor	Qual provedor de nuvem você usará para este pool de armazenamento 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. • Armazenamento de Blobs do Azure
Balde ou recipiente	O nome do bucket S3 externo ou do contêiner do Azure. Não é possível alterar esse valor depois que o Pool de Armazenamento em Nuvem for salvo.

3. Com base na seleção do tipo de provedor, insira as informações do ponto de extremidade do serviço.

Amazon S3/GCP

- a. Para o protocolo, selecione HTTPS ou HTTP.



Não use conexões HTTP para dados confidenciais.

- b. Digite o nome do host. Exemplo:

`s3-aws-region.amazonaws.com`

- c. Selecione o estilo de URL:

Opção	Descrição
Detecção automática	Tente detectar automaticamente qual estilo de URL usar, com base nas informações fornecidas. Por exemplo, se você especificar um endereço IP, o StorageGRID usará um URL no estilo de caminho. Selecione esta opção somente se você não souber qual estilo específico usar.
Estilo de hospedagem virtual	Use uma URL de estilo de hospedagem virtual para acessar o bucket. URLs de 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 estilo de caminho para acessar o bucket. URLs no estilo de caminho incluem o nome do bucket no final. Exemplo: <code>https://s3.company.com/bucket-name/key-name</code> Observação: A opção de URL no estilo 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.

Armazenamento de Blobs do Azure

- a. Usando um dos seguintes formatos, insira o URI para o ponto de extremidade 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 será usada para HTTPS e a porta 80 será usada para HTTP.

4. Selecione **Continuar**. Em seguida, selecione o tipo de autenticação e insira as informações necessárias para o ponto de extremidade 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 para a conta que possui o bucket externo.
- b. **Chave de acesso secreta:** Digite a chave de acesso secreta.

Funções IAM em qualquer lugar

Para o serviço AWS IAM Roles Anywhere

O StorageGRID usa 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 Cloud Storage Pool. Por exemplo, `us-east-1`.
- b. **URN da âncora de confiança:** insira o URN da âncora de confiança que valida 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 do IAM que pode ser assumido 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 não mais que 12 horas.
- f. **Certificado de CA do servidor** (opcional): Um ou mais certificados de CA confiáveis, no formato PEM, para verificar o servidor do IAM Roles Anywhere. Se omitido, o servidor não será verificado.
- g. **Certificado de entidade final:** A chave pública, no formato PEM, do certificado X509 assinado pela âncora de confiança. O AWS IAM Roles Anywhere usa essa chave para emitir um token STS.
- h. **Chave privada da entidade final:** A chave privada para o certificado da entidade final.

CAP (portal de acesso C2S)

Para serviços de nuvem comercial (C2S) serviço S3

- a. **URL de credenciais temporárias:** insira a URL completa que o 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 o StorageGRID usará para verificar o servidor CAP. O certificado deve ser codificado em PEM e emitido por uma Autoridade Certificadora (CA) governamental apropriada.
- c. **Certificado do cliente:** Selecione **Procurar** e carregue o certificado que o StorageGRID usará para se identificar no servidor CAP. O certificado do cliente deve ser codificado em PEM, emitido por uma Autoridade de Certificação Governamental (CA) apropriada e ter acesso concedido 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 descriptografá-la. 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 suportado.

Armazenamento de Blobs do Azure

Para Armazenamento de Blobs do Azure, somente Chave Compartilhada

- a. **Nome da conta:** Insira o nome da conta de armazenamento que possui o contêiner externo
- b. **Chave da conta:** Insira a chave secreta da conta de armazenamento

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
Usar certificados de CA raiz no sistema operacional do nó de armazenamento	Use os certificados Grid CA instalados no sistema operacional para proteger conexões.
Usar certificado CA personalizado	Use um certificado CA personalizado. Selecione Procurar e carregue o certificado codificado em PEM.
Não verificar certificado	Selecionar esta opção significa que as conexões TLS com o Cloud Storage Pool não são seguras.

6. Selecione **Salvar**.

Quando você salva um pool de armazenamento em nuvem, o StorageGRID faz o seguinte:

- Valida se o bucket ou contêiner e o ponto de extremidade de 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 pool de armazenamento em nuvem. Nunca remova este arquivo, que é chamado `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 especificado ainda não existir.

7. Se ocorrer um erro, consulte o ["instruções para solução de problemas de pools de armazenamento em nuvem"](#), resolva quaisquer problemas e tente salvar o Cloud Storage Pool novamente.

Ver detalhes do pool de armazenamento em nuvem

Você pode visualizar os detalhes de um pool de armazenamento em nuvem para determinar onde ele é usado e ver quais nós e níveis de armazenamento estão incluídos.

Antes de começar

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

Passos

1. Selecione **ILM > Pools de armazenamento > Pools de armazenamento em nuvem**.

A tabela Pools de armazenamento em nuvem inclui as seguintes informações para cada pool de armazenamento em nuvem que inclui nós de armazenamento:

- **Nome:** O nome de exibição exclusivo do pool.
- **URI:** O Identificador Uniforme de Recursos do Pool de Armazenamento em Nuvem.
- **Tipo de provedor:** Qual provedor de nuvem é usado para este pool de armazenamento em nuvem.
- **Container:** O nome do bucket usado para o Cloud Storage Pool.
- **Uso do ILM:** Como o pool está sendo usado atualmente. Um pool de armazenamento em nuvem pode não estar sendo utilizado ou pode estar sendo usado em uma ou mais regras de ILM, perfis de codificação de eliminação ou ambos.
- **Último erro:** O último erro detectado durante uma verificação de integridade deste pool de armazenamento em nuvem.

2. Para visualizar detalhes de um pool de armazenamento em nuvem específico, selecione seu nome.

A página de detalhes do pool é exibida.

3. Veja a aba **Autenticação** para saber mais sobre o tipo de autenticação para este Pool de Armazenamento em Nuvem e para editar os detalhes de autenticação.
4. Veja a aba **Verificação do servidor** para saber mais sobre detalhes da verificação, editar a verificação, baixar um novo certificado ou copiar o PEM do certificado.
5. Veja a aba **Uso do ILM** para determinar se o Cloud Storage Pool está sendo usado atualmente em alguma regra do ILM ou perfil de codificação de eliminação.
6. Opcionalmente, vá para a **página de regras do ILM** para ["aprender e gerenciar quaisquer regras"](#) que usam o Cloud Storage Pool.

Editar um pool de armazenamento em nuvem

Você pode editar um Pool de Armazenamento em Nuvem para alterar seu nome, ponto de extremidade de serviço ou outros detalhes; no entanto, não é possível alterar o bucket S3 ou o contêiner do Azure para um Pool de Armazenamento em Nuvem.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem ["permissões de acesso específicas"](#) .
- Você revisou o ["considerações para pools de armazenamento em nuvem"](#) .

Passos

1. Selecione **ILM > Pools de armazenamento > Pools de armazenamento em nuvem**.

A tabela Pools de armazenamento em nuvem lista os pools de armazenamento em nuvem existentes.

2. Marque a caixa de seleção do Pool de Armazenamento em Nuvem que você deseja editar e selecione **Ações > Editar**.

Como alternativa, selecione o nome do Pool de Armazenamento em Nuvem e selecione **Editar**.

3. Conforme necessário, altere o nome do pool de armazenamento em nuvem, o ponto de extremidade do serviço, as credenciais de autenticação ou o método de verificação do certificado.



Não é possível alterar o tipo de provedor, o bucket S3 ou o contêiner do Azure para um pool de armazenamento em nuvem.

Se você já carregou um certificado de servidor ou cliente, pode expandir o acordeão **Detalhes do certificado** para revisar o certificado que está em uso no momento.

4. Selecione **Salvar**.

Quando você salva um pool de armazenamento em nuvem, o StorageGRID valida se o bucket ou contêiner e o ponto de extremidade de serviço existem e se podem ser acessados usando as credenciais especificadas.

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.

Veja as instruções para "[solução de problemas de pools de armazenamento em nuvem](#)", resolva o problema e tente salvar o Cloud Storage Pool novamente.

Remover um pool de armazenamento em nuvem

Você pode remover um pool de armazenamento em nuvem se ele não for usado em uma regra de ILM e não contiver dados de objeto.

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você tem o "[permissões de acesso necessárias](#)".

Se necessário, use o ILM para mover dados do objeto

Se o pool de armazenamento em nuvem que você deseja remover contiver dados de objeto, você deverá usar o ILM para mover os dados para um local diferente. Por exemplo, você pode mover os dados para nós de armazenamento na sua grade ou para um pool de armazenamento em nuvem diferente.

Passos

1. Selecione **ILM > Pools de armazenamento > Pools de armazenamento em nuvem**.
2. Observe a coluna de uso do ILM na tabela para determinar se você pode remover o Cloud Storage Pool.

Não é possível remover um pool de armazenamento em nuvem se ele estiver sendo usado em uma regra de ILM ou em um perfil de codificação de eliminação.
3. Se o Cloud Storage Pool estiver sendo usado, selecione **nome do pool de armazenamento em nuvem > uso do ILM**.
4. "[Clonar cada regra ILM](#)" que atualmente coloca objetos no Cloud Storage Pool que você deseja remover.

5. Determine para onde você deseja mover os objetos existentes gerenciados por cada regra clonada.

Você pode usar um ou mais pools de armazenamento ou um pool de armazenamento em nuvem diferente.

6. Edite cada uma das regras que você clonou.

Para a Etapa 2 do assistente Criar regra ILM, selecione o novo local no campo **cópias em**.

7. "[Criar uma nova política de ILM](#)" e substituir cada uma das regras antigas por uma regra clonada.

8. Ative a nova política.

9. Aguarde o ILM remover objetos do Cloud Storage Pool e colocá-los no novo local.

Excluir pool de armazenamento em nuvem

Quando o Cloud Storage Pool estiver vazio e não for usado em nenhuma regra do ILM, você poderá excluí-lo.

Antes de começar

- Você removeu todas as regras do ILM que poderiam ter usado o pool.
- Você confirmou que o bucket S3 ou o contêiner do Azure não contém nenhum objeto.

Ocorrerá um erro se você tentar remover um pool de armazenamento em nuvem se ele contiver objetos. Ver "[Solucionar problemas de pools de armazenamento em nuvem](#)".



Quando você cria 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 é chamado `x-ntap-sgws-cloud-pool-uuid`.

Passos

1. Selecione **ILM > Pools de armazenamento > Pools de armazenamento em nuvem**.
2. Se a coluna de uso do ILM indicar que o Cloud Storage Pool não está sendo usado, marque a caixa de seleção.
3. Selecione **Ações > Remover**.
4. Selecione **OK**.

Solucionar problemas de pools de armazenamento em nuvem

Use estas etapas de solução de problemas para ajudar a resolver erros que você pode encontrar ao criar, editar ou excluir um pool de armazenamento em nuvem.

Determinar se ocorreu um erro

O StorageGRID executa uma verificação de integridade simples em cada pool de armazenamento em nuvem 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 o StorageGRID encontra um erro no endpoint, ele executa uma verificação de integridade a cada minuto em cada nó de armazenamento. Quando o erro for resolvido, as verificações de integridade serão interrompidas. Se uma verificação de integridade detectar um problema, uma mensagem será exibida na coluna Último erro da tabela Pools de armazenamento em nuvem na página Pools de armazenamento.

A tabela mostra o erro mais recente detectado para cada pool de armazenamento em nuvem e indica há quanto tempo o erro ocorreu.

Além disso, um alerta de **erro de conectividade do Cloud Storage Pool** será 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 Pools de armazenamento (selecione **ILM > Pools de armazenamento**), revise as mensagens de erro na coluna Último erro e consulte as diretrizes de solução de problemas abaixo.

Verifique se um erro foi resolvido

Depois de resolver quaisquer problemas subjacentes, você pode determinar se o erro foi resolvido. Na página Pool de armazenamento em nuvem, selecione o ponto de extremidade e selecione **Limpar erro**. Uma mensagem de confirmação indica que o StorageGRID corrigiu o erro do Cloud Storage Pool.

Se o problema subjacente tiver sido resolvido, a mensagem de erro não será mais exibida. Entretanto, se o problema subjacente não tiver sido corrigido (ou se um erro diferente for encontrado), a mensagem de erro será exibida na coluna Último erro dentro de alguns minutos.

Erro: Falha na verificação de integridade. Erro do ponto final

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. Este erro ocorre quando a operação PUT não tem um cabeçalho HTTP com um valor de soma de verificação de carga útil, como Content-MD5. Este valor de cabeçalho é exigido pela AWS para operações PUT em buckets com o S3 Object Lock habilitado.

Para corrigir esse problema, siga as etapas em "[Editar um pool de armazenamento em nuvem](#)" sem fazer nenhuma alteração. Esta ação aciona a validação da configuração do Cloud Storage Pool que detecta e atualiza automaticamente o sinalizador de bloqueio de objeto do S3 em uma configuração de ponto de extremidade 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 pool de armazenamento em nuvem. Este erro ocorre se o bucket ou contêiner incluir o `x-ntap-sgws-cloud-pool-uuid` arquivo marcador, mas esse arquivo não tem 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 uma destas etapas para corrigir o problema:

- Se você estiver configurando um novo pool de armazenamento em nuvem e o bucket contiver o `x-ntap-sgws-cloud-pool-uuid` arquivo e chaves de objeto adicionais semelhantes ao exemplo a seguir, crie um novo bucket e use esse novo bucket.

Exemplo de uma chave de objeto adicional: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Se o `x-ntap-sgws-cloud-pool-uuid` o arquivo é o único objeto no bucket, exclua este 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 ponto final

Você pode encontrar esse erro nas seguintes circunstâncias:

- Quando você tenta criar ou editar um pool de armazenamento em nuvem.
- Quando você seleciona uma plataforma, autenticação ou combinação de protocolo não suportada com o S3 Object Lock durante a configuração de um novo Cloud Storage Pool. Ver ["Considerações sobre pools de armazenamento em nuvem"](#).

Este erro indica que um problema de conectividade ou configuração está impedindo o 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 ponto de extremidade 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 nós de armazenamento acessem o ponto de extremidade de serviço usado para o pool de armazenamento em nuvem.
- Se o erro for devido a uma plataforma, autenticação ou protocolo não suportado, altere para uma configuração suportada com o S3 Object Lock e tente salvar o novo Cloud Storage Pool novamente.
- Para todas as outras mensagens de erro de 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 especificado para o Cloud Storage Pool e tente salvar o novo Cloud Storage Pool novamente.

Erro: Falha ao analisar o certificado CA

Você pode encontrar esse erro ao tentar criar ou editar um pool de armazenamento em nuvem. O erro ocorre se o StorageGRID não puder analisar o certificado inserido ao configurar o Cloud Storage Pool.

Para corrigir o problema, verifique se há problemas no certificado da CA fornecido.

Erro: Um pool de armazenamento em nuvem com este ID não foi encontrado

Você pode encontrar esse erro ao tentar editar ou excluir um pool de armazenamento em nuvem. Esse erro ocorre se o endpoint retornar uma resposta 404, o que pode significar qualquer um dos seguintes:

- 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 tem as permissões necessárias.
- Edite o Cloud Storage Pool com credenciais que tenham as permissões necessárias.
- Se as permissões estiverem corretas, entre em contato com o suporte.

Erro: Não foi possível verificar o conteúdo do pool de armazenamento em nuvem. Erro do ponto final

Você pode encontrar esse erro ao tentar excluir um pool de armazenamento em nuvem. Este erro indica que algum tipo de problema de conectividade ou configuração está impedindo o 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 pool de armazenamento em nuvem. Não é possível excluir um pool de armazenamento em nuvem se ele contiver dados que foram movidos para lá pelo ILM, dados que estavam no bucket antes de você configurar o pool de armazenamento em nuvem ou dados que foram colocados no bucket por alguma outra fonte depois que o pool de armazenamento em nuvem foi criado.

Tente uma ou mais destas etapas para corrigir o problema:

- Siga as instruções para mover objetos de volta para o StorageGRID em "Ciclo de vida de um objeto de pool de armazenamento em nuvem".
- 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 pool de armazenamento em nuvem 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 armazenamento não transparente entre os nós de armazenamento e o ponto de extremidade S3 externo usado para o pool de armazenamento em nuvem. Este erro ocorre se o servidor proxy externo não conseguir acessar o ponto de extremidade 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 armazenamento.

Erro: O certificado X.509 está fora do período de validade

Você pode encontrar esse erro ao tentar excluir um pool de armazenamento em nuvem. Este erro ocorre quando a autenticação requer um certificado X.509 para garantir que o pool de armazenamento em nuvem externo correto seja validado e que o pool externo esteja vazio antes que a configuração do pool de armazenamento em nuvem seja excluída.

Tente estas etapas 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 pool de armazenamento em nuvem seja resolvido.

Informações relacionadas

Gerenciar perfis de codificação de eliminação

Você pode visualizar os detalhes de um perfil de codificação de eliminação e renomear um perfil, se necessário. Você pode desativar um perfil de codificação de eliminação se ele não estiver sendo usado atualmente em nenhuma regra do ILM.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem o ["permissões de acesso necessárias"](#).

Ver detalhes do perfil de codificação de eliminação

Você pode visualizar os detalhes de um perfil de codificação de eliminação para determinar seu status, o esquema de codificação de eliminação usado e outras informações.

Passos

1. Selecione **CONFIGURAÇÃO > Sistema > Codificação de eliminação**.
2. Selecione o perfil. A página de detalhes do perfil é exibida.
3. Opcionalmente, visualize a guia Regras do ILM para obter uma lista de regras do ILM que usam o perfil e as políticas do ILM que usam essas regras.
4. Opcionalmente, visualize a guia Nós de Armazenamento para obter detalhes sobre cada Nó de Armazenamento no pool de armazenamento do perfil, como o local onde ele está localizado e o uso do armazenamento.

Renomear um perfil de codificação de eliminação

Talvez você queira renomear um perfil de codificação de eliminação para deixar mais óbvio o que o perfil faz.

Passos

1. Selecione **CONFIGURAÇÃO > Sistema > Codificação de eliminação**.
2. Selecione o perfil que você deseja renomear.
3. Selecione **Renomear**.
4. Insira um nome exclusivo para o perfil de codificação de eliminação.

O nome do perfil de codificação de eliminação é anexado ao nome do pool de armazenamento na instrução de posicionamento de uma regra ILM.



Os nomes de perfis de codificação de eliminação devem ser exclusivos. Um erro de validação ocorre 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 eliminação

Você pode desativar um perfil de codificação de eliminação se não planeja mais usá-lo e se o perfil não estiver sendo usado atualmente em nenhuma regra do ILM.



Confirme se não há operações de reparo de dados codificados para eliminação ou procedimentos de desativação em andamento. Uma mensagem de erro será retornada se você tentar desativar um perfil de codificação de eliminação enquanto qualquer uma dessas operações estiver em andamento.

Sobre esta tarefa

O StorageGRID impede que você desative um perfil de codificação de eliminação se qualquer uma das seguintes condições for verdadeira:

- O perfil de codificação de eliminação é usado atualmente em uma regra ILM.
- O perfil de codificação de eliminação não é mais usado em nenhuma regra ILM, mas dados de objeto e fragmentos de paridade para o perfil ainda existem.

Passos

1. Selecione **CONFIGURAÇÃO > Sistema > Codificação de eliminação**.
2. Na guia Ativo, revise a coluna **Status** para confirmar se o perfil de codificação de eliminação que você deseja desativar não é usado em nenhuma regra do ILM.

Não é possível desativar um perfil de codificação de eliminação se ele for usado em qualquer regra do ILM. No exemplo, o perfil 2+1 Data Center 1 é usado em pelo menos uma regra 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 eliminação que você deseja desativar.
 - c. Se a regra do ILM usar o perfil de codificação de eliminação que você deseja desativar, determine se a regra é usada em alguma política do ILM.
 - d. Conclua as etapas adicionais na tabela, com base em onde o perfil de codificação de eliminação é usado.

Onde o perfil foi usado?	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

Onde o perfil foi usado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Em uma regra ILM que nunca foi usada em nenhuma política ILM	i. Edite ou exclua todas as regras de ILM afetadas. Se você editar a regra, remova todos os posicionamentos que usam o perfil de codificação de eliminação. ii. Continue com este procedimento.	"Trabalhar com regras e políticas do ILM"
Em uma regra de ILM que está atualmente em uma política de ILM ativa	i. Clone a política. ii. Remova a regra ILM que usa o perfil de codificação de eliminação. iii. Adicione uma ou mais novas regras de 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 adicionadas. Observação: Dependendo do número de objetos e do tamanho do seu sistema StorageGRID , pode levar semanas ou até meses para que as operações do ILM movam os objetos para novos locais, com base nas novas regras do ILM. Embora você possa tentar desativar com segurança um perfil de codificação de eliminação enquanto ele ainda estiver associado aos dados, a operação de desativação falhará. Uma mensagem de erro informará 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 eliminação. vii. Continue com este procedimento.	"Criar uma política de ILM" "Trabalhar com regras e políticas do ILM"

Onde o perfil foi usado?	Etapas adicionais a serem executadas antes de desativar o perfil	Consulte estas instruções adicionais
Em uma regra de ILM que está atualmente em uma política de ILM	i. Edite a política. ii. Remova a regra ILM que usa o perfil de codificação de eliminação. iii. Adicione uma ou mais novas regras de 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 eliminação. vi. Continue com este procedimento.	"Criar uma política de ILM" "Trabalhar com regras e políticas do ILM"

e. Atualize a página Perfis de codificação de eliminação para garantir que o perfil não seja usado em uma regra do 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 eliminação é exibida.



Você pode selecionar vários perfis para desativar ao mesmo tempo, desde que cada perfil não seja usado em nenhuma regra.

- Se tiver certeza de que deseja desativar o perfil, selecione **Desativar**.

Resultados

- Se o StorageGRID conseguir desativar o perfil de codificação de eliminação, seu status será Desativado. Você não pode mais selecionar este perfil para nenhuma regra do ILM. Você não pode reativar um perfil desativado.
- Se o StorageGRID não conseguir desativar o perfil, uma mensagem de erro será exibida. Por exemplo, uma mensagem de erro aparece se os dados do objeto ainda estiverem associados a este perfil. Pode ser necessário esperar várias semanas antes de tentar o processo de desativação novamente.

Configurar regiões (opcional e somente S3)

As regras do ILM podem filtrar objetos com base nas regiões onde os buckets do S3 são criados, permitindo que você armazene objetos de diferentes regiões em diferentes locais de armazenamento.

Se você quiser usar uma região de bucket do S3 como um filtro em uma regra, primeiro crie as regiões que podem ser usadas pelos buckets no seu sistema.



Não é possível alterar a região de um bucket depois que ele foi criado.

Antes de começar

- Você está conectado ao Grid Manager usando um [navegador da web compatível](#).

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

Sobre esta tarefa

Ao criar um bucket S3, você pode especificar que o bucket 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 aos requisitos regulatórios.

Ao criar uma regra de 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 S3 criados no `us-west-2` região. Você pode então especificar que cópias desses objetos sejam colocadas em nós de armazenamento em um site de data center dentro dessa região para otimizar a latência.

Ao configurar regiões, siga estas diretrizes:

- Por padrão, todos os buckets são considerados pertencentes ao `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 S3 PUT Bucket API. Ocorrerá um erro se uma solicitação PUT Bucket usar uma região que não foi definida em StorageGRID.
- Você deve usar o nome exato da região ao criar o bucket S3. Os nomes de regiões diferenciam maiúsculas de minúsculas. Caracteres válidos são números, letras e hifens.



UE não é considerado um alias para eu-west-1. Se você quiser usar a região UE ou eu-west-1, deverá usar o nome exato.

- Você não pode excluir ou modificar uma região se ela for usada em uma regra atribuída a qualquer política (ativa ou inativa).
- Se você usar uma região inválida como filtro avançado em uma regra de ILM, não poderá adicionar essa regra a uma política.

Uma região inválida pode ocorrer se você usar uma região como um filtro avançado em uma regra ILM, mas depois excluir essa região, ou se usar a API de gerenciamento de grade para criar uma regra e especificar uma região que você não definiu.

- Se você excluir uma região após usá-la para criar um bucket do S3, será necessário adicioná-la novamente se quiser usar o filtro avançado Restrição de Localização para encontrar objetos nesse bucket.

Passos

1. Selecione **ILM > Regiões**.

A página Regiões é exibida, com as regiões definidas atualmente listadas. **Região 1** mostra a região padrão, `us-east-1`, que não pode ser modificado ou removido.

2. Para adicionar uma região:

- a. Selecione **Adicionar outra região**.
- b. Insira o nome de uma região que você deseja usar ao criar buckets do S3.

Você deve usar esse nome de região exato como o elemento de solicitação `LocationConstraint` ao criar o bucket S3 correspondente.

3. Para remover uma região não utilizada, selecione o ícone de exclusão .

Uma mensagem de erro aparece se você tentar remover uma região que está sendo usada atualmente em qualquer política (ativa ou inativa).

4. 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. Ver "[Usar filtros avançados em regras de ILM](#)".

Criar regra ILM

Use regras do ILM para gerenciar objetos

Para gerenciar objetos, crie um conjunto de regras de gerenciamento do ciclo de vida das informações (ILM) e organize-as em uma política de ILM.

Cada objeto ingerido 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 o StorageGRID executa para copiar e armazenar esse objeto.



Metadados de objetos não são gerenciados por regras de ILM. Em vez disso, os metadados do objeto são armazenados em um banco de dados Cassandra no qual é conhecido como repositório de metadados. Três cópias dos metadados do objeto são mantidas automaticamente em cada site para proteger os dados contra perdas.

Elementos de uma regra ILM

Uma regra ILM tem 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, o StorageGRID aplicará a regra e criará 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 do objeto. Cada regra pode incluir uma sequência de instruções de posicionamento para alterar o número, o tipo e a localização das cópias do objeto ao longo do tempo. Quando o período de uma colocação expira, as instruções da próxima colocação 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 à medida que são ingeridos (quando um cliente S3 salva um objeto na grade).

Filtragem de regras ILM

Ao criar uma regra de 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 regra (padrão) em uma política de ILM. A regra padrão fornece instruções de armazenamento para objetos que não correspondem aos filtros de outra regra.

- Filtros básicos permitem que você aplique regras diferentes a grupos grandes e distintos de objetos. Esses filtros permitem que você aplique uma regra a contas de locatários específicas, buckets S3 específicos ou ambos.

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 locatários separadas para cada departamento ou depois de segregar 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.

- Filtros avançados oferecem controle granular. Você pode criar filtros para selecionar objetos com base nas seguintes propriedades do objeto:
 - Tempo de ingestão
 - Último horário 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 com pouca frequência depois disso, enquanto objetos que contêm informações de visitas de pacientes podem precisar ser copiados para o departamento de cobrança na sede da rede de saúde. Você pode criar filtros que identifiquem 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 grandes arquivos de imagem de forma diferente dos registros de fornecedores, enquanto o departamento de Recursos Humanos pode precisar armazenar registros de pessoal em uma geografia específica e informações de políticas centralmente. Nesse caso, você pode criar regras que filtram 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 colocação se aplica a um único período de tempo.

Ao criar instruções de posicionamento:

- Comece 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 inativo 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 a quando o objeto foi ingerido.
- Por fim, você especifica o tipo de cópias (replicação ou codificação de eliminação) 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 vários posicionamentos para um único período de tempo e posicionamentos

diferentes para períodos de tempo diferentes.

- Para colocar objetos em vários locais durante um único período de tempo, selecione **Adicionar outro tipo ou local** para adicionar mais de uma linha para esse período de tempo.
- Para colocar objetos em locais diferentes em períodos de tempo diferentes, selecione **Adicionar outro período de tempo** para adicionar o próximo período de tempo. 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 store for days

Store objects by

copies at ,

and store objects by using

[Add other type or location](#)

Time period 2

From Day store forever

Store objects by

copies at

[Add other type or location](#)

A primeira instrução de posicionamento **1** tem duas linhas para o primeiro ano:

- A primeira linha cria duas cópias de objetos replicados em dois sites de data center.
- A segunda linha cria uma cópia codificada para eliminação 6+3 usando todos os sites do data center.

A segunda instrução de posicionamento **2** cria duas cópias após um ano e as mantém 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 intervalos entre os períodos de tempo definidos e que a instrução de posicionamento final continue para sempre ou até que você não precise mais de cópias de objetos.

À medida que cada período da 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 de regras do ILM

O comportamento de ingestão controla se as cópias do objeto são colocadas imediatamente de acordo com

as instruções da regra ou se cópias intermediárias são feitas e as instruções de posicionamento são aplicadas posteriormente. Os seguintes comportamentos de ingestão estão disponíveis para regras de ILM:

- **Balanceado:** O StorageGRID tenta fazer todas as cópias especificadas na regra ILM na ingestão; se isso não for possível, cópias provisórias são feitas e o sucesso é retornado ao cliente. As cópias especificadas na regra ILM são feitas quando possível.
- **Rigorous:** Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja retornado ao cliente.
- **Dual commit:** O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

Informações relacionadas

- ["Opções de ingestão"](#)
- ["Vantagens, desvantagens e limitações das opções de ingestão"](#)
- ["Como a consistência e as regras do ILM interagem para afetar a proteção de dados"](#)

Exemplo de regra ILM

Por exemplo, uma regra ILM poderia especificar o seguinte:

- Aplicar somente aos objetos pertencentes ao Locatário A.
- Faça duas cópias replicadas desses objetos e armazene cada cópia em um local diferente.
- Mantenha as duas cópias "para sempre", o que significa que o StorageGRID não as excluirá automaticamente. Em vez disso, o StorageGRID manterá esses objetos até que eles sejam excluídos por uma solicitação de exclusão do cliente ou pelo término do ciclo de vida de um bucket.
- Use a opção Balanceado para o comportamento de ingestão: a instrução de posicionamento de dois sites é aplicada assim que o Locatário 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 Locatário A salvar um objeto, o StorageGRID fará duas cópias provisórias nos Nós de Armazenamento no Site 1. Assim que o Site 2 estiver disponível, o StorageGRID fará a cópia necessária naquele site.

Informações relacionadas

- ["O que é um pool de armazenamento"](#)
- ["O que é um pool de armazenamento em nuvem"](#)

Acesse o assistente Criar uma regra ILM

As regras do ILM permitem que você gerencie o posicionamento dos dados do objeto ao longo do tempo. Para criar uma regra de ILM, use o assistente Criar uma regra de ILM.

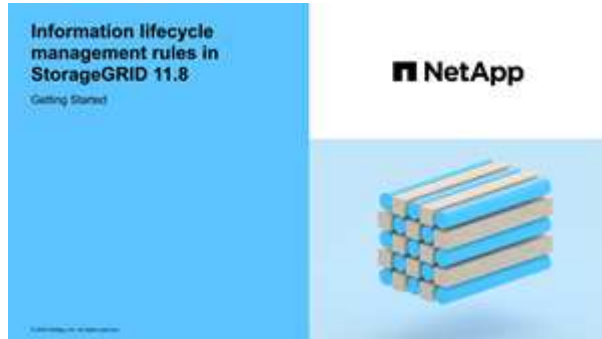


Se você quiser criar a regra ILM padrão para uma política, siga o ["instruções para criar uma regra ILM padrão"](#) em vez de.

Antes de começar

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

- Se você quiser especificar a quais contas de locatários esta regra se aplica, você tem o "[Permissão de contas de inquilino](#)" ou você sabe o ID da conta de cada conta.
- Se você quiser que a regra filtre objetos com base nos metadados do último horário de acesso, as atualizações do último horário de acesso devem ser habilitadas pelo bucket do S3.
- Você configurou todos os pools de armazenamento em nuvem que planeja usar. Ver "[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 está familiarizado com o "[requisitos para bloqueio de objeto S3](#)".
- Opcionalmente, você assistiu ao vídeo: "[Vídeo: Visão geral das regras do ILM](#)".



Sobre esta tarefa

Ao criar regras de ILM:

- Considere a topologia e as configurações de armazenamento do sistema StorageGRID.
- Considere quais tipos de cópias de objetos você deseja fazer (replicadas ou codificadas para eliminação) e o número de cópias de cada objeto que são necessárias.
- Determine quais tipos de metadados de objeto são usados nos aplicativos que se conectam ao sistema StorageGRID. As regras do ILM filtram objetos com base em seus metadados.
- Considere onde você quer que as cópias dos objetos sejam colocadas ao longo do tempo.
- Decida qual opção de ingestão usar (balanceada, restrita ou confirmação dupla).

Passos

1. Selecione **ILM > Regras**.
2. Selecione **Criar**. "[Etapa 1 \(Insira os detalhes\)](#)" do assistente Criar uma regra ILM é exibido.

Etapa 1 de 3: Insira os detalhes

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 são opcionais.

Sobre esta tarefa

Ao avaliar um objeto em relação a um "[Regra ILM](#)" O StorageGRID compara os metadados do objeto com os filtros da regra. Se os metadados do objeto corresponderem a todos os filtros, o StorageGRID usará a regra para posicionar o objeto. Você pode criar uma regra para aplicar a todos os objetos ou especificar filtros básicos, como uma ou mais contas de locatários ou nomes de buckets, ou filtros avançados, como o tamanho

do objeto ou metadados do usuário.

Passos

1. Digite 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 poder reconhecê-la mais tarde.

3. Opcionalmente, selecione uma ou mais contas de locatário do S3 às quais esta regra se aplica. Se esta regra se aplicar a todos os inquilinos, deixe este campo em branco.

Se você não tiver a permissão de acesso Root ou a permissão de contas de locatário, não poderá selecionar locatários da lista. Em vez disso, insira o ID do locatário ou insira vários IDs como uma sequência de caracteres delimitada por vírgulas.

4. Opcionalmente, especifique os buckets do S3 aos quais esta regra se aplica.

Se **aplica-se a todos os buckets** for selecionado (padrão), a regra será aplicada a todos os buckets do S3.

5. Para locatários do S3, selecione opcionalmente **Sim** para aplicar a regra somente a versões mais antigas de objetos em buckets do S3 que tenham o controle de versão habilitado.

Se você selecionar **Sim**, "Horário não atual" será selecionado automaticamente para Tempo de referência em ["Etapa 2 do assistente Criar uma regra ILM"](#).



O tempo não atual se aplica somente a objetos S3 em buckets habilitados para controle de versão. Ver ["Operações em buckets, PutBucketVersioning"](#) e ["Gerenciar objetos com o S3 Object Lock"](#).

Você pode usar esta opção para reduzir o impacto do armazenamento de objetos versionados filtrando por versões de objetos não atuais. Ver ["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 será aplicada a todos os objetos que corresponderem aos filtros básicos. Para obter mais informações sobre filtragem avançada, consulte [Usar filtros avançados em regras de ILM](#) e [Especifique vários tipos e valores de metadados](#).

7. Selecione **Continuar**. ["Etapa 2 \(Definir posicionamentos\)"](#) do assistente Criar uma regra ILM é exibido.

Usar filtros avançados em regras de ILM

A filtragem avançada permite que você crie regras de 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 metadados que deseja corresponder, seleciona um operador e especifica um valor de metadados. Quando os objetos são avaliados, a regra ILM é aplicada somente aos objetos que têm metadados correspondentes 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 • está em ou antes • é depois • está ligado ou depois	Hora e data em que o objeto foi ingerido. Observação: para evitar problemas de recursos ao ativar uma nova política de 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 como maior ou igual ao tempo aproximado em que a nova política entrará em vigor para garantir que os objetos existentes não sejam movidos desnecessariamente.
Chave	• é igual a • não é igual a • 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 combinar objetos que terminam com <code>.txt</code> ou comece com <code>test-object/</code>.
Último horário de acesso	• é • não é • é antes • está em ou antes • é depois • está ligado ou depois	Hora e data em que o objeto foi recuperado pela última vez (lido ou visualizado). Nota: Se você planeja "usar último horário de acesso" como um filtro avançado, as atualizações de hora do último acesso devem ser habilitadas para o bucket S3.
Restrição de localização (somente S3)	• é igual a • não é igual a	A região onde um bucket S3 foi criado. Use ILM > Regiões para definir as regiões que são mostradas. Observação: Um valor de <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. Ver "Configurar regiões (opcional e somente S3)".

Tipo de metadados	Operadores suportados	Valor de metadados
Tamanho do objeto	• é igual a • não é igual a • menor que • menor ou igual a • maior que • maior ou igual a	O tamanho do objeto. A codificação de eliminação é mais adequada para objetos maiores que 1 MB. Não use codificação de eliminação para objetos menores que 200 KB para evitar a sobrecarga de gerenciamento de fragmentos muito pequenos codificados por eliminação.
Metadados do usuário	• contém • termina com • é igual a • existe • começa com • não contém • não termina com • não é igual a • 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 de usuário de <code>color=blue</code>, especifique <code>color</code> para Nome de metadados do usuário, <code>equals</code> para o operador, e <code>blue</code> para Valor de metadados. Observação: Os nomes de metadados do usuário não diferenciam maiúsculas de minúsculas; os valores de metadados do usuário diferenciam maiúsculas de minúsculas.
Tag de objeto (somente S3)	• contém • termina com • é igual a • existe • começa com • não contém • não termina com • não é igual a • 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 do objeto, <code>equals</code> para o operador, e <code>True</code> para valor da tag do objeto. Observação: Os nomes de tags de objeto e os valores de tags de objeto diferenciam maiúsculas de minúsculas. Você deve inserir esses itens exatamente como foram definidos para o objeto.

Especifique vários tipos e valores de metadados

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 entre 10 MB e 100 MB de tamanho, selecione o tipo de metadados **Tamanho do objeto** e especifique dois valores de metadados.

- O primeiro valor de metadados especifica objetos maiores ou iguais a 10 MB.
- O segundo valor de metadados especifica objetos menores ou iguais 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	✕

Usar várias entradas permite que você tenha controle preciso sobre quais objetos são correspondidos. No exemplo a seguir, a regra se aplica a objetos que têm Marca A ou Marca B como valor dos metadados do usuário camera_type. No entanto, a regra só se aplica aos objetos da Marca B que são menores que 10 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

User metadata	camera_type	equals	Brand A	✕

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule: ✕

User metadata	camera_type	equals	Brand B	✕
and				
Object size	less than or equal to	10	MB	✕

[Add another advanced filter](#)

Etapa 2 de 3: Definir posicionamentos

A etapa **Definir posicionamentos** do assistente Criar regra ILM permite que você defina as instruções de posicionamento que determinam por quanto tempo os objetos são armazenados, o tipo de cópias (replicadas ou codificadas para eliminação), o local de armazenamento e o número de cópias.



As capturas de tela mostradas são exemplos. Seus resultados podem variar dependendo da versão do StorageGRID .

Sobre esta tarefa

Uma regra ILM pode incluir uma ou mais instruções de posicionamento. Cada instrução de colocação 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 para sempre 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 para eliminação 2+1 é feita 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. Para **Tempo de referência**, selecione o tipo de tempo 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 horário de acesso	A hora em que o objeto foi recuperado (lido ou visualizado) pela última vez. Para usar esta opção, as atualizações do Último horário de acesso devem ser habilitadas para o bucket S3. Consulte "Usar a hora do último acesso nas regras do ILM" .
Tempo de criação definido pelo usuário	Um tempo especificado em metadados definidos pelo usuário.
Tempo não atual	"Tempo não atual" é selecionado automaticamente se você selecionou Sim para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com controle de versão habilitado)?" em "Etapa 1 do assistente Criar uma regra ILM" .

Se você quiser criar uma regra *compatível*, selecione **Tempo de ingestão**. Consulte ["Gerenciar objetos com o S3 Object Lock"](#) .

2. Na seção **Período de tempo e posicionamentos**, insira um horário de início e uma duração para o primeiro período de tempo.

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 quiser criar cópias replicadas:

- a. Na lista suspensa **Armazenar objetos por**, selecione **replicando**.
- b. Selecione o número de cópias que você deseja fazer.

Um aviso aparecerá se você alterar o número de cópias para 1. Uma regra de 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:

- Aumentar o número de cópias para o período.
- Adicione cópias a outros pools de armazenamento ou a um pool de armazenamento em nuvem.
- Selecione **codificação de eliminação** 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 armazenamento que deseja adicionar.

Se você especificar apenas um pool de armazenamento, esteja ciente de que o StorageGRID pode armazenar apenas uma cópia replicada de um objeto em qualquer nó de armazenamento. Se sua grade incluir três nós de armazenamento e você selecionar 4 como o número de cópias, apenas três cópias serão feitas, uma cópia para cada nó de armazenamento.

O alerta **ILM placement unachievable** é acionado para indicar que a regra ILM não pôde ser aplicada completamente.

Se você especificar mais de um pool de armazenamento, tenha estas regras em mente:

- O número de cópias não pode ser maior que o número de pools de armazenamento.
- Se o número de cópias for igual ao número de pools de armazenamento, uma cópia do objeto será armazenada em cada pool de armazenamento.
- Se o número de cópias for menor que o número de pools de armazenamento, uma cópia será armazenada no site de ingestão e, em seguida, o sistema distribui as cópias restantes para manter o uso do disco entre os pools equilibrado, garantindo que nenhum site receba mais de uma cópia de um objeto.
- Se os pools de armazenamento se sobrepuserem (contiverem os mesmos nós de armazenamento), todas as cópias do objeto poderão ser salvas em apenas um site. Por esse motivo, não especifique o pool de armazenamento All Storage Nodes (StorageGRID 11.6 e anteriores) e outro pool de armazenamento.

4. Se você quiser criar uma cópia codificada para eliminação:

- a. Na lista suspensa **Armazenar objetos por**, selecione **codificação de eliminação**.



A codificação de eliminação é mais adequada para objetos maiores que 1 MB. Não use codificação de eliminação para objetos menores que 200 KB para evitar a sobrecarga de gerenciamento de fragmentos muito pequenos codificados por eliminação.

- 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 **Tamanho do objeto** para qualquer valor maior que 200 KB.
- c. Selecione o pool de armazenamento que deseja adicionar e o esquema de codificação de eliminação

que deseja usar.

O local de armazenamento de uma cópia codificada para eliminação inclui o nome do esquema de codificação para eliminação, seguido pelo nome do pool de armazenamento.

Os esquemas de codificação de eliminação disponíveis são limitados pelo número de nós de armazenamento no pool de armazenamento selecionado. UM Recommended O emblema aparece ao lado dos esquemas que fornecem o "[melhor proteção ou menor sobrecarga de armazenamento](#)".

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 períodos de tempo diferentes.

As exclusões de objetos ocorrem com base nas seguintes configurações:



- Os objetos são excluídos automaticamente no final do período de tempo final, a menos que outro período de tempo termine com **para sempre**.
- Dependendo de "[configurações de período de retenção de bucket e locatário](#)", os objetos podem não ser excluídos mesmo que o período de retenção do ILM termine.

6. Se você quiser armazenar objetos em um pool de armazenamento em nuvem:

- a. Na lista suspensa **Armazenar objetos por**, selecione **replicando**.
- b. Selecione o campo **cópias em** e, em seguida, selecione um Pool de Armazenamento em Nuvem.

Ao usar pools de armazenamento em nuvem, tenha estas regras em mente:

- Não é possível selecionar mais de um Cloud Storage Pool em uma única instrução de posicionamento. Da mesma forma, você não pode selecionar um Cloud Storage Pool e um pool de armazenamento na mesma instrução de posicionamento.
- Você pode armazenar apenas uma cópia de um objeto em qualquer pool de armazenamento em nuvem. Uma mensagem de erro aparece se você definir **Cópias** como 2 ou mais.
- Não é possível armazenar mais de uma cópia de objeto em nenhum pool de armazenamento em nuvem ao mesmo tempo. Uma mensagem de erro será exibida se vários posicionamentos que usam um pool de armazenamento em nuvem tiverem datas sobrepostas ou se várias linhas no mesmo posicionamento usarem um pool de armazenamento em nuvem.
- Você pode armazenar um objeto em um Cloud Storage Pool ao mesmo tempo em que ele está sendo armazenado como cópias replicadas ou codificadas para eliminação no StorageGRID. No entanto, você deve incluir mais de uma linha na instrução de posicionamento para o período de tempo, para que possa especificar o número e os tipos de cópias para cada local.

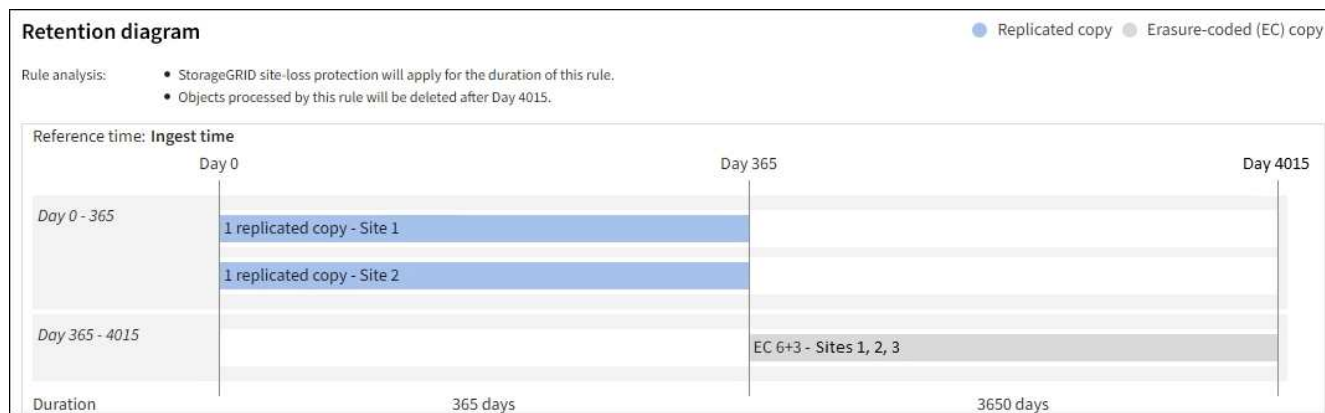
7. No diagrama de retenção, confirme suas instruções de posicionamento.

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 codificada para eliminação 6+3 será salva em três locais. Após 11 anos no total, os objetos serão excluídos do StorageGRID.

A seção 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 site."](#)



8. Selecione **Continuar**. ["Etapa 3 \(Selecionar comportamento de ingestão\)"](#) do assistente Criar uma regra ILM é exibido.

Usar a hora do último acesso nas regras do ILM

Você pode usar o Último horário de acesso como horário de referência em uma regra do ILM. Por exemplo, você pode querer deixar objetos que foram visualizados nos últimos três meses em Nós de Armazenamento locais, enquanto move objetos que não foram visualizados recentemente para um local externo. Você também pode usar a Hora do último acesso como um filtro avançado se quiser que uma regra do ILM se aplique somente a objetos que foram acessados pela última vez em uma data específica.

Sobre esta tarefa

Antes de usar o Último horário de acesso em uma regra do ILM, revise as seguintes considerações:

- Ao usar o Último horário de acesso como referência, esteja ciente de que alterar o Último horário 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 objeto ser acessado.

Leve essa latência em consideração ao criar regras de ILM com base no último horário de acesso e evite posicionamentos que usem períodos curtos (menos de um mês).

- Ao usar o Último horário de acesso como um filtro avançado ou como um horário de referência, você deve habilitar as atualizações do último horário de acesso para os buckets do S3. Você pode usar o ["Gerente de inquilinos"](#) ou o ["API de gerenciamento de inquilinos"](#).



As atualizações do último horário de acesso são desabilitadas por padrão para buckets do S3.



Esteja ciente de que habilitar atualizações de horário do último acesso pode reduzir o desempenho, especialmente em sistemas com objetos pequenos. O impacto no desempenho ocorre porque o StorageGRID deve atualizar os objetos com novos registros de data e hora sempre que os objetos são recuperados.

A tabela a seguir resume se o horário do último acesso é atualizado para todos os objetos no bucket para diferentes tipos de solicitações.

Tipo de solicitação	Se o último horário de acesso é atualizado quando as atualizações do último horário de acesso são desabilitadas	Se o último horário de acesso é atualizado quando as atualizações do último horário de acesso são habilitadas
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 de origem • Sim, para a cópia de destino	• Sim, para a cópia de origem • Sim, para a cópia de destino
Solicitação para concluir um upload multiparte	Sim, para o objeto montado	Sim, para o objeto montado

Etapas 3 de 3: Selecione o comportamento de ingestão

A etapa **Selecionar comportamento de ingestão** do assistente Criar regra ILM permite que você escolha como os objetos filtrados por esta regra serão protegidos à medida que são ingeridos.

Sobre esta tarefa

O StorageGRID pode fazer cópias provisórias e enfileirar os objetos para avaliação posterior do ILM, ou pode fazer cópias para atender às instruções de posicionamento da regra imediatamente.

Passos

1. Selecione o ["comportamento de ingestão"](#) para usar.

Para obter mais informações, consulte ["Vantagens, desvantagens e limitações das opções de ingestão"](#).



Você não pode usar a opção Balanceado ou Estrito se a regra usar um destes posicionamentos:

- Um pool de armazenamento em nuvem no dia 0
- Um pool de armazenamento em nuvem quando a regra usa um horário de criação definido pelo usuário como horário de referência

Ver ["Exemplo 5: regras e política do ILM para comportamento de ingestão estrita"](#).

2. Selecione **Criar**.

A regra ILM é criada. A regra não se torna ativa até que seja adicionada a um ["Política de ILM"](#) e essa política é ativada.

Para visualizar os detalhes da regra, selecione o nome da regra na página de regras do ILM.

Criar uma regra ILM padrão

Antes de criar uma política de ILM, você deve criar uma regra padrão para colocar quaisquer objetos que não correspondam a outra regra na política. A regra padrão não pode usar nenhum filtro. Ele deve ser aplicado a todos os locatários, todos os buckets e todas as versões de objetos.

Antes de começar

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

Sobre esta tarefa

A regra padrão é a última regra a ser avaliada em uma política de ILM, portanto, ela não pode usar nenhum filtro. As instruções de posicionamento da regra padrão são aplicadas a todos os objetos que não correspondem a outra regra na política.

Nesta política de exemplo, a primeira regra se aplica somente a objetos pertencentes ao test-tenant-1. A regra padrão, que é a última, se aplica a objetos pertencentes a todas as outras contas de locatários.

Proposed policy name

Reason for change

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.

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 estes requisitos:

- A regra padrão será automaticamente colocada como a última regra quando você adicioná-la 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 use uma regra que crie cópias codificadas para eliminação como regra padrão para uma política. As regras de codificação de eliminação devem usar um filtro avançado para evitar que objetos menores sejam codificados por eliminação.

- Em geral, a regra padrão deve manter objetos para sempre.
- Se você estiver usando (ou planeja habilitar) a configuração global de Bloqueio de Objeto do S3, a regra padrão deverá ser compatível.

Passos

1. Selecione **ILM > Regras**.
2. Selecione **Criar**.

A etapa 1 (Inserir detalhes) do assistente Criar regra ILM é exibida.

3. Insira um nome exclusivo para a regra no campo **Nome da regra**.
4. Opcionalmente, insira uma breve descrição para a regra no campo **Descrição**.
5. Deixe o campo **Contas de inquilinos** em branco.

A regra padrão deve ser aplicada a todas as contas de locatários.

6. Deixe a seleção suspensa Nome do bucket como **aplica-se a todos os buckets**.

A regra padrão deve ser aplicada a todos os buckets do S3.

7. Mantenha a resposta padrão, **Não**, para a pergunta "Aplicar esta regra somente a versões mais antigas de objetos (em buckets do S3 com controle de versão habilitado)?"
8. Não adicione filtros avançados.

A regra padrão não pode especificar nenhum filtro.

9. Selecione **Avançar**.

A etapa 2 (Definir posicionamentos) é exibida.

10. Para Tempo de referência, selecione qualquer opção.

Se você mantivesse a resposta padrão, **Não**, para a pergunta "Aplicar esta regra somente a versões mais antigas do objeto?" O tempo não atual não será incluído na lista suspensa. A regra padrão deve aplicar todas as versões do objeto.

11. Especifique as instruções de posicionamento para a regra padrão.
 - A regra padrão deve manter objetos para sempre. Um aviso aparece quando você ativa uma nova política se a regra padrão não retém objetos para sempre. Você deve confirmar se esse é o comportamento esperado.
 - A regra padrão deve criar cópias replicadas.



Não use uma regra que crie cópias codificadas para eliminação como regra padrão para uma política. As regras de codificação de eliminação devem incluir o filtro avançado **Tamanho do objeto (MB) maior que 200 KB** para evitar que objetos menores sejam codificados para eliminação.

- Se você estiver usando (ou planeja habilitar) a configuração global de bloqueio de objeto do S3, a regra padrão deve ser compatível:
 - Ele deve criar pelo menos duas cópias de objetos replicados ou uma cópia codificada para eliminação.
 - Essas cópias devem existir nos Nós de Armazenamento durante toda a duração de cada linha nas instruções de posicionamento.
 - Cópias de objetos não podem ser salvas em um pool de armazenamento em nuvem.
 - Pelo menos uma linha das instruções de posicionamento deve começar no dia 0, usando o tempo de ingestão como tempo de referência.
 - Pelo menos uma linha das instruções de posicionamento deve ser "para sempre".

12. Observe o diagrama de retenção para confirmar suas instruções de posicionamento.

13. Selecione **Continuar**.

A etapa 3 (Selecionar comportamento de ingestão) é exibida.

14. Selecione a opção de ingestão a ser usada e selecione **Criar**.

Gerenciar políticas de ILM

Usar políticas de ILM

Uma política de gerenciamento do ciclo de vida das informações (ILM) é um conjunto ordenado de regras de ILM que determina como o sistema StorageGRID gerencia dados de objetos ao longo do tempo.



Uma política de ILM configurada incorretamente pode resultar em perda irrecuperável de dados. Antes de ativar uma política de ILM, revise cuidadosamente a política de ILM e suas regras de ILM e, em seguida, simule a política de ILM. Sempre confirme se a política de ILM funcionará conforme o esperado.

Política ILM padrão

Quando você instala o StorageGRID e adiciona sites, uma política de ILM padrão é criada automaticamente, da seguinte maneira:

- Se sua grade contiver um site, a política padrão conterá uma regra padrão que replica duas cópias de cada objeto naquele site.
- Se sua grade contiver mais de um site, a regra padrão replicará uma cópia de cada objeto em cada site.

Se a política padrão não atender aos seus requisitos de armazenamento, você poderá criar suas próprias regras e políticas. Ver "[Criar uma regra ILM](#)" e "[Criar uma política de ILM](#)".

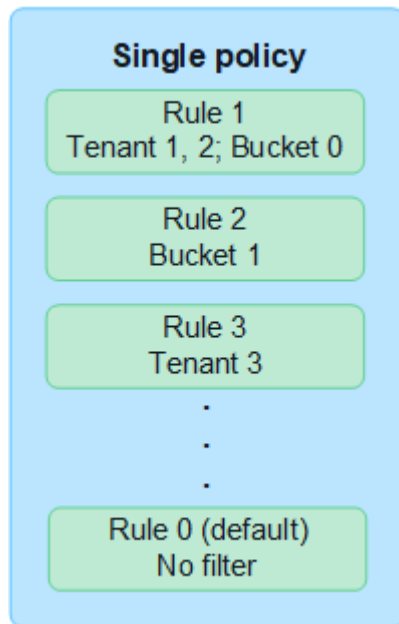
Uma ou muitas políticas de ILM ativas?

Você pode ter uma ou mais políticas de ILM ativas por vez.

Uma política

Se sua grade usar um esquema simples de proteção de dados com poucas regras específicas de locatário e de bucket, use uma única política de ILM ativa. As regras do ILM podem conter filtros para gerenciar

diferentes buckets ou locatários.



Quando você tem apenas uma política e os requisitos de um locatário mudam, você deve criar uma nova política de ILM ou clonar a política existente para aplicar as alterações, simular e, em seguida, ativar a nova política de ILM. Alterações na política do ILM podem resultar em movimentações de objetos que podem levar muitos dias e causar latência no sistema.

Políticas múltiplas

Para fornecer diferentes opções de qualidade de serviço aos inquilinos, você pode ter mais de uma política ativa ao mesmo tempo. Cada política pode gerenciar locatários, buckets S3 e objetos específicos. Quando você aplica ou altera uma política para um conjunto específico de locatários ou objetos, as políticas aplicadas a outros locatários e objetos não são afetadas.

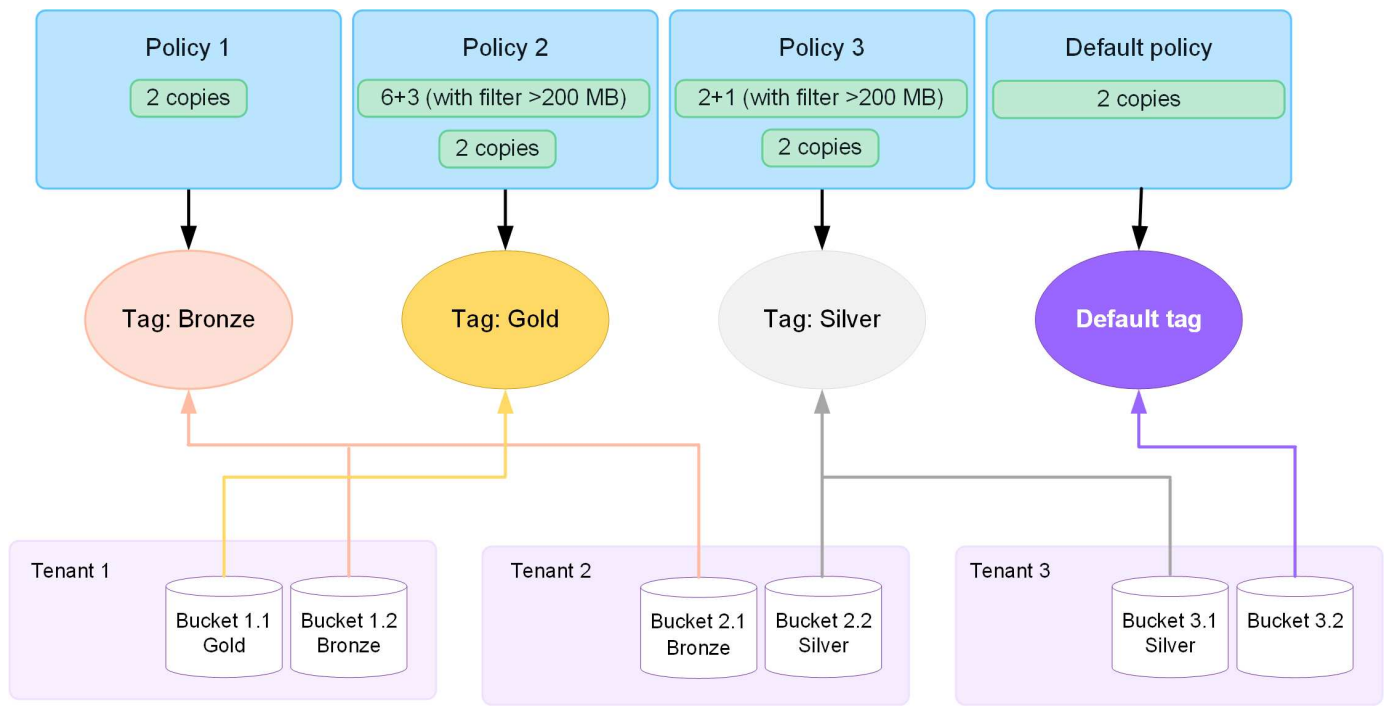
Tags de política do ILM

Se você quiser permitir que os locatários alternem facilmente entre várias políticas de proteção de dados por bucket, use várias políticas de ILM com *tags de política de ILM*. Você atribui cada política de ILM a uma tag e, em seguida, os locatários marcam um bucket para aplicar a política a esse bucket. Você pode definir tags de política do ILM somente em buckets do S3.

Por exemplo, você pode ter três tags chamadas Ouro, Prata e Bronze. Você pode atribuir uma política de ILM a cada tag, com base em quanto tempo e onde essa política armazena objetos. Os inquilinos podem escolher qual política usar marcando seus buckets. Um bucket marcado como Gold é gerenciado pela política Gold e recebe o nível Gold de proteção de dados e desempenho.

Tag de política ILM padrão

Uma tag de política ILM padrão é criada automaticamente quando você instala o StorageGRID. Cada grade deve ter uma política ativa atribuída à tag Padrão. A política padrão se aplica a todos os buckets S3 não marcados.



Como uma política de ILM avalia objetos?

Uma política de ILM ativa controla o posicionamento, 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 de ILM na política, da seguinte maneira:

1. Se os filtros da primeira regra na política corresponderem a um objeto, o objeto será 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 será 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 ser aplicada 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 de ILM

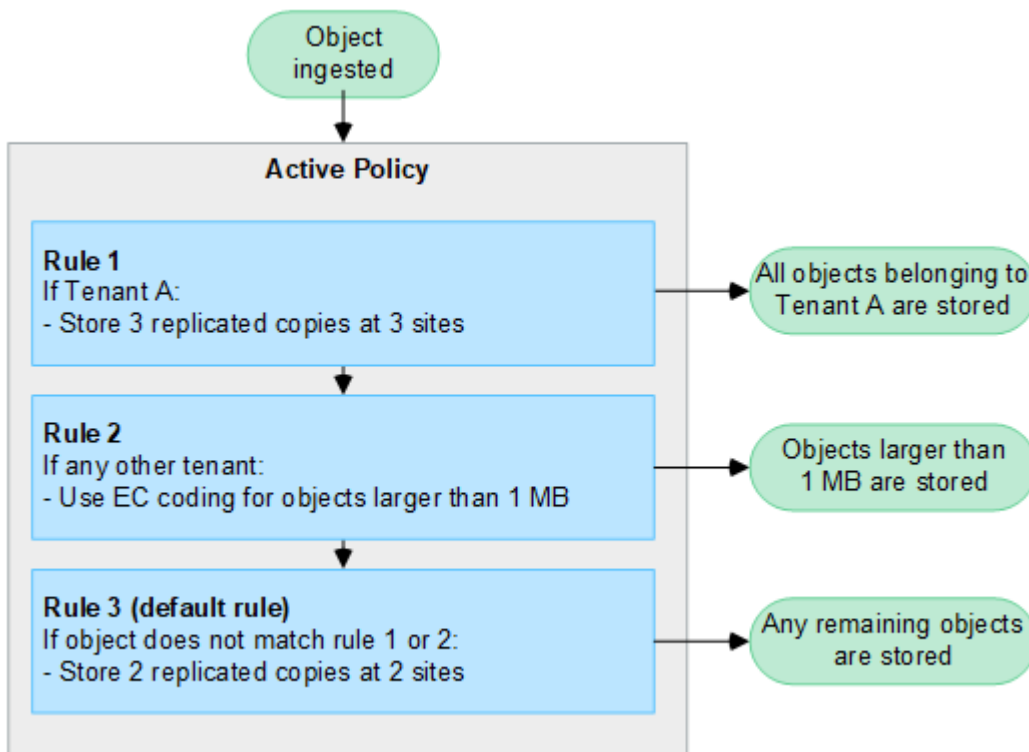
Por exemplo, uma política de ILM pode conter três regras de ILM que especificam o seguinte:

- **Regra 1: Cópias replicadas para o inquilino A**
 - Combine todos os objetos pertencentes ao Locatário A.
 - Armazene esses objetos como três cópias replicadas em três locais.
 - Objetos pertencentes a outros inquilinos não são correspondidos pela Regra 1, então eles são avaliados de acordo com a Regra 2.
- **Regra 2: Codificação de eliminação 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 eliminação 6+3 em três locais.
 - Não corresponde a objetos de 1 MB ou menores, portanto esses objetos são avaliados de acordo com

a Regra 3.

- **Regra 3: 2 cópias para 2 data centers** (padrão)

- É a última regra padrão da política. Não utiliza filtros.
- Faça duas cópias replicadas de todos os objetos não correspondidos pela Regra 1 ou Regra 2 (objetos que não pertencem ao Locatário A e que têm 1 MB ou menos).



O que são políticas ativas e inativas?

Cada sistema StorageGRID deve ter pelo menos uma política de ILM ativa. Se você quiser ter mais de uma política de ILM ativa, crie tags de política de ILM e atribua uma política a cada tag. Os locatários então aplicam tags aos buckets do S3. A política padrão é aplicada a todos os objetos em buckets que não têm uma tag de política atribuída.

Ao criar uma política de ILM pela primeira vez, você seleciona uma ou mais regras de ILM e as organiza em uma ordem específica. Depois de simular a política para confirmar seu comportamento, você a ativa.

Quando você ativa uma política de ILM, o 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 de ILM na nova política são implementadas.

Se você ativar mais de uma política de ILM por vez 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 a criação de uma política de ILM

- Use somente a política fornecida pelo sistema, a política de cópias da Linha de Base 2, em sistemas de teste. Para o StorageGRID 11.6 e versões anteriores, a regra Fazer 2 cópias nesta política usa o pool de armazenamento Todos os nós de armazenamento, 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.



O pool de armazenamento 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 Todos os nós de armazenamento ainda existirá. Se você instalar o StorageGRID 11.7 ou posterior como uma nova instalação, o pool Todos os nós de armazenamento não será criado.

- Ao projetar uma nova política, considere todos os diferentes tipos de objetos que podem ser ingeridos em sua grade. Certifique-se de que a política inclua regras para corresponder e posicionar esses objetos conforme necessário.
- Mantenha a política de ILM o mais simples possível. Isso evita situações potencialmente perigosas em que os dados do objeto não são protegidos conforme o esperado quando alterações são feitas no sistema StorageGRID ao longo do tempo.
- Certifique-se de que as regras da política estejam na ordem correta. Quando a política é ativada, objetos novos e existentes são avaliados pelas regras na ordem listada, começando pelo 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 de ILM é a regra de ILM padrão, que não pode usar nenhum filtro. Se um objeto não for correspondido por outra regra, a regra padrão controlará onde esse objeto será colocado e por quanto tempo ele será 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.

Criar políticas de ILM

Crie uma ou mais políticas de ILM para atender aos seus requisitos de qualidade de serviço.

Ter uma política de ILM ativa permite que você aplique as mesmas regras de ILM a todos os locatários e buckets.

Ter várias políticas de ILM ativas permite que você aplique as regras de ILM apropriadas a locatários e buckets específicos para atender a vários requisitos de qualidade de serviço.

Criar uma política de ILM

Sobre esta tarefa

Antes de criar sua própria política, verifique se o "[política ILM padrão](#)" não atende aos seus requisitos de armazenamento.



Use somente as políticas fornecidas pelo sistema, 2 cópias da Política (para grades de um site) ou 1 cópia por site (para grades de vários sites), em sistemas de teste. Para o StorageGRID 11.6 e versões anteriores, a regra padrão nesta política usa o pool de armazenamento Todos os nós de armazenamento, 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.



Se o "[a configuração global de bloqueio de objeto S3 foi habilitada](#)", você deve garantir que a política do ILM esteja em conformidade com os requisitos dos buckets que têm o Bloqueio de Objeto S3 habilitado. Nesta seção, siga as instruções que mencionam ter o S3 Object Lock habilitado.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["permissões de acesso necessárias"](#) .
- Você tem ["criou regras ILM"](#) com base na ativação do bloqueio de objeto S3.

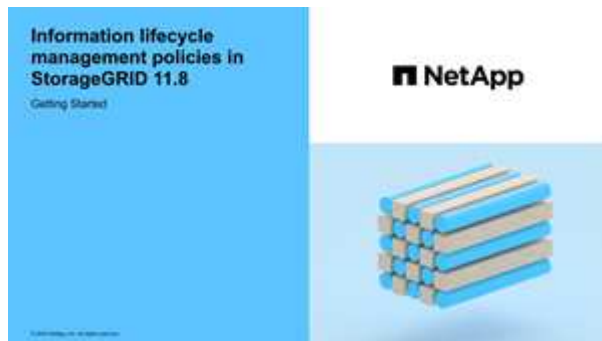
Bloqueio de objeto S3 não habilitado

- Você tem ["criou as regras do ILM"](#) que você 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 habilitado

- O ["a configuração global de bloqueio de objeto S3 já está habilitada"](#) para o sistema StorageGRID .
- Você tem ["criou as regras ILM compatíveis e não compatíveis"](#) que você 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: ["Vídeo: Visão geral das políticas do ILM"](#)



Veja também ["Usar políticas de ILM"](#) .

Passos

1. Selecione **ILM > Políticas**.

Se a configuração global de Bloqueio de Objeto do S3 estiver habilitada, a página de políticas do ILM indicará quais regras do ILM são compatíveis.

2. Determine como você deseja criar a política de ILM.

Criar nova política

- a. Selecione **Criar política**.

Clonar política existente

- a. Marque a caixa de seleção da política com a qual deseja começar e selecione **Clonar**.

Editar política existente

- a. Se uma política estiver inativa, você poderá editá-la. Marque a caixa de seleção da política inativa com a qual deseja começar e selecione **Editar**.

3. No campo **Nome da política**, insira um nome exclusivo para a política.
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 um nome de regra para visualizar as configurações dessa regra.

Se você estiver clonando uma política:

- As regras usadas pela política que você está clonando são selecionadas.
- Se a política que você está clonando usou alguma regra sem filtros que não fosse a regra padrão, você será solicitado a remover todas, exceto uma dessas regras.
- Se a regra padrão usou um filtro, você será solicitado a selecionar uma nova regra padrão.
- Se a regra padrão não for a última regra, você poderá movê-la para o final da nova política.

Bloqueio de objeto S3 não habilitado

- 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 qualquer objeto que não corresponda a outra regra na política. A regra padrão não pode usar nenhum filtro e é sempre avaliada por último.



Não use a regra Fazer 2 cópias como regra padrão para uma política. A regra Fazer 2 cópias usa um único pool de armazenamento, Todos os nós de armazenamento, 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 habilitado

- 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 são compatíveis e não usam nenhum filtro.



Não use a regra Fazer 2 cópias como regra padrão para uma política. A regra Fazer 2 cópias usa um único pool de armazenamento, Todos os nós de armazenamento, que contém todos os sites. Se você usar essa regra, várias cópias de um objeto poderão 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 tenham o S3 Object Lock habilitado.



Você só pode selecionar uma regra não compatível que não use um filtro.

Veja também ["Exemplo 7: Política ILM compatível para bloqueio de objeto S3"](#).

6. Quando terminar de selecionar a regra padrão, selecione **Continuar**.
7. Para a etapa Outras regras, selecione quaisquer outras regras que você deseja adicionar à política. Essas regras usam pelo menos um filtro (conta de locatário, nome do bucket, filtro avançado ou tempo 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 Bloqueio de Objeto S3 estiver habilitado e você também tiver selecionado uma regra "padrão" não compatível, essa regra será adicionada como a penúltima regra na política.



Um aviso aparece se alguma regra não retém objetos para sempre. Ao ativar esta política, você deve confirmar que deseja que o StorageGRID exclua objetos quando as instruções de posicionamento da regra padrão expirarem (a menos que um ciclo de vida do 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.

Você não pode mover a regra padrão. Se o Bloqueio de Objeto S3 estiver habilitado, você também não poderá mover a regra "padrão" não compatível, caso uma tenha sido selecionada.



Você deve confirmar se as regras do ILM estão na ordem correta. Quando a política é ativada, objetos novos e existentes são avaliados pelas regras na ordem listada, começando pelo topo.

9. Conforme necessário, selecione **Selecionar regras** para adicionar ou remover regras.
10. Quando terminar, selecione **Salvar**.
11. Repita essas etapas para criar políticas de ILM adicionais.
12. [Simular uma política de ILM](#) . Você deve sempre simular uma política antes de ativá-la para garantir que ela funcione conforme o esperado.

Simular uma política

Simule uma política em objetos de teste antes de ativar a política e aplicá-la aos seus dados de produção.

Antes de começar

- Você conhece o bucket/chave de objeto do S3 para cada objeto que deseja testar.

Passos

1. Usando um cliente S3 ou o ["Console S3"](#) , ingira os objetos necessários para testar cada regra.
2. Na página de políticas do ILM, marque a caixa de seleção da política e 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 controle de versão do S3 estiver habilitado, opcionalmente insira um ID de versão para o objeto no campo **ID da versão**.
5. Selecione **Simular**.
6. Na seção Resultados da simulação, confirme se cada objeto foi correspondido pela regra correta.
7. Para determinar qual pool de armazenamento ou perfil de codificação de eliminação está em vigor, selecione o nome da regra correspondente para acessar a página de detalhes da regra.



Revise quaisquer alterações no posicionamento de objetos replicados e codificados para eliminação existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos são avaliados e implementados.

Resultados

Quaisquer edições nas regras da política serão refletidas nos resultados da simulação e mostrarão a nova correspondência e a correspondência anterior. A janela Simular política retém os objetos que você testou até que você selecione **Limpar tudo** ou o ícone remover para cada objeto na lista de resultados da simulação.

Informações relacionadas

["Exemplos de simulações de políticas de ILM"](#)

Ativar uma política

Quando você ativa uma única nova política de ILM, os objetos existentes e os objetos recém-ingeridos são gerenciados por essa política. Quando você ativa várias políticas, as tags de política do ILM atribuídas aos buckets determinam os objetos a serem gerenciados.

Antes de ativar uma nova política:

1. Simule a política para confirmar se ela se comporta conforme o esperado.
2. Revise quaisquer alterações no posicionamento de objetos replicados e codificados para eliminação existentes. Alterar a localização de um objeto existente pode resultar em problemas temporários de recursos quando os novos posicionamentos são avaliados e implementados.



Erros em uma política de ILM podem causar perda irreversível de dados.

Sobre esta tarefa

Quando você ativa uma política de 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 grade 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 grade não sejam removidos acidentalmente. Especificamente:

- Se você fizer alterações de política que **umentem 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 de 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 grade 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 Política ativa, mas não entrará em vigor até que todos os nós estejam online e disponíveis.

Passos

Siga as etapas para ativar uma ou várias políticas:

Ativar uma política

Siga estas etapas se você tiver apenas uma política ativa. Se você já tiver uma ou mais políticas ativas e estiver ativando políticas adicionais, siga as etapas para ativar várias políticas.

1. Quando estiver pronto para ativar uma política, selecione **ILM > Políticas**.

Como alternativa, você pode ativar uma única política na página **ILM > Tags de política**.

2. Na guia Políticas, marque a caixa de seleção da política que você deseja ativar e selecione **Ativar**.
3. Siga o passo apropriado:
 - Se uma mensagem de aviso solicitar que você confirme se deseja ativar a política, selecione **OK**.
 - Se uma mensagem de aviso contendo detalhes sobre a política for exibida:
 - i. Revise os detalhes para garantir que a política gerenciará 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 armazena objetos para sempre, mas uma ou mais outras regras têm retenção limitada, digite **sim** na caixa de texto.
 - iv. Selecione **Ativar política**.

Ativar várias políticas

Para ativar várias políticas, você deve criar tags e atribuir uma política a cada tag.



Quando várias tags estão em uso, se os locatários reatribuírem frequentemente tags de política aos buckets, o desempenho da grade poderá ser afetado. Se você tiver inquilinos não confiáveis, considere usar apenas a tag Padrão.

1. Selecione **ILM > Tags de política**.
2. Selecione **Criar**.
3. Na caixa de diálogo Criar tag de política, digite um nome de tag e, opcionalmente, uma descrição para a tag.



Os nomes e descrições das tags são visíveis para os inquilinos. Escolha valores que ajudarão os inquilinos 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 do ILM, use o menu suspenso para selecionar uma política a ser atribuída à tag.
6. Se avisos aparecerem na coluna Limitações da política, selecione **Exibir detalhes da política** para revisá-la.
7. Garanta que cada política gerencie os dados conforme o esperado.
8. Selecione **Ativar políticas atribuídas**. Ou selecione **Limpar alterações** para remover a atribuição de política.

9. Na caixa de diálogo Ativar políticas com novas tags, revise as descrições de como cada tag, política e regra gerenciará 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 e selecione **Ativar políticas**.

Informações relacionadas

["Exemplo 6: Alterando uma política de ILM"](#)

Exemplos de simulações de políticas de ILM

Os exemplos de simulações de políticas de ILM fornecem diretrizes para estruturar e modificar simulações para seu ambiente.

Exemplo 1: Verificar regras ao simular uma política de ILM

Este exemplo descreve como verificar regras ao simular uma política.

Neste exemplo, a **Política ILM de exemplo** está sendo simulada em relação aos objetos ingeridos em dois buckets. A política inclui três regras, a saber:

- A primeira regra, **Duas cópias, dois anos para o bucket-a**, aplica-se somente a objetos no bucket-a.
- A segunda regra, **Objetos EC > 1 MB**, se aplica a todos os buckets, mas filtra objetos maiores que 1 MB.
- A terceira regra, **Duas cópias, dois data centers**, é a regra padrão. Não inclui nenhum filtro e não usa o tempo de referência não atual.

Depois de simular a política, confirme se 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`, então não correspondia à primeira regra. Em vez disso, ele foi correspondido corretamente pela segunda regra, que filtra objetos maiores que 1 MB.

- `bucket-b/test object less than 1 MB.pdf` não correspondeu aos filtros nas duas primeiras regras, então será colocado pela regra padrão, que não inclui filtros.

Exemplo 2: Regras de reordenação ao simular uma política de ILM

Este exemplo mostra como você pode reordenar regras para alterar os resultados ao simular uma política.

Neste exemplo, a política **Demo** está sendo simulada. Esta política, que visa encontrar objetos que tenham metadados de usuário `series=x-men`, inclui três regras, como segue:

- A primeira regra, **PNGs**, filtra nomes de chaves que terminam em `.png`.
- A segunda regra, **X-men**, aplica-se apenas a objetos para o Inquilino A e filtros para `series=x-men` metadados do usuário.
- A última regra, **Duas cópias, dois data centers**, é a regra padrão, que corresponde a todos os objetos que não correspondem às duas primeiras regras.

Passos

1. Depois de adicionar as regras e salvar a política, selecione **Simular**.
2. No campo **Objeto**, insira o bucket/chave de objeto S3 para um objeto de teste e selecione **Simular**.

Os resultados da simulação aparecem, 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` foi criado para testar a regra dos **X-men**.

3. Para resolver o problema, reordene as regras.
 - a. Selecione **Concluir** para fechar a janela Simular política de 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 testados anteriormente são reavaliados em relação à política atualizada, e os novos resultados da simulação são exibidos. No exemplo, a coluna Regra correspondida mostra que o `Havok.png` o objeto agora corresponde à regra de metadados dos 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 de 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. Esta política tem como objetivo encontrar objetos que tenham `series=x-men` metadados do usuário. No entanto, resultados inesperados ocorreram ao simular esta política contra o `Beast.jpg` objeto. Em vez de corresponder à regra de metadados dos X-men, o objeto correspondeu à regra padrão: Duas cópias de 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. Revise a conta do locatário da regra, o tempo de referência e os critérios de filtragem.

Por exemplo, suponha que os metadados da regra dos X-men foram inseridos como "x-men01" em vez de "x-men".

3. Para resolver o erro, corrija a regra da seguinte maneira:
 - Se a regra fizer parte da política, você poderá cloná-la ou removê-la da política e editá-la.
 - Se a regra fizer parte da política ativa, você deverá cloná-la. Você não pode editar ou remover uma regra da política ativa.
4. Execute a simulação novamente.

Neste exemplo, a regra corrigida dos X-men agora corresponde à `Beast.jpg` objeto baseado no `series=x-men` metadados do usuário, conforme 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

Gerenciar tags de política do ILM

Você pode visualizar detalhes da tag de política do ILM, editar uma tag ou remover uma tag.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem o ["permissões de acesso necessárias"](#).

Exibir detalhes da tag de política do 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 do ILM



Os nomes e descrições das tags são visíveis para os inquilinos. Escolha valores que ajudarão os inquilinos 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 tag existente:

1. Selecione **ILM > Tags de política**.
2. Selecione a caixa de seleção da tag e 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 tag de política ILM

Quando você remove uma tag de política, todos os buckets aos quais essa tag foi atribuída terão a política Padrão aplicada.

Para remover uma tag:

1. Selecione **ILM > Tags de política**.
2. Marque a caixa de seleção da tag e selecione **Remover**. Uma caixa de diálogo de confirmação é exibida.

Como alternativa, selecione o nome da tag. A página de detalhes da tag é exibida e você pode selecionar **Remover** nessa página.

3. Selecione **Sim** para excluir a tag.

Verificar uma política de ILM com consulta de metadados de objeto

Depois de ativar uma política de ILM, ingira objetos de teste representativos no sistema StorageGRID e execute uma pesquisa de metadados do objeto para confirmar se as cópias estão sendo feitas conforme o esperado e colocadas nos locais corretos.

Antes de começar

Você tem um identificador de objeto, que pode ser um dos seguintes: * **UUID**: Identificador Universalmente Único do objeto. * **CBID**: O identificador exclusivo do objeto dentro do StorageGRID. Você pode obter o CBID de um objeto no log de auditoria. Digite o CBDID em letras maiúsculas. * **Chave de bucket e objeto S3**: Quando um objeto é ingerido por meio da interface S3, o aplicativo cliente usa uma combinação de chave de bucket e objeto para armazenar e identificar o objeto. Se o bucket do S3 tiver versão e você quiser consultar uma versão específica de um objeto do S3 usando o bucket e a chave do objeto, você terá o **ID da versão**.

Passos

1. Ingerir o objeto.
2. Selecione **ILM > Consulta de metadados do objeto**.
3. Digite o identificador do objeto no campo **Identificador**. Você pode inserir um UUID, CBID ou chave de objeto/bucket S3.
4. Opcionalmente, insira um ID de versão para o objeto (somente S3).
5. Selecione **Procurar**.

Os resultados da pesquisa de metadados do objeto são exibidos. Esta página lista os seguintes tipos de informações:

- 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 de exemplo 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 codificadas por eliminação, o local de armazenamento atual de cada fragmento.
- Para cópias de objetos em um pool de armazenamento em nuvem, o local do objeto, incluindo o nome do bucket externo e o identificador exclusivo do objeto.
- Para objetos segmentados e objetos multipartes, uma lista de segmentos de objetos, incluindo identificadores de segmento e tamanhos de dados. Para objetos com mais de 100 segmentos, somente os primeiros 100 segmentos são mostrados.

- Todos os metadados do objeto no formato de armazenamento interno não processado. Esses metadados brutos incluem metadados internos do sistema que não têm garantia de persistência de uma versão para outra.

6. Confirme se o objeto está armazenado no(s) local(is) correto(s) e se é o tipo correto de cópia.

Se a opção Auditoria estiver habilitada, você também poderá monitorar o log de auditoria para a mensagem Regras de objeto ORLM atendidas. 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 exatidão do posicionamento dos dados do objeto ou a integridade da política do ILM. Você deve avaliar isso você mesmo. Para obter detalhes, consulte ["Revisar logs de auditoria"](#).

O exemplo a seguir mostra os resultados da pesquisa de metadados de objeto para um objeto de teste S3 armazenado como duas cópias replicadas.



A captura de tela a seguir é um exemplo. Seus resultados variarão dependendo da 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": "CNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36056",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",
```

Informações relacionadas

Trabalhar com políticas e regras do ILM

À medida que seus requisitos de armazenamento mudam, pode ser necessário implementar políticas adicionais ou modificar as regras de ILM associadas a uma política. Você pode visualizar métricas do ILM para determinar o desempenho do sistema.

Antes de começar

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

Ver políticas do ILM

Para visualizar políticas de ILM ativas e inativas e o histórico de ativação de 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 de datas de início e término de ativação das políticas.
4. Selecione um nome de política para visualizar os detalhes da política.



Se você visualizar os detalhes de uma política cujo status é Editado ou Excluído, uma mensagem será exibida explicando que você está visualizando a versão da política que estava ativa durante o período especificado e que desde então foi editada ou excluída.

Editar uma política de ILM

Você só pode editar uma política inativa. Se você quiser editar uma política ativa, desative-a ou crie um clone e edite o clone.

Para editar uma política:

1. Selecione **ILM > Políticas**.
2. Marque a caixa de seleção da política que você deseja editar e selecione **Editar**.
3. Edite a política seguindo as instruções em ["Criar políticas de ILM"](#) .
4. Simule a política antes de reativá-la.



Uma política de ILM configurada incorretamente pode resultar em perda irreversível de dados. Antes de ativar uma política de ILM, revise cuidadosamente a política de ILM e suas regras de ILM e, em seguida, simule a política de ILM. Sempre confirme se a política de ILM funcionará conforme o esperado.

Clonar uma política de ILM

Para clonar uma política ILM:

1. Selecione **ILM > Políticas**.
2. Marque a caixa de seleção da política que você deseja clonar e selecione **Clonar**.
3. Crie uma nova política começando com a política que você clonou seguindo as instruções em "[Criar políticas de ILM](#)".



Uma política de ILM configurada incorretamente pode resultar em perda irreversível de dados. Antes de ativar uma política de ILM, revise cuidadosamente a política de ILM e suas regras de ILM e, em seguida, simule a política de ILM. Sempre confirme se a política de ILM funcionará conforme o esperado.

Remover uma política de ILM

Você só pode remover uma política de ILM se ela estiver inativa. Para remover uma política:

1. Selecione **ILM > Políticas**.
2. Marque a caixa de seleção da política inativa que você deseja remover.
3. Selecione **Remover**.

Ver detalhes da regra do 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 for usada em qualquer política.

Clonar uma regra ILM

Você pode clonar uma regra existente se quiser criar uma nova regra que use algumas das configurações da regra existente. Se você precisar editar uma regra usada em qualquer política, clone a regra e faça alterações no clone. Depois de fazer 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 do ILM se ela foi criada usando o StorageGRID versão 10.2 ou anterior.

Passos

1. Selecione **ILM > Regras**.
2. Marque a caixa de seleção da regra que você deseja clonar e 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 as etapas para [editando 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

Pode ser necessário editar uma regra do ILM para alterar um filtro ou uma instrução de posicionamento.

Você não pode editar uma regra se ela for usada em qualquer política do ILM. Em vez disso, você pode [clonar a regra](#) e faça as alterações necessárias na cópia clonada.



Uma política de ILM configurada incorretamente pode resultar em perda irreversível de dados. Antes de ativar uma política de ILM, revise cuidadosamente a política de ILM e suas regras de ILM e, em seguida, simule a política de ILM. Sempre confirme se a política de ILM funcionará conforme o esperado.

Passos

1. Selecione **ILM > Regras**.
2. Confirme se a regra que você deseja editar não é usada em nenhuma política do 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 do ILM. Conforme necessário, siga os passos para ["criando uma regra ILM"](#) e ["usando filtros avançados em regras ILM"](#).

Ao editar uma regra ILM, você não pode alterar seu nome.

Remover uma regra ILM

Para manter a lista de regras atuais do ILM gerenciável, remova quaisquer regras do ILM que você provavelmente não usará.

Passos

Para remover uma regra de ILM que está sendo usada atualmente 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 de ILM que está sendo usada atualmente em uma política inativa.

Para remover uma regra ILM que está sendo usada atualmente em uma política inativa:

1. Selecione a política inativa.
2. Remova a regra ILM da política ou [remover a política](#).
3. Vá para as etapas para remover uma regra do ILM que não está sendo usada no momento.

Para remover uma regra ILM que não está sendo usada no momento:

1. Selecione **ILM > Regras**.
2. Confirme se a regra que você deseja remover não é 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 elas ao mesmo tempo.
4. Selecione **Sim** para confirmar que deseja remover a regra ILM.

Ver métricas do ILM

Você pode visualizar métricas para 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 taxa de avaliação pode indicar que o sistema não consegue acompanhar a taxa de ingestão, que a carga dos aplicativos clientes é excessiva ou que existe alguma condição anormal.

Passos

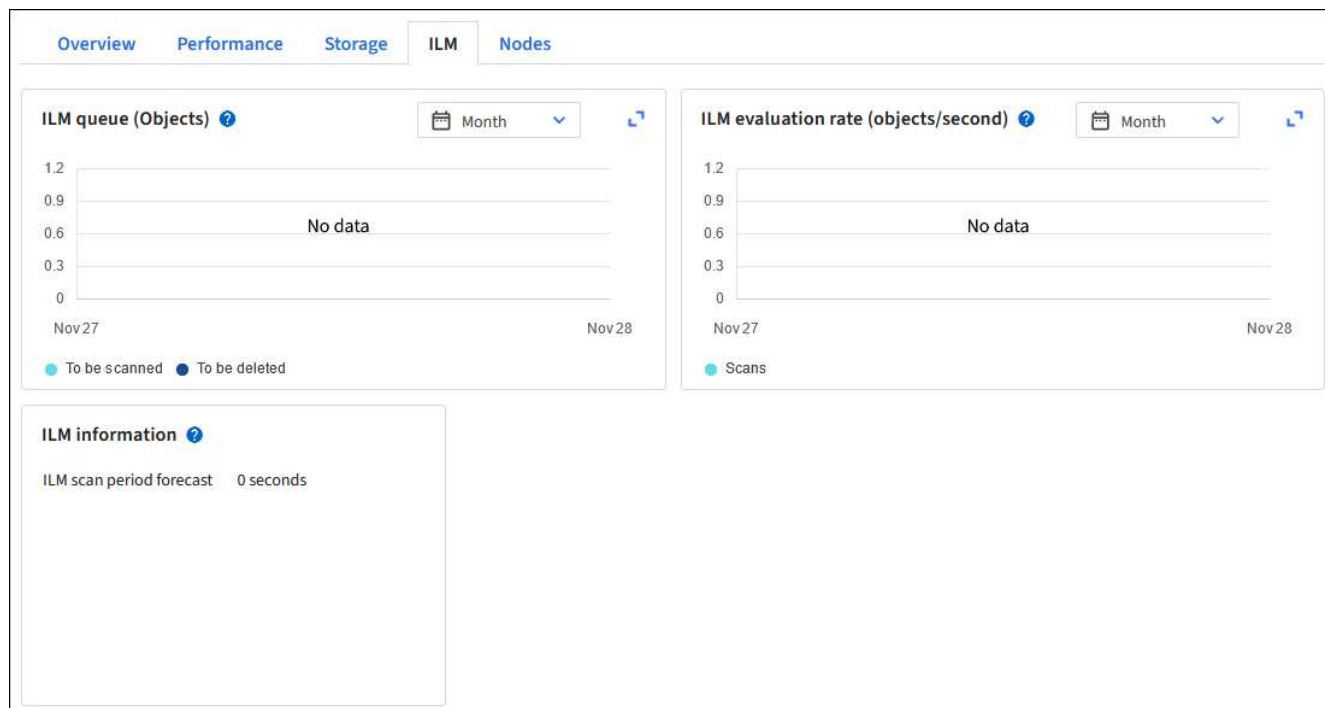
1. Selecione **Painel > ILM**.



Como o painel 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 aba ILM.



Usar bloqueio de objeto S3

Gerenciar objetos com o S3 Object Lock

Como administrador de grade, você pode habilitar o S3 Object Lock para seu sistema StorageGRID e implementar uma política de ILM compatível para ajudar a garantir que objetos em buckets S3 específicos não sejam excluídos ou substituídos por um período de tempo especificado.

O que é o S3 Object Lock?

O recurso StorageGRID S3 Object Lock é uma solução de proteção de objetos equivalente ao S3 Object Lock no Amazon Simple Storage Service (Amazon S3).

Quando a configuração global do S3 Object Lock está habilitada para um sistema StorageGRID, uma conta de locatário do S3 pode criar buckets com ou sem o S3 Object Lock habilitado. Se um bucket tiver o S3 Object Lock ativado, o controle de versão do bucket será necessário e ativado automaticamente.

Um bucket sem bloqueio de objeto S3 só pode ter objetos sem configurações de retenção especificadas. Nenhum objeto ingerido terá configurações de retenção.

Um bucket com bloqueio de objeto S3 pode ter objetos com e sem configurações de retenção especificadas por aplicativos cliente S3. Alguns objetos ingeridos terão configurações de retenção.

Um bucket com bloqueio de objeto S3 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, porque a configuração de retenção não foi configurada no nível do objeto.

Efetivamente, todos os objetos recém-ingерidos têm configurações de retenção quando a retenção padrão é configurada. Objetos existentes sem configurações de retenção de objetos 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 data de retenção seja atingida.
 - A data de retenção do objeto pode ser aumentada, mas não diminuída.
 - A data de retenção do objeto não pode ser removida até que essa data seja atingida.
- No 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 do objeto antes que sua data de retenção seja atingida.
 - Esses usuários podem aumentar, diminuir ou remover a data de retenção de um objeto.

Configurações de retenção para versões de objeto

Se um bucket for criado com o Bloqueio de Objeto S3 habilitado, os usuários poderão usar o aplicativo cliente S3 para especificar opcionalmente as seguintes configurações de retenção para cada objeto adicionado ao bucket:

- **Modo de retenção:** conformidade ou governança.
- **Reter-até-data:** Se a data de retenção de uma versão do objeto for no futuro, o objeto poderá ser recuperado, mas não poderá ser excluído.
- **Retenção legal:** Aplicar uma retenção legal a uma versão de objeto bloqueia imediatamente esse objeto. Por exemplo, você pode precisar reter legalmente um objeto relacionado a uma investigação ou disputa legal. Uma retenção legal não tem data de expiração, mas permanece em vigor até ser explicitamente removida. As retenções legais são independentes da retenção até a data.



Se um objeto estiver sob retenção legal, ninguém poderá excluí-lo, independentemente do seu modo de retenção.

Para obter detalhes sobre as configurações do objeto, consulte ["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#).

Configuração de retenção padrão para buckets

Se um bucket for criado com o S3 Object Lock habilitado, os usuários poderão, opcionalmente, especificar as seguintes configurações padrão para o bucket:

- **Modo de retenção padrão:** conformidade ou governança.
- **Período de retenção padrão:** por quanto tempo novas versões de objetos adicionadas a este bucket devem ser retidas, a partir do dia em que são adicionadas.

As configurações de bucket padrão se aplicam somente a novos objetos que não têm suas próprias configurações de retenção. Objetos de bucket existentes não são afetados quando você adiciona ou altera essas configurações padrão.

Ver ["Criar um bucket S3"](#) e ["Atualizar retenção padrão do bloqueio de objeto S3"](#).

Comparando o bloqueio de objeto S3 com a conformidade legada

O S3 Object Lock substitui o recurso de conformidade 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 StorageGRID Compliance, que agora é chamado de "Conformidade herdada".



A configuração global de Conformidade está obsoleta. Se você habilitou essa configuração usando uma versão anterior do StorageGRID, a configuração de Bloqueio de Objeto do S3 será habilitada automaticamente. Você pode continuar a usar o StorageGRID para gerenciar as configurações de buckets compatíveis existentes; no entanto, não é possível criar novos buckets compatíveis. Para mais detalhes, veja ["Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"](#) .

Se você usou o recurso de conformidade legado em uma versão anterior do StorageGRID, consulte a tabela a seguir para saber como ele se compara ao recurso de bloqueio de objeto do S3 no StorageGRID.

	Bloqueio de Objeto S3	Conformidade (legado)
Como o recurso é habilitado globalmente?	No Grid Manager, selecione CONFIGURAÇÃO > Sistema > Bloqueio de Objeto S3 .	Não é mais suportado.
Como o recurso é habilitado para um bucket?	Os usuários devem habilitar o bloqueio de objeto do S3 ao criar um novo bucket usando o Tenant Manager, a Tenant Management API ou a S3 REST API.	Não é mais suportado.
O controle de versão de bucket é suportado?	Sim. O controle de versão do bucket é necessário e é habilitado automaticamente quando o S3 Object Lock é habilitado para o bucket.	Não.
Como a retenção de objetos é definida?	Os usuários podem definir uma data de retenção para cada versão do 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.

	Bloqueio de Objeto S3	Conformidade (legado)
O período de retenção pode ser alterado?	- No modo de conformidade, o período de retenção até a data para uma versão do objeto pode ser aumentado, mas nunca diminuído. - 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 retenção legal é controlada?	Os usuários podem colocar ou retirar uma retenção legal para qualquer versão de objeto no bucket.	Uma retenção legal é colocada no bucket e afeta todos os objetos no bucket.
Quando os objetos podem ser excluídos?	- No modo de conformidade, uma versão do objeto pode ser excluída após a data de retenção ser atingida, supondo que o objeto não esteja sob retenção legal. - No modo de governança, usuários com permissões especiais podem excluir um objeto antes que sua data de retenção seja atingida, supondo que o objeto não esteja sob retenção legal.	Um objeto pode ser excluído após o término do período de retenção, desde que o bucket não esteja sob retenção legal. Os objetos podem ser excluídos automática ou manualmente.
A configuração do ciclo de vida do bucket é suportada?	Sim	Não

Tarefas de bloqueio de objeto S3

Como administrador de grade, você deve coordenar-se estreitamente com os usuários locatários para garantir que os objetos sejam protegidos de uma maneira que atenda aos seus requisitos de retenção.



A aplicação das configurações do locatário na grade 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 grade e usuários locatários contêm as tarefas de alto nível para usar o recurso S3 Object Lock.

Administrador de rede

- Habilitar a configuração global de bloqueio de objeto S3 para todo o sistema StorageGRID .
- Garantir que as políticas de gestão do ciclo de vida da informação (ILM) sejam *compatíveis*; ou seja, que atendam aos "requisitos de buckets com bloqueio de objeto S3 habilitado" .
- Conforme necessário, permita que um locatário use Conformidade como modo de retenção. Caso contrário, somente o modo Governança é permitido.
- Conforme necessário, defina um período máximo de retenção para um locatário.

Usuário locatário

- Revise as considerações para buckets e objetos com o S3 Object Lock.
- Conforme necessário, entre em contato com o administrador da grade para habilitar a configuração global de bloqueio de objeto do S3 e definir permissões.
- Crie buckets com o S3 Object Lock habilitado.
- Opcionalmente, configure as definições de retenção padrão para um bucket:
 - Modo de retenção padrão: Governança ou Conformidade, se permitido pelo administrador da rede.
 - Período de retenção padrão: deve ser menor ou igual ao período máximo de retenção 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 rede.
 - Data de retenção: deve ser menor ou igual ao que é permitido pelo período máximo de retenção definido pelo administrador da grade.

Requisitos para bloqueio de objeto S3

Você deve revisar os requisitos para habilitar a configuração global do S3 Object Lock, os requisitos para criar regras e políticas de ILM compatíveis e as restrições que o StorageGRID impõe aos buckets e objetos que usam o S3 Object Lock.

Requisitos para usar a configuração global de bloqueio de objeto do S3

- Você deve habilitar a configuração global de Bloqueio de Objeto do S3 usando o Grid Manager ou a API de Gerenciamento de Grade antes que qualquer locatário do S3 possa criar um bucket com o Bloqueio de Objeto do S3 habilitado.
- Habilitar a configuração global de Bloqueio de Objeto S3 permite que todas as contas de locatários do S3 criem buckets com o Bloqueio de Objeto S3 habilitado.
- Depois de habilitar a configuração global de Bloqueio de Objeto do S3, você não poderá desabilitá-la.
- Não é possível habilitar o bloqueio de objeto S3 global, a menos que a regra padrão em todas as políticas ativas do ILM seja *compatível* (ou seja, a regra padrão deve estar em conformidade com os requisitos de buckets com o bloqueio de objeto S3 habilitado).
- Quando a configuração global de Bloqueio de Objeto S3 estiver habilitada, você não poderá criar uma nova política de ILM ou ativar uma política de ILM existente, a menos que a regra padrão na política esteja em conformidade. Depois que a configuração global de Bloqueio de Objeto do S3 for habilitada, as páginas de regras e políticas do ILM indicam quais regras do ILM são compatíveis.

Requisitos para regras ILM compatíveis

Se você quiser habilitar a configuração global de Bloqueio de Objeto do S3, deverá garantir que a regra padrão em todas as políticas ativas do ILM esteja em conformidade. Uma regra compatível satisfaz os requisitos de ambos os buckets com o Bloqueio de Objeto S3 habilitado e de quaisquer buckets existentes que tenham a Conformidade herdada habilitada:

- Ele deve criar pelo menos duas cópias de objetos replicados ou uma cópia codificada para eliminação.
- Essas cópias devem existir nos Nós de Armazenamento durante toda a duração de cada linha nas instruções de posicionamento.
- Cópias de objetos não podem ser salvas em um pool de armazenamento em nuvem.
- Pelo menos uma linha das instruções de posicionamento deve começar no dia 0, usando **Horário de ingestão** como horário de referência.
- Pelo menos uma linha das instruções de posicionamento deve ser "para sempre".

Requisitos para políticas de ILM

Quando a configuração global de Bloqueio de Objeto do S3 está habilitada, as políticas ativas e inativas do ILM podem incluir regras compatíveis e não compatíveis.

- A regra padrão em uma política de ILM ativa ou inativa deve ser compatível.
- Regras não compatíveis só se aplicam a objetos em buckets que não têm o Bloqueio de Objeto do S3 habilitado ou que não têm o recurso de Conformidade legado habilitado.
- Regras de conformidade podem ser aplicadas a objetos em qualquer bucket; o bloqueio de objeto S3 ou a conformidade herdada não precisam ser habilitados para o bucket.

"Exemplo de uma política de ILM compatível para bloqueio de objeto S3"

Requisitos para buckets com bloqueio de objeto S3 habilitado

- Se a configuração global do S3 Object Lock estiver habilitada para o sistema StorageGRID , você poderá usar o Tenant Manager, a Tenant Management API ou a S3 REST API para criar buckets com o S3 Object Lock habilitado.
- Se você planeja usar o S3 Object Lock, deverá habilitar o S3 Object Lock ao criar o bucket. Não é possível habilitar o S3 Object Lock para um bucket existente.
- Quando o S3 Object Lock é habilitado para um bucket, o StorageGRID habilita automaticamente o controle de versão para esse bucket. Não é possível desabilitar o bloqueio de objeto do S3 ou suspender o controle de versão do 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 retenção até a data para cada versão do objeto quando ele for carregado.
- A configuração do ciclo de vida do bucket é suportada para buckets com o S3 Object Lock habilitado.
- A replicação do CloudMirror não é suportada para buckets com S3 Object Lock habilitado.

Requisitos para objetos em buckets com bloqueio de objeto S3 habilitado

- Para proteger uma versão do objeto, você pode especificar configurações de retenção padrão para o bucket ou especificar configurações de retenção para cada versão do objeto. As configurações de

retenção no nível do objeto podem ser especificadas usando o aplicativo cliente S3 ou a API REST do S3.

- As configurações de retenção se aplicam a versões de objetos individuais. Uma versão de objeto pode ter uma configuração de retenção até a data e uma configuração de retenção legal, uma mas não a outra, ou nenhuma delas. Especificar uma configuração de retenção até a data ou de retenção 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 bloqueio de objeto S3 habilitado

Cada objeto salvo em um bucket com o S3 Object Lock habilitado passa por estas etapas:

1. Ingestão de objetos

Quando uma versão de objeto é adicionada ao bucket que tem o S3 Object Lock ativado, as configurações de retenção são aplicadas da seguinte maneira:

- Se as configurações de retenção forem especificadas para o objeto, as configurações no nível do objeto serão aplicadas. Todas as configurações de bucket padrão são ignoradas.
- Se nenhuma configuração de retenção for especificada para o objeto, as configurações de bucket padrão serão aplicadas, se existirem.
- Se nenhuma configuração de retenção for especificada para o objeto ou o bucket, o objeto não será protegido pelo S3 Object Lock.

Se as configurações de retenção forem aplicadas, tanto o objeto quanto quaisquer metadados definidos pelo usuário do S3 serão 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 objetos e os locais de armazenamento são determinados pelas regras de conformidade nas políticas ativas do ILM. Se um objeto protegido pode ser excluído antes que sua data de retenção seja atingida depende do seu modo de retenção.

- Se um objeto estiver sob retenção legal, ninguém poderá excluí-lo, independentemente do seu modo de retenção.

Informações relacionadas

- ["Criar um bucket S3"](#)
- ["Atualizar retenção padrão do bloqueio de objeto S3"](#)
- ["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)
- ["Exemplo 7: Política ILM compatível para bloqueio de objeto S3"](#)

Habilitar bloqueio de objeto S3 globalmente

Se uma conta de locatário do S3 precisar estar em conformidade com requisitos regulatórios ao salvar dados de objeto, você deverá habilitar o Bloqueio de Objeto do S3 para todo o seu sistema StorageGRID . Habilitar a configuração global do S3 Object Lock permite que qualquer usuário locatário do S3 crie e gerencie buckets e objetos com o S3 Object Lock.

Antes de começar

- Você tem o "[Permissão de acesso root](#)".
- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você revisou o fluxo de trabalho do S3 Object Lock e entende as considerações.
- Você confirmou que a regra padrão na política ILM ativa é compatível. Ver "[Criar uma regra ILM padrão](#)" para mais detalhes.

Sobre esta tarefa

Um administrador de grade deve habilitar a configuração global de Bloqueio de Objeto S3 para permitir que usuários locatários criem novos buckets que tenham o Bloqueio de Objeto S3 habilitado. Depois que essa configuração for ativada, ela não poderá ser desativada.

Revise as configurações de conformidade dos locatários existentes depois de habilitar a configuração global de Bloqueio de Objeto do S3. Quando você habilita essa configuração, as configurações por locatário do S3 Object Lock dependem da versão do StorageGRID no momento em que o locatário foi criado.



A configuração global de Conformidade está obsoleta. Se você habilitou essa configuração usando uma versão anterior do StorageGRID, a configuração de Bloqueio de Objeto do S3 será habilitada automaticamente. Você pode continuar a usar o StorageGRID para gerenciar as configurações de buckets compatíveis existentes; no entanto, não é possível criar novos buckets compatíveis. Para mais detalhes, veja "[Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5](#)".

Passos

1. Selecione **CONFIGURAÇÃO > Sistema > Bloqueio de Objeto S3**.

A página Configurações de bloqueio de objeto do S3 é exibida.

2. Selecione **Ativar bloqueio de objeto S3**.
3. Selecione **Aplicar**.

Uma caixa de diálogo de confirmação é exibida e lembra que não é possível desabilitar o S3 Object Lock depois que ele for habilitado.

4. Se você tiver certeza de que deseja habilitar permanentemente o S3 Object Lock para todo o seu sistema, selecione **OK**.

Quando você seleciona **OK**:

- Se a regra padrão na política ILM ativa estiver em conformidade, o Bloqueio de Objeto S3 agora estará habilitado para toda a grade e não poderá ser desabilitado.
- Se a regra padrão não for compatível, um erro será exibido. Você deve criar e ativar uma nova política de ILM que inclua uma regra compatível como regra padrão. Selecione **OK**. Em seguida, crie uma nova política, simule-a e ative-a. Ver "[Criar política de ILM](#)" para obter instruções.

Resolver erros de consistência ao atualizar o bloqueio de objeto S3 ou a configuração de conformidade herdada

Se um site de data center ou vários nós de armazenamento em um site ficarem indisponíveis, talvez seja necessário ajudar os usuários do locatário do S3 a aplicar alterações no bloqueio de objeto do S3 ou na configuração de conformidade herdada.

Usuários locatários que têm buckets com o Bloqueio de Objeto S3 (ou Conformidade herdada) habilitado podem alterar determinadas configurações. Por exemplo, um usuário locatário que utiliza o S3 Object Lock pode precisar colocar uma versão do objeto em retenção legal.

Quando um usuário locatário atualiza as configurações de um bucket do S3 ou uma versão de objeto, o StorageGRID tenta atualizar imediatamente os metadados do bucket ou do objeto na grade. Se o sistema não conseguir atualizar os metadados porque um site de data center ou vários nós de armazenamento não estão disponíveis, ele retornará 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 estas etapas:

1. Tente tornar todos os nós de armazenamento ou sites disponíveis novamente o mais rápido possível.
2. Se você não conseguir disponibilizar nós de armazenamento suficientes em cada site, entre em contato com o suporte técnico, que pode ajudar você a recuperar nós e garantir que as alterações sejam aplicadas de forma consistente em toda a grade.
3. Depois que o problema subjacente for resolvido, lembre o usuário locatário de tentar novamente as alterações de configuração.

Informações relacionadas

- ["Use uma conta de inquilino"](#)
- ["Usar API REST do S3"](#)
- ["Recuperar e manter"](#)

Exemplo de regras e políticas do ILM

Exemplo 1: regras e políticas do ILM para armazenamento de objetos

Você pode usar as seguintes regras e políticas de exemplo como ponto de partida ao definir uma política de ILM para atender aos seus requisitos de proteção e retenção de objetos.



As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Regra 1 do ILM, por exemplo 1: Copiar dados do objeto para dois sites

Este exemplo de regra ILM copia dados de objeto para pools de armazenamento em dois sites.

Definição de regra	Valor de exemplo
Pools de armazenamento de um único local	Dois pools de armazenamento, cada um contendo sites diferentes, chamados Site 1 e Site 2.

Definição de regra	Valor de exemplo
Nome da regra	Duas cópias, dois sites
Tempo de referência	Tempo de ingestão
Posicionamentos	Do Dia 0 até sempre, mantenha uma cópia replicada no Site 1 e uma cópia replicada no Site 2.

A seção Análise de regras do diagrama de retenção afirma:

- A proteção contra perda de site do StorageGRID será aplicada durante a vigência desta regra.
- Objetos processados por esta regra não serão excluídos pelo ILM.

Regra 2 do ILM, por exemplo 1: Perfil de codificação de apagamento com correspondência de bucket

Este exemplo de regra ILM usa um perfil de codificação de eliminação e um bucket S3 para determinar onde e por quanto tempo o objeto é armazenado.

Definição de regra	Valor de exemplo
Pool de armazenamento com vários locais	• Um pool de armazenamento em três locais (locais 1, 2, 3) • Use o esquema de codificação de apagamento 6+3
Nome da regra	Registros financeiros do S3 Bucket
Tempo de referência	Tempo de ingestão
Posicionamentos	Para objetos no bucket do S3 denominados finance-records, crie uma cópia codificada para eliminação no pool especificado pelo perfil de codificação para eliminação. Guarde esta cópia para sempre.

Política ILM, por exemplo 1

Na prática, a maioria das políticas de ILM são simples, embora o sistema StorageGRID permita que você crie políticas de ILM sofisticadas e complexas.

Uma política de ILM típica para uma grade multisite pode incluir regras de ILM como as seguintes:

- Na ingestão, armazene todos os objetos pertencentes ao bucket S3 denominado `finance-records` em um pool de armazenamento que contém três sites. Use a codificação de eliminação 6+3.
- Se um objeto não corresponder à primeira regra do ILM, use a regra do ILM padrão da política, Duas Cópias, Dois Data Centers, para armazenar uma cópia desse objeto no Site 1 e uma cópia no Site 2.

Informações relacionadas

- ["Usar políticas de ILM"](#)

- "Criar políticas de ILM"

Exemplo 2: regras e políticas do ILM para filtragem de tamanho de objeto EC

Você pode usar as seguintes regras e políticas de exemplo como pontos de partida para definir uma política de ILM que filtre por tamanho de objeto para atender aos requisitos de EC recomendados.



As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Regra 1 do ILM, exemplo 2: Use EC para objetos maiores que 1 MB

Este exemplo de regra de eliminação do ILM codifica objetos maiores que 1 MB.



A codificação de eliminação é mais adequada para objetos maiores que 1 MB. Não use codificação de eliminação para objetos menores que 200 KB para evitar a sobrecarga de gerenciamento de fragmentos muito pequenos codificados por eliminação.

Definição de regra	Valor de exemplo
Nome da regra	Objetos somente EC > 1 MB
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Tamanho do objeto maior que 1 MB
Posicionamentos	Crie uma cópia codificada para eliminação 2+1 usando três sites

Regra 2 do ILM, por exemplo 2: Duas cópias replicadas

Este exemplo de regra ILM cria duas cópias replicadas e não filtra por tamanho do objeto. Esta regra é a regra padrão para a política. Como a primeira regra filtra todos os objetos maiores que 1 MB, esta regra só se aplica a objetos com 1 MB ou menos.

Definição de regra	Valor de exemplo
Nome da regra	Duas cópias replicadas
Tempo de referência	Tempo de ingestão
Filtro avançado para tamanho do objeto	Nenhum
Posicionamentos	Do Dia 0 até sempre, mantenha uma cópia replicada no Site 1 e uma cópia replicada no Site 2.

Política ILM para exemplo 2: Usar EC para objetos maiores que 1 MB

Este exemplo de política de ILM inclui duas regras de ILM:

- A primeira regra de eliminação codifica todos os objetos maiores que 1 MB.
- A segunda regra ILM (padrão) cria duas cópias replicadas. Como objetos maiores que 1 MB foram filtrados pela regra 1, a regra 2 se aplica somente a objetos com 1 MB ou menos.

Exemplo 3: Regras e políticas do ILM para melhor proteção de arquivos de imagem

Você pode usar os seguintes exemplos de regras e políticas para garantir que imagens maiores que 1 MB sejam codificadas para eliminação e que duas cópias sejam feitas de imagens menores.



As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Regra 1 do ILM, exemplo 3: Use EC para arquivos de imagem maiores que 1 MB

Este exemplo de regra ILM usa filtragem avançada para apagar o código de todos os arquivos de imagem maiores que 1 MB.



A codificação de eliminação é mais adequada para objetos maiores que 1 MB. Não use codificação de eliminação para objetos menores que 200 KB para evitar a sobrecarga de gerenciamento de fragmentos muito pequenos codificados por eliminação.

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 maior que 1 MB
Filtros avançados para Chave	• Termina com .jpg • Termina com .png
Posicionamentos	Crie uma cópia codificada para eliminação 2+1 usando três sites

Como essa regra é configurada como a primeira regra na política, a instrução de posicionamento de codificação de eliminação só se aplica a arquivos .jpg e .png maiores que 1 MB.

Regra 2 do ILM, exemplo 3: Crie 2 cópias replicadas para todos os arquivos de imagem restantes

Este exemplo de regra ILM usa filtragem avançada para especificar que arquivos de imagem menores sejam replicados. Como a primeira regra da política já correspondeu a arquivos de imagem maiores que 1 MB, esta regra se aplica a arquivos de imagem com 1 MB ou menos.

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
Posicionamentos	Crie 2 cópias replicadas em dois pools de armazenamento

Política de ILM, exemplo 3: Melhor proteção para arquivos de imagem

Este exemplo de política de ILM inclui três regras:

- A primeira regra de eliminação codifica 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 menos).
- A regra padrão se aplica a todos os objetos restantes (ou seja, quaisquer arquivos que não sejam de imagem).

Exemplo 4: regras e políticas do ILM para objetos versionados do S3

Se você tiver um bucket do S3 com controle de versão habilitado, poderá gerenciar as versões de objetos não atuais incluindo regras na sua política do ILM que usam "Tempo não atual" como tempo de referência.



Se você especificar um tempo de retenção limitado para objetos, eles serão excluídos permanentemente após o período ser atingido. Certifique-se de entender 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 posicionamento diferentes para versões de objetos não atuais.



As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.



Para executar a simulação de política do ILM em uma versão não atual de um objeto, você deve 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, por exemplo 4: Guarde três cópias por 10 anos

Este exemplo de regra ILM armazena uma cópia de cada objeto em três sites por 10 anos.

Esta regra se aplica a todos os objetos, independentemente de terem ou não controle de versão.

Definição de regra	Valor de exemplo
Pools de armazenamento	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
Tempo de referência	Tempo de ingestão
Posicionamentos	No Dia 0, mantenha três cópias replicadas por 10 anos (3.652 dias), uma no Local 1, uma no Local 2 e uma no Local 3. Ao final de 10 anos, exclua todas as cópias do objeto.

Regra 2 do ILM, exemplo 4: Salve duas cópias de versões não atuais por 2 anos

Este exemplo de regra ILM 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 usa "Tempo não atual" como tempo de referência, selecione **Sim** para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com controle de versão habilitado)?" na Etapa 1 (Inserir detalhes) do assistente Criar uma regra do ILM. Quando você seleciona **Sim**, *Horário não atual* é selecionado automaticamente como horário de referência, e você não pode selecionar um horário 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 diferentes data centers, Site 1 e Site 2.
Nome da regra	Versões não atuais: duas cópias, dois anos
Tempo de referência	Tempo não atual Selecionado automaticamente quando você seleciona Sim para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas (em buckets do S3 com controle de versão habilitado)?" no assistente Criar uma regra do ILM.
Posicionamentos	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 o exemplo 4: objetos versionados S3

Se você quiser gerenciar versões mais 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 do ILM antes das regras que se aplicam à versão atual do objeto.

Uma política de ILM para objetos versionados do S3 pode incluir regras de ILM como as seguintes:

- Mantenha todas as versões mais 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 de objetos não atuais nunca serão correspondidas pela regra "Tempo não atual".

- Na 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 maneira:

- Qualquer versão de objeto não atual seria correspondida pela primeira regra. Se uma versão de objeto não atual tiver mais de 2 anos, ela será excluída permanentemente pelo ILM (todas as cópias da versão não atual serão removidas da grade).
- A versão atual do objeto seria correspondida pela segunda regra. Quando a versão atual do objeto é 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 vez que ocorrer uma avaliação do ILM, esta versão não atual será correspondida pela primeira regra. Como resultado, a cópia no Site 3 é eliminada e as duas cópias no Site 1 e no Site 2 são armazenadas por mais 2 anos.

Exemplo 5: regras e política do ILM para comportamento de ingestão estrita

Você pode usar um filtro de localização e o comportamento de ingestão Estrito em uma regra para impedir que objetos sejam salvos em um local específico do data center.

Neste exemplo, um inquilino baseado em Paris não quer 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 seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se 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, por exemplo 5: ingestão rigorosa para garantir o data center de Paris

Este exemplo de regra do ILM usa o comportamento de ingestão Strict para garantir que objetos salvos por um locatário baseado em Paris em buckets do S3 com a região definida como eu-west-3 (Paris) nunca sejam armazenados no data center dos EUA.

Esta regra se aplica a objetos que pertencem ao locatário de Paris e que têm a região do bucket S3 definida como eu-west-3 (Paris).

Definição de regra	Valor de exemplo
Conta de inquilino	inquilino de Paris
Filtro avançado	A restrição de localização é igual a eu-west-3
Pools de armazenamento	Sítio 1 (Paris)
Nome da regra	Ingestão rigorosa para garantir o centro de dados de Paris
Tempo de referência	Tempo de ingestão
Posicionamentos	No Dia 0, mantenha duas cópias replicadas para sempre no Site 1 (Paris)
Comportamento de ingestão	Estrito. Sempre use os posicionamentos desta regra na ingestão. A ingestão falha 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

411

Regra 2 do ILM, exemplo 5: ingestão balanceada para outros objetos

Este exemplo de regra de ILM usa o comportamento de ingestão balanceada para fornecer eficiência ideal de ILM para quaisquer objetos não correspondidos pela primeira regra. Duas cópias de todos os objetos correspondentes a esta regra serão armazenadas: uma no centro de dados dos EUA e outra no centro de dados de Paris. Se a regra não puder ser cumprida imediatamente, cópias provisórias serão armazenadas em qualquer local disponível.

Esta regra se aplica a objetos que pertencem a qualquer locatário e qualquer região.

Definição de regra	Valor de exemplo
Conta de inquilino	Ignorar
Filtro avançado	<i>Não especificado</i>
Pools de armazenamento	Site 1 (Paris) e Site 2 (EUA)
Nome da regra	2 Cópias 2 Data Centers
Tempo de referência	Tempo de ingestão
Posicionamentos	No Dia 0, mantenha duas cópias replicadas para sempre em dois data centers
Comportamento de ingestão	Equilibrado. Objetos que correspondem a essa regra são colocados de acordo com as instruções de posicionamento da regra, se possível. Caso contrário, cópias provisórias serão feitas em qualquer local disponível.

Política de ILM para o exemplo 5: Combinando comportamentos de ingestão

O exemplo de política de ILM inclui duas regras que têm comportamentos de ingestão diferentes.

Uma política de ILM que usa dois comportamentos de ingestão diferentes pode incluir regras de ILM como as seguintes:

- Armazene objetos que pertencem ao locatário de Paris e que tenham a região do bucket S3 definida como eu-west-3 (Paris) somente no data center de Paris. Falha na 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) no data center dos EUA e no data center de Paris. Faça cópias provisórias em qualquer local disponível se a instrução de posicionamento não puder ser atendida.

Ao simular a política de exemplo, você espera que os objetos de teste sejam avaliados da seguinte maneira:

- Todos os objetos que pertencem ao locatário de Paris e que têm 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 falhará.
- Todos os outros objetos são correspondidos pela segunda regra, incluindo objetos que pertencem 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 centro de dados. No entanto, como a segunda regra usa ingestão balanceada, se um data center não estiver disponível, duas cópias provisórias serão salvas em qualquer local disponível.

Exemplo 6: Alterar uma política de ILM

Se sua proteção de dados precisar ser alterada ou você adicionar novos sites, você poderá criar e ativar uma nova política de ILM.

Antes de alterar uma política, você deve entender como as alterações 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 de ILM ativa precisa ser implementada para armazenar dados no novo site. Para implementar uma nova política ativa, primeiro ["criar uma política"](#) . Depois, você deve ["simular"](#) e então ["ativar"](#) a nova política.



As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se 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 de ILM, o desempenho do seu sistema StorageGRID pode ser temporariamente afetado, especialmente se as instruções de posicionamento na nova política exigirem que muitos objetos existentes sejam movidos para novos locais.

Quando você ativa uma nova política de ILM, o StorageGRID a usa para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Antes de ativar uma nova política de ILM, revise quaisquer alterações no posicionamento de objetos replicados e codificados para eliminação 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 de ILM não afete o posicionamento de objetos replicados e codificados para eliminação existentes, você pode ["crie uma regra ILM com um filtro de tempo de ingestão"](#) . Por exemplo, **O tempo de ingestão é em ou após <data e hora>**, de modo que a nova regra se aplica somente a objetos ingeridos na data e hora especificadas ou após ela.

Os tipos de alterações na política do ILM que podem afetar temporariamente o desempenho do StorageGRID incluem o seguinte:

- Aplicar um perfil de codificação de eliminação diferente a objetos codificados por eliminação existentes.



O StorageGRID considera cada perfil de codificação de eliminação como único e não reutiliza fragmentos de codificação de eliminação 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 codificados para eliminação.
- Mover cópias de objetos existentes para um local completamente diferente; por exemplo, mover um grande número de objetos de ou para um pool de armazenamento em nuvem ou de ou para um site remoto.

Política de ILM ativa, por exemplo 6: Proteção de dados em dois sites

Neste exemplo, a política ILM ativa foi projetada inicialmente para um sistema StorageGRID de dois sites e usa 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	—

Nesta política de ILM, os objetos pertencentes ao Locatário A são protegidos pela codificação de eliminação 2+1 em um único site, enquanto os objetos pertencentes a todos os outros locatários são protegidos em dois sites usando replicação de 2 cópias.

Regra 1: Codificação de eliminação de um site para o Locatário A

Definição de regra	Valor de exemplo
Nome da regra	Codificação de eliminação de um site para o inquilino A
Conta de inquilino	Inquilino A
Pool de armazenamento	Sítio 1
Posicionamentos	Codificação de eliminação 2+1 no Site 1 do dia 0 até sempre

Regra 2: Replicação de dois sites para outros locatários

Definição de regra	Valor de exemplo
Nome da regra	Replicação de dois sites para outros locatários
Conta de inquilino	Ignorar
Pools de armazenamento	Sítio 1 e Sítio 2

Definição de regra	Valor de exemplo
Posicionamentos	Duas cópias replicadas do dia 0 até sempre: uma cópia no Site 1 e uma cópia no Site 2.

Política de ILM, 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 sites.

Após executar uma expansão para adicionar o novo site, o administrador da grade criou dois novos pools de armazenamento: um pool de armazenamento para o Site 3 e um pool de armazenamento contendo todos os três sites (não o mesmo que o pool de armazenamento padrão Todos os Nós de Armazenamento). Em seguida, o administrador criou duas novas regras de ILM e uma nova política de ILM, projetadas para proteger dados em todos os três sites.

Quando essa nova política de ILM for ativada, os objetos pertencentes ao Locatário A serão protegidos pela codificação de eliminação 2+1 em três sites, enquanto os objetos pertencentes a outros locatários (e objetos menores pertencentes ao Locatário A) serão protegidos em três sites usando replicação de 3 cópias.

Regra 1: Codificação de eliminação de três sites para o Locatário A

Definição de regra	Valor de exemplo
Nome da regra	Codificação de eliminação de três sites para o inquilino A
Conta de inquilino	Inquilino A
Pool de armazenamento	Todos os 3 sites (inclui Site 1, Site 2 e Site 3)
Posicionamentos	Codificação de eliminação 2+1 em todos os 3 sites do dia 0 até sempre

Regra 2: Replicação de três sites para outros inquilinos

Definição de regra	Valor de exemplo
Nome da regra	Replicação de três sites para outros inquilinos
Conta de inquilino	Ignorar
Pools de armazenamento	Sítio 1, Sítio 2 e Sítio 3
Posicionamentos	Três cópias replicadas do dia 0 até sempre: uma cópia no Local 1, uma cópia no Local 2 e uma cópia no Local 3.

Ativando a política ILM, por exemplo 6

Quando você ativa uma nova política de ILM, 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 irreversível de dados. Revise e simule cuidadosamente a política antes de ativá-la para confirmar se ela funcionará conforme o esperado.



Quando você ativa uma nova política de ILM, o StorageGRID a usa para gerenciar todos os objetos, incluindo objetos existentes e objetos recém-ingeridos. Antes de ativar uma nova política de ILM, revise quaisquer alterações no posicionamento de objetos replicados e codificados para eliminação 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 Locatário A são protegidos usando codificação de eliminação 2+1 no Site 1. Na nova política de ILM, os objetos pertencentes ao Locatário A serão protegidos usando codificação de eliminação 2+1 nos Sites 1, 2 e 3.

Quando a nova política de ILM é ativada, ocorrem as seguintes operações de ILM:

- Novos objetos ingeridos pelo Tenant A são divididos em dois fragmentos de dados e um fragmento de paridade é adicionado. Então, cada um dos três fragmentos é armazenado em um local diferente.
- Os objetos existentes pertencentes ao Locatário A são reavaliados durante o processo de verificação do ILM em andamento. Como as instruções de posicionamento do ILM usam um novo perfil de codificação de eliminação, fragmentos inteiramente novos codificados por eliminação são criados e distribuídos para os três locais.



Os fragmentos 2+1 existentes no Sítio 1 não são reutilizados. O StorageGRID considera cada perfil de codificação de eliminação como único e não reutiliza fragmentos de codificação de eliminação quando um novo perfil é usado.

O que acontece quando as instruções de replicação mudam

Na política de ILM atualmente ativa para este exemplo, objetos pertencentes a outros locatários são protegidos usando duas cópias replicadas em pools de armazenamento nos Sites 1 e 2. Na nova política de ILM, objetos pertencentes a outros locatários serão protegidos usando três cópias replicadas em pools de armazenamento nos Sites 1, 2 e 3.

Quando a nova política de ILM é ativada, ocorrem as seguintes operações de ILM:

- Quando qualquer locatário diferente do Locatário A ingere um novo objeto, o StorageGRID cria três cópias e salva uma cópia em cada site.
- Objetos existentes pertencentes a esses outros inquilinos são reavaliados durante o processo de verificação contínua 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, o StorageGRID precisa criar apenas uma nova cópia do objeto para o Site 3.

Impacto no desempenho da ativação desta política

Quando a política ILM neste exemplo for ativada, o desempenho geral deste sistema StorageGRID será temporariamente afetado. Serão necessários níveis de recursos de grade maiores que o normal para criar

novos fragmentos codificados por eliminação para os objetos existentes do Locatário A e novas cópias replicadas no Site 3 para os objetos existentes de outros locatários.

Como resultado da alteração da política de ILM, as solicitações de leitura e gravação do cliente podem apresentar latências temporariamente maiores que o normal. As latências retornarão aos níveis normais depois que as instruções de posicionamento forem totalmente implementadas na grade.

Para evitar problemas de recursos ao ativar uma nova política de 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 como maior ou igual ao tempo aproximado em que a nova política entrará em vigor para garantir que os objetos existentes não sejam movidos desnecessariamente.



Entre em contato com o suporte técnico se precisar diminuir ou aumentar a taxa de processamento de objetos após uma alteração na política do ILM.

Exemplo 7: Política ILM compatível para bloqueio de objeto S3

Você pode usar o bucket do S3, as regras do ILM e a política do ILM neste exemplo como ponto de partida ao definir uma política do ILM para atender aos requisitos de proteção e retenção de objetos em buckets com o Bloqueio de Objeto do S3 habilitado.



Se você usou o recurso de conformidade legado em versões anteriores do StorageGRID , também pode usar este exemplo para ajudar a gerenciar quaisquer buckets existentes que tenham o recurso de conformidade legado habilitado.



As seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas.

Informações relacionadas

- ["Gerenciar objetos com o S3 Object Lock"](#)
- ["Criar uma política de ILM"](#)

Exemplo de bucket e objetos para bloqueio de objeto S3

Neste exemplo, uma conta de locatário do S3 chamada Bank of ABC usou o Tenant Manager para criar um bucket com o S3 Object Lock habilitado para armazenar registros bancários críticos.

Definição de balde	Valor de exemplo
Nome da conta do inquilino	Banco do ABC
Nome do balde	registros bancários
Região do balde	us-east-1 (padrão)

Cada objeto e versão de objeto que for adicionado ao bucket de registros bancários usará 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 tem sua própria <code>retain-until-date</code> contexto. Esta configuração pode ser aumentada, mas não diminuída.
<code>legal hold</code>	"OFF" (Não em vigor) Uma retenção legal pode ser colocada ou suspensa em qualquer versão do objeto a qualquer momento durante o período de retenção. Se um objeto estiver sob retenção legal, o objeto não poderá ser excluído, mesmo que <code>retain-until-date</code> foi alcançado.

Exemplo de regra 1 do ILM para bloqueio de objeto S3: perfil de codificação de eliminação com correspondência de bucket

Este exemplo de regra do ILM se aplica somente à conta de locatário do S3 chamada Bank of ABC. Ele corresponde a qualquer objeto no `bank-records` bucket e, em seguida, usa codificação de eliminação para armazenar o objeto em nós de armazenamento em três locais de data center usando um perfil de codificação de eliminação 6+3. Esta regra atende aos requisitos de buckets com o S3 Object Lock habilitado: uma cópia é mantida nos nós de armazenamento do dia 0 até sempre, usando o tempo 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 - Banco do ABC
Conta de inquilino	Banco do ABC
Nome do balde	<code>bank-records</code>
Filtro avançado	Tamanho do objeto (MB) maior que 1 Observação: Este filtro garante que a codificação de eliminação não seja usada para objetos de 1 MB ou menores.

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Posicionamentos	Desde o dia 0, armazene para sempre
Perfil de codificação de apagamento	• Crie uma cópia codificada para eliminação em nós de armazenamento em três locais de data center • Utiliza esquema de codificação de apagamento 6+3

Exemplo de regra 2 do ILM para bloqueio de objeto S3: regra não compatível

Este exemplo de regra ILM armazena inicialmente duas cópias de objetos replicadas em nós de armazenamento. Após um ano, ele armazena uma cópia em um pool de armazenamento em nuvem para sempre. Como essa regra usa um pool de armazenamento em nuvem, ela não é compatível e não se aplicará aos objetos em buckets com o bloqueio de objeto do S3 habilitado.

Definição de regra	Valor de exemplo
Nome da regra	Regra não compatível: usar pool de armazenamento em nuvem
Contas de inquilinos	Não especificado
Nome do balde	Não especificado, mas só será aplicado a buckets que não tenham o S3 Object Lock (ou o recurso de conformidade legado) habilitado.
Filtro avançado	Não especificado

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão
Posicionamentos	• No Dia 0, mantenha duas cópias replicadas nos Nós de Armazenamento no Data Center 1 e no Data Center 2 por 365 dias • Após 1 ano, mantenha uma cópia replicada em um pool de armazenamento em nuvem para sempre

Exemplo de regra 3 do ILM para bloqueio de objeto S3: regra padrão

Este exemplo de regra ILM copia dados de objeto para pools de armazenamento em dois data centers. Esta regra compatível foi criada para ser a regra padrão na política do ILM. Ele não inclui nenhum filtro, não usa o tempo de referência Não Atual e atende aos requisitos de buckets com Bloqueio de Objeto S3 habilitado: duas cópias de objeto são mantidas em Nós de Armazenamento do dia 0 até sempre, usando Ingestão como o tempo de referência.

Definição de regra	Valor de exemplo
Nome da regra	Regra padrão compatível: Duas cópias, dois data centers
Conta de inquilino	Não especificado
Nome do balde	Não especificado
Filtro avançado	Não especificado

Definição de regra	Valor de exemplo
Tempo de referência	Tempo de ingestão

Definição de regra	Valor de exemplo
Posicionamentos	Do Dia 0 até sempre, mantenha duas cópias replicadas: uma nos Nós de Armazenamento no Data Center 1 e uma nos Nós de Armazenamento no Data Center 2.

Exemplo de política de ILM compatível para bloqueio de objeto S3

Para criar uma política de ILM que proteja efetivamente todos os objetos no seu sistema, incluindo aqueles em buckets com o S3 Object Lock habilitado, você deve selecionar regras de ILM que atendam aos requisitos de armazenamento para todos os objetos. Então, você deve simular e ativar a política.

Adicionar regras à política

Neste exemplo, a política de ILM inclui três regras de ILM, na seguinte ordem:

1. Uma regra compatível que usa codificação de eliminação para proteger objetos maiores que 1 MB em um bucket específico com o S3 Object Lock habilitado. Os objetos são armazenados em nós de armazenamento do dia 0 até sempre.
2. Uma regra não compatível que cria duas cópias de objetos replicadas em nós de armazenamento por um ano e depois move uma cópia de objeto para um pool de armazenamento em nuvem para sempre. Esta regra não se aplica a buckets com o S3 Object Lock habilitado porque ele usa um Cloud Storage Pool.
3. A regra padrão compatível que cria duas cópias de objetos replicadas em nós de armazenamento do dia 0 até sempre.

Simule a política

Depois de adicionar regras à sua política, escolher uma regra padrão compatível e organizar as outras regras, você deve simular a política testando objetos do bucket com o Bloqueio de Objeto S3 habilitado e de outros buckets. Por exemplo, ao simular a política de exemplo, você esperaria que os objetos de teste fossem avaliados da seguinte maneira:

- A primeira regra corresponderá somente a objetos de teste maiores que 1 MB nos registros bancários do bucket para o locatário do Bank of ABC.
- A segunda regra corresponderá a todos os objetos em todos os buckets não compatíveis para todas as outras contas de locatários.
- A regra padrão corresponderá a estes objetos:
 - Objetos de 1 MB ou menores nos registros bancários do bucket para o locatário do Bank of ABC.
 - Objetos em qualquer outro bucket que tenha o Bloqueio de Objeto do S3 habilitado para todas as outras contas de locatário.

Ativar a política

Quando estiver completamente satisfeito de que a nova política protege os dados do objeto conforme o esperado, você poderá ativá-la.

Exemplo 8: Prioridades para o ciclo de vida do bucket S3 e política de ILM

Dependendo da configuração do seu ciclo de vida, os objetos seguem as configurações de retenção do ciclo de vida do bucket do S3 ou de uma política do ILM.

Exemplo de ciclo de vida de bucket tendo prioridade sobre política de ILM

Política de ILM

- Regra baseada em referência de tempo não 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 balde

```
"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 do prefixo "docs/".
 - Após 100 dias, um marcador de exclusão é criado e "docs/text" se torna não atual.
 - Após 5 dias, um total de 105 dias desde a ingestão, "docs/text" é excluído.
 - Após 95 dias, um total de 200 dias desde a ingestão e 100 dias desde a criação do marcador de exclusão, o marcador de exclusão expirado é excluído.
- Um objeto chamado "vídeo/filme" é ingerido. Ele não corresponde ao filtro e usa a política de retenção do ILM.
 - Após 50 dias, um marcador de exclusão é criado e "vídeo/filme" deixa de ser atual.
 - Após 20 dias, um total de 70 dias desde a ingestão, "vídeo/filme" é excluído.
 - Após 30 dias, um total de 100 dias desde a ingestão e 50 dias desde a criação do marcador de exclusão, o marcador de exclusão expirado é excluído.

Exemplo de ciclo de vida de bucket mantendo implicitamente para sempre

Política de ILM

- Regra baseada em referência de tempo não 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 balde

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":  
true}
```

Resultado

- Um objeto chamado "docs/text" é ingerido. Ele corresponde ao filtro de ciclo de vida do bucket do prefixo "docs/".

O `Expiration` a ação se aplica somente 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 "vídeo/filme" é ingerido. Ele não corresponde ao filtro e usa a política de retenção do ILM.
 - Após 50 dias, um marcador de exclusão é criado e "vídeo/filme" deixa de ser atual.
 - Após 20 dias, um total de 70 dias desde a ingestão, "vídeo/filme" é excluído.
 - Após 30 dias, um total de 100 dias desde a ingestão 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 de ILM

- Regra baseada em referência de tempo não atual: No dia 0, mantenha X cópias por 20 dias
- Regra baseada na referência de tempo de ingestão (padrão): No dia 0, manter X cópias para sempre

Ciclo de vida do balde

```
"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 ILM foi projetada para remover objetos manualmente e limpar versões não atuais após 20 dias. Consequentemente, a regra de tempo de ingestão manterá os marcadores de exclusão expirados para sempre.
 - O ciclo de vida do bucket duplica o comportamento da política ILM ao adicionar "ExpiredObjectDeleteMarker": true, que remove marcadores de exclusão quando eles expiram
- Um objeto é ingerido. Nenhum 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 expira.
 - Pouco depois, o marcador de exclusão expirado é excluído.

Endurecimento do sistema

Considerações gerais para o reforço do sistema

O reforço do sistema é o processo de eliminar o máximo possível de riscos de segurança de um sistema StorageGRID .

Ao instalar e configurar o StorageGRID, use estas diretrizes para ajudar a atender a quaisquer objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade.

Você já deve estar usando as melhores práticas padrão do setor para reforço do sistema. Por exemplo, você usa senhas fortes para StorageGRID, usa HTTPS em vez de HTTP e habilita a autenticação baseada em certificado quando disponível.

O StorageGRID segue o ["Política de tratamento de vulnerabilidades da NetApp"](#) . As vulnerabilidades relatadas são verificadas e tratadas de acordo com o processo de resposta a incidentes de segurança do produto.

Ao fortalecer um sistema StorageGRID , considere o seguinte:

- *Qual das três redes StorageGRID * você implementou? Todos os sistemas StorageGRID devem usar a Rede Grid, mas você também pode usar a Rede de administração, a Rede de cliente ou ambas. Cada rede tem diferentes considerações de segurança.

- **O tipo de plataforma** que você usa para os nós individuais no seu sistema StorageGRID . Os nós do StorageGRID podem ser implantados em máquinas virtuais VMware, dentro de um mecanismo de contêiner em hosts Linux ou como dispositivos de hardware dedicados. Cada tipo de plataforma tem seu próprio conjunto de práticas recomendadas de proteção.
- **Quão confiáveis são as contas dos inquilinos.** Se você for um provedor de serviços com contas de locatários não confiáveis, terá preocupações de segurança diferentes do que se usasse apenas locatários internos confiáveis.
- **Quais requisitos e convenções de segurança** sua organização segue. Talvez seja necessário cumprir requisitos regulatórios ou corporativos específicos.

Diretrizes de reforço para atualizações de software

Você deve manter seu sistema StorageGRID e serviços relacionados atualizados para se defender contra ataques.

Atualizações para o 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 reduz a área geral da superfície de ataque. Além disso, as versões mais recentes do StorageGRID geralmente contêm recursos de reforço de segurança que não estão incluídos nas versões anteriores.

Consulte o "[Ferramenta de Matriz de Interoperabilidade da NetApp](#)" (IMT) para determinar qual versão do software StorageGRID você deve usar. Quando um hotfix é necessário, a NetApp prioriza a criação de atualizações para as versões mais recentes. Alguns patches podem não ser compatíveis com versões anteriores.

- Para baixar os lançamentos e hotfixes mais recentes do StorageGRID , acesse "[Downloads da NetApp : StorageGRID](#)" .
- Para atualizar o software StorageGRID , consulte o "[instruções de atualização](#)" .
- Para aplicar um hotfix, consulte o "[Procedimento de correção do StorageGRID](#)" .

Atualizações para serviços externos

Serviços externos podem ter vulnerabilidades que afetam o StorageGRID indiretamente. Você deve garantir que os serviços dos quais o StorageGRID depende sejam mantidos atualizados. Esses serviços incluem LDAP, KMS (ou servidor KMIP), DNS e NTP.

Para obter uma lista de versões suportadas, consulte o "[Ferramenta de Matriz de Interoperabilidade da NetApp](#)" .

Atualizações para hipervisores

Se os seus nós StorageGRID estiverem em execução no VMware ou em outro hipervisor, você deverá garantir que o software e o firmware do hipervisor estejam atualizados.

Para obter uma lista de versões suportadas, consulte o "[Ferramenta de Matriz de Interoperabilidade da NetApp](#)" .

Atualizações para nós Linux

Se os seus nós StorageGRID estiverem usando plataformas host Linux, você deverá garantir que as atualizações de segurança e as atualizações do kernel sejam aplicadas ao sistema operacional host. Além disso, você deve aplicar atualizações de firmware ao hardware vulnerável quando essas atualizações estiverem disponíveis.

Para obter uma lista de versões suportadas, consulte o ["Ferramenta de Matriz de Interoperabilidade da NetApp"](#) .

Diretrizes de proteção para redes StorageGRID

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

Para obter informações detalhadas sobre redes StorageGRID , consulte o ["Tipos de rede StorageGRID"](#) .

Diretrizes para Rede de Grade

Você deve configurar uma Grid Network para todo o tráfego interno do StorageGRID . Todos os nós da grade estão na Rede da Grade e devem ser capazes de se comunicar com todos os outros nós.

Ao configurar a rede Grid, siga estas diretrizes:

- Certifique-se de que a rede esteja protegida de clientes não confiáveis, como aqueles na internet aberta.
- Sempre que possível, use a Grid Network exclusivamente para tráfego interno. Tanto a Rede de Administração quanto a Rede de Cliente têm restrições adicionais de firewall que bloqueiam o tráfego externo para serviços internos. O uso da Grid Network para tráfego de clientes externos é suportado, mas esse uso oferece menos camadas de proteção.
- Se a implantação do StorageGRID abranger vários data centers, use uma rede privada virtual (VPN) ou equivalente na Grid Network para fornecer proteção adicional para o tráfego interno.
- Alguns procedimentos de manutenção exigem acesso SSH (Secure Shell) na porta 22 entre o nó de administração primário 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 de administração normalmente é usada para tarefas administrativas (funcionários confiáveis usando o Grid Manager ou SSH) e para comunicação com outros serviços confiáveis, como LDAP, DNS, NTP ou KMS (ou servidor KMIP). No entanto, o StorageGRID não impõe esse uso internamente.

Se você estiver usando a Rede de Administração, siga estas diretrizes:

- Bloqueie todas as portas de tráfego interno na rede de administração. Veja o ["lista de portas internas"](#) .
- Se clientes não confiáveis puderem acessar a rede de administração, bloqueie o acesso ao StorageGRID na rede de administração com um firewall externo.

Diretrizes para Rede de Clientes

A Rede do Cliente normalmente é usada para locatários e para comunicação com serviços externos, como o serviço de replicação do CloudMirror ou outro serviço de plataforma. No entanto, o StorageGRID não impõe

esse uso internamente.

Se você estiver usando a Rede de Clientes, siga estas diretrizes:

- Bloqueie todas as portas de tráfego interno na rede do cliente. Veja o "[lista de portas internas](#)".
- Aceite tráfego de entrada de clientes somente em endpoints configurados explicitamente. Veja as informações sobre "[gerenciando controles de firewall](#)".

Diretrizes de proteção para nós do StorageGRID

Os nós do StorageGRID podem ser implantados 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 tem seu próprio conjunto de práticas recomendadas de proteção.

Controle o acesso remoto do IPMI ao BMC

Você pode habilitar ou desabilitar o acesso remoto IPMI para todos os dispositivos que contêm um BMC. A interface IPMI remota permite acesso de hardware de baixo nível aos seus dispositivos StorageGRID por qualquer pessoa com uma conta e senha BMC. Se você não precisar de acesso IPMI remoto ao BMC, desative esta opção.

- Para controlar o acesso remoto do IPMI ao BMC no Grid Manager, vá para **CONFIGURAÇÃO > Segurança > Configurações de segurança > Dispositivos**:
 - Desmarque a caixa de seleção **Habilitar acesso IPMI remoto** para desabilitar o acesso IPMI ao BMC.
 - Marque a caixa de seleção **Habilitar acesso IPMI remoto** para habilitar o acesso IPMI ao BMC.

Configuração de firewall

Como parte do processo de proteção do sistema, você deve revisar as configurações do firewall externo e modificá-las para que o tráfego seja aceito apenas dos endereços IP e nas portas dos quais ele é estritamente necessário.

O StorageGRID inclui um firewall interno em cada nó que aumenta a segurança da sua grade, permitindo que você controle o acesso da rede ao nó. Você deve "[gerenciar controles internos de firewall](#)" para impedir o acesso à rede em todas as portas, exceto aquelas necessárias para sua implantação de grade específica. As alterações de configuração feitas na página de controle do Firewall são implantadas em 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 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 você 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 "[Referência de](#)

[porta de rede](#)" .

Desabilitar 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 planeja usar DHCP, use o Grid Manager para fechar a porta 68. Selecione **CONFIGURAÇÃO > Controle de firewall > Gerenciar acesso externo**. Em seguida, altere a alternância de 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 software não confiável. Não presuma que as proteções do hipervisor impedirão que malware acesse dados protegidos StorageGRID se o StorageGRID e o malware existirem no mesmo hardware físico. Por exemplo, os ataques Meltdown e Spectre exploram vulnerabilidades críticas em processadores modernos e permitem que programas roubem dados na memória do mesmo computador.

Proteja os nós durante a instalação

Não permita que usuários não confiáveis acessem nós do StorageGRID pela rede quando os nós estiverem sendo instalados. Os nós não estão totalmente seguros até que se juntem à grade.

Diretrizes para nós de administração

Os nós de administração fornecem serviços de gerenciamento, como configuração do sistema, monitoramento e registro. Ao fazer login no Grid Manager ou no Tenant Manager, você está se conectando a um nó de administração.

Siga estas diretrizes para proteger os nós de administração no seu sistema StorageGRID :

- Proteja todos os nós de administração de clientes não confiáveis, como aqueles na Internet aberta. Certifique-se de que nenhum cliente não confiável possa acessar qualquer nó de administração na rede Grid, na rede de administração ou na rede de clientes.
- Os grupos 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 endpoints do balanceador de carga StorageGRID , use nós de gateway em vez de nós de administração para tráfego de cliente não confiável.
- Se você tiver locatários não confiáveis, não permita que eles tenham acesso direto ao Gerenciador de Locatários ou à API de Gerenciamento de Locatários. Em vez disso, faça com que os locatários não confiáveis usem um portal de locatários ou um sistema externo de gerenciamento de locatários, que interage com a API de gerenciamento de locatários.
- Opcionalmente, use um proxy de administrador para obter mais controle sobre a comunicação do AutoSupport dos nós de administração para o suporte da NetApp . Veja os passos para ["criando um proxy de administrador"](#) .
- Opcionalmente, use 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 do locatário à porta 9443 para proteção adicional.
- Opcionalmente, use nós de administração separados para administradores de grade e usuários locatários.

Para 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 no seu sistema StorageGRID .

- Não permita que clientes não confiáveis se conectem diretamente aos nós de armazenamento. Use um ponto de extremidade do balanceador de carga atendido por um nó de gateway ou um balanceador de carga de terceiros.
- Não habilite serviços de saída para locatários não confiáveis. Por exemplo, ao criar uma conta para um locatário não confiável, não permita que o locatário use sua própria fonte de identidade e não permita o uso de serviços da plataforma. Veja os passos para ["criando uma conta de inquilino"](#) .
- 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, use um proxy de armazenamento para obter mais controle sobre os pools de armazenamento em nuvem e a comunicação dos serviços de plataforma dos nós de armazenamento para serviços externos. Veja os passos para ["criando um proxy de armazenamento"](#) .
- Opcionalmente, conecte-se a serviços externos usando a Rede do Cliente. Em seguida, selecione **CONFIGURAÇÃO > Segurança > Controle de firewall > Redes de clientes não confiáveis** e indique que a Rede de clientes no nó de armazenamento não é confiável. O nó de armazenamento não aceita mais nenhum tráfego de entrada na rede do cliente, mas continua permitindo solicitações de saída para serviços de plataforma.

Diretrizes para nós de gateway

Os nós de gateway fornecem uma interface de balanceamento de carga opcional que os aplicativos clientes podem usar para se conectar ao StorageGRID. Siga estas diretrizes para proteger quaisquer nós de gateway no seu sistema StorageGRID :

- Configurar e usar endpoints do balanceador de carga. Ver ["Considerações para balanceamento de carga"](#) .
- Use um balanceador de carga de terceiros entre o cliente e o nó de gateway ou nós de armazenamento para tráfego de cliente não confiável. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques. Se você usar um balanceador de carga de terceiros, o tráfego de rede ainda poderá ser configurado para passar por um ponto de extremidade do balanceador de carga interno ou ser enviado diretamente para os nós de armazenamento.
- Se você estiver usando endpoints do balanceador de carga, opcionalmente, faça com que os clientes se conectem pela Rede do Cliente. Em seguida, selecione **CONFIGURAÇÃO > Segurança > Controle de firewall > Redes de clientes não confiáveis** e indique que a Rede de clientes no nó de gateway não é confiável. O nó de gateway aceita apenas tráfego de entrada nas portas explicitamente configuradas como pontos de extremidade do balanceador de carga.

Diretrizes para nós de dispositivos de hardware

Os dispositivos de hardware StorageGRID são especialmente projetados para uso em um sistema StorageGRID . Alguns aparelhos podem ser usados como nós de armazenamento. Outros dispositivos podem ser usados como nós de administração ou nós de gateway. Você pode combinar nós de dispositivos com nós baseados em software ou implantar grades totalmente projetadas para todos os dispositivos.

Siga estas diretrizes para proteger quaisquer nós de dispositivos de hardware no seu sistema StorageGRID :

- Se o dispositivo usar o SANtricity System Manager para gerenciamento do controlador de armazenamento, impeça que clientes não confiáveis acessem o SANtricity System Manager pela rede.

- Se o dispositivo tiver um controlador de gerenciamento de placa base (BMC), esteja ciente de que a porta de gerenciamento do BMC permite acesso de hardware de baixo nível. Conecte a porta de gerenciamento do BMC somente a uma rede de gerenciamento interna segura e confiável. Se nenhuma rede desse tipo estiver disponível, deixe a porta de gerenciamento do BMC desconectada ou bloqueada, a menos que uma conexão BMC seja solicitada pelo suporte técnico.
- Se o dispositivo oferecer suporte ao 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 remoto IPMI para todos os dispositivos que contêm um BMC. A interface IPMI remota permite acesso de hardware de baixo nível aos seus dispositivos StorageGRID por qualquer pessoa com uma conta e senha BMC. Se você não precisar de acesso IPMI remoto ao BMC, desative esta opção usando um dos seguintes métodos: + No Grid Manager, vá para **CONFIGURAÇÃO > Segurança > Configurações de segurança > Dispositivos** e desmarque a caixa de seleção **Habilitar acesso IPMI remoto**. + Na API de gerenciamento de grade, use o ponto de extremidade privado: PUT /private/bmc .

- Para modelos de dispositivos que contêm unidades SED, FDE ou FIPS NL-SAS que você gerencia com o SANtricity System Manager, "[habilitar e configurar o SANtricity Drive Security](#)".
- Para modelos de dispositivos que contêm SSDs SED ou FIPS NVMe que você gerencia usando o StorageGRID Appliance Installer e o Grid Manager, "[habilitar e configurar a criptografia de unidade StorageGRID](#)".
- Para dispositivos sem unidades SED, FDE ou FIPS, habilite e configure a criptografia do nó de software StorageGRID "[usando um Servidor de Gerenciamento de Chaves \(KMS\)](#)".

Diretrizes de proteção para TLS e SSH

Você deve substituir os certificados padrão criados durante a instalação 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 pelos seus próprios certificados personalizados.

Para muitas organizações, o certificado digital autoassinado para acesso à web do StorageGRID não é compatível com suas políticas de segurança da informação. Em sistemas de produção, você deve instalar um certificado digital assinado por CA para uso na autenticação do StorageGRID.

Especificamente, você deve usar certificados de servidor personalizados em vez destes certificados padrão:

- **Certificado de interface de gerenciamento:** usado para proteger o acesso ao Grid Manager, ao Tenant Manager, à Grid Management API e à Tenant Management API.
- **Certificado de API S3:** usado para proteger o acesso aos nós de armazenamento e nós de gateway, que os aplicativos cliente S3 usam para carregar e baixar dados de objetos.

Ver "[Gerenciar certificados de segurança](#)" para obter detalhes e instruções.



O StorageGRID gerencia os certificados usados para endpoints do balanceador de carga separadamente. Para configurar 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 uma *subjectAltName* que corresponde às entradas DNS para StorageGRID. Para obter detalhes, consulte a seção 4.2.1.6, "Nome alternativo do assunto", em ["RFC 5280: Certificado PKIX e Perfil CRL"](#).
- Sempre que possível, evite o uso de certificados curinga. Uma exceção a essa diretriz é o certificado para um ponto de extremidade de estilo hospedado virtual S3, que requer o uso de um curinga se os nomes dos buckets não forem conhecidos com antecedência.
- Quando você precisar usar curingas em certificados, tome medidas adicionais para reduzir os riscos. Use um padrão curinga como `*.s3.example.com`, e não use o `s3.example.com` sufixo para outras aplicações. Este padrão também funciona com acesso S3 no estilo de caminho, como `dc1-s1.s3.example.com/mybucket`.
- Defina os tempos de expiração dos certificados como curtos (por exemplo, 2 meses) e use a API de gerenciamento de grade 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 comunicar com o StorageGRID.

Diretrizes de reforço para política 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 TLS e SSH criptografam dados em movimento. Como prática recomendada, você deve desabilitar opções de criptografia que não são necessárias para compatibilidade do aplicativo. Use a política Moderna padrão, a menos que seu sistema precise ser compatível com os Critérios Comuns ou você precise usar outras cifras.

Ver ["Gerenciar a política TLS e SSH"](#) para obter detalhes e instruções.

Outras diretrizes de endurecimento

Além de seguir as diretrizes de proteção para redes e nós do StorageGRID, você deve seguir as diretrizes de proteção 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 do usuário, a API de instalação e `configure-storagegrid.py` roteiro.

Para mais informações, consulte:

- ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)

- ["Instalar o StorageGRID no Ubuntu ou Debian"](#)
- ["Instalar o StorageGRID no VMware"](#)
- ["Instalar o dispositivo StorageGRID"](#)

Logs e mensagens de auditoria

Sempre proteja os logs do StorageGRID e a saída das mensagens de auditoria de maneira segura. Os logs e 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 do StorageGRID e na saída das mensagens de auditoria são geralmente de natureza confidencial.

Configure o StorageGRID para enviar eventos de segurança para um servidor syslog externo. Se estiver usando a exportação syslog, selecione TLS e RELP/TLS para os protocolos de transporte.

Veja o ["Referência de arquivos de log"](#) para obter mais informações sobre logs do StorageGRID .

Ver ["Mensagens de auditoria"](#) para obter mais informações sobre mensagens de auditoria do StorageGRID .

AutoSupport da NetApp

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 do AutoSupport para a NetApp é habilitado quando o StorageGRID é configurado pela primeira vez.

O recurso AutoSupport pode ser desativado. No entanto, a NetApp recomenda habilitá-lo porque o AutoSupport ajuda a acelerar a identificação e a resolução de problemas caso surjam problemas no seu sistema StorageGRID .

O AutoSupport suporta HTTPS, HTTP e SMTP para protocolos de transporte. Devido à natureza sensível dos pacotes do AutoSupport , a NetApp recomenda fortemente o uso de HTTPS como o protocolo de transporte padrão para enviar pacotes do AutoSupport para a NetApp.

Compartilhamento de recursos de origem cruzada (CORS)

Você pode configurar o compartilhamento de recursos entre origens (CORS) para um bucket do S3 se quiser que esse bucket e os objetos nele sejam acessíveis a aplicativos da Web em outros domínios. Em geral, não habilite o CORS, a menos que seja necessário. Se o CORS for necessário, restrinja-o a origens confiáveis.

Veja os passos para ["configurando compartilhamento de recursos de origem cruzada \(CORS\)"](#) .

Dispositivos de segurança externos

Uma solução de proteção completa deve abordar mecanismos de segurança fora do 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 intrusão (IPSs) e outros dispositivos de segurança.

Um balanceador de carga de terceiros é recomendado para tráfego de clientes não confiáveis. O balanceamento de carga de terceiros oferece mais controle e camadas adicionais de proteção contra ataques.

Mitigação de ransomware

Ajude a proteger os dados do seu objeto contra ataques de ransomware seguindo as recomendações em ["Defesa contra ransomware com StorageGRID"](#) .

Configurar StorageGRID para FabricPool

Configurar StorageGRID para FabricPool

Se você usar o software NetApp ONTAP , poderá usar o NetApp FabricPool para hierarquizar dados inativos em um sistema de armazenamento de objetos NetApp StorageGRID .

Use estas instruções para:

- Aprenda as considerações e práticas recomendadas para configurar o StorageGRID para uma carga de trabalho do FabricPool .
- Aprenda a configurar um sistema de armazenamento de objetos StorageGRID para uso com FabricPool.
- Aprenda como fornecer os valores necessários ao ONTAP ao anexar o StorageGRID como uma camada de nuvem do FabricPool .

Início rápido para configurar o StorageGRID para FabricPool

1

Planeje sua configuração

- Decida qual política de divisão de volumes do FabricPool você usará para dividir dados ONTAP inativos em camadas no StorageGRID.
- Planeje e instale um sistema StorageGRID para atender às suas necessidades de capacidade de armazenamento e desempenho.
- Familiarize-se com o software do sistema StorageGRID , incluindo o ["Gerenciador de grade"](#) e o ["Gerente de inquilinos"](#) .
- Revise as práticas recomendadas do FabricPool para ["Grupos HA"](#) , ["balanceamento de carga"](#) , ["ILM"](#) , e ["mais"](#) .
- Revise estes recursos adicionais, que fornecem detalhes sobre o uso e a configuração do ONTAP e do FabricPool:

["TR-4598: Melhores práticas do FabricPool no ONTAP"](#)

["Documentação ONTAP para FabricPool"](#)

2

Executar tarefas de pré-requisito

Obter o ["informações necessárias para anexar o StorageGRID como uma camada de nuvem"](#) , incluindo:

- Endereços IP
- Nomes de domínio
- Certificado SSL

Opcionalmente, configure ["federação de identidade"](#) e ["login único"](#) .

3

Configurar as definições do StorageGRID

Use StorageGRID para obter os valores que o ONTAP precisa para se conectar à grade.

Usando o "[Assistente de configuração do FabricPool](#)" é a maneira 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 o ONTAP para "[adicionar uma camada de nuvem](#)" que usa os valores StorageGRID . Então, "[configurar entradas DNS](#)" para associar endereços IP a quaisquer nomes de domínio que você planeja usar.

5

Monitorar e gerenciar

Quando seu sistema estiver instalado e funcionando, execute tarefas contínuas no ONTAP e no StorageGRID para gerenciar e monitorar a hierarquização de dados do FabricPool ao longo do tempo.

O que é FabricPool?

FabricPool é uma solução de armazenamento híbrido ONTAP que usa um agregado flash de alto desempenho como camada de desempenho e um armazenamento de objetos como camada de nuvem. Usar agregados habilitados para FabricPool ajuda a reduzir os custos de armazenamento sem comprometer o desempenho, a eficiência ou a proteção.

O 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 do FabricPool podem então aproveitar a hierarquização, mantendo dados ativos (quentes) no armazenamento de alto desempenho (a camada local) e hierarquizando dados inativos (frios) no armazenamento de objetos externo (a camada de nuvem).

Nenhuma alteração arquitetônica é necessária e você pode continuar gerenciando seus dados e ambiente de aplicativos a partir do sistema de armazenamento central ONTAP .

O que é StorageGRID?

O NetApp StorageGRID é uma arquitetura de armazenamento que gerencia dados como objetos, ao contrário de outras arquiteturas de armazenamento, como armazenamento 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 armazenamento de objetos geralmente ofereça desempenho inferior ao armazenamento 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 o StorageGRID como uma camada de nuvem do FabricPool ?

O FabricPool pode hierarquizar dados ONTAP para vários provedores de armazenamento de objetos, incluindo o StorageGRID. Ao contrário das nuvens públicas que podem definir um número máximo de operações de entrada/saída suportadas por segundo (IOPS) no nível do bucket ou contêiner, o desempenho do StorageGRID é dimensionado com o número de nós em um sistema. Usar o StorageGRID como uma camada de nuvem do FabricPool permite que você mantenha seus dados frios em sua própria nuvem privada para obter o mais alto desempenho e controle total sobre seus dados.

Além disso, uma licença FabricPool não é necessária quando você usa o StorageGRID como camada de nuvem.

Informações necessárias para anexar o StorageGRID como uma camada de nuvem

Antes de poder anexar o 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 eu preciso?

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 de extremidade do balanceador de carga	Gerenciador de Sistema ONTAP > Adicionar Nível de Nuvem
Certificado SSL	StorageGRID > Ponto de extremidade do balanceador de carga	Gerenciador de Sistema ONTAP > Adicionar Nível de Nuvem
Nome do servidor (FQDN)	StorageGRID > Ponto de extremidade do balanceador de carga	Entrada DNS
ID da chave de acesso e chave de acesso secreta	StorageGRID > Locatário e bucket	Gerenciador de Sistema ONTAP > Adicionar Nível de Nuvem
Nome do balde/recipient	StorageGRID > Locatário e bucket	Gerenciador de Sistema ONTAP > Adicionar Nível de Nuvem

Como obtenho esses valores?

Dependendo de suas necessidades, você pode fazer o seguinte para obter as informações necessárias:

- Use o ["Assistente de configuração do FabricPool"](#). O assistente de configuração 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 nas etapas necessárias e ajuda a garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID e do FabricPool.
- Configure cada item manualmente. Em seguida, insira os valores no ONTAP System Manager ou no ONTAP CLI. Siga estes passos:
 - a. ["Configurar um grupo de alta disponibilidade \(HA\) para o FabricPool"](#).
 - b. ["Crie um ponto de extremidade do balanceador de carga para o FabricPool"](#).
 - c. ["Crie uma conta de locatário para o FabricPool"](#).
 - d. Sign in na conta do inquilino e ["crie o bucket e as chaves de acesso para o usuário root"](#).

- e. Crie uma regra de ILM para dados do FabricPool e adicione-a às suas políticas de ILM ativas. Ver ["Configurar ILM para dados do FabricPool"](#) .
- f. Opcionalmente, ["crie uma política de classificação de tráfego para FabricPool"](#) .

Use o assistente de configuração do FabricPool

Usar o assistente de configuração do FabricPool : considerações e requisitos

Você pode usar o assistente de configuração do FabricPool para configurar o StorageGRID como o sistema de armazenamento de objetos para uma camada de nuvem do FabricPool . Após concluir o assistente de configuração, você pode inserir os detalhes necessários no ONTAP System Manager.

Quando usar o assistente de configuração do FabricPool

O assistente de configuração do FabricPool orienta você em cada etapa da configuração do StorageGRID para uso com o FabricPool e configura automaticamente determinadas entidades para você, como o ILM e as políticas de classificação de tráfego. Como parte da conclusão do assistente, você baixa um arquivo que pode ser usado para inserir valores no ONTAP System Manager. Use o assistente para configurar seu sistema mais rapidamente e garantir que suas configurações estejam em conformidade com as práticas recomendadas do StorageGRID e do FabricPool .

Supondo que você tenha permissão de acesso Root, você pode concluir o assistente de configuração do FabricPool quando começar a usar o StorageGRID Grid Manager ou pode acessar e concluir o assistente 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 o ONTAP precisa em um único arquivo.



Use o assistente de configuração do FabricPool , a menos que você saiba que tem requisitos especiais ou que sua implementação exija personalização significativa.

Antes de usar o assistente

Confirme se você concluiu estas etapas de pré-requisito.

Revisar as melhores práticas

- Você tem uma compreensão geral do ["informações necessárias para anexar o StorageGRID como uma camada de nuvem"](#) .
- Você revisou as práticas recomendadas do FabricPool para:
 - ["Grupos de alta disponibilidade \(HA\)"](#)
 - ["Balanceamento de carga"](#)
 - ["Regras e políticas do ILM"](#)

Obter endereços IP e configurar interfaces VLAN

Se você configurar um grupo HA, saberá a quais nós o ONTAP se conectará e qual rede StorageGRID será usada. Você também sabe quais valores inserir para o CIDR de 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. Ver ["Configurar interfaces VLAN"](#) .

Configurar federação de identidade e SSO

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 root para a conta de locatário que o ONTAP usará. Ver ["Usar federação de identidade"](#) e ["Configurar logon único"](#) .

Obter e configurar nomes de domínio

- Você sabe qual nome de domínio totalmente qualificado (FQDN) usar para StorageGRID. As entradas do servidor de nomes de domínio (DNS) mapearão esse FQDN para os endereços IP virtuais (VIP) do grupo HA que você criar usando o assistente. Ver ["Configurar servidor DNS"](#) .
- Se você planeja usar solicitações de estilo de hospedagem virtual S3, você tem ["nomes de domínio de endpoint S3 configurados"](#) . O ONTAP usa URLs no estilo de caminho por padrão, mas é recomendado usar solicitações no estilo de hospedagem virtual.

Revisar os requisitos do balanceador de carga e do certificado de segurança

Se você planeja usar o balanceador de carga StorageGRID , você revisou o geral ["considerações para balanceamento de carga"](#) . Você tem os certificados que irá enviar ou os valores necessários para gerar um certificado.

Se você planeja usar um ponto de extremidade de balanceador de carga externo (de terceiros), você tem o nome de domínio totalmente qualificado (FQDN), a porta e o certificado para esse balanceador de carga.

Confirmar configuração do pool de armazenamento ILM

se você instalou inicialmente o StorageGRID 11.6 ou anterior, você configurou o pool de armazenamento que usará. Em geral, você deve criar um pool de armazenamento para cada site StorageGRID que usará para armazenar dados ONTAP .



Este pré-requisito não se aplica se você instalou inicialmente o StorageGRID 11.7 ou 11.8. Quando você instala inicialmente qualquer uma dessas versões, os pools de armazenamento são criados automaticamente para cada site.

Relação entre o ONTAP e a camada de nuvem StorageGRID

O assistente FabricPool orienta você no processo de criação de uma única camada de nuvem StorageGRID que inclui um locatário do StorageGRID , um conjunto de chaves de acesso e um bucket do StorageGRID . Você pode anexar esta camada de nuvem StorageGRID a uma ou mais camadas locais do ONTAP .

Anexar uma única camada de nuvem a várias camadas locais em um cluster é a melhor prática geral. No entanto, dependendo dos seus requisitos, talvez você queira usar mais de um bucket ou até mesmo mais de um locatário do StorageGRID para as camadas locais em um único cluster. Usar diferentes buckets e locatários permite isolar dados e acesso a dados entre camadas locais do ONTAP , mas é um pouco mais complexo de configurar e gerenciar.

A NetApp não recomenda anexar uma única camada de nuvem a camadas locais em vários clusters.



Para obter as práticas recomendadas para usar o StorageGRID com o NetApp MetroCluster™ e o FabricPool Mirror, consulte ["TR-4598: Melhores práticas do FabricPool no ONTAP"](#) .

Opcional: use um bucket diferente para cada nível 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 HA, ponto de extremidade do balanceador de carga, locatário e chaves de acesso, mas usa um contêiner diferente (bucket StorageGRID). Siga estas etapas gerais:

1. No StorageGRID Grid Manager, conclua o assistente de configuração do FabricPool para a primeira camada 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 criado pelo assistente e crie um segundo bucket.
4. Conclua o assistente do FabricPool novamente. Selecione o grupo HA existente, o ponto de extremidade do balanceador de carga e o locatário. Em seguida, selecione o novo bucket que você criou manualmente. Crie uma nova regra de ILM para o novo bucket e ative uma política de ILM para incluir essa regra.
5. No ONTAP, adicione uma segunda camada de nuvem, mas forneça o novo nome do bucket.

Opcional: use um locatário e um bucket diferentes para cada nível local

Para usar mais de um locatário 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, ponto de extremidade do balanceador de carga, mas usa um locatário, chaves de acesso e contêiner diferentes (bucket StorageGRID). Siga estas etapas gerais:

1. No StorageGRID Grid Manager, conclua o assistente de configuração do FabricPool para a primeira camada 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 do FabricPool novamente. Selecione o grupo HA existente e o ponto de extremidade do balanceador de carga. Crie um novo inquilino e bucket. Crie uma nova regra de ILM para o novo bucket e ative uma política de ILM para incluir essa regra.
4. No ONTAP, adicione uma segunda camada de nuvem, mas forneça a nova chave de acesso, a chave secreta e o nome do bucket.

Acesse e conclua o assistente de configuração do FabricPool

Você pode usar o assistente de configuração do FabricPool para configurar o StorageGRID como o sistema de armazenamento de objetos para uma camada de nuvem do FabricPool .

Antes de começar

- Você revisou o ["considerações e requisitos"](#) para usar o assistente de configuração do FabricPool .



Se você quiser configurar o StorageGRID para uso com qualquer outro aplicativo cliente S3, vá para ["Use o assistente de configuração do S3"](#) .

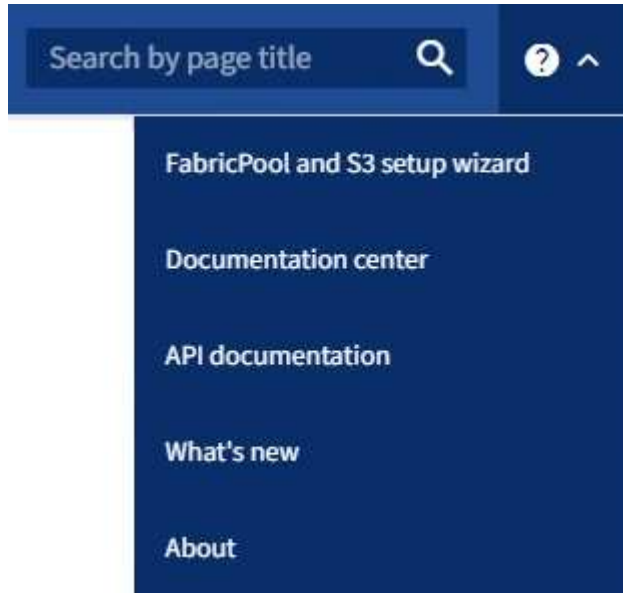
- Você tem o ["Permissão de acesso root"](#) .

Acesse o assistente

Você pode concluir o assistente de configuração do FabricPool ao começar a usar o StorageGRID Grid Manager ou pode acessar e concluir o assistente posteriormente.

Passos

1. Sign in no Grid Manager usando um ["navegador da web compatível"](#) .
2. Se o banner * Assistente de configuração do FabricPool e do S3* 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 * Assistente de configuração do FabricPool e S3*.



3. Na seção FabricPool da página do assistente de configuração do FabricPool e do S3, selecione **Configurar agora**.

Etapas 1 de 9: Configurar grupo HA aparece.

Etapas 1 de 9: Configurar grupo HA

Um grupo de alta disponibilidade (HA) é uma coleção de nós que contém o serviço StorageGRID Load Balancer. Um grupo HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo 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 HA. Selecione **Ignorar esta etapa** e vá para [Etapa 2 de 9: Configurar o ponto de extremidade do balanceador de carga](#) .
2. Para usar o balanceador de carga StorageGRID , crie um novo grupo de HA ou use um grupo de HA existente.

Criar grupo HA

- Para criar um novo grupo HA, selecione **Criar grupo HA**.
- Para a 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.

- Para a etapa **Adicionar interfaces**, selecione as interfaces de nó que deseja usar neste grupo de HA.

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 pode selecionar apenas uma interface para cada nó.

- Para a etapa **Priorizar interfaces**, determine a interface primária e quaisquer interfaces de backup para este grupo de HA.

Arraste as linhas para alterar os valores na coluna **Ordem de prioridade**.

A primeira interface na 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 IP virtuais (VIP) serão movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de backup e assim por diante. Quando as falhas são resolvidas, os endereços VIP retornam para a interface de maior prioridade disponível.

- Para a etapa **Inserir endereços IP**, preencha os seguintes campos.

Campo	Descrição
CIDR de 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 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 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 depois selecione **Concluir** para retornar ao assistente de configuração 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 ponto de extremidade do balanceador de carga

O StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de aplicativos clientes, como o FabricPool. O balanceamento de carga maximiza a velocidade e a capacidade de conexão entre vários nós de armazenamento.

Você pode usar o serviço StorageGRID Load Balancer, que existe em todos os nós de gateway e administração, ou pode se conectar a um balanceador de carga externo (de terceiros). É recomendado usar o balanceador de carga StorageGRID .

Para obter detalhes sobre esta tarefa, consulte o geral "[considerações para balanceamento de carga](#)" e o "[melhores práticas para balanceamento de carga para FabricPool](#)".

Passos

1. Selecione ou crie um ponto de extremidade do balanceador de carga StorageGRID ou use um balanceador de carga externo.

Criar ponto final

- Selecione **Criar ponto de extremidade**.
- Para a etapa **Inserir detalhes do ponto de extremidade**, preencha os seguintes campos.

Campo	Descrição
Nome	Um nome descritivo para o ponto de extremidade.
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo assume como padrão 10433 para o primeiro ponto de extremidade criado, mas você pode inserir qualquer porta externa não utilizada. Se você digitar 80 ou 443, o ponto de extremidade será configurado somente em nós de gateway, porque essas portas são reservadas em nós de administração. Observação: Portas usadas por outros serviços de rede não são permitidas. Veja o "Referência de porta de rede".
Tipo de cliente	Deve ser S3 .
Protocolo de rede	Selecione HTTPS. Observação: a comunicação com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada.

- Para a etapa **Selecionar modo de vinculação**, especifique o modo de vinculação. O modo de vinculação controla como o ponto de extremidade é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

Modo	Descrição
Global (padrão)	Os clientes podem acessar o ponto de extremidade usando o endereço IP de qualquer nó de gateway ou nó de administração, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração Global (padrão), a menos que você precise restringir a acessibilidade deste ponto de extremidade.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este ponto de extremidade. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.

Modo	Descrição
Interfaces de nó	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar este ponto de extremidade.
Tipo de nó	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó de administração ou o endereço IP (ou FQDN correspondente) de qualquer nó de gateway para acessar esse ponto de extremidade.

d. Para a etapa **Acesso do locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os inquilinos (padrão)	Todas as contas de locatários podem usar esse endpoint para acessar seus buckets. Permitir todos os locatários é quase sempre a opção apropriada para o ponto de extremidade do balanceador de carga usado para FabricPool. Você deve selecionar esta opção se estiver usando o assistente de configuração do FabricPool para um novo sistema StorageGRID e ainda não tiver criado nenhuma conta de locatário.
Permitir inquilinos selecionados	Somente as contas de locatários selecionadas podem usar este ponto de extremidade para acessar seus buckets.
Bloquear inquilinos selecionados	As contas de locatários selecionadas não podem usar este ponto de extremidade para acessar seus buckets. Todos os outros inquilinos podem usar este ponto de extremidade.

e. Para a etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Carregar certificado (recomendado)	Use esta opção para carregar um certificado de servidor assinado pela CA, uma chave privada de certificado e um pacote de CA opcional.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Ver " Configurar pontos de extremidade do balanceador de carga " para obter detalhes sobre o que inserir.
Usar certificado StorageGRID S3	Esta opção estará disponível somente se você já tiver carregado ou gerado uma versão personalizada do certificado global StorageGRID . Ver " Configurar certificados da API S3 " para mais detalhes.

f. Selecione **Concluir** para retornar ao assistente de configuração do FabricPool .

g. Selecione **Continuar** para ir para a etapa do locatário e do bucket.



Alterações em um certificado de ponto de extremidade podem levar até 15 minutos para serem aplicadas a todos os nós.

Usar ponto de extremidade do balanceador de carga existente

- Selecione o nome de um ponto de extremidade existente na lista suspensa **Selecionar um ponto de extremidade do balanceador de carga**.
- Selecione **Continuar** para ir para a etapa do locatário e do bucket.

Usar balanceador de carga externo

- Preencha os seguintes campos para o balanceador de carga externo.

Campo	Descrição
FQDN	O nome de domínio totalmente qualificado (FQDN) do balanceador de carga externo.
Porta	O número da porta que o 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 do locatário e do bucket.

Etapa 3 de 9: inquilino e bucket

Um locatário é uma entidade que pode usar aplicativos S3 para armazenar e recuperar objetos no StorageGRID. Cada locatário tem seus próprios usuários, chaves de acesso, buckets, objetos e um conjunto específico de recursos. Você deve criar um locatário do StorageGRID antes de poder criar o bucket que o FabricPool usará.

Um bucket é um contêiner usado para armazenar objetos e metadados de objetos de um locatário. Embora alguns locatários possam ter muitos buckets, o assistente permite que você crie ou selecione apenas um locatário e um bucket por vez. Você pode usar o Gerenciador de Tenants mais tarde para adicionar quaisquer buckets adicionais necessários.

Você pode criar um novo locatário e bucket para uso do FabricPool ou selecionar um locatário e bucket existentes. Se você criar um novo locatário, o sistema criará 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 o FabricPool"](#) e ["Crie um bucket S3 e obtenha uma chave de acesso"](#).

Passos

Crie um novo locatário e bucket ou selecione um locatário existente.

Novo inquilino e balde

1. Para criar um novo locatário e bucket, insira um **Nome de locatário**. Por exemplo, `FabricPool tenant`.
2. Defina o acesso root para a conta do locatário, com base no uso do seu sistema StorageGRID "[federação de identidade](#)", "[logon único \(SSO\)](#)", ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver habilitada	Especifique a senha a ser usada ao fazer login no locatário como usuário root local.
Se a federação de identidade estiver habilitada	a. Selecione um grupo federado existente para ter permissão de acesso Root para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário root local.
Se a federação de identidade e o logon único (SSO) estiverem habilitados	Selecione um grupo federado existente para ter permissão de acesso Root para o locatário. Nenhum usuário local pode fazer login.

3. Para **Nome do bucket**, insira o nome do bucket que o FabricPool usará para armazenar dados ONTAP. Por exemplo, `fabricpool-bucket`.



Não é possível alterar o nome do bucket após 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 inquilino e o bucket

A conta de locatário existente deve ter pelo menos um bucket que não tenha o controle de versão habilitado. Não é possível selecionar uma conta de locatário existente se não houver nenhum bucket para esse locatário.

1. Selecione o inquilino existente na lista suspensa **Nome do inquilino**.
2. Selecione o bucket existente na lista suspensa **Nome do bucket**.

O FabricPool não oferece suporte ao controle de versão de objetos, portanto, os buckets que têm o controle de versão habilitado não são exibidos.



Não selecione um bucket que tenha o S3 Object Lock habilitado para uso com FabricPool.

3. Selecione **Continuar** para prosseguir para a etapa de download de dados.

Etapa 4 de 9: Baixe as configurações do ONTAP

Durante esta etapa, você baixa um arquivo que pode ser usado para inserir valores no ONTAP System Manager.

Passos

1. Opcionalmente, selecione o ícone de cópia () 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 de download, mas talvez você queira salvá-los separadamente.

2. Selecione ***Baixar configurações do ONTAP *** para baixar um arquivo de texto que contém os valores que você inseriu até agora.

O `ONTAP_FabricPool_settings_bucketname.txt` O arquivo inclui as informações necessárias para configurar o StorageGRID como o sistema de armazenamento de objetos para uma camada de nuvem do FabricPool , incluindo:

- Detalhes de conexão do balanceador de carga, incluindo o nome do servidor (FQDN), porta e certificado
- Nome do balde
- ID da chave de acesso e chave de acesso secreta para o usuário raiz da conta do locatário

3. Salve as chaves copiadas e o arquivo baixado em um local seguro.



Não feche esta página até ter copiado ambas as chaves de acesso, baixado as configurações do ONTAP ou ambos. As chaves não estarão disponíveis depois que 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. Marque 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 armazenamento do ILM.

Etapa 5 de 9: Selecione um pool de armazenamento

Um pool de armazenamento é um grupo de nós de armazenamento. Ao selecionar um pool de armazenamento, você determina quais nós o StorageGRID usará para armazenar os dados em camadas do ONTAP.

Para obter detalhes sobre esta etapa, consulte ["Criar um pool de armazenamento"](#) .

Passos

1. Na lista suspensa **Site**, selecione o site StorageGRID que você deseja usar para os dados em camadas do ONTAP.
2. Na lista suspensa **Pool de armazenamento**, selecione o pool de armazenamento para esse site.

O pool de armazenamento de um site inclui todos os nós de armazenamento naquele site.

3. Selecione **Continuar** para ir para a etapa da regra ILM.

Etapa 6 de 9: Revise a regra ILM para FabricPool

As regras de gerenciamento do ciclo de vida das informações (ILM) controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos no seu sistema StorageGRID .

O assistente de configuração do FabricPool cria automaticamente a regra de ILM recomendada para uso do FabricPool . Esta regra se aplica somente ao bucket que você especificou. Ele usa codificação de eliminação 2+1 em um único local para armazenar os dados em camadas do ONTAP.

Para obter detalhes sobre esta etapa, consulte ["Criar regra ILM"](#) e ["Melhores práticas para usar ILM com dados do FabricPool"](#) .

Passos

1. Revise 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 balde Esta regra se aplica somente a objetos salvos no bucket especificado.
Tempo de referência	Tempo de ingestão A instrução de posicionamento começa quando os objetos são salvos inicialmente no bucket.
Instruções de posicionamento	Use a codificação de apagamento 2+1

2. Classifique o diagrama de retenção por **Período de tempo** e **Pool de armazenamento** para confirmar as instruções de posicionamento.
 - O **período de tempo** para a regra é **Dia 0 - para sempre**. **Dia 0** significa que a regra é aplicada quando os dados são hierarquizados do ONTAP. **Para sempre** significa que o StorageGRID ILM não excluirá dados que foram hierarquizados do ONTAP.
 - O **pool de armazenamento** para a regra é o pool de armazenamento que você selecionou. **EC 2+1** significa que os dados serão armazenados usando codificação de eliminação 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 diferentes nós de armazenamento em um único local.
3. Selecione **Criar e continuar** para criar esta regra e ir para a etapa da política de ILM.

Etapa 7 de 9: Revise e ative a política do ILM

Depois que o assistente de configuração do FabricPool cria a regra do ILM para uso do FabricPool , ele cria uma política do ILM. Você deve simular e revisar cuidadosamente esta política antes de ativá-la.

Para obter detalhes sobre esta etapa, consulte ["Criar política de ILM"](#) e ["Melhores práticas para usar ILM com dados do FabricPool"](#) .



Quando você ativa uma nova política de ILM, o 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, a ativação de uma nova política pode fazer com que objetos existentes sejam movidos para novos locais.



Para evitar perda de dados, não use uma regra de ILM que irá expirar ou excluir dados da camada de nuvem do FabricPool. Defina o período de retenção como **para sempre** para garantir que os objetos do FabricPool não sejam excluídos pelo StorageGRID ILM.

Passos

1. Opcionalmente, atualize o **Nome da política** gerado pelo sistema. Por padrão, o sistema anexa "+ FabricPool" ao nome da sua política ativa ou inativa, mas você pode fornecer seu próprio nome.
2. Revise a lista de regras na política inativa.
 - Se sua grade não tiver uma política de ILM inativa, o assistente criará uma política inativa clonando sua política ativa e adicionando a nova regra ao topo.
 - Se sua grade já tiver uma política de ILM inativa e essa política usar as mesmas regras e a mesma ordem que a política de ILM ativa, o assistente adicionará a nova regra ao topo da política inativa.
 - Se sua política inativa contiver regras diferentes ou uma ordem diferente da política ativa, o assistente criará uma nova política inativa clonando sua política ativa e adicionando a nova regra ao topo.
3. Revise a ordem das regras na nova política inativa.

Como a regra FabricPool é a primeira regra, todos os objetos no bucket FabricPool são colocados antes que as outras regras na política sejam avaliadas. Objetos em quaisquer outros buckets são colocados por regras subsequentes na política.

4. Revise o diagrama de retenção para saber como diferentes objetos serão retidos.
 - a. Selecione **Expandir tudo** para ver um diagrama de retenção para cada regra na política inativa.
 - b. Selecione **Período de tempo** e **Pool de armazenamento** para revisar o diagrama de retenção. Confirme se todas as regras que se aplicam ao bucket ou localitório do FabricPool retêm objetos **para sempre**.
5. Após revisar a política inativa, selecione **Ativar e continuar** para ativar a política e ir para a etapa de classificação de tráfego.



Erros em uma política de ILM podem causar perda irreparável de dados. Revise a política cuidadosamente antes de ativar.

Etapa 8 de 9: Criar política de classificação de tráfego

Como opção, o assistente de configuração 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. Esta política monitora apenas o tráfego; ela não limita o tráfego para o FabricPool ou quaisquer outros clientes.

Para obter detalhes sobre esta etapa, consulte ["Crie uma política de classificação de tráfego para o FabricPool"](#).

Passos

1. Revise a política.

2. Se você quiser criar esta política de classificação de tráfego, selecione **Criar e continuar**.

Assim que o FabricPool começar a hierarquizar dados para o StorageGRID, você poderá acessar a página Políticas de classificação de tráfego para visualizar as métricas de tráfego de rede para esta política. Posteriormente, 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: Resumo da revisão

O resumo fornece detalhes sobre os itens que você configurou, incluindo o nome do balanceador de carga, locatário e bucket, a política de classificação de tráfego e a política ILM ativa.

Passos

1. Revise o resumo.
2. Selecione **Concluir**.

Próximos passos

Após concluir o assistente do FabricPool, execute estas etapas adicionais.

Passos

1. Vá para "[Configurar o ONTAP System Manager](#)" para inserir os valores salvos e concluir o lado ONTAP da conexão. Você deve adicionar StorageGRID como uma camada de nuvem, anexar a camada de nuvem a uma camada local para criar um FabricPool e definir políticas de camadas de volume.
2. Vá para "[Configurar o servidor DNS](#)" e certifique-se de que o DNS inclua um registro para associar o nome do servidor StorageGRID (nome de domínio totalmente qualificado) a cada endereço IP do StorageGRID que você usará.
3. Vá para "[Outras práticas recomendadas para StorageGRID e FabricPool](#)" para aprender as melhores práticas para logs de auditoria do StorageGRID e outras opções de configuração global.

Configurar o StorageGRID manualmente

Crie um grupo de alta disponibilidade (HA) para o FabricPool

Ao configurar o StorageGRID para uso com o FabricPool, você pode, opcionalmente, criar um ou mais grupos de alta disponibilidade (HA). Um grupo HA é uma coleção de nós que contêm o serviço StorageGRID Load Balancer. Um grupo HA pode conter nós de gateway, nós de administração ou ambos.

Você pode usar um grupo 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 poderá 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 configuração do FabricPool para concluir esta tarefa, vá para "[Acesse e conclua o assistente de configuração do FabricPool](#)".

Antes de começar

- Você revisou o "[melhores práticas para grupos de alta disponibilidade](#)".
- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você tem o "[Permissão de acesso root](#)".
- Se você planeja usar uma VLAN, você criou a interface VLAN. Ver "[Configurar interfaces VLAN](#)".

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Grupos de alta disponibilidade**.
2. Selecione **Criar**.
3. Para a 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. Para a etapa **Adicionar interfaces**, selecione as interfaces de nó que deseja usar neste grupo de HA.

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 pode selecionar apenas uma interface para cada nó.

5. Para a etapa **Priorizar interfaces**, determine a interface primária e quaisquer interfaces de backup para este grupo de HA.

Arraste as linhas para alterar os valores na coluna **Ordem de prioridade**.

A primeira interface na 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 IP virtuais (VIP) serão movidos para a primeira interface de backup na ordem de prioridade. Se essa interface falhar, os endereços VIP serão movidos para a próxima interface de backup e assim por diante. Quando as falhas são resolvidas, os endereços VIP retornam para a interface de maior prioridade disponível.

6. Para a etapa **Inserir endereços IP**, preencha os seguintes campos.

Campo	Descrição
CIDR de 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.

Campo	Descrição
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 VIP do StorageGRID. O endereço IP do gateway local deve estar dentro da sub-rede VIP.
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 depois selecione **Concluir**.

Crie um ponto de extremidade do balanceador de carga para o FabricPool

O StorageGRID usa um balanceador de carga para gerenciar a carga de trabalho de aplicativos clientes, como o FabricPool. O balanceamento de carga maximiza a velocidade e a capacidade de conexão entre vários nós de armazenamento.

Ao configurar o StorageGRID para uso com o FabricPool, você deve configurar um ponto de extremidade do balanceador de carga e carregar ou gerar um certificado de ponto de extremidade do balanceador de carga, que é usado para proteger a conexão entre o ONTAP e o StorageGRID.

Para usar o assistente de configuração do FabricPool para concluir esta tarefa, vá para ["Acesse e conclua o assistente de configuração do FabricPool"](#).

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).
- Você revisou o geral ["considerações para 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 **Criar**.
3. Para a etapa **Inserir detalhes do ponto de extremidade**, preencha os seguintes campos.

Campo	Descrição
Nome	Um nome descritivo para o ponto de extremidade.

Campo	Descrição
Porta	A porta StorageGRID que você deseja usar para balanceamento de carga. Este campo assume como padrão 10433 para o primeiro ponto de extremidade criado, mas você pode inserir qualquer porta externa não utilizada. Se você digitar 80 ou 443, o ponto de extremidade será configurado somente em nós de gateway. Essas portas são reservadas em nós de administração. Observação: Portas usadas por outros serviços de rede não são permitidas. Veja o "Referência de porta de rede". Você fornecerá esse número ao ONTAP ao anexar o StorageGRID como uma camada de nuvem do FabricPool.
Tipo de cliente	Selecione S3 .
Protocolo de rede	Selecione HTTPS. Observação: a comunicação com o StorageGRID sem criptografia TLS é suportada, mas não é recomendada.

4. Para a etapa **Selecionar modo de vinculação**, especifique o modo de vinculação. O modo de vinculação controla como o ponto de extremidade é acessado usando qualquer endereço IP ou usando endereços IP e interfaces de rede específicos.

Modo	Descrição
Global (padrão)	Os clientes podem acessar o ponto de extremidade usando o endereço IP de qualquer nó de gateway ou nó de administração, o endereço IP virtual (VIP) de qualquer grupo de HA em qualquer rede ou um FQDN correspondente. Use a configuração Global (padrão), a menos que você precise restringir a acessibilidade deste ponto de extremidade.
IPs virtuais de grupos HA	Os clientes devem usar um endereço IP virtual (ou FQDN correspondente) de um grupo HA para acessar este ponto de extremidade. Os endpoints com esse modo de vinculação podem usar o mesmo número de porta, desde que os grupos de HA selecionados para os endpoints não se sobreponham.
Interfaces de nó	Os clientes devem usar os endereços IP (ou FQDNs correspondentes) das interfaces de nó selecionadas para acessar este ponto de extremidade.
Tipo de nó	Com base no tipo de nó selecionado, os clientes devem usar o endereço IP (ou FQDN correspondente) de qualquer nó de administração ou o endereço IP (ou FQDN correspondente) de qualquer nó de gateway para acessar esse ponto de extremidade.

5. Para a etapa **Acesso do locatário**, selecione uma das seguintes opções:

Campo	Descrição
Permitir todos os inquilinos (padrão)	Todas as contas de locatários podem usar esse endpoint para acessar seus buckets. Permitir todos os locatários é quase sempre a opção apropriada para o ponto de extremidade do balanceador de carga usado para FabricPool. Você deve selecionar esta opção se ainda não tiver criado nenhuma conta de locatário.
Permitir inquilinos selecionados	Somente as contas de locatários selecionadas podem usar este ponto de extremidade para acessar seus buckets.
Bloquear inquilinos selecionados	As contas de locatários selecionadas não podem usar este ponto de extremidade para acessar seus buckets. Todos os outros inquilinos podem usar este ponto de extremidade.

6. Para a etapa **Anexar certificado**, selecione uma das seguintes opções:

Campo	Descrição
Carregar certificado (recomendado)	Use esta opção para carregar um certificado de servidor assinado pela CA, uma chave privada de certificado e um pacote de CA opcional.
Gerar certificado	Use esta opção para gerar um certificado autoassinado. Ver " Configurar pontos de extremidade do balanceador de carga " para obter detalhes sobre o que inserir.
Usar certificado StorageGRID S3	Esta opção estará disponível somente se você já tiver carregado ou gerado uma versão personalizada do certificado global StorageGRID . Ver " Configurar certificados da API S3 " para mais detalhes.

7. Selecione **Criar**.



Alterações em um certificado de ponto de extremidade podem levar até 15 minutos para serem aplicadas a todos os nós.

Crie uma conta de locatário para o FabricPool

Você deve criar uma conta de locatário no Grid Manager para uso do FabricPool .

Contas de locatário permitem que aplicativos clientes armazenem e recuperem objetos no StorageGRID. Cada conta de locatário tem seu próprio ID de conta, grupos e usuários autorizados, buckets e objetos.

Para obter detalhes sobre esta tarefa, consulte "[Criar conta de inquilino](#)" . Para usar o assistente de configuração do FabricPool para concluir esta tarefa, vá para "[Acesse e conclua o assistente de configuração do FabricPool](#)" .

Antes de começar

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

Passos

1. Selecione **LOCATÁRIOS**.
2. Selecione **Criar**.
3. Para as etapas de Inserir detalhes, insira as seguintes informações.

Campo	Descrição
Nome	Um nome para a conta do locatário. Os nomes dos inquilinos 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 inquilino.
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 de plataforma**.

Os locatários do FabricPool normalmente não precisam usar serviços de plataforma, como a replicação do CloudMirror.

- b. Opcionalmente, selecione **Usar fonte de identidade própria**.

- c. Não selecione **Permitir seleção S3**.

Os locatários do FabricPool normalmente não precisam usar o S3 Select.

- d. Opcionalmente, selecione **Usar conexão de federação de grade** para permitir que o locatário use uma ["conexão de federação de rede"](#) para clonagem de conta e replicação entre grades. Em seguida, selecione a conexão de federação de rede a ser usada.

5. Para a etapa Definir acesso root, especifique qual usuário terá a permissão de acesso root inicial para a conta do locatário, com base no uso do sistema StorageGRID ["federação de identidade"](#) , ["logon único \(SSO\)"](#) , ou ambos.

Opção	Faça isso
Se a federação de identidade não estiver habilitada	Especifique a senha a ser usada ao fazer login no locatário como usuário root local.

Opção	Faça isso
Se a federação de identidade estiver habilitada	a. Selecione um grupo federado existente para ter permissão de acesso Root para o locatário. b. Opcionalmente, especifique a senha a ser usada ao fazer login no locatário como usuário root local.
Se a federação de identidade e o logon único (SSO) estiverem habilitados	Selecione um grupo federado existente para ter permissão de acesso Root para o locatário. Nenhum usuário local pode fazer login.

6. Selecione **Criar inquilino**.

Crie um bucket S3 e obtenha chaves de acesso

Antes de usar o StorageGRID com uma carga de trabalho do FabricPool, você deve criar um bucket S3 para seus dados do FabricPool. Você também precisa obter uma chave de acesso e uma chave de acesso secreta para a conta de locatário que você usará para o FabricPool.

Para obter detalhes sobre esta tarefa, consulte ["Criar bucket S3"](#) e ["Crie suas próprias chaves de acesso S3"](#). Para usar o assistente de configuração do FabricPool para concluir esta tarefa, vá para ["Acesse e conclua o assistente de configuração do FabricPool"](#).

Antes de começar

- Você criou uma conta de locatário para uso do FabricPool.
- Você tem acesso Root à conta do locatário.

Passos

1. Sign in no Gerenciador de Inquilinos.

Você pode fazer qualquer um dos seguintes:

- Na página Contas de locatário no Grid Manager, selecione o link * Sign in* para o locatário e insira suas credenciais.
- Insira a URL da conta do locatário em um navegador da web e insira suas credenciais.

2. Crie um bucket S3 para dados do FabricPool.

Você deve criar um bucket exclusivo para cada cluster ONTAP que planeja usar.

- Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
- Selecione **Criar bucket**.
- Insira o nome do bucket StorageGRID que você deseja usar com FabricPool. Por exemplo, `fabricpool-bucket`.



Não é possível alterar o nome do bucket após criá-lo.

- Selecione a região para este bucket.

Por padrão, todos os buckets são criados no `us-east-1` região.

- e. Selecione **Continuar**.
- f. Selecione **Criar bucket**.



Não selecione **Habilitar controle de versão de objeto** para o bucket FabricPool . Da mesma forma, não edite um bucket FabricPool para usar **Disponível** ou uma consistência não padrão. A consistência de bucket recomendada para buckets do 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 **ARMAZENAMENTO (S3) > Minhas chaves de acesso**.
- 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 inserirá esses valores no ONTAP ao configurar o StorageGRID como uma camada de nuvem do FabricPool .



Se você gerar uma nova chave de acesso e uma 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 poderá perder temporariamente o acesso ao StorageGRID.

Configurar ILM para dados do FabricPool

Você pode usar este exemplo simples de política como ponto de partida para suas próprias regras e políticas de ILM.

Este exemplo pressupõe que você esteja projetando as regras do ILM e uma política do ILM para um sistema StorageGRID que tem 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 seguintes regras e políticas do ILM são apenas exemplos. Há muitas maneiras de configurar regras de ILM. Antes de ativar uma nova política, simule-a para confirmar se ela funcionará conforme o esperado para proteger o conteúdo contra perdas. Para saber mais, consulte "[Gerenciar objetos com ILM](#)" .



Para evitar perda de dados, não use uma regra de ILM que irá expirar ou excluir dados da camada de nuvem do FabricPool . Defina o período de retenção como **para sempre** para garantir que os objetos do FabricPool não sejam excluídos pelo StorageGRID ILM.

Antes de começar

- Você revisou o "[melhores práticas para usar ILM com dados do FabricPool](#)" .
- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)" .

- Você tem o "[Permissão de acesso ILM ou Root](#)".
- Se você atualizou para o StorageGRID 11.9 de uma versão anterior do StorageGRID, você configurou o pool de armazenamento que usará. Em geral, você deve criar um pool de armazenamento para cada site StorageGRID que usará para armazenar dados.



Este pré-requisito não se aplica se você instalou inicialmente o StorageGRID 11.7 ou 11.8. Quando você instala inicialmente qualquer uma dessas versões, os pools de armazenamento 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 codificadas para eliminação.

Definição de regra	Valor de exemplo
Nome da regra	Codificação de eliminação 2 + 1 para dados do FabricPool
Nome do balde	<code>fabricpool-bucket</code> Você também pode filtrar pela conta de locatário do FabricPool.
Filtros avançados	Tamanho do objeto maior que 0,2 MB. Observação: O FabricPool grava apenas objetos de 4 MB, mas você deve adicionar um filtro de tamanho de objeto porque esta regra usa codificação de eliminação.
Tempo de referência	Tempo de ingestão
Período de tempo e colocações	Desde o dia 0, guarde para sempre Armazene objetos por meio de codificação de eliminação usando o esquema EC 2+1 em Denver e retenha esses objetos no StorageGRID para sempre. Para evitar perda de dados, não use uma regra de ILM que irá expirar ou excluir dados da camada de nuvem do FabricPool.
Comportamento de ingestão	Equilibrado

2. Crie uma regra ILM padrão que criará duas cópias replicadas de quaisquer objetos não correspondidos pela primeira regra. Não selecione um filtro básico (conta de locatário ou nome do bucket) ou nenhum filtro avançado.

Definição de regra	Valor de exemplo
Nome da regra	Duas cópias replicadas

Definição de regra	Valor de exemplo
Nome do balde	<i>nenhum</i>
Filtros avançados	<i>nenhum</i>
Tempo de referência	Tempo de ingestão
Período de tempo e colocações	Desde o dia 0, guarde para sempre Armazene objetos replicando 2 cópias em Denver.
Comportamento de ingestão	Equilibrado

3. Crie uma política de ILM e selecione as duas regras. Como a regra de replicação não usa nenhum filtro, ela pode ser a regra padrão (última) para a política.
4. Ingerir objetos de teste na grade.
5. Simule a política com os objetos de teste para verificar o comportamento.
6. Ative a política.

Quando esta política é ativada, o StorageGRID coloca os dados do objeto da seguinte maneira:

- Os dados hierarquizados do FabricPool em `fabricpool-bucket` será codificado por eliminação usando o esquema de codificação de eliminação 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 nós de armazenamento diferentes.
- As cópias serão mantidas no StorageGRID para sempre. O StorageGRID ILM não excluirá esses objetos.

Crie uma política de classificação de tráfego para o FabricPool

Opcionalmente, você pode projetar uma política de classificação de tráfego 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 configuração do FabricPool para concluir esta tarefa, vá para ["Acesse e conclua o assistente de configuração do FabricPool"](#) .

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Permissão de acesso root"](#) .

Sobre esta tarefa

As práticas recomendadas para criar uma política de classificação de tráfego para o FabricPool dependem da carga de trabalho, da seguinte forma:

- Se você planeja hierarquizar os dados da carga de trabalho primária do FabricPool para o StorageGRID, 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 de priorizar do que as operações de gravação.

Por exemplo, se outros clientes S3 usarem este sistema StorageGRID , você deverá criar uma política de classificação de tráfego. Você pode limitar o tráfego de rede para outros buckets, locatários, sub-redes de IP ou pontos de extremidade do balanceador de carga.

- Geralmente, você não deve impor limites de qualidade de serviço em nenhuma carga de trabalho do 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 de trabalho. Os limites impostos também variam de acordo com o dimensionamento e as capacidades da sua rede e com a quantidade esperada de utilização.

Passos

1. Selecione **CONFIGURAÇÃO > Rede > Classificação de tráfego**.
2. Selecione **Criar**.
3. Insira um nome e uma descrição (opcional) para a política e selecione **Continuar**.
4. Para a etapa Adicionar regras de correspondência, adicione pelo menos uma regra.
 - a. Selecione **Adicionar regra**
 - b. Para 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 ou o bucket do locatário do FabricPool .
 - c. Se você quiser que esta política de tráfego limite o tráfego para os outros pontos de extremidade, selecione **Correspondência inversa**.
5. Opcionalmente, adicione um ou mais limites para controlar o tráfego de rede correspondido pela regra.



O StorageGRID coleta métricas mesmo se você não adicionar nenhum limite, para que você possa 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 **Continuar**.
 7. Leia e revise a política de classificação de tráfego. Use o botão **Anterior** para voltar e fazer as alterações necessárias. Quando estiver satisfeito com a política, selecione **Salvar e continuar**.

Depois de terminar

"[Exibir métricas de tráfego de rede](#)" para verificar se as políticas estão aplicando os limites de tráfego esperados.

Configurar o ONTAP System Manager

Depois de 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 configuração do FabricPool , você tem o `ONTAP_FabricPool_settings_bucketname.txt` arquivo que você baixou.
- Se você configurou o StorageGRID manualmente, terá o nome de domínio totalmente qualificado (FQDN) que está usando para o StorageGRID ou o endereço IP virtual (VIP) para o grupo HA do StorageGRID , o número da porta para o ponto de extremidade 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 locatário e o nome do bucket que o ONTAP usará nesse locatário.

Gerenciador de Sistema Access ONTAP

Estas instruções descrevem como usar o ONTAP System Manager para adicionar o StorageGRID como uma camada de nuvem. Você pode concluir a mesma configuração usando o ONTAP CLI. Para obter instruções, acesse "[Documentação ONTAP para FabricPool](#)".

Passos

1. Acesse o System Manager para o cluster ONTAP que você deseja hierarquizar no StorageGRID.
2. Sign in 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

Ver "[Documentação ONTAP para FabricPool](#)" para maiores 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 esta camada de nuvem. Você pode aceitar o valor padrão.
Estilo de URL	Se você "nomes de domínio de endpoint S3 configurados" , selecione URL de estilo de hospedagem virtual. URL no estilo de caminho é o padrão para ONTAP, mas usar solicitações no estilo de hospedagem virtual é recomendado para StorageGRID. Você deve usar URL no estilo de caminho se fornecer um endereço IP em vez de um nome de domínio para o campo Nome do servidor (FQDN).

Campo	Descrição
Nome do servidor (FQDN)	Insira o nome de domínio totalmente qualificado (FQDN) que você está usando para o StorageGRID ou o endereço IP virtual (VIP) para o grupo StorageGRID HA. 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 ponto de extremidade do balanceador de carga StorageGRID. • Se você fornecer um nome de domínio, o registro DNS deverá mapear cada endereço IP que você usará para se conectar ao StorageGRID. Ver "Configurar o servidor DNS".
SSL	Ativado (padrão).
Certificado de armazenamento de objetos	Cole o certificado PEM que você está usando para o ponto de extremidade do balanceador de carga StorageGRID, incluindo: <pre>-----BEGIN CERTIFICATE----- e -----END CERTIFICATE----- .</pre> Observação: Se uma CA intermediária emitiu o certificado StorageGRID, você deve fornecer o certificado da CA intermediária. Se o certificado StorageGRID foi emitido diretamente pela CA raiz, você deve fornecer o certificado da CA raiz.
Porta	Insira a porta usada pelo ponto de extremidade do balanceador de carga StorageGRID. O ONTAP usará esta porta quando 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 para o usuário raiz da conta de locatário do StorageGRID. Dica: Se você gerar uma nova chave de acesso e uma 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 poderá perder temporariamente o acesso ao StorageGRID.
Nome do contêiner	Insira o nome do bucket StorageGRID que você criou para uso com esta camada ONTAP.

2. Conclua a configuração final do FabricPool no ONTAP.

- Anexe um ou mais agregados à camada de nuvem.
- Opcionalmente, crie uma política de níveis de volume.

Configurar o servidor DNS

Depois de configurar grupos de alta disponibilidade, pontos de extremidade do balanceador de carga e nomes de domínio de ponto de extremidade 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 usar.

Ver ["Considerações para balanceamento de carga"](#) .

Entradas DNS para o nome do servidor StorageGRID

Adicione entradas de DNS para associar o nome do servidor StorageGRID (nome de domínio totalmente qualificado) a cada endereço IP do StorageGRID que você usará. Os endereços IP que você insere no DNS dependem se você está usando um grupo HA de nós de balanceamento de carga:

- Se você tiver configurado um grupo HA, o ONTAP se conectará aos endereços IP virtuais desse grupo HA.
- Se você não estiver usando um grupo HA, o ONTAP poderá se conectar ao serviço StorageGRID Load Balancer usando o endereço IP de qualquer nó de gateway ou nó de administração.
- Se o nome do servidor for resolvido para mais de um endereço IP, o ONTAP estabelecerá conexões de cliente com todos os endereços IP (até um máximo de 16 endereços IP). Os endereços IP são coletados em um método round-robin quando as conexões são estabelecidas.

Entradas de DNS para solicitações de estilo de hospedagem virtual

Se você definiu ["Nomes de domínio de endpoint S3"](#) e você usará solicitações de estilo de hospedagem virtual, adicionará entradas DNS para todos os nomes de domínio de ponto de extremidade S3 necessários, incluindo quaisquer nomes curinga.

Melhores práticas do StorageGRID para FabricPool

Melhores práticas para grupos de alta disponibilidade (HA)

Antes de anexar o StorageGRID como uma camada de nuvem do FabricPool , saiba mais sobre 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 uma coleção de interfaces de vários nós de gateway do StorageGRID , nós de administração 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 poderá gerenciar a carga de trabalho com pouco impacto nas operações do FabricPool .

Cada grupo HA fornece acesso de alta disponibilidade aos serviços compartilhados nos nós associados. Por exemplo, um grupo de HA que consiste em interfaces somente em nós de gateway ou em nós de administração e nós de gateway fornece acesso de alta disponibilidade ao serviço compartilhado do balanceador de carga.

Para saber mais sobre grupos de alta disponibilidade, consulte ["Gerenciar grupos de alta disponibilidade \(HA\)"](#) .

Usando grupos HA

As práticas recomendadas para criar um grupo HA do StorageGRID para o FabricPool dependem da carga de

trabalho.

- Se você planeja usar o FabricPool com dados de carga de trabalho primários, deverá criar um grupo de HA que inclua pelo menos dois nós de balanceamento de carga para evitar a interrupção da recuperação de dados.
- Se você planeja usar a política de níveis de volume somente de instantâneo do FabricPool ou níveis de desempenho local não primários (por exemplo, locais de recuperação de desastres ou destinos do NetApp SnapMirror®), você pode configurar um grupo de HA com apenas um nó.

Estas instruções descrevem a configuração de um grupo de HA para HA de backup ativo (um nó é ativo e um nó é de 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 HA"](#).

Melhores práticas para balanceamento de carga para FabricPool

Antes de anexar o StorageGRID como uma camada de nuvem do FabricPool, revise as práticas recomendadas para usar balanceadores de carga com o FabricPool.

Para obter informações gerais sobre o balanceador de carga StorageGRID e o certificado do balanceador de carga, consulte ["Considerações para balanceamento de carga"](#).

Melhores práticas para acesso de locatário ao ponto de extremidade do balanceador de carga usado para FabricPool

Você pode controlar quais locatários podem usar um ponto de extremidade específico do balanceador de carga para acessar seus buckets. Você pode permitir todos os inquilinos, permitir alguns inquilinos ou bloquear alguns inquilinos. Ao criar um ponto de extremidade de balanceamento de carga para uso do FabricPool, selecione **Permitir todos os locatários**. O ONTAP criptografa os dados colocados nos buckets do StorageGRID, portanto, pouca segurança adicional seria fornecida por essa camada de segurança extra.

Melhores práticas para o certificado de segurança

Ao criar um ponto de extremidade do balanceador de carga StorageGRID para uso do FabricPool, você fornece o certificado de segurança que permitirá que o ONTAP se autentique com o StorageGRID.

Na maioria dos casos, a conexão entre o ONTAP e o StorageGRID deve usar criptografia TLS (Transport Layer Security). O uso do FabricPool sem criptografia TLS é suportado, mas não recomendado. Ao selecionar o protocolo de rede para o ponto de extremidade do balanceador de carga 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 ponto de extremidade de balanceamento de carga:

- ["Gerenciar certificados de segurança"](#)
- ["Considerações para balanceamento de carga"](#)
- ["Diretrizes de proteção para certificados de servidor"](#)

Adicionar certificado ao ONTAP

Ao adicionar o StorageGRID como uma camada de nuvem do FabricPool, você deve instalar o mesmo certificado no cluster ONTAP, incluindo os certificados raiz e quaisquer certificados de autoridade de certificação (CA) subordinada.

Gerenciar expiração de certificado



Se o certificado usado para proteger a conexão entre o ONTAP e o StorageGRID expirar, o FabricPool deixará de funcionar temporariamente e o ONTAP perderá temporariamente o acesso aos dados em camadas no StorageGRID.

Para evitar problemas de expiração de certificado, siga estas práticas recomendadas:

- Monitore cuidadosamente todos os alertas que avisam sobre a aproximação das datas de expiração do certificado, como os alertas **Expiração do certificado de ponto de extremidade do balanceador de carga** e **Expiração do certificado do servidor global para a API S3**.
- Mantenha sempre as versões StorageGRID e ONTAP do certificado sincronizadas. Se você substituir ou renovar o certificado usado para um ponto de extremidade do balanceador de carga, deverá substituir ou renovar o certificado equivalente usado pelo ONTAP para a camada de nuvem.
- Use um certificado de CA assinado publicamente. Se você usar um certificado assinado por uma CA, poderá usar a API de gerenciamento de grade para automatizar a rotação de certificados. Isso permite que você substitua certificados prestes a expirar sem interrupções.
- Se você gerou um certificado StorageGRID autoassinado e esse certificado estiver prestes a expirar, você deverá substituí-lo manualmente no StorageGRID e no ONTAP antes que o certificado existente expire. Se um certificado autoassinado já tiver expirado, desative a validação do certificado no ONTAP para evitar perda de acesso.

Ver ["Base de conhecimento da NetApp : como configurar um novo certificado de servidor autoassinado StorageGRID em uma implantação ONTAP FabricPool existente"](#) para obter instruções.

Melhores práticas para usar ILM com dados do FabricPool

Se você estiver usando o FabricPool para hierarquizar dados no StorageGRID, deverá entender os requisitos para usar o gerenciamento do ciclo de vida das informações (ILM) do StorageGRID com dados do FabricPool .



O FabricPool não tem conhecimento das regras ou políticas do StorageGRID ILM. Pode ocorrer perda de dados se a política do StorageGRID ILM estiver configurada incorretamente. Para obter informações detalhadas, consulte ["Use regras do ILM para gerenciar objetos"](#) e ["Criar políticas de ILM"](#) .

Diretrizes para usar ILM com FabricPool

Quando você usa o assistente de configuração do FabricPool , o assistente cria automaticamente uma nova regra do ILM para cada bucket do S3 criado e adiciona essa regra a uma política inativa. Você será solicitado a ativar a política. A regra criada automaticamente segue as melhores práticas recomendadas: ela usa codificação de eliminação 2+1 em um único site.

Se você estiver configurando o StorageGRID manualmente em vez de usar o assistente de configuração do FabricPool , revise estas diretrizes para garantir que suas regras e políticas do ILM sejam adequadas aos dados do FabricPool e aos seus requisitos comerciais. 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 eliminação para proteger dados da camada de nuvem.

A melhor prática recomendada é usar a codificação de eliminação 2+1 em um site para proteção de dados com melhor custo-benefício. A codificação de eliminação usa mais CPU, mas oferece significativamente menos capacidade de armazenamento do que a replicação. Os esquemas 4+1 e 6+1 usam menos capacidade que o esquema 2+1. No entanto, os esquemas 4+1 e 6+1 são menos flexíveis se você precisar adicionar nós de armazenamento durante a expansão da grade. Para obter detalhes, consulte ["Adicionar capacidade de armazenamento para objetos codificados por eliminação"](#).

- Cada regra aplicada aos dados do FabricPool deve usar codificação de eliminação ou criar pelo menos duas cópias replicadas.



Uma regra de 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 nó de armazenamento falhar ou tiver 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 o ONTAP para recuperar todos os dados do volume FabricPool e promovê-lo ao nível de desempenho.



Para evitar perda de dados, não use uma regra de ILM que expire ou exclua dados da camada de nuvem do FabricPool. Defina o período de retenção em cada regra do ILM como **para sempre** para garantir que os objetos do FabricPool não sejam excluídos pelo StorageGRID ILM.

- Não crie regras que movam os dados da camada de nuvem do FabricPool do bucket para outro local. Não é possível 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 suportado devido à latência adicional para recuperar um objeto do destino do Cloud Storage Pool.

- A partir do ONTAP 9.8, você pode, opcionalmente, criar tags de objeto para ajudar a classificar e ordenar dados em camadas para facilitar o gerenciamento. Por exemplo, você pode definir tags somente em volumes FabricPool anexados ao StorageGRID. Então, ao criar regras de ILM no StorageGRID, você pode usar o filtro avançado Object Tag para selecionar e colocar esses dados.

Outras práticas recomendadas para StorageGRID e FabricPool

Ao configurar um sistema StorageGRID para uso com FabricPool, talvez seja necessário alterar outras opções do StorageGRID. Antes de alterar uma configuração global, considere como a alteração afetará outros aplicativos S3.

Destinos de mensagens e logs de auditoria

As cargas de trabalho do FabricPool geralmente têm uma alta taxa de operações de leitura, o que pode gerar um alto volume de mensagens de auditoria.

- Se você não precisar de um registro de operações de leitura do cliente para o FabricPool ou qualquer outro aplicativo S3, opcionalmente vá para **CONFIGURAÇÃO > Monitoramento > Auditoria e servidor syslog**. Altere a configuração **Leituras do cliente** para **Erro** para diminuir o número de mensagens de auditoria registradas no log de auditoria. Ver ["Configurar mensagens de auditoria e destinos de log"](#) para mais detalhes.

- Se você tiver uma grade grande, usar vários tipos de aplicativos S3 ou quiser manter 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. Ver "[Considerações para servidor syslog externo](#)" para mais detalhes.

Criptografia de objetos

Ao configurar o StorageGRID, você pode opcionalmente habilitar o "[opção global para criptografia de objetos armazenados](#)" se a criptografia de dados for necessária para outros clientes StorageGRID . Os dados que são hierarquizados do FabricPool para o StorageGRID já estão criptografados, portanto, não é necessário habilitar a configuração StorageGRID . As chaves de criptografia do lado do cliente são de propriedade do ONTAP.

Compressão de objetos

Ao configurar o StorageGRID, não habilite o "[opção global para compactar objetos armazenados](#)" . Os dados que são hierarquizados do FabricPool para o StorageGRID já estão compactados. Usar a opção StorageGRID não reduzirá ainda mais o tamanho de um objeto.

Consistência do balde

Para buckets do FabricPool , a consistência de bucket recomendada é **Leitura-após-nova-gravação**, que é a consistência padrão para um novo bucket. Não edite os buckets do FabricPool para usar **Available** ou **Strong-site**.

Hierarquização do FabricPool

Se um nó StorageGRID usar armazenamento atribuído de um sistema NetApp ONTAP , confirme se o volume não tem uma política de camadas FabricPool habilitada. Por exemplo, se um nó StorageGRID estiver em execução em um host VMware, certifique-se de que o volume que faz o backup do armazenamento de dados para o nó StorageGRID não tenha uma política de camadas FabricPool habilitada. Desabilitar a hierarquização do FabricPool para volumes usados com nós StorageGRID simplifica a solução de problemas e as operações de armazenamento.



Nunca use o FabricPool para hierarquizar quaisquer dados relacionados ao StorageGRID de volta ao próprio StorageGRID . A hierarquização dos dados do StorageGRID de volta ao StorageGRID aumenta a complexidade operacional e de solução de problemas.

Remover dados do FabricPool do StorageGRID

Se precisar remover os dados do FabricPool que estão atualmente armazenados no StorageGRID, você deverá usar o ONTAP para recuperar todos os dados do volume do FabricPool e promovê-lo ao nível de desempenho.

Antes de começar

- Você revisou as instruções e considerações em "[Promova dados para o nível de desempenho](#)" .
- Você está usando o ONTAP 9.8 ou posterior.
- Você está usando um "[navegador da web compatível](#)" .
- Você pertence a um grupo de usuários do StorageGRID para a conta de locatário do FabricPool que tem o "[Gerenciar todos os buckets ou permissão de acesso root](#)" .

Sobre esta tarefa

Estas instruções explicam como mover dados do StorageGRID de volta para o FabricPool. Execute este

procedimento usando o ONTAP e o StorageGRID Tenant Manager.

Passos

1. Do ONTAP, emita o `volume modify` comando.

Definir `tiering-policy` para `none` para parar novas camadas e definir `cloud-retrieval-policy` para `promote` para retornar todos os dados que foram previamente hierarquizados para StorageGRID.

Ver ["Promova todos os dados de um volume FabricPool para a camada de desempenho"](#) .

2. Aguarde a conclusão da operação.

Você pode usar o `volume object-store` comando com o `tiering` opção para ["verificar o status da promoção do nível de desempenho"](#) .

3. Quando a operação de promoção estiver concluída, entre no StorageGRID Tenant Manager para a conta de locatário do FabricPool .
4. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
5. Confirme se o bucket FabricPool agora está vazio.
6. Se o balde estiver vazio, ["exclua o balde"](#) .

Depois que você terminar

Quando você exclui o bucket, a hierarquização do FabricPool para o StorageGRID não pode mais continuar. No entanto, como a camada local ainda está anexada à camada 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 o seguinte:

- Use o FabricPool Mirror para anexar uma camada de nuvem diferente ao agregado.
- Mova os dados do agregado FabricPool para um agregado não FabricPool e exclua o agregado não utilizado.

Veja o ["Documentação ONTAP para FabricPool"](#) para obter instruções.

Informações sobre direitos autorais

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

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

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS 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.