



Documentação do software StorageGRID 11.9

StorageGRID software

NetApp
December 03, 2025

This PDF was generated from <https://docs.netapp.com/pt-br/storagegrid-119/index.html> on December 03, 2025. Always check docs.netapp.com for the latest.

Índice

Documentação do software StorageGRID 11.9	1
Dispositivos StorageGRID	2
Notas de lançamento	3
Comece com um sistema StorageGRID	4
Saiba mais sobre o StorageGRID	4
O que é StorageGRID?	4
Nuvens híbridas com StorageGRID	6
Arquitetura e topologia de rede do StorageGRID	7
Nós e serviços de grade	11
Como o StorageGRID gerencia dados	23
Explorar StorageGRID	35
Diretrizes de rede	43
Diretrizes de rede	44
Tipos de rede StorageGRID	45
Exemplos de topologia de rede	49
Requisitos de rede	55
Requisitos específicos da rede	57
Considerações de rede específicas para implantação	59
Instalação e provisionamento de rede	62
Diretrizes pós-instalação	63
Referência de porta de rede	63
Início rápido para StorageGRID	74
Instalar, atualizar e corrigir o StorageGRID	77
Dispositivos StorageGRID	77
Instalar o StorageGRID no Red Hat Enterprise Linux	77
Início rápido para instalar o StorageGRID no Red Hat Enterprise Linux	77
Planeje e prepare a instalação no Red Hat	78
Automatize a instalação do StorageGRID no Red Hat Enterprise Linux	105
Implantar nós de grade virtual (Red Hat)	108
Configurar a grade e concluir a instalação (Red Hat)	131
Instalação REST API	144
Para onde ir a seguir	145
Solucionar problemas de instalação	146
Exemplo /etc/sysconfig/network-scripts	147
Instalar o StorageGRID no Ubuntu ou Debian	149
Início rápido para instalar o StorageGRID no Ubuntu ou Debian	149
Planeje e prepare a instalação no Ubuntu ou Debian	150
Automatize a instalação (Ubuntu ou Debian)	178
Implantar nós de grade virtual (Ubuntu ou Debian)	180
Configurar a grade e concluir a instalação (Ubuntu ou Debian)	203
Instalação REST API	216
Para onde ir a seguir	217
Solucionar problemas de instalação	218

Exemplo /etc/network/interfaces	219
Instalar o StorageGRID no VMware	220
Início rápido para instalar o StorageGRID no VMware	220
Planeje e prepare a instalação no VMware	221
Automatize a instalação (VMware)	231
Implantar nós de grade de máquina virtual (VMware)	244
Configurar a grade e concluir a instalação (VMware)	253
Instalação REST API	266
Para onde ir a seguir	267
Solucionar problemas de instalação	268
Atualizar o software StorageGRID	270
Atualizar o software StorageGRID	270
Novidades no StorageGRID 11.9	270
Recursos e funcionalidades removidos ou obsoletos	273
Alterações na API de gerenciamento de grade	275
Alterações na API de gerenciamento de locatários	276
Planeje e prepare-se para a atualização	276
Atualizar software	284
Solucionar problemas de atualização	299
Aplicar hotfix do StorageGRID	302
Procedimento de correção do StorageGRID	302
Como seu sistema é afetado quando você aplica um hotfix	303
Obtenha os materiais necessários para o hotfix	304
Baixar arquivo de hotfix	304
Verifique a condição do sistema antes de aplicar o hotfix	305
Aplicar hotfix	306
Configurar e gerenciar um sistema StorageGRID	310
Administrar StorageGRID	310
Administrar StorageGRID	310
Comece a usar o Grid Manager	310
Controle o acesso ao StorageGRID	341
Usar federação de grade	389
Gerenciar segurança	426
Gerenciar inquilinos	495
Configurar conexões do cliente	515
Gerenciar redes e conexões	556
Usar AutoSupport	575
Gerenciar nós de armazenamento	590
Gerenciar nós de administração	604
Gerenciar objetos com ILM	607
Gerenciar objetos com ILM	607
ILM e ciclo de vida do objeto	608
Criar e atribuir níveis de armazenamento	630
Use pools de armazenamento	633
Use pools de armazenamento em nuvem	641

Gerenciar perfis de codificação de eliminação	662
Configurar regiões (opcional e somente S3)	665
Criar regra ILM	667
Gerenciar políticas de ILM	683
Trabalhar com políticas e regras do ILM	700
Usar bloqueio de objeto S3	704
Exemplo de regras e políticas do ILM	712
Endurecimento do sistema	731
Considerações gerais para o reforço do sistema	731
Diretrizes de reforço para atualizações de software	732
Diretrizes de proteção para redes StorageGRID	733
Diretrizes de proteção para nós do StorageGRID	734
Diretrizes de proteção para TLS e SSH	737
Outras diretrizes de endurecimento	738
Configurar StorageGRID para FabricPool	740
Configurar StorageGRID para FabricPool	740
Informações necessárias para anexar o StorageGRID como uma camada de nuvem	742
Use o assistente de configuração do FabricPool	743
Configurar o StorageGRID manualmente	756
Configurar o ONTAP System Manager	766
Configurar o servidor DNS	768
Melhores práticas do StorageGRID para FabricPool	769
Remover dados do FabricPool do StorageGRID	773
Use locatários e clientes do StorageGRID	775
Use uma conta de inquilino	775
Use uma conta de inquilino	775
Como entrar e sair	776
Entenda o painel do Tenant Manager	781
API de gerenciamento de inquilinos	784
Usar conexões de federação de grade	789
Gerenciar grupos e usuários	803
Gerenciar chaves de acesso S3	822
Gerenciar buckets S3	828
Gerenciar serviços da plataforma S3	851
Usar API REST do S3	884
Versões e atualizações suportadas pela API REST do S3	884
Referência rápida: solicitações de API do S3 suportadas	887
Testar configuração da API REST do S3	906
Como o StorageGRID implementa a API REST do S3	907
Suporte para API REST do Amazon S3	922
Operações personalizadas do StorageGRID	972
Políticas de acesso a grupos e buckets	994
Operações S3 rastreadas nos logs de auditoria	1020
Use a API REST do Swift (fim da vida útil)	1021
Usar a API REST do Swift	1021

Monitorar e solucionar problemas de um sistema StorageGRID	1022
Monitorar o sistema StorageGRID	1022
Monitorar um sistema StorageGRID	1022
Visualizar e gerenciar o painel	1022
Ver a página de nós	1025
Informações para monitorar regularmente	1059
Gerenciar alertas	1089
Referência de arquivos de log	1126
Configurar destinos de mensagens e logs de auditoria	1145
Usar monitoramento SNMP	1160
Coletar dados adicionais do StorageGRID	1172
Solucionar problemas do sistema StorageGRID	1207
Solucionar problemas de um sistema StorageGRID	1207
Solucionar problemas de objetos e armazenamento	1214
Solucionar problemas de metadados	1243
Solucionar erros de certificado	1244
Solucionar problemas do nó de administração e da interface do usuário	1246
Solucionar problemas de rede, hardware e plataforma	1249
Solucionar problemas de um servidor syslog externo	1257
Revisar logs de auditoria	1260
Mensagens e logs de auditoria	1260
Fluxo e retenção de mensagens de auditoria	1261
Arquivo de log de auditoria de acesso	1264
Rotação do arquivo de log de auditoria	1265
Formato de arquivo de log de auditoria	1265
Formato de mensagem de auditoria	1278
Mensagens de auditoria e o ciclo de vida do objeto	1282
Mensagens de auditoria	1290
Expandir uma grade	1342
Tipos de expansão	1342
Plano de expansão do StorageGRID	1343
Adicionar capacidade de armazenamento	1343
Adicionar capacidade de metadados	1351
Adicione nós de grade para adicionar recursos ao seu sistema	1353
Adicionar um novo site	1353
Reúna os materiais necessários	1354
Baixe e extraia os arquivos de instalação do StorageGRID	1355
Verificar hardware e rede	1361
Adicionar volumes de armazenamento	1362
Adicionar volumes de armazenamento aos nós de armazenamento	1362
VMware: Adicionar volumes de armazenamento ao nó de armazenamento	1365
Linux: Adicionar volumes SAN ou de conexão direta ao nó de armazenamento	1367
Adicionar nós de grade ou site	1370
Adicionar nós de grade ao site existente ou adicionar um novo site	1370
Atualizar sub-redes para a rede Grid	1371

Implantar novos nós de grade	1372
Executar expansão	1378
Configurar sistema expandido	1385
Etapas de configuração após expansão	1385
Verifique se o nó de armazenamento está ativo	1387
Copiar banco de dados do nó de administração	1387
Copiar métricas do Prometheus	1389
Copiar logs de auditoria	1390
Rebalancear dados codificados para eliminação após adicionar nós de armazenamento	1392
Solucionar problemas de expansão	1395
Manter um sistema StorageGRID	1397
Manutenção da rede	1397
Antes de começar	1397
Procedimentos de manutenção para aparelhos	1397
Baixar pacote de recuperação	1397
Descomissionar nós ou site	1398
Desativar nó ou local	1398
Descomissionar nós	1398
Local de descomissionamento	1418
Renomear grade, site ou nó	1440
Use o procedimento de renomeação	1440
Adicionar ou atualizar nomes de exibição	1444
Procedimentos de nó	1450
Procedimentos de manutenção de nós	1450
Procedimentos do Gerenciador de Servidores	1450
Procedimentos de reinicialização, desligamento e energia	1460
Procedimentos de remapeamento de portas	1472
Procedimentos de rede	1476
Atualizar sub-redes para a rede Grid	1476
Configurar endereços IP	1478
Adicionar interfaces ao nó existente	1495
Configurar servidores DNS	1499
Modificar a configuração de DNS para um único nó de grade	1500
Gerenciar servidores NTP	1502
Restaurar a conectividade de rede para nós isolados	1503
Procedimentos de host e middleware	1505
Linux: Migrar nó de grade para novo host	1505
VMware: Configurar máquina virtual para reinicialização automática	1507
Recuperar ou substituir nós	1508
Avisos e considerações para recuperação de nós de rede	1508
Pré-condições para recuperação de nós de grade	1508
Ordem de recuperação do nó se um servidor que hospeda mais de um nó de grade falhar	1509
Endereços IP para nós recuperados	1509
Reúna os materiais necessários para a recuperação dos nós da grade	1509
Baixe e extraia os arquivos de instalação do StorageGRID	1510

Selecione o procedimento de recuperação do nó	1516
Recuperar de falhas do nó de armazenamento	1517
Recuperar de falhas do nó de armazenamento	1517
Recuperar nó de armazenamento do dispositivo	1518
Recuperar de falha de volume de armazenamento onde a unidade do sistema está intacta	1540
Recuperar de falha de unidade do sistema	1555
Restaurar dados de objetos usando o Grid Manager	1573
Monitorar trabalhos de reparo de dados	1576
Recuperar de falhas do nó de administração	1578
Recuperação do nó de administração primário ou não primário	1578
Recuperar de falhas do nó de administração primário	1578
Recuperar de falhas de nó de administração não primário	1587
Recuperar de falhas do nó de gateway	1595
Substituir nó de gateway	1595
Selecione Iniciar recuperação para configurar o nó do gateway	1595
Recuperar de falhas do nó de arquivo	1597
Recuperar de falhas do nó de arquivo	1597
Substituir nó Linux	1597
Substituir nó Linux	1597
Implantar novos hosts Linux	1598
Restaurar nós de grade para o host	1599
Próximo passo: execute etapas adicionais de recuperação, se necessário	1603
Substituir nó VMware	1605
Substituir nó com falha por dispositivo de serviços	1606
Substituir nó com falha por dispositivo de serviços	1606
Instalar serviço de appliance (somente mudança de plataforma)	1606
Preparar o aparelho para reinstalação (somente substituição da plataforma)	1607
Iniciar instalação de software no dispositivo de serviços	1607
Instalação de aparelhos de serviços de monitoramento	1611
Como o suporte técnico recupera um site	1614
Como habilitar o StorageGRID em seu ambiente	1616
Como gerenciar o StorageGRID usando o NetApp Console	1617
Avisos legais	1618
Direitos autorais	1618
Marcas Registradas	1618
Patentes	1618
Política de Privacidade	1618
Código aberto	1618

Documentação do software StorageGRID 11.9

Dispositivos StorageGRID

Vá para "[Documentação do dispositivo StorageGRID](#)" para aprender como instalar, configurar e manter dispositivos de armazenamento e serviços StorageGRID .

Notas de lançamento

Obtenha informações específicas da versão sobre problemas corrigidos e problemas conhecidos.

Faça login no site de suporte da NetApp para "[visualizar ou baixar um arquivo PDF](#)" contendo as notas de versão do StorageGRID 11.9.

Comece com um sistema StorageGRID

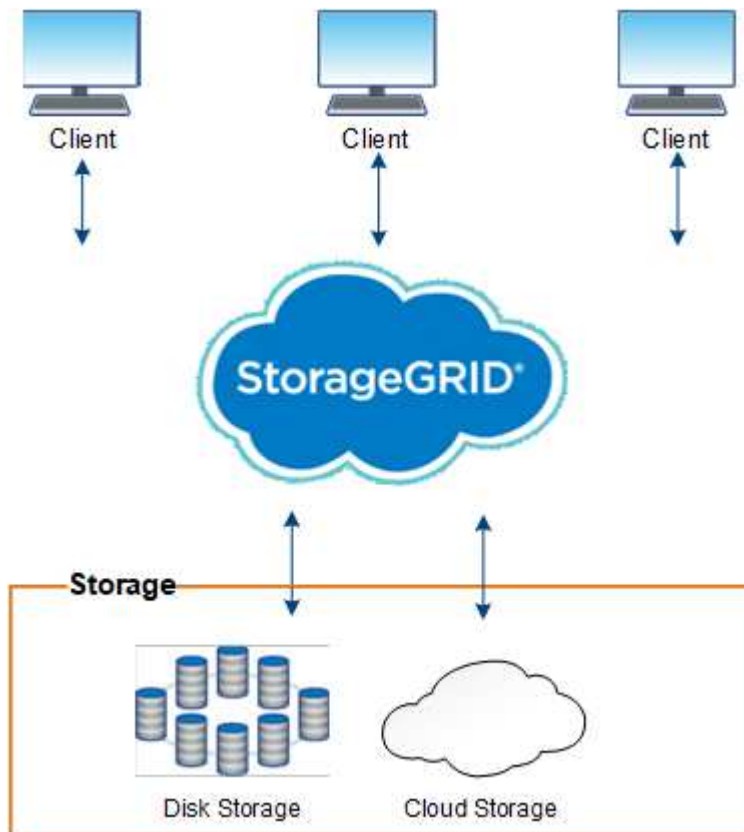
Saiba mais sobre o StorageGRID

O que é StorageGRID?

O NetApp® StorageGRID® é um conjunto de armazenamento de objetos definido por software que oferece suporte a uma ampla variedade de casos de uso em ambientes multicloud públicos, privados e híbridos. O StorageGRID oferece suporte nativo para a API do Amazon S3 e fornece inovações líderes do setor, como gerenciamento automatizado do ciclo de vida para armazenar, proteger, proteger e preservar dados não estruturados de forma econômica por longos períodos.

O StorageGRID fornece armazenamento seguro e durável para dados não estruturados em escala. Políticas integradas de gerenciamento de ciclo de vida orientadas por metadados otimizam onde seus dados ficam ao longo de sua vida útil. O conteúdo é colocado no local certo, na hora certa e no nível de armazenamento certo para reduzir custos.

O StorageGRID é composto de nós geograficamente distribuídos, redundantes e heterogêneos, que podem ser integrados a aplicativos clientes existentes e de próxima geração.



O suporte para nós de arquivo foi removido. A movimentação de objetos de um nó de arquivo para um sistema de armazenamento de arquivo externo por meio da API S3 foi substituída por "[Pools de armazenamento em nuvem ILM](#)", que oferecem mais funcionalidade.

Benefícios do StorageGRID

As vantagens do sistema StorageGRID incluem o seguinte:

- Repositório de dados distribuído geograficamente para dados não estruturados, altamente escalável e fácil de usar.
- Protocolos padrão de armazenamento de objetos:
 - Serviço de armazenamento simples da Amazon Web Services (S3)
 - OpenStack Swift



O suporte para aplicativos cliente Swift foi descontinuado e será removido em uma versão futura.

- Habilitado para nuvem híbrida. O gerenciamento do ciclo de vida das informações (ILM) baseado em políticas armazena objetos em nuvens públicas, incluindo Amazon Web Services (AWS) e Microsoft Azure. Os serviços da plataforma StorageGRID permitem replicação de conteúdo, notificação de eventos e pesquisa de metadados de objetos armazenados em nuvens públicas.
- Proteção de dados flexível para garantir durabilidade e disponibilidade. Os dados podem ser protegidos usando replicação e codificação de eliminação em camadas. A verificação de dados em repouso e em voo garante integridade para retenção de longo prazo.
- Gerenciamento dinâmico do ciclo de vida de dados para ajudar a gerenciar os custos de armazenamento. Você pode criar regras de ILM que gerenciam o ciclo de vida dos dados no nível do objeto, personalizando a localidade, a durabilidade, o desempenho, o custo e o tempo de retenção dos dados.
- Alta disponibilidade de armazenamento de dados e algumas funções de gerenciamento, com balanceamento de carga integrado para otimizar a carga de dados nos recursos do StorageGRID .
- Suporte para várias contas de locatários de armazenamento para segregar os objetos armazenados no seu sistema por diferentes entidades.
- Diversas ferramentas para monitorar a integridade do seu sistema StorageGRID , incluindo um sistema de alerta abrangente, um painel gráfico e status detalhados para todos os nós e sites.
- Suporte para implantação baseada em software ou hardware. Você pode implantar o StorageGRID em qualquer um dos seguintes:
 - Máquinas virtuais em execução no VMware.
 - Mecanismos de contêiner em hosts Linux.
 - Dispositivos projetados pela StorageGRID .
 - Os dispositivos de armazenamento fornecem armazenamento de objetos.
 - Os dispositivos de serviços fornecem serviços de administração de rede e balanceamento de carga.
- Em conformidade com os requisitos de armazenamento relevantes destes regulamentos:
 - Comissão de Valores Mobiliários (SEC) em 17 CFR § 240.17a-4(f), que regulamenta membros de bolsas, corretores ou negociantes.
 - Regra 4511(c) da Autoridade Reguladora do Setor Financeiro (FINRA), que difere dos requisitos de formato e mídia da Regra 17a-4(f) da SEC.
 - Commodity Futures Trading Commission (CFTC) no regulamento 17 CFR § 1.31(c)-(d), que regulamenta a negociação de futuros de commodities.
- Operações de atualização e manutenção não disruptivas. Mantenha o acesso ao conteúdo durante os

procedimentos de atualização, expansão, desativação e manutenção.

- Gerenciamento de identidade federada. Integra-se com o Active Directory, OpenLDAP ou Oracle Directory Service para autenticação de usuários. Oferece suporte ao logon único (SSO) usando o padrão Security Assertion Markup Language 2.0 (SAML 2.0) para trocar dados de autenticação e autorização entre o StorageGRID e o Active Directory Federation Services (AD FS).

Nuvens híbridas com StorageGRID

Use o StorageGRID em uma configuração de nuvem híbrida implementando o gerenciamento de dados orientado por políticas para armazenar objetos em pools de armazenamento em nuvem, aproveitando os serviços da plataforma StorageGRID e hierarquizando dados do ONTAP para o StorageGRID com o NetApp FabricPool.

Pools de armazenamento em nuvem

Os pools de armazenamento em nuvem permitem que você armazene objetos fora do 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 de objetos StorageGRID , que pode ser usado para recuperar dados perdidos devido a uma falha de volume de armazenamento ou nó de armazenamento.

O armazenamento de terceiros também é suportado, incluindo armazenamento em disco e fita.



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.

Serviços da plataforma S3

Os serviços da plataforma S3 oferecem a capacidade de usar serviços remotos como pontos de extremidade para replicação de objetos, notificações de eventos ou integração de pesquisa. Os serviços de plataforma operam independentemente das regras de ILM da grade e são habilitados para buckets S3 individuais. Os seguintes serviços são suportados:

- O serviço de replicação do CloudMirror espelha automaticamente objetos especificados em um bucket S3 de destino, que pode estar no Amazon S3 ou em um segundo sistema StorageGRID .
- O serviço de notificação de eventos envia mensagens sobre ações especificadas para um ponto de extremidade externo que oferece suporte ao recebimento de eventos do Simple Notification Service (Amazon SNS).
- O serviço de integração de pesquisa envia metadados de objetos para um serviço Elasticsearch externo, permitindo que os metadados sejam pesquisados, visualizados e analisados usando ferramentas de terceiros.

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.

Camadas de dados ONTAP usando FabricPool

Você pode reduzir o custo do armazenamento ONTAP hierarquizando dados no StorageGRID usando o FabricPool. O FabricPool permite o armazenamento automatizado de dados em camadas de armazenamento de objetos de baixo custo, no local ou externamente.

Ao contrário das soluções de hierarquização manual, o FabricPool reduz o custo total de propriedade ao automatizar a hierarquização de dados para diminuir o custo de armazenamento. Ele oferece os benefícios da economia da nuvem por meio de camadas em nuvens públicas e privadas, incluindo StorageGRID.

Informações relacionadas

- ["O que é Cloud Storage Pool?"](#)
- ["Gerenciar serviços de plataforma"](#)
- ["Configurar StorageGRID para FabricPool"](#)

Arquitetura e topologia de rede do StorageGRID

Um sistema StorageGRID consiste em vários tipos de nós de grade em um ou mais locais de data center.

Veja o ["descrições dos tipos de nós da grade"](#) .

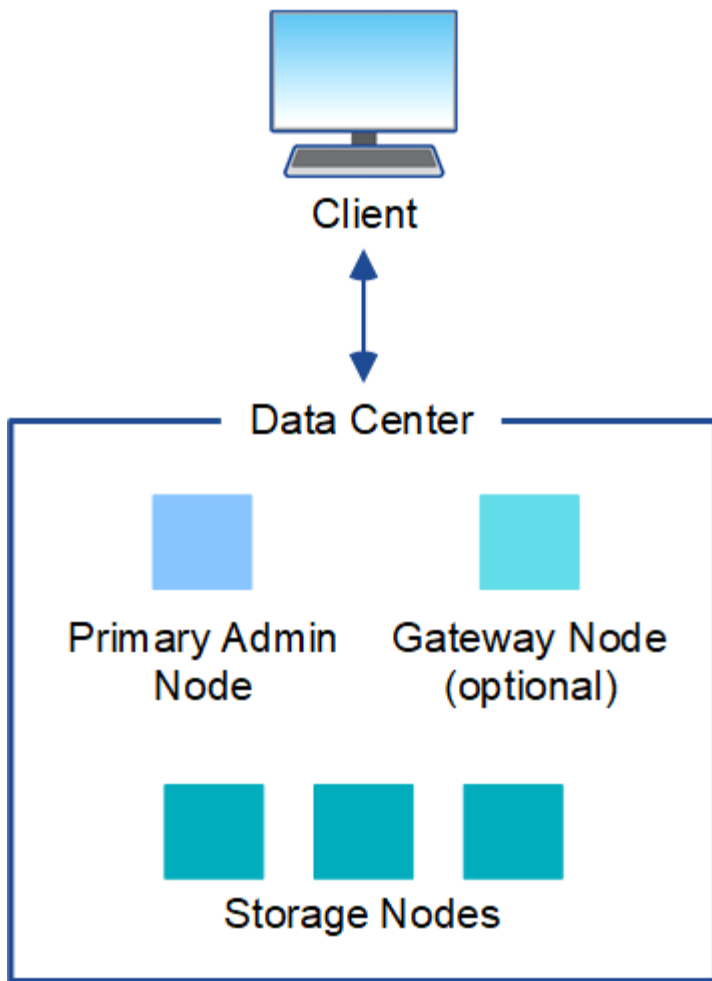
Para obter informações adicionais sobre a topologia da rede StorageGRID , requisitos e comunicações de grade, consulte o ["Diretrizes de rede"](#) .

Topologias de implantação

O sistema StorageGRID pode ser implantado em um único local de data center ou em vários locais de data center.

Site único

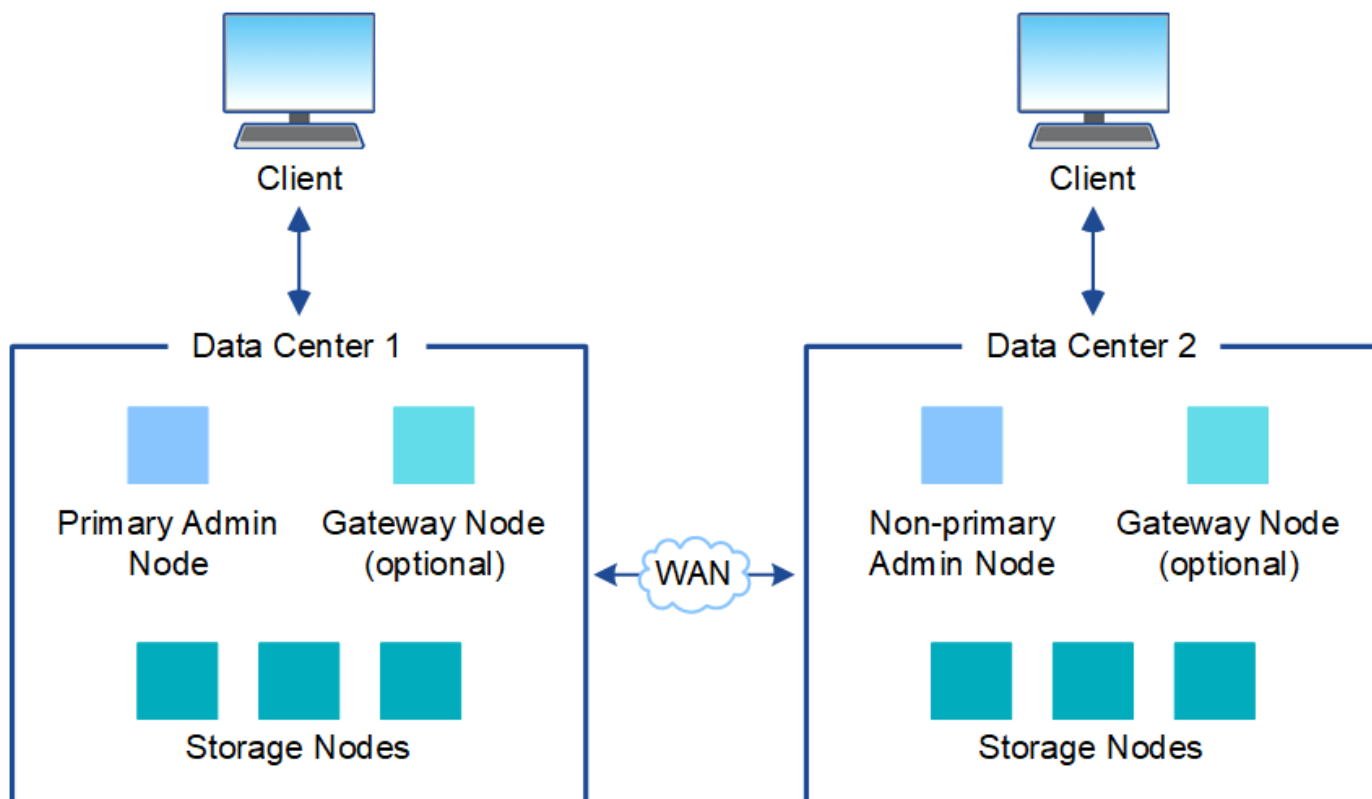
Em uma implantação com um único site, a infraestrutura e as operações do sistema StorageGRID são centralizadas.



Vários sites

Em uma implantação com vários sites, diferentes tipos e números de recursos do StorageGRID podem ser instalados em cada site. Por exemplo, pode ser necessário mais armazenamento em um data center do que em outro.

Diferentes locais geralmente estão localizados em locais geograficamente diferentes em diferentes domínios de falhas, como uma falha geológica causada por terremotos ou uma planície de inundação. O compartilhamento de dados e a recuperação de desastres são obtidos pela distribuição automatizada de dados para outros sites.



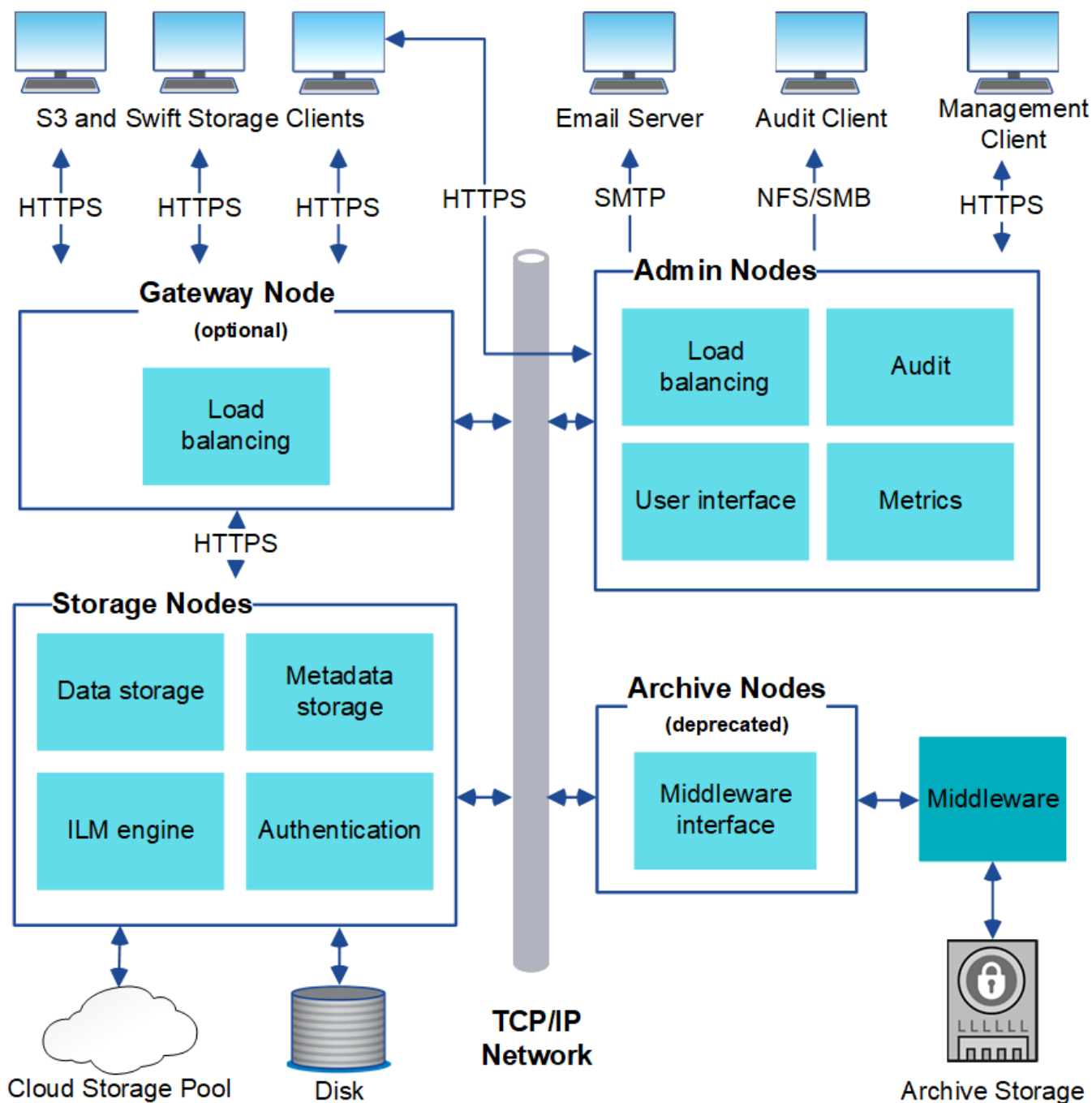
Vários sites lógicos também podem existir em um único data center para permitir o uso de replicação distribuída e codificação de eliminação para aumentar a disponibilidade e a resiliência.

Redundância de nós de grade

Em uma implantação de site único ou de vários sites, você pode, opcionalmente, incluir mais de um nó de administração ou nó de gateway para redundância. Por exemplo, você pode instalar mais de um nó de administração em um único site ou em vários sites. No entanto, cada sistema StorageGRID pode ter apenas um nó de administração primário.

Arquitetura do sistema

Este diagrama mostra como os nós da grade são organizados dentro de um sistema StorageGRID .



Os clientes S3 armazenam e recuperam objetos no StorageGRID. Outros clientes são usados para enviar notificações por e-mail, para acessar a interface de gerenciamento do StorageGRID e, opcionalmente, para acessar o compartilhamento de auditoria.

Os clientes S3 podem se conectar a um nó de gateway ou a um nó de administração para usar a interface de balanceamento de carga para nós de armazenamento. Como alternativa, os clientes S3 podem se conectar diretamente aos nós de armazenamento usando HTTPS.

Os objetos podem ser armazenados no StorageGRID em nós de armazenamento baseados em software ou hardware, ou em pools de armazenamento em nuvem, que consistem em buckets S3 externos ou contêineres de armazenamento de Blobs do Azure.

Nós e serviços de grade

Nós e serviços de grade

O bloco de construção básico de um sistema StorageGRID é o nó de grade. Os nós contêm serviços, que são módulos de software que fornecem um conjunto de recursos a um nó de grade.

Tipos de nós de grade

O sistema StorageGRID usa quatro tipos de nós de grade:

Nós de administração

Fornecer serviços de gerenciamento, como configuração do sistema, monitoramento e registro. Ao fazer login no Grid Manager, você está se conectando a um nó de administração. Cada grade deve ter um nó administrativo primário e pode ter nós administrativos não primários adicionais para redundância. Você pode se conectar a qualquer nó administrativo, e cada nó administrativo exibe uma visão semelhante do sistema StorageGRID. No entanto, os procedimentos de manutenção devem ser executados usando o nó de administração principal.

Os nós de administração também podem ser usados para balancear a carga do tráfego do cliente S3.

Ver "[O que é um nó de administração?](#)"

Nós de armazenamento

Gerencie e armazene dados de objetos e metadados. Cada site no seu sistema StorageGRID deve ter pelo menos três nós de armazenamento.

Ver "[O que é um nó de armazenamento?](#)"

Nós de gateway (opcional)

Forneça uma interface de balanceamento de carga que os aplicativos clientes podem usar para se conectar ao StorageGRID. Um balanceador de carga direciona os clientes perfeitamente para um nó de armazenamento ideal, de modo que a falha de nós ou até mesmo de um site inteiro seja transparente.

Ver "[O que é um nó de gateway?](#)"

Nós de hardware e software

Os nós do StorageGRID podem ser implantados como nós de dispositivos do StorageGRID ou como nós baseados em software.

Nós do dispositivo StorageGRID

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 de dispositivos totalmente projetadas, sem dependências de hipervisores externos, armazenamento ou hardware de computação.

Veja o seguinte para saber mais sobre os aparelhos disponíveis:

- "[Documentação do dispositivo StorageGRID](#)"

- ["Hardware Universe da NetApp"](#)

Nós baseados em software

Os nós de grade baseados em software podem ser implantados como máquinas virtuais VMware ou em mecanismos de contêiner em um host Linux.

- Máquina virtual (VM) no VMware vSphere: Consulte ["Instalar o StorageGRID no VMware"](#) .
- Dentro de um mecanismo de contêiner no Red Hat Enterprise Linux: Veja ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#) .
- Dentro de um mecanismo de contêiner no Ubuntu ou Debian: Veja ["Instalar o StorageGRID no Ubuntu ou Debian"](#) .

Use o ["Ferramenta de Matriz de Interoperabilidade NetApp \(IMT\)"](#) para determinar as versões suportadas.

Durante a instalação inicial de um novo nó de armazenamento baseado em software, você pode especificar que ele seja usado apenas para ["armazenar metadados"](#) .

Serviços StorageGRID

A seguir está uma lista completa de serviços do StorageGRID .

Serviço	Descrição	Localização
Encaminhador de serviços de conta	Fornecer uma interface para o serviço Load Balancer consultar o Account Service em hosts remotos e fornecer notificações de alterações de configuração do Load Balancer Endpoint para o serviço Load Balancer.	Serviço de balanceador de carga em nós de administração e nós de gateway
ADC (Controlador de Domínio Administrativo)	Mantém informações de topologia, fornece serviços de autenticação e responde a consultas dos serviços LDR e CMN.	Pelo menos três nós de armazenamento contendo o serviço ADC em cada site
AMS (Sistema de Gestão de Auditoria)	Monitora e registra todos os eventos e transações do sistema auditados em um arquivo de log de texto.	Nós de administração
Cassandra Reaper	Executa reparos automáticos de metadados de objetos.	Nós de armazenamento
Serviço de pedaços	Gerencia dados codificados por eliminação e fragmentos de paridade.	Nós de armazenamento
CMN (Nó de Gerenciamento de Configuração)	Gerencia configurações de todo o sistema e tarefas de grade. Cada grade tem um serviço CMN.	Nó de administração primário

Serviço	Descrição	Localização
DDS (Armazenamento de Dados Distribuídos)	Faz interface com o banco de dados Cassandra para gerenciar metadados de objetos.	Nós de armazenamento
DMV (Movimentador de Dados)	Move dados para pontos de extremidade na nuvem.	Nós de armazenamento
IP dinâmico (dynip)	Monitora a grade em busca de alterações dinâmicas de IP e atualiza as configurações locais.	Todos os nós
Grafana	Usado para visualização de métricas no Grid Manager.	Nós de administração
Alta disponibilidade	Gerencia IPs virtuais de alta disponibilidade em nós configurados na página Grupos de alta disponibilidade. Este serviço também é conhecido como serviço keepalived.	Nós de administração e gateway
Identidade (idnt)	Federa identidades de usuários do LDAP e do Active Directory.	Nós de armazenamento que usam o serviço ADC
Árbitro Lambda	Gerencia solicitações SelectObjectContent do S3 Select.	Todos os nós
Balanceador de carga (nginx-gw)	Fornece balanceamento de carga do tráfego S3 de clientes para nós de armazenamento. O serviço Load Balancer pode ser configurado por meio da página de configuração de endpoints do Load Balancer. Este serviço também é conhecido como serviço nginx-gw.	Nós de administração e gateway
LDR (Roteador de Distribuição Local)	Gerencia o armazenamento e a transferência de conteúdo dentro da grade.	Nós de armazenamento
Daemon de controle do serviço de informações MISCd	Fornece uma interface para consultar e gerenciar serviços em outros nós e para gerenciar configurações ambientais no nó, como consultar o estado de serviços em execução em outros nós.	Todos os nós
nginx	Atua como um mecanismo de autenticação e comunicação segura para vários serviços de grade (como Prometheus e IP dinâmico) para poder se comunicar com serviços em outros nós por meio de APIs HTTPS.	Todos os nós

Serviço	Descrição	Localização
nginx-gw	Alimenta o serviço Load Balancer.	Nós de administração e gateway
NMS (Sistema de Gerenciamento de Rede)	Fornecer energia às opções de monitoramento, geração de relatórios e configuração que são exibidas por meio do Grid Manager.	Nós de administração
Persistência	Gerencia arquivos no disco raiz que precisam persistir após uma reinicialização.	Todos os nós
Prometeu	Coleta métricas de séries temporais de serviços em todos os nós.	Nós de administração
RSM (Máquina de Estados Replicada)	Garante que as solicitações de serviço da plataforma sejam enviadas aos seus respectivos endpoints.	Nós de armazenamento que usam o serviço ADC
SSM (Monitor de status do servidor)	Monitora as condições do hardware e reporta ao serviço NMS.	Uma instância está presente em cada nó da grade
Coletor de traços	Executa a coleta de rastreamento para reunir informações para uso pelo suporte técnico. O serviço coletor de rastreamento usa o software Jaeger de código aberto.	Nós de administração

O que é um nó de administração?

Os nós de administração fornecem serviços de gerenciamento, como configuração do sistema, monitoramento e registro. Os nós de administração também podem ser usados para balancear a carga do tráfego do cliente S3. Cada grade deve ter um nó administrativo primário e pode ter qualquer número de nós administrativos não primários para redundância.

Diferenças entre nós administrativos primários e não primários

Ao fazer login no Grid Manager ou no Tenant Manager, você está se conectando a um nó de administração. Você pode se conectar a qualquer nó administrativo, e cada nó administrativo exibe uma visão semelhante do sistema StorageGRID. No entanto, o nó administrativo primário fornece mais funcionalidades do que os nós administrativos não primários. Por exemplo, a maioria dos procedimentos de manutenção deve ser executada nos nós de administração primários.

A tabela resume os recursos dos nós administrativos primários e não primários.

Capacidades	Nó de administração primário	Nó de administração não primário
Inclui oAMS serviço	Sim	Sim
Inclui oCMN serviço	Sim	Não
Inclui oNMS serviço	Sim	Sim
Inclui oPrometeu serviço	Sim	Sim
Inclui oSSM serviço	Sim	Sim
Inclui oBalanceador de carga eAlta disponibilidade serviços	Sim	Sim
Suporta oInterface de Programa de Aplicação de Gerenciamento (mgmt-api)	Sim	Sim
Pode ser usado para todas as tarefas de manutenção relacionadas à rede, por exemplo, alteração de endereço IP e atualização de servidores NTP	Sim	Não
Pode executar o rebalanceamento do EC após a expansão do nó de armazenamento	Sim	Não
Pode ser usado para o procedimento de restauração de volume	Sim	Sim
Pode coletar arquivos de log e dados do sistema de um ou mais nós	Sim	Não
Envia notificações de alerta, pacotes AutoSupport e traps SNMP e informa	Sim. Atua como remetente preferencial .	Sim. Atua como um remetente de espera.

Nó de administração do remetente preferencial

Se sua implantação do StorageGRID incluir vários nós de administração, o nó de administração principal será o remetente preferencial para notificações de alerta, pacotes de AutoSupport e traps e informações SNMP.

Em operações normais do sistema, somente o remetente preferido envia notificações. Entretanto, todos os outros nós administrativos monitoram o remetente preferido. Se um problema for detectado, outros nós administrativos atuam como *remetentes em espera*.

Várias notificações podem ser enviadas nestes casos:

- Se os nós administrativos ficarem "ilhados" uns dos outros, tanto o remetente preferencial quanto os remetentes em espera tentarão enviar notificações, e várias cópias das notificações poderão ser recebidas.

- Se o remetente em espera detectar problemas com o remetente preferencial e começar a enviar notificações, o remetente preferencial poderá recuperar sua capacidade de enviar notificações. Se isso ocorrer, notificações duplicadas poderão ser enviadas. O remetente em espera deixará de enviar notificações quando não detectar mais erros no remetente preferido.



Quando você testa pacotes do AutoSupport , todos os nós administrativos enviam o teste. Ao testar notificações de alerta, você deve fazer login em cada nó de administração para verificar a conectividade.

Serviços primários para nós de administração

A tabela a seguir mostra os principais serviços para nós de administração; no entanto, esta tabela não lista todos os serviços dos nós.

Serviço	Função principal
Sistema de Gestão de Auditoria (AMS)	Rastreia atividades e eventos do sistema.
Nó de Gerenciamento de Configuração (CMN)	Gerencia a configuração de todo o sistema.
[[alta disponibilidade]]Alta disponibilidade	Gerencia endereços IP virtuais de alta disponibilidade para grupos de nós de administração e nós de gateway. Observação: Este serviço também é encontrado em nós de gateway.
Balanceador de carga	Fornecer balanceamento de carga do tráfego S3 de clientes para nós de armazenamento. Observação: Este serviço também é encontrado em nós de gateway.
Interface de Programa de Aplicativo de Gerenciamento (mgmt-api)	Processa solicitações da API de gerenciamento de grade e da API de gerenciamento de locatários.
Sistema de gerenciamento de rede (NMS)	Fornecer funcionalidade para o Grid Manager.
Prometeu	Coleta e armazena métricas de séries temporais dos serviços em todos os nós.
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

O que é um nó de armazenamento?

Os nós de armazenamento gerenciam e armazenam dados de objetos e metadados. Os nós de armazenamento incluem os serviços e processos necessários para armazenar,

mover, verificar e recuperar dados de objetos e metadados no disco.

Cada site no seu sistema StorageGRID deve ter pelo menos três nós de armazenamento.

Tipos de nós de armazenamento

Durante a instalação, você pode selecionar o tipo de nó de armazenamento que deseja instalar. Esses tipos estão disponíveis para nós de armazenamento baseados em software e para nós de armazenamento baseados em dispositivos que oferecem suporte ao recurso:

- Nó de armazenamento de dados e metadados combinados
- Nó de armazenamento somente de metadados
- Nó de armazenamento somente de dados

Você pode selecionar o tipo de nó de armazenamento nestas situações:

- Ao instalar inicialmente um nó de armazenamento
- Quando você adiciona um nó de armazenamento durante a expansão do sistema StorageGRID



Não é possível alterar o tipo após a conclusão da instalação do Nó de Armazenamento.

Nó de armazenamento de dados e metadados (combinado)

Por padrão, todos os novos nós de armazenamento armazenarão dados de objetos e metadados. Este tipo de nó de armazenamento é chamado de nó de armazenamento *combinado*.

Nó de armazenamento somente de metadados

Usar um nó de armazenamento exclusivamente para metadados pode fazer sentido se sua grade armazenar um número muito grande de objetos pequenos. A instalação de capacidade de metadados dedicada proporciona um melhor equilíbrio entre o espaço necessário para um número muito grande de objetos pequenos e o espaço necessário para os metadados desses objetos. Além disso, nós de armazenamento somente de metadados hospedados em dispositivos de alto desempenho podem aumentar o desempenho.

Os nós de armazenamento somente de metadados têm requisitos de hardware específicos:

- Ao usar dispositivos StorageGRID , nós somente de metadados podem ser configurados somente em dispositivos SGF6112 com doze unidades de 1,9 TB ou doze de 3,8 TB.
- Ao usar nós baseados em software, os recursos de nós somente de metadados devem corresponder aos recursos de nós de armazenamento existentes. Por exemplo:
 - Se o site StorageGRID existente estiver usando dispositivos SG6000 ou SG6100, os nós somente de metadados baseados em software deverão atender aos seguintes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - 8 TB SSD ou armazenamento equivalente para o banco de dados Cassandra (rangedb/0)
 - Se o site StorageGRID existente estiver usando nós de armazenamento virtuais com 24 GB de RAM, CPU de 8 núcleos e 3 TB ou 4 TB de armazenamento de metadados, os nós somente de metadados baseados em software deverão usar recursos semelhantes (24 GB de RAM, CPU de 8 núcleos e 4 TB de armazenamento de metadados (rangedb/0)).
- Ao adicionar um novo site StorageGRID , a capacidade total de metadados do novo site deve, no mínimo,

corresponder aos sites StorageGRID existentes e os novos recursos do site devem corresponder aos nós de armazenamento nos sites StorageGRID existentes.

Ao instalar nós somente de metadados, a grade também deve conter um número mínimo de nós para armazenamento de dados:

- Para uma grade de site único, configure pelo menos dois nós de armazenamento combinados ou somente de dados.
- Para uma grade de vários sites, configure pelo menos um nó de armazenamento combinado ou somente de dados *por site*.



Embora os nós de armazenamento somente de metadados conttenham o [Serviço LDR](#) e pode processar solicitações de clientes S3, o desempenho do StorageGRID pode não aumentar.

Nó de armazenamento somente de dados

Usar um nó de armazenamento exclusivamente para dados pode fazer sentido se seus nós de armazenamento tiverem características de desempenho diferentes. Por exemplo, para aumentar potencialmente o desempenho, você pode ter nós de armazenamento de disco giratório de alta capacidade e somente dados, acompanhados por nós de armazenamento de alto desempenho somente metadados.

Ao instalar nós somente de dados, a grade deve conter o seguinte:

- Um mínimo de dois nós de armazenamento combinados ou somente de dados *por grade*
- Pelo menos um nó de armazenamento combinado ou somente de dados *por site*
- Um mínimo de três nós de armazenamento combinados ou somente de metadados *por site*

Serviços primários para nós de armazenamento

A tabela a seguir mostra os principais serviços para nós de armazenamento; no entanto, esta tabela não lista todos os serviços de nós.



Alguns serviços, como o serviço ADC e o serviço RSM, normalmente existem apenas em três nós de armazenamento em cada site.

Serviço	Função principal
Conta (acct)	Gerencia contas de inquilinos.

Serviço	Função principal
Controlador de Domínio Administrativo (ADC)	Mantém a topologia e a configuração de toda a grade. Observação: Nós de armazenamento somente de dados não hospedam o serviço ADC. Detalhes O serviço Controlador de Domínio Administrativo (ADC) autentica nós de grade e suas conexões entre si. O serviço ADC é hospedado em no mínimo três nós de armazenamento em um site. O serviço ADC mantém informações de topologia, incluindo a localização e a disponibilidade dos serviços. Quando um nó de grade requer informações de outro nó de grade ou uma ação a ser executada por outro nó de grade, ele entra em contato com um serviço ADC para encontrar o melhor nó de grade para processar sua solicitação. Além disso, o serviço ADC retém uma cópia dos pacotes de configuração da implantação do StorageGRID , permitindo que qualquer nó de grade recupere informações de configuração atuais. Para facilitar operações distribuídas e isoladas, cada serviço ADC sincroniza certificados, pacotes de configuração e informações sobre serviços e topologia com os outros serviços ADC no sistema StorageGRID . Em geral, todos os nós da grade mantêm uma conexão com pelo menos um serviço ADC. Isso garante que os nós da grade estejam sempre acessando as informações mais recentes. Quando os nós da grade se conectam, eles armazenam em cache os certificados de outros nós da grade, permitindo que os sistemas continuem funcionando com nós da grade conhecidos, mesmo quando um serviço ADC não estiver disponível. Novos nós de grade só podem estabelecer conexões usando um serviço ADC. A conexão de cada nó da grade permite que o serviço ADC reúna informações de topologia. Essas informações do nó da grade incluem a carga da CPU, o espaço em disco disponível (se houver armazenamento), os serviços suportados e o ID do site do nó da grade. Outros serviços solicitam ao serviço ADC informações de topologia por meio de consultas de topologia. O serviço ADC responde a cada consulta com as informações mais recentes recebidas do sistema StorageGRID .
Cassandra	Armazena e protege metadados de objetos. Observação: Os nós de armazenamento somente de dados não hospedam o serviço Cassandra.
Cassandra Reaper	Executa reparos automáticos de metadados de objetos. Observação: Os nós de armazenamento somente de dados não hospedam o serviço Cassandra Reaper.

Serviço	Função principal
Pedaço	Gerencia dados codificados por eliminação e fragmentos de paridade.
Movedor de dados (dmv)	Move dados para pools de armazenamento em nuvem.
Armazenamento de dados distribuídos (DDS)	Monitora o armazenamento de metadados de objetos. Detalhes Cada nó de armazenamento inclui o serviço Distributed Data Store (DDS). Este serviço faz interface com o banco de dados Cassandra para executar tarefas em segundo plano nos metadados do objeto armazenados no sistema StorageGRID . O serviço DDS rastreia o número total de objetos ingeridos no sistema StorageGRID , bem como o número total de objetos ingeridos por meio de cada uma das interfaces suportadas do sistema (S3).
Identidade (idnt)	Federa identidades de usuários do LDAP e do Active Directory.

Serviço	Função principal
Roteador de Distribuição Local (LDR)	Processa solicitações de protocolo de armazenamento de objetos e gerencia dados de objetos no disco.

Serviço	Função principal
Máquina de Estado Replicada (RSM)	Garante que as solicitações de serviços da plataforma S3 sejam enviadas aos seus respectivos endpoints.
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

O serviço LDR faz a maior parte do trabalho pesado do sistema StorageGRID, manipulando cargas de transferência de dados e funções de tráfego de dados.

O que é um nó de gateway?

Os nós de gateway fornecem uma interface de balanceamento de carga dedicada que os aplicativos cliente S3 podem usar para se conectar ao StorageGRID. O balanceamento de carga maximiza a velocidade e a capacidade de conexão distribuindo a carga de trabalho entre vários nós de armazenamento. Os nós de gateway são opcionais.

O serviço StorageGRID Load Balancer é fornecido em todos os nós de administração e todos os nós de gateway. Ele executa o encerramento de sessões de clientes, o protocolo TLS (Transport Layer Security), inspeciona as solicitações e estabelece novas conexões seguras com os nós de armazenamento. O serviço Load Balancer direciona os clientes perfeitamente para um nó de armazenamento ideal, de modo que a falha de nós ou até mesmo de um site inteiro seja transparente.

Configure um ou mais pontos de extremidade do balanceador de carga para definir a porta e o protocolo de rede (HTTPS ou HTTP) que as solicitações de entrada e saída do cliente usarão para acessar os serviços do balanceador de carga nos nós de gateway e de administração. O ponto de extremidade do balanceador de carga também define o tipo de cliente (S3), o modo de vinculação e, opcionalmente, uma lista de locatários permitidos ou bloqueados. Ver ["Considerações para balanceamento de carga"](#).

Conforme necessário, você pode agrupar as interfaces de rede de vários nós de gateway e nós de administração 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 do aplicativo cliente. Ver ["Gerenciar grupos de alta disponibilidade \(HA\)"](#).

Serviços primários para nós de gateway

Os objetos armazenados em um nó de armazenamento são identificados por um número hexadecimal de 0000 a 002F, conhecido como ID do volume. O espaço é reservado no primeiro armazenamento de objetos (volume 0) para metadados de objetos em um banco de dados

A tabela a seguir mostra os principais serviços para nós de gateway; no entanto, esta tabela não lista todos os serviços de nós.

Serviço	Função principal
Alta disponibilidade	Gerencia endereços IP virtuais de alta disponibilidade para grupos de nós de administração e nós de gateway. Observação: Este serviço também é encontrado em nós de administração.
Balanceador de carga	Fornecer balanceamento de carga da Camada 7 do tráfego S3 dos clientes para os Nós de Armazenamento. Este é o mecanismo de balanceamento de carga recomendado. Observação: Este serviço também é encontrado em nós de administração.

Para garantir redundância e, portanto, proteção contra perdas, três cópias de metadados de objetos são mantidas em cada site. Esta replicação não é configurável e é executada automaticamente. Para

Serviço	Função principal
Monitor de status do servidor (SSM)	Monitora o sistema operacional e o hardware subjacente.

O que é um nó de arquivo?

O suporte para nós de arquivo foi removido.

Para obter informações sobre nós de arquivo, consulte "[O que é um nó de arquivo \(site de documentação do StorageGRID 11.8\)](#)".

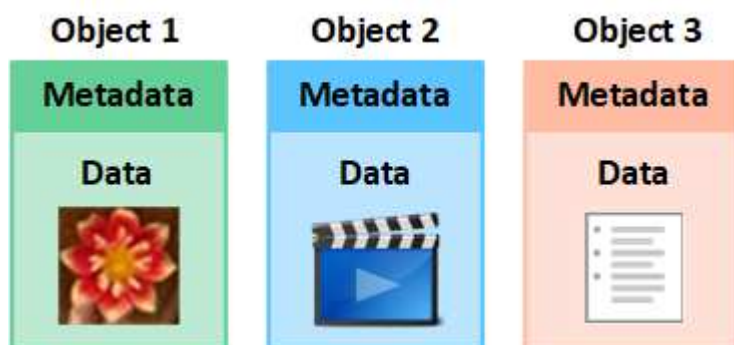
Como o StorageGRID gerencia dados

O que é um objeto

Com o armazenamento de objetos, a unidade de armazenamento é um objeto, em vez de um arquivo ou um bloco. Diferentemente da hierarquia em forma de árvore de um sistema de arquivos ou armazenamento em bloco, o armazenamento de objetos organiza os dados em um layout simples e não estruturado.

O armazenamento de objetos separa a localização física dos dados do método usado para armazenar e recuperar esses dados.

Cada objeto em um sistema de armazenamento baseado em objetos tem duas partes: dados do objeto e metadados do objeto.



O que são dados de objeto?

Dados de objetos podem ser qualquer coisa; por exemplo, uma fotografia, um filme ou um registro médico.

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.

Os metadados do objeto incluem informações como as seguintes:

- Metadados do sistema, incluindo um ID exclusivo para cada objeto (UUID), o nome do objeto, o nome do bucket S3 ou contêiner Swift, 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.

- O local de armazenamento atual de cada cópia de objeto ou fragmento codificado para eliminação.
- Quaisquer metadados do usuário associados ao objeto.

Os metadados do objeto são personalizáveis e expansíveis, tornando-os flexíveis para uso por aplicativos.

Para obter informações detalhadas sobre como e onde o StorageGRID armazena metadados de objetos, acesse "[Gerenciar armazenamento de metadados de objetos](#)".

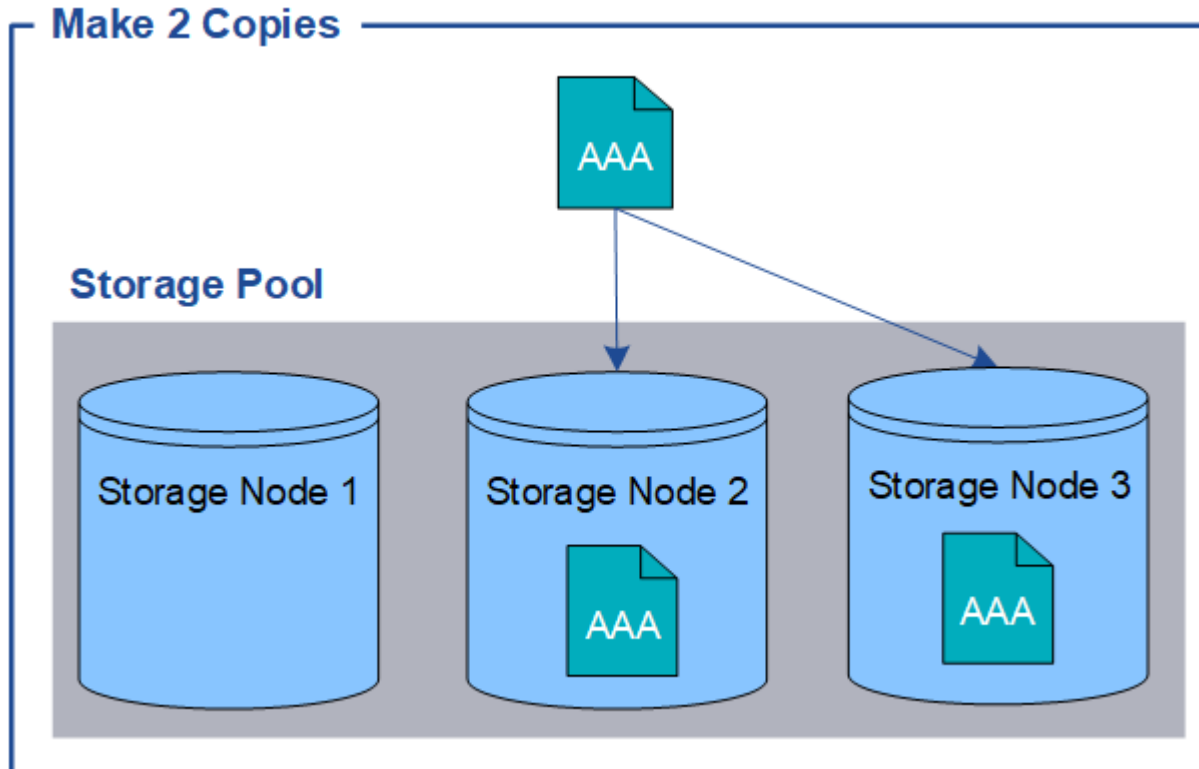
Como os dados do objeto são protegidos?

O sistema StorageGRID fornece dois mecanismos para proteger dados de objetos contra perda: replicação e codificação de eliminação.

Replicação

Quando o StorageGRID corresponde objetos a uma regra de gerenciamento do ciclo de vida das informações (ILM) configurada para criar cópias replicadas, o sistema cria cópias exatas dos dados do objeto e as armazena em nós de armazenamento ou pools de armazenamento em nuvem. As regras do ILM determinam o número de cópias feitas, onde essas cópias são armazenadas e por quanto tempo elas são retidas pelo sistema. Se uma cópia for perdida, por exemplo, como resultado da perda de um nó de armazenamento, o objeto ainda estará disponível se houver uma cópia dele em outro lugar no sistema StorageGRID.

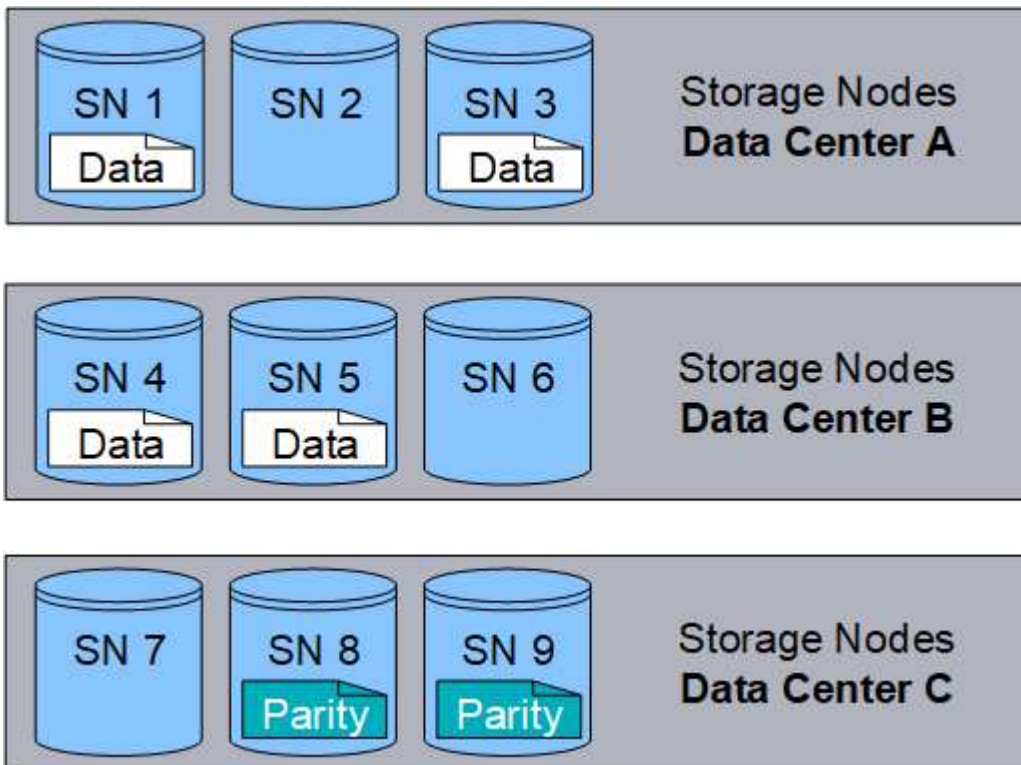
No exemplo a seguir, a regra Fazer 2 cópias especifica que duas cópias replicadas de cada objeto sejam colocadas em um pool de armazenamento que contém três nós de armazenamento.



Codificação de apagamento

Quando o StorageGRID corresponde objetos a uma regra ILM configurada para criar cópias codificadas para eliminação, ele divide os dados do objeto em fragmentos de dados, calcula fragmentos de paridade adicionais e armazena cada fragmento 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. As regras do ILM e os perfis de codificação de eliminação determinam o esquema de codificação de eliminação usado.

O exemplo a seguir ilustra o uso da 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 de armazenamento diferente em três data centers para fornecer proteção de dados em caso de falhas de nó ou perda de site.



Informações relacionadas

- ["Gerenciar objetos com ILM"](#)
- ["Use o gerenciamento do ciclo de vida da informação"](#)

A vida de um objeto

A vida de um objeto consiste em vários estágios. Cada estágio representa as operações que ocorrem com o objeto.

A vida de um objeto inclui as operações de ingestão, gerenciamento de cópias, recuperação e exclusão.

- **Ingestão:** O processo de um aplicativo cliente S3 salvando um objeto via HTTP no sistema StorageGRID. Nesta fase, o sistema StorageGRID começa a gerenciar o objeto.
- **Gerenciamento de cópias:** O processo de gerenciamento de cópias replicadas e codificadas para

eliminação no StorageGRID, conforme descrito pelas regras do ILM nas políticas ativas do ILM. Durante o estágio de gerenciamento de cópias, o StorageGRID protege os dados do objeto contra perdas criando e mantendo o número e o tipo especificados de cópias do objeto em nós de armazenamento ou em um pool de armazenamento em nuvem.

- **Recuperar:** O processo de um aplicativo cliente acessando um objeto armazenado pelo sistema StorageGRID . O cliente lê o objeto, que é recuperado de um nó de armazenamento ou pool de armazenamento em nuvem.
- **Excluir:** O processo de remoção de todas as cópias de objetos da grade. Os objetos podem ser excluídos como resultado do envio de uma solicitação de exclusão ao sistema StorageGRID pelo aplicativo cliente ou como resultado de um processo automático que o StorageGRID executa quando a vida útil do objeto expira.



Informações relacionadas

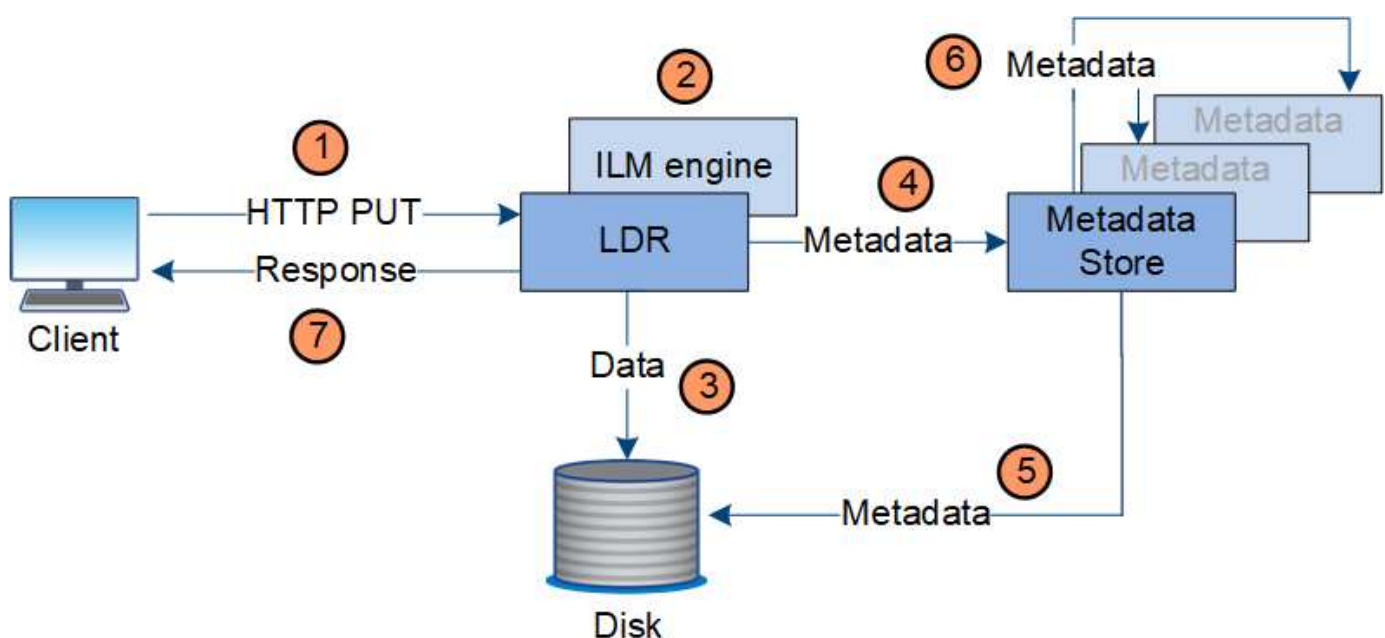
- ["Gerenciar objetos com ILM"](#)
- ["Use o gerenciamento do ciclo de vida da informação"](#)

Fluxo de ingestão de dados

Uma operação de ingestão ou salvamento consiste em um fluxo de dados definido entre o cliente e o sistema StorageGRID .

Fluxo de dados

Quando um cliente ingere um objeto no sistema StorageGRID , o serviço LDR nos nós de armazenamento processa a solicitação e armazena os metadados e dados no disco.



1. O aplicativo cliente cria o objeto e o envia ao sistema StorageGRID por meio de uma solicitação HTTP PUT.
2. O objeto é avaliado em relação à política de ILM do sistema.
3. O serviço LDR salva os dados do objeto como uma cópia replicada ou como uma cópia codificada para eliminação. (O diagrama mostra uma versão simplificada do armazenamento de uma cópia replicada em disco.)
4. O serviço LDR envia os metadados do objeto para o armazenamento de metadados.
5. O armazenamento de metadados salva os metadados do objeto no disco.
6. O armazenamento de metadados propaga cópias de metadados de objetos para outros nós de armazenamento. Essas cópias também são salvas no disco.
7. O serviço LDR retorna uma resposta HTTP 200 OK ao cliente para confirmar que o objeto foi ingerido.

Gerenciamento de cópias

Os dados do objeto são gerenciados pelas políticas ativas do ILM e pelas regras associadas do ILM. As regras do ILM fazem cópias replicadas ou codificadas para eliminação para proteger dados de objetos contra perdas.

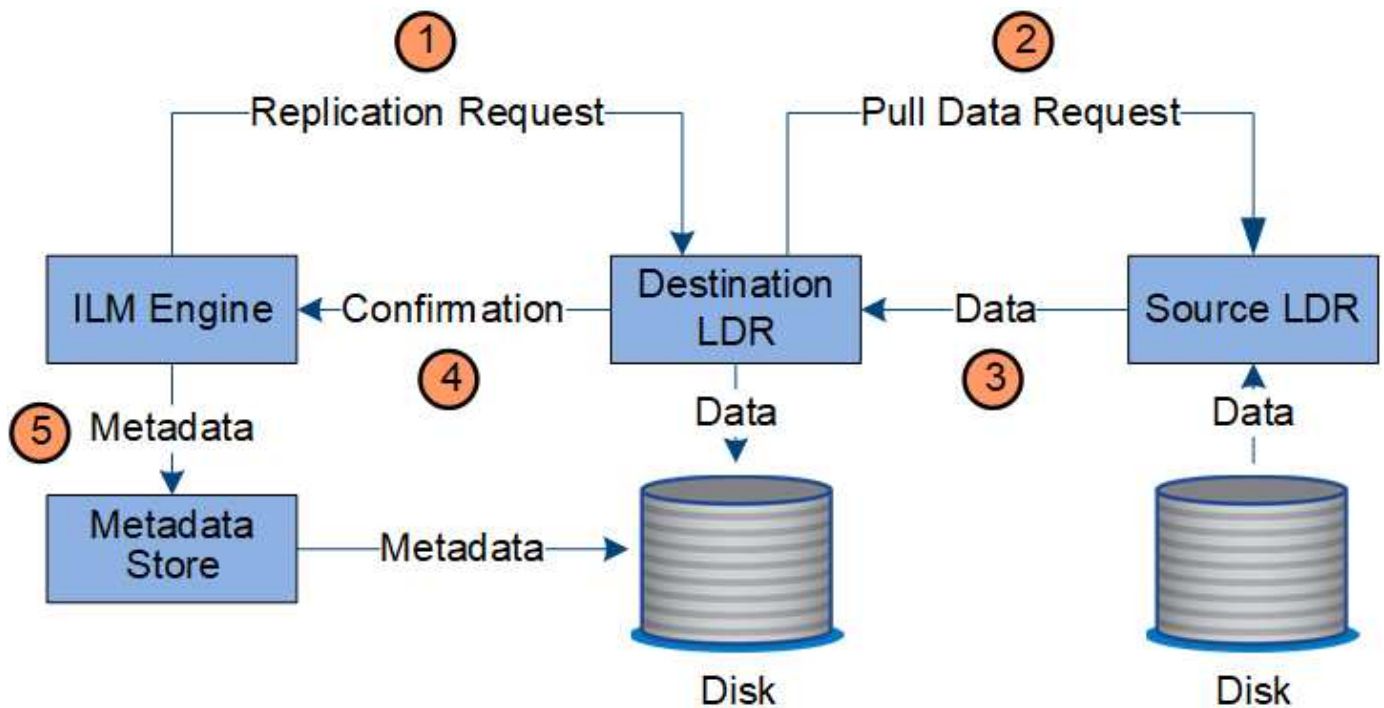
Diferentes tipos ou locais de cópias de objetos podem ser necessários em diferentes momentos da vida do objeto. As regras do ILM são avaliadas periodicamente para garantir que os objetos sejam colocados conforme necessário.

Os dados do objeto são gerenciados pelo serviço LDR.

Proteção de conteúdo: replicação

Se as instruções de posicionamento de conteúdo de uma regra de ILM exigirem cópias replicadas de dados de objeto, cópias serão feitas e armazenadas em disco pelos nós de armazenamento que compõem o pool de armazenamento configurado.

O mecanismo ILM no serviço LDR controla a replicação e garante que o número correto de cópias seja armazenado nos locais corretos e pelo período de tempo correto.

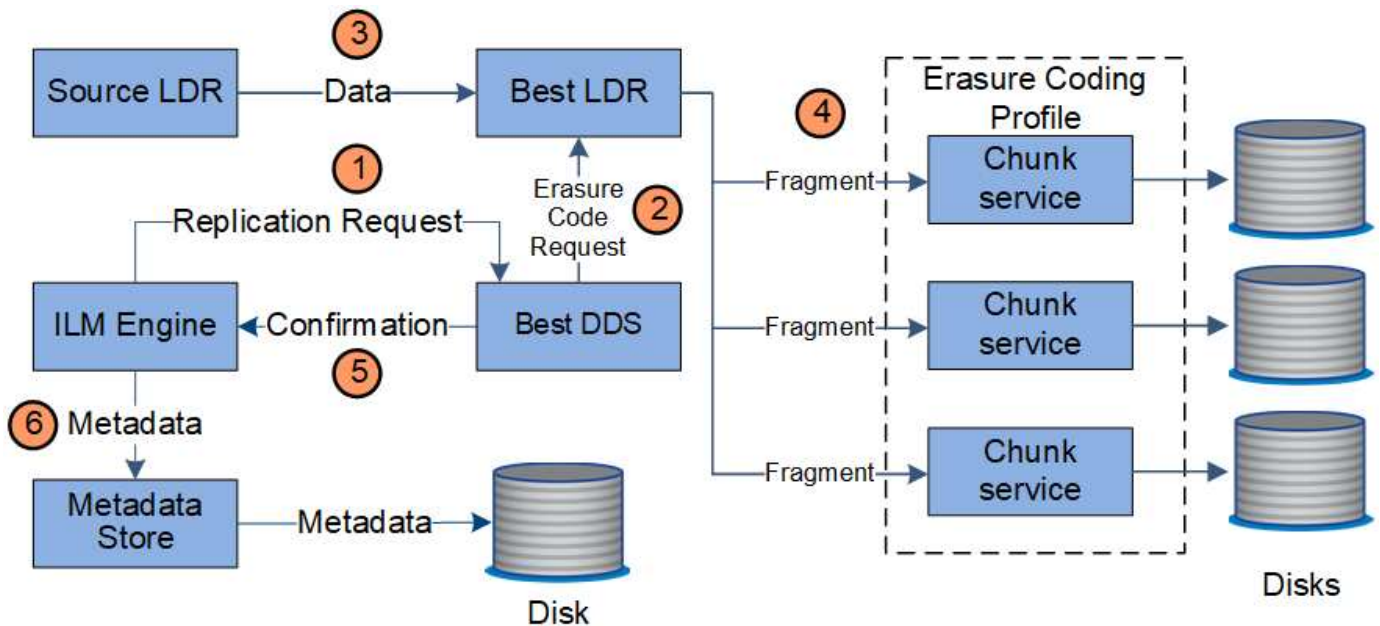


1. O mecanismo ILM consulta o serviço ADC para determinar o melhor serviço LDR de destino dentro do pool de armazenamento especificado pela regra ILM. Em seguida, ele envia ao serviço LDR um comando para iniciar a replicação.
2. O serviço LDR de destino consulta o serviço ADC para obter o melhor local de origem. Em seguida, ele envia uma solicitação de replicação ao serviço LDR de origem.
3. O serviço LDR de origem envia uma cópia para o serviço LDR de destino.
4. O serviço LDR de destino notifica o mecanismo ILM de que os dados do objeto foram armazenados.
5. O mecanismo ILM atualiza o armazenamento de metadados com metadados de localização de objetos.

Proteção de conteúdo: codificação de eliminação

Se uma regra de ILM incluir instruções para fazer cópias codificadas para eliminação de dados de objeto, o esquema de codificação de eliminação aplicável divide os dados de objeto em fragmentos de dados e paridade e distribui esses fragmentos entre os nós de armazenamento configurados no perfil de codificação de eliminação.

O mecanismo ILM, que é um componente do serviço LDR, controla a codificação de eliminação e garante que o perfil de codificação de eliminação seja aplicado aos dados do objeto.

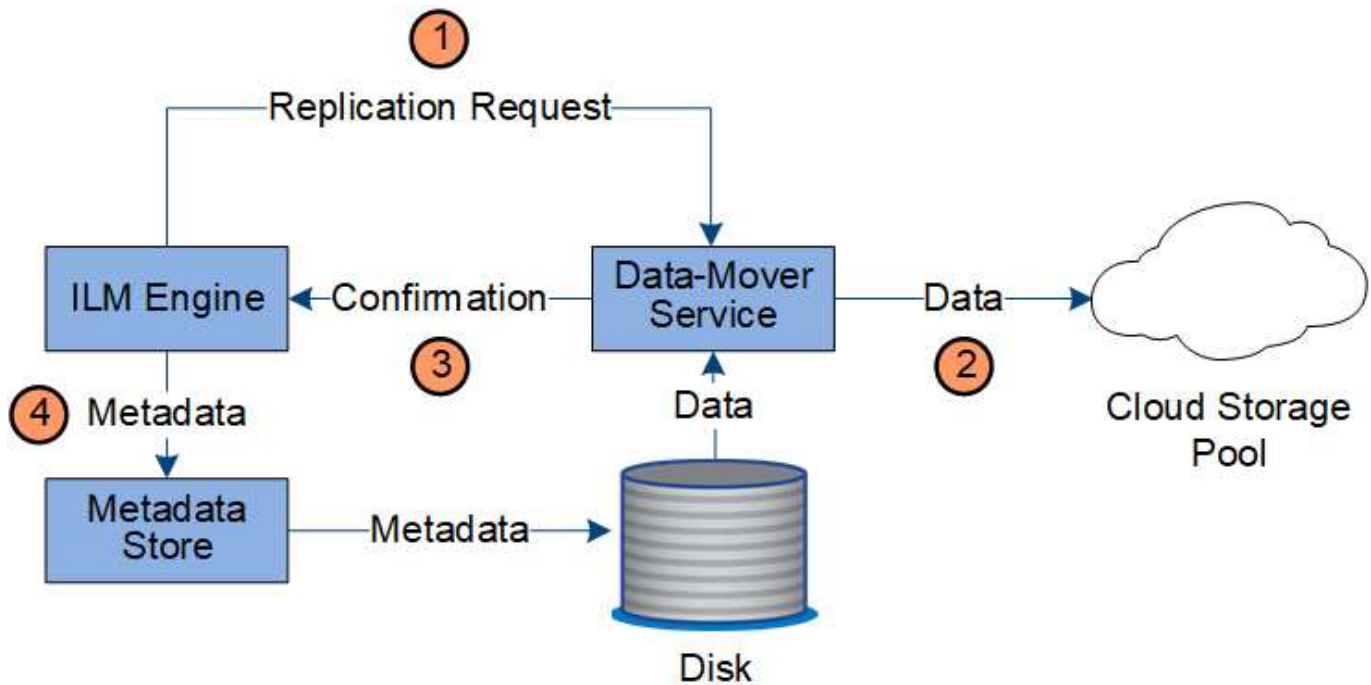


1. O mecanismo ILM consulta o serviço ADC para determinar qual serviço DDS pode executar melhor a operação de codificação de eliminação. Quando determinado, o mecanismo ILM envia uma solicitação de "início" para esse serviço.
2. O serviço DDS instrui um LDR a apagar o código dos dados do objeto.
3. O serviço LDR de origem envia uma cópia para o serviço LDR selecionado para codificação de eliminação.
4. Depois de criar o número apropriado de fragmentos de paridade e dados, o serviço LDR distribui esses fragmentos entre os nós de armazenamento (serviços de bloco) que compõem o pool de armazenamento do perfil de codificação de eliminação.
5. O serviço LDR notifica o mecanismo ILM, confirmando que os dados do objeto foram distribuídos com sucesso.
6. O mecanismo ILM atualiza o armazenamento de metadados com metadados de localização de objetos.

Proteção de conteúdo: Cloud Storage Pool

Se as instruções de posicionamento de conteúdo de uma regra de ILM exigirem que uma cópia replicada dos dados do objeto seja armazenada em um Pool de Armazenamento em Nuvem, os dados do objeto serão duplicados no bucket S3 externo ou no contêiner de armazenamento de Blobs do Azure que foi especificado para o Pool de Armazenamento em Nuvem.

O mecanismo ILM, que é um componente do serviço LDR, e o serviço Data Mover controlam a movimentação de objetos para o Cloud Storage Pool.



1. O mecanismo ILM seleciona um serviço Data Mover para replicar no Cloud Storage Pool.
2. O serviço Data Mover envia os dados do objeto para o Cloud Storage Pool.
3. O serviço Data Mover notifica o mecanismo ILM de que os dados do objeto foram armazenados.
4. O mecanismo ILM atualiza o armazenamento de metadados com metadados de localização de objetos.

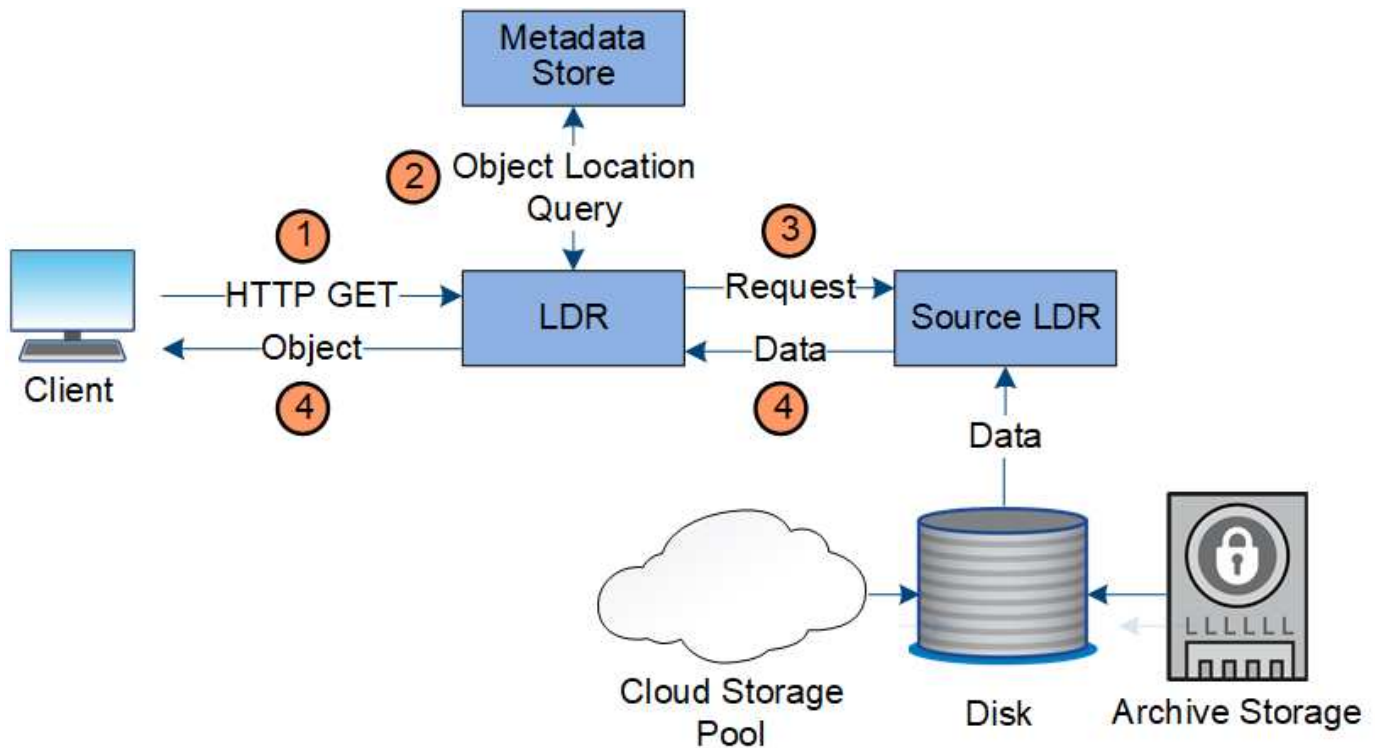
Recuperar fluxo de dados

Uma operação de recuperação consiste em um fluxo de dados definido entre o sistema StorageGRID e o cliente. O sistema usa atributos para rastrear a recuperação do objeto de um nó de armazenamento ou, se necessário, de um pool de armazenamento em nuvem.

O serviço LDR do nó de armazenamento consulta o repositório de metadados para saber a localização dos dados do objeto e os recupera do serviço LDR de origem. De preferência, a recuperação é feita a partir de um nó de armazenamento. Se o objeto não estiver disponível em um nó de armazenamento, a solicitação de recuperação será direcionada a um pool de armazenamento em nuvem.



Se a única cópia do objeto estiver no armazenamento AWS Glacier ou na camada do Azure Archive, o aplicativo cliente deverá emitir uma solicitação S3 RestoreObject para restaurar uma cópia recuperável para o Cloud Storage Pool.



1. O serviço LDR recebe uma solicitação de recuperação do aplicativo cliente.
2. O serviço LDR consulta o repositório de metadados para obter a localização dos dados do objeto e os metadados.
3. O serviço LDR encaminha a solicitação de recuperação para o serviço LDR de origem.
4. O serviço LDR de origem retorna os dados do objeto do serviço LDR consultado e o sistema retorna o objeto ao aplicativo cliente.

Excluir fluxo de dados

Todas as cópias de objetos são removidas do sistema StorageGRID quando um cliente executa uma operação de exclusão ou quando a vida útil do objeto expira, acionando sua remoção automática. Há um fluxo de dados definido para exclusão de objetos.

Hierarquia de exclusão

O StorageGRID fornece vários métodos para controlar quando os objetos são retidos ou excluídos. Os objetos podem ser excluídos por solicitação do cliente ou automaticamente. O StorageGRID sempre prioriza quaisquer configurações de bloqueio de objeto do S3 em relação às solicitações de exclusão do cliente, que são priorizadas em relação ao ciclo de vida do bucket do S3 e às instruções de posicionamento do ILM.

- **Bloqueio de Objeto S3:** Se a configuração global de Bloqueio de Objeto S3 estiver habilitada para a grade, os clientes S3 poderão criar buckets com o Bloqueio de Objeto S3 habilitado e, em seguida, usar a API REST 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.

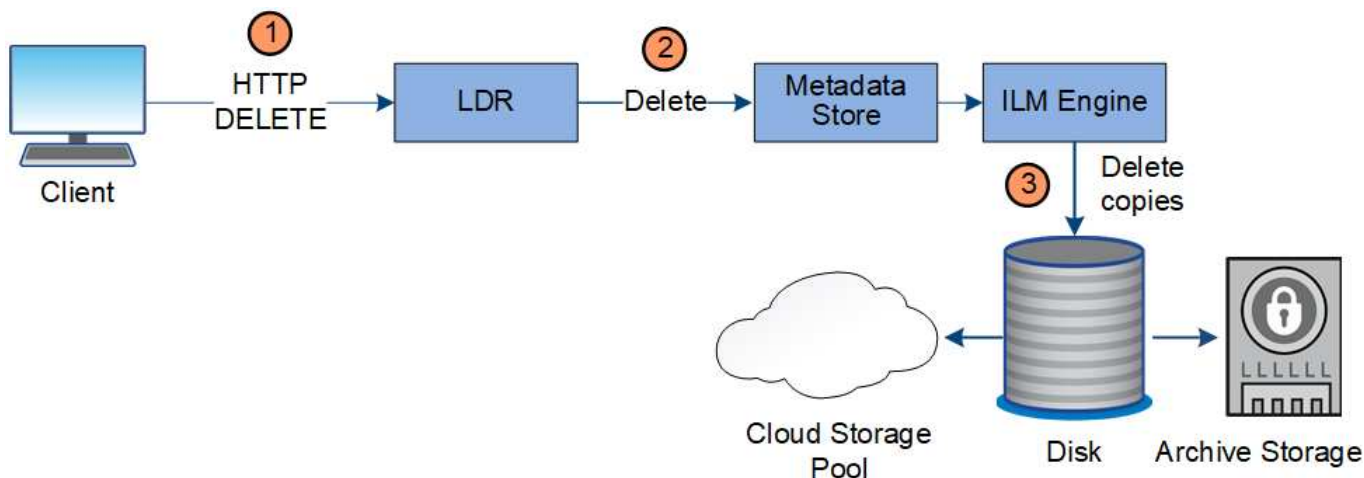
- Se os clientes S3 aplicarem uma retenção até a data padrão ao bucket, eles não precisarão especificar uma retenção até a data para cada objeto.
- **Solicitação de exclusão de cliente:** Um cliente S3 pode emitir uma solicitação de exclusão de objeto. Quando um cliente exclui um objeto, todas as cópias do objeto são removidas do sistema StorageGRID .
- **Excluir objetos no bucket:** os usuários do Tenant Manager podem usar esta opção para remover permanentemente todas as cópias dos objetos e versões de objetos em buckets selecionados do sistema StorageGRID .
- **Ciclo de vida do bucket S3:** os clientes 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 excluirá automaticamente todas as cópias de um objeto quando a data ou o número de dias especificado na ação Expiração forem atingidos, a menos que o cliente exclua o objeto primeiro.
- **Instruções de posicionamento do ILM:** Supondo que o bucket não tenha o S3 Object Lock habilitado e que não haja um ciclo de vida do bucket, o StorageGRID exclui automaticamente um objeto quando o último período na regra do ILM termina e não há mais posicionamentos especificados para o objeto.



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.

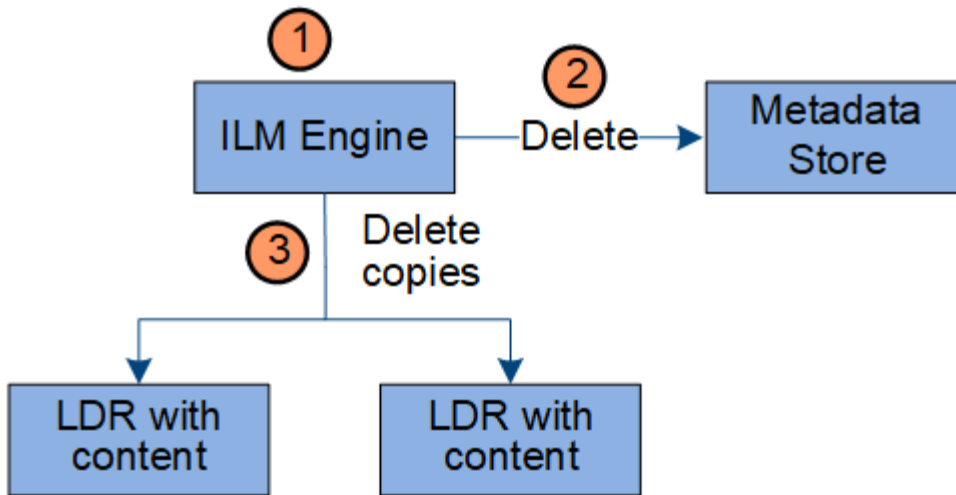
Ver "[Como os objetos são excluídos](#)" para maiores informações.

Fluxo de dados para exclusões de clientes



1. O serviço LDR recebe uma solicitação de exclusão do aplicativo cliente.
2. O serviço LDR atualiza o armazenamento de metadados para que o objeto pareça excluído para solicitações do cliente e instrui o mecanismo ILM a remover todas as cópias dos dados do objeto.
3. O objeto é removido do sistema. O armazenamento de metadados é atualizado para remover metadados de objetos.

Fluxo de dados para exclusões de ILM



1. O mecanismo ILM determina que o objeto precisa ser excluído.
2. O mecanismo ILM notifica o armazenamento de metadados. O armazenamento de metadados atualiza os metadados do objeto para que o objeto pareça excluído nas solicitações do cliente.
3. O mecanismo ILM remove todas as cópias do objeto. O armazenamento de metadados é atualizado para remover metadados de objetos.

Gestão do ciclo de vida da informação

Use o gerenciamento do ciclo de vida das informações (ILM) para controlar o posicionamento, a duração e o comportamento de ingestão de todos os objetos no seu sistema StorageGRID . As regras do ILM determinam como o StorageGRID armazena objetos ao longo do tempo. Configure uma ou mais regras de ILM e adicione-as a uma política de ILM. Uma grade pode ter mais de uma política ativa ao mesmo tempo.

As regras do ILM definem:

- Quais objetos devem ser armazenados. Uma regra pode ser aplicada a todos os objetos, ou você pode especificar filtros para identificar a quais objetos uma regra se aplica. Por exemplo, uma regra pode ser aplicada somente a objetos associados a determinadas contas de locatários, buckets S3 ou contêineres Swift específicos ou valores de metadados específicos.
- O tipo e a localização do armazenamento. Os objetos podem ser armazenados em nós de armazenamento ou em pools de armazenamento em nuvem.
- O tipo de cópias de objetos feitas. As cópias podem ser replicadas ou codificadas para eliminação.
- Para cópias replicadas, o número de cópias feitas.
- Para cópias codificadas por apagamento, o esquema de codificação por apagamento é usado.
- As mudanças ao longo do tempo no local de armazenamento de um objeto e no tipo de cópias.
- Como os dados do objeto são protegidos à medida que os objetos são ingeridos na grade (posicionamento síncrono ou confirmação dupla).

Observe que os metadados do objeto não são gerenciados pelas regras do ILM. Em vez disso, os metadados do objeto são armazenados em um banco de dados Cassandra no que é conhecido como repositório de metadados. Três cópias dos metadados do objeto são mantidas automaticamente em cada site para proteger os dados contra perdas.

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.

Como uma política de ILM avalia objetos

As políticas de ILM ativas para seu sistema StorageGRID controlam o posicionamento, a duração e o comportamento de ingestão de todos os objetos.

Quando os clientes salvam objetos no StorageGRID, os objetos são avaliados em relação ao conjunto ordenado de regras de ILM na política ativa, da seguinte maneira:

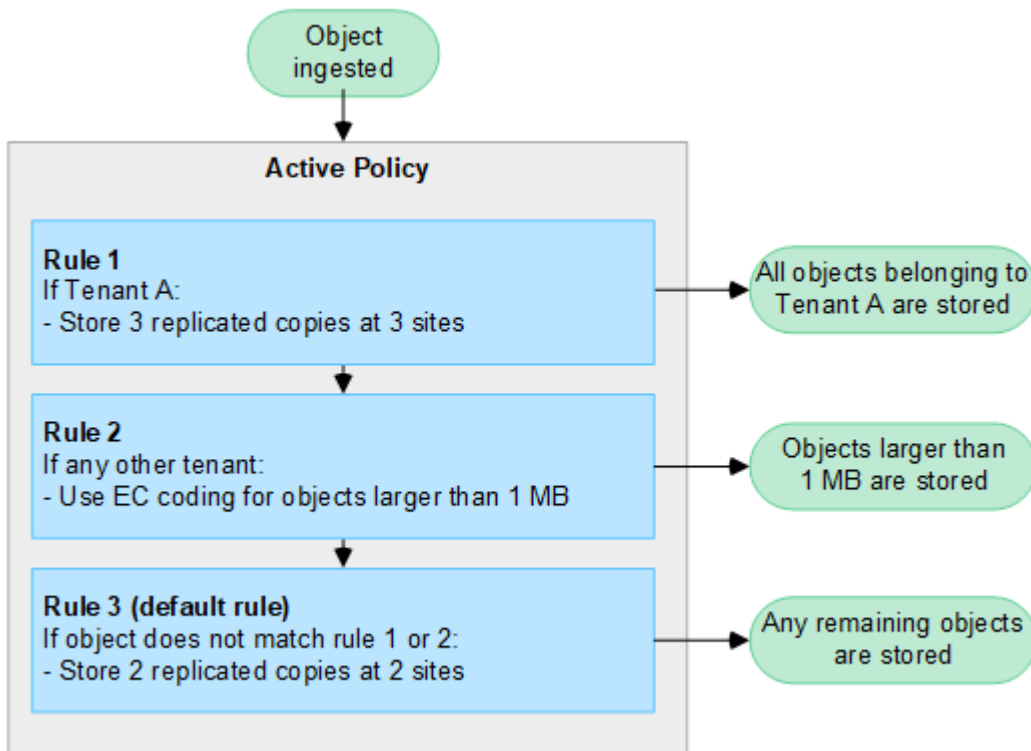
1. Se os filtros da primeira regra na política corresponderem a um objeto, o objeto será ingerido de acordo com o comportamento de ingestão dessa regra e armazenado de acordo com as instruções de posicionamento dessa regra.
2. Se os filtros da primeira regra não corresponderem ao objeto, o objeto será 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 e não pode usar nenhum filtro. Ele deve ser aplicado a todos os locatários, todos os buckets e todas as versões de objetos.

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).



Informações relacionadas

- ["Gerenciar objetos com ILM"](#)

Explorar StorageGRID

Explore o Grid Manager

O Grid Manager é a interface gráfica baseada em navegador que permite configurar, gerenciar e monitorar seu sistema StorageGRID .



O Grid Manager é atualizado a cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

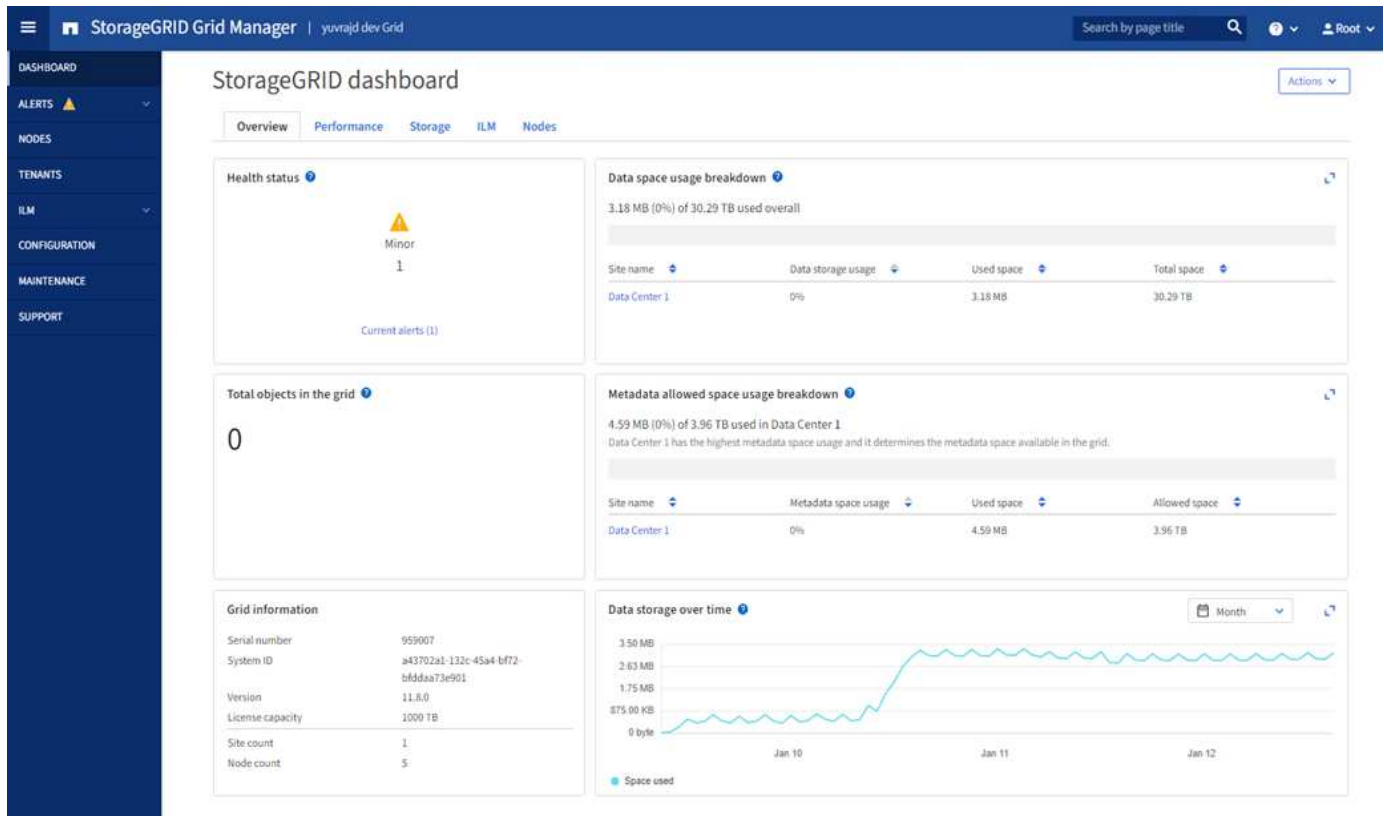
Ao fazer login no Grid Manager, você está se conectando a um nó de administração. Cada sistema StorageGRID inclui um nó administrativo primário e qualquer número de nós administrativos não primários. Você pode se conectar a qualquer nó administrativo, e cada nó administrativo exibe uma visão semelhante do sistema StorageGRID .

Você pode acessar o Grid Manager usando um ["navegador da web compatível"](#) .

Painel do Grid Manager

Ao fazer login pela primeira vez no Grid Manager, você pode usar o painel para ["monitorar atividades do sistema"](#) num relance.

O painel contém informações sobre a integridade e o desempenho do sistema, uso de armazenamento, processos do ILM, operações do S3 e os nós na grade. Você pode ["configurar o painel"](#) selecionando entre uma coleção de cartões que contêm as informações necessárias para monitorar seu sistema de forma eficaz.



Para obter uma explicação das informações mostradas em cada cartão, selecione o ícone de ajuda para esse cartão.

Campo de pesquisa

O campo **Pesquisar** na barra de cabeçalho permite que você navegue rapidamente para uma página específica no Grid Manager. Por exemplo, você pode digitar **km** para acessar a página do servidor de gerenciamento de chaves (KMS).

Você pode usar **Pesquisar** para encontrar entradas na barra lateral do Grid Manager e nos menus Configuração, Manutenção e Suporte. Você também pode pesquisar por nome itens como nós de grade e contas de locatários.

Menu de ajuda

O menu de ajuda fornece acesso a:

- O ["FabricPool"](#) e ["Configuração do S3"](#) mago
- O centro de documentação do StorageGRID para a versão atual
- ["Documentação do API"](#)
- Informações sobre qual versão do StorageGRID está instalada atualmente

Menu de alertas

O menu Alertas fornece uma interface fácil de usar para detectar, avaliar e resolver problemas que podem

ocorrer durante a operação do StorageGRID .

No menu Alertas, você pode fazer o seguinte para ["gerenciar alertas"](#) :

- Revisar alertas atuais
- Revisar alertas resolvidos
- Configurar silêncios para suprimir notificações de alerta
- Definir regras de alerta para condições que acionam alertas
- Configurar o servidor de e-mail para notificações de alerta

Página de nós

O ["Página de nós"](#) exibe informações sobre toda a grade, cada site na grade e cada nó em um site.

A página inicial dos Nós exibe métricas combinadas para toda a grade. Para visualizar informações de um site ou nó específico, selecione o site ou nó.

Nodes

View the list and status of sites and grid nodes.

Total node count: 14

Name ?	Type	Object data used ?	Object metadata used ?	CPU usage ?
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

Página de inquilinos

O ["Página de inquilinos"](#) permite que você ["criar e monitorar as contas de locatários de armazenamento"](#) para seu sistema StorageGRID . Você deve criar pelo menos uma conta de locatário para especificar quem pode armazenar e recuperar objetos e qual funcionalidade está disponível para eles.

A página Locatários também fornece detalhes de uso para cada locatário, incluindo a quantidade de armazenamento usada e o número de objetos. Se você definir uma cota ao criar o locatário, poderá ver quanto dessa cota foi usado.

Tenants

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

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

Displaying 2 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	S3 Tenant	0 bytes	0%	100.00 GB	0	→ 📄
☐	Swift Tenant	0 bytes	0%	100.00 GB	0	→ 📄

← Previous 1 Next →

Menu ILM

O "Menu ILM" permite que você [configure as regras e políticas de gerenciamento do ciclo de vida da informação \(ILM\)](#) que regem a durabilidade e a disponibilidade dos dados. Você também pode inserir um identificador de objeto para visualizar os metadados desse objeto.

No menu ILM, você pode visualizar e gerenciar o ILM:

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

Menu de configuração

O menu Configuração permite que você especifique configurações de rede, configurações de segurança, configurações do sistema, opções de monitoramento e opções de controle de acesso.

Tarefas de rede

As tarefas de rede incluem:

- ["Gerenciando grupos de alta disponibilidade"](#)
- ["Gerenciando endpoints do balanceador de carga"](#)
- ["Configurando nomes de domínio de endpoint S3"](#)
- ["Gerenciando políticas de classificação de tráfego"](#)
- ["Configurando interfaces VLAN"](#)

Tarefas de segurança

As tarefas de segurança incluem:

- "Gerenciando certificados de segurança"
- "Gerenciando controles internos de firewall"
- "Configurando servidores de gerenciamento de chaves"
- Configurar as definições de segurança, incluindo "Política de TLS e SSH" , "opções de segurança de rede e objeto" , e "configurações de segurança da interface" .
- Configurando as configurações para um "proxy de armazenamento" ou um "proxy de administrador"

Tarefas do sistema

As tarefas do sistema incluem:

- Usando "federação de grade" para clonar informações de conta de locatário e replicar dados de objeto entre dois sistemas StorageGRID .
- Opcionalmente, habilitando o "Compactar objetos armazenados" opção.
- "Gerenciando bloqueio de objeto S3"
- Compreendendo opções de armazenamento, como "segmentação de objetos" e "marcas d'água de volume de armazenamento" .
- "Gerenciar perfis de codificação de eliminação" .

Tarefas de monitoramento

As tarefas de monitoramento incluem:

- "Configurando mensagens de auditoria e destinos de log"
- "Usando monitoramento SNMP"

Tarefas de controle de acesso

As tarefas de controle de acesso incluem:

- "Gerenciando grupos de administradores"
- "Gerenciando usuários administradores"
- Mudando o "senha de provisionamento" ou "senhas do console do nó"
- "Usando federação de identidade"
- "Configurando SSO"

Menu de manutenção

O menu Manutenção permite que você execute tarefas de manutenção, manutenção do sistema e manutenção da rede.

Tarefas

As tarefas de manutenção incluem:

- ["Operações de descomissionamento"](#) para remover nós e sites de grade não utilizados
- ["Operações de expansão"](#) para adicionar novos nós e sites de grade
- ["Procedimentos de recuperação de nós de grade"](#) para substituir um nó com falha e restaurar dados
- ["Procedimentos de renomeação"](#) para alterar os nomes de exibição da sua grade, sites e nós
- ["Operações de verificação de existência de objetos"](#) para verificar a existência (embora não a exatidão) dos dados do objeto
- Executando um ["reinicialização contínua"](#) para reiniciar vários nós de grade
- ["Operações de restauração de volume"](#)

Sistema

As tarefas de manutenção do sistema que você pode executar incluem:

- ["Visualizando informações da licença do StorageGRID"](#) ou ["atualizando informações de licença"](#)
- Gerando e baixando o ["Pacote de Recuperação"](#)
- Executar atualizações de software do StorageGRID , incluindo upgrades de software, hotfixes e atualizações do software SANtricity OS em dispositivos selecionados
 - ["Procedimento de atualização"](#)
 - ["Procedimento de correção"](#)
 - ["Atualizar o SANtricity OS nos controladores de armazenamento SG6000 usando o Grid Manager"](#)
 - ["Atualizar o SANtricity OS nos controladores de armazenamento SG5700 usando o Grid Manager"](#)

Rede

As tarefas de manutenção de rede que você pode executar incluem:

- ["Configurando servidores DNS"](#)
- ["Atualizando sub-redes da rede de grade"](#)
- ["Gerenciando servidores NTP"](#)

Menu de suporte

O menu Suporte fornece opções que ajudam o suporte técnico a analisar e solucionar problemas do seu sistema.

Ferramentas

Na seção Ferramentas do menu Suporte, você pode:

- ["Configurar AutoSupport"](#)
- ["Executar diagnósticos"](#) sobre o estado atual da rede
- ["Acesse a árvore de topologia da grade"](#) para visualizar informações detalhadas sobre nós de grade, serviços e atributos
- ["Coletar arquivos de log e dados do sistema"](#)
- ["Revisar métricas de suporte"](#)



As ferramentas disponíveis na opção **Métricas** destinam-se ao uso pelo suporte técnico. Alguns recursos e itens de menu nessas ferramentas são intencionalmente não funcionais.

Alarmes (legado)

As informações sobre alarmes legados foram removidas desta versão da documentação. Consulte "[Gerenciar alertas e alarmes \(documentação do StorageGRID 11.8\)](#)".

Outro

Na seção Outros do menu Suporte, você pode:

- Gerenciar "[custo do link](#)"
- Visualizar "[Sistema de Gerenciamento de Rede \(NMS\)](#)" entradas
- Gerenciar "[marcas d'água de armazenamento](#)"

Explore o Gerenciador de Inquilinos

O "[Gerente de inquilinos](#)" é a interface gráfica baseada em navegador que os usuários locatários acessam para configurar, gerenciar e monitorar suas contas de armazenamento.



O Tenant Manager é atualizado a cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

Quando usuários locatários efetuam login no Gerenciador de Locatários, eles estão se conectando a um Nó de Administração.

Painel do gerente de inquilinos

Depois que um administrador de grade cria uma conta de locatário usando o Grid Manager ou a Grid Management API, os usuários locatários podem fazer login no Tenant Manager.

O painel do Tenant Manager permite que os usuários do tenant monitorem o uso do armazenamento rapidamente. O painel Uso de armazenamento contém uma lista dos maiores buckets (S3) ou contêineres (Swift) para o locatário. O valor do espaço usado é a quantidade total de dados do objeto no bucket ou contêiner. O gráfico de barras representa os tamanhos relativos desses baldes ou contêineres.

O valor mostrado acima do gráfico de barras é a soma do espaço usado para todos os buckets ou contêineres do locatário. Se o número máximo de gigabytes, terabytes ou petabytes disponíveis para o locatário foi especificado quando a conta foi criada, a quantidade de cota usada e restante também será exibida.

Dashboard

16**Buckets**[View buckets](#)**2****Platform services****endpoints**[View endpoints](#)**0****Groups**[View groups](#)**1****User**[View users](#)

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage [?](#)

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details [?](#)

Name:	Tenant02
ID:	3341 1240 0546 8283 2208
	Platform services enabled
	Can use own identity source
	S3 Select enabled

Menu de armazenamento (S3)

O menu Armazenamento é fornecido somente para contas de locatários do S3. Este menu permite que os usuários do S3 gerenciem chaves de acesso; criem, gerenciem e excluam buckets; gerenciem pontos de extremidade de serviços de plataforma; e visualizem quaisquer conexões de federação de grade que eles têm permissão para usar.

Minhas chaves de acesso

Os usuários do tenant do S3 podem gerenciar chaves de acesso da seguinte maneira:

- Usuários que têm a permissão Gerenciar suas próprias credenciais do S3 podem criar ou remover suas próprias chaves de acesso do S3.
- Usuários que têm permissão de acesso Root podem gerenciar as chaves de acesso para a conta root do S3, sua própria conta e todos os outros usuários. As chaves de acesso root também fornecem acesso total aos buckets e objetos do locatário, a menos que sejam explicitamente desabilitadas por uma política de bucket.



O gerenciamento das chaves de acesso para outros usuários ocorre no menu Gerenciamento de Acesso.

Baldes

Usuários locatários do S3 com as permissões apropriadas podem executar as seguintes tarefas para seus

buckets:

- Criar baldes
- Habilitar o bloqueio de objeto S3 para um novo bucket (supõe que o bloqueio de objeto S3 esteja habilitado para o sistema StorageGRID)
- Atualizar valores de consistência
- Habilitar e desabilitar atualizações do último horário de acesso
- Habilitar ou suspender o controle de versão do objeto
- Atualizar retenção padrão do bloqueio de objeto S3
- Configurar compartilhamento de recursos de origem cruzada (CORS)
- Excluir todos os objetos em um bucket
- Excluir baldes vazios
- Use o "[Console S3](#)" para gerenciar objetos de bucket

Se um administrador de grade tiver habilitado o uso de serviços de plataforma para a conta do locatário, um usuário locatário do S3 com as permissões apropriadas também poderá executar estas tarefas:

- Configure notificações de eventos do S3, que podem ser enviadas para um serviço de destino compatível com o Amazon Simple Notification Service.
- Configure a replicação do CloudMirror, que permite ao locatário replicar objetos automaticamente para um bucket S3 externo.
- Configure a integração de pesquisa, que envia metadados de objetos para um índice de pesquisa de destino sempre que um objeto é criado, excluído ou seus metadados ou tags são atualizados.

Pontos de extremidade de serviços de plataforma

Se um administrador de grade tiver habilitado o uso de serviços de plataforma para a conta do locatário, um usuário locatário do S3 com a permissão Gerenciar endpoints poderá configurar um endpoint de destino para cada serviço de plataforma.

Conexões de federação de rede

Se um administrador de grade tiver habilitado o uso de uma conexão de federação de grade para a conta do locatário, um usuário locatário do S3 que tenha permissão de acesso Root poderá visualizar o nome da conexão, acessar a página de detalhes do bucket para cada bucket que tenha replicação entre grades habilitada e visualizar o erro mais recente que ocorreu quando os dados do bucket estavam sendo replicados para a outra grade na conexão. Ver "[Ver conexões de federação de grade](#)".

Menu de gerenciamento de acesso

O menu Gerenciamento de acesso permite que os locatários do StorageGRID importem grupos de usuários de uma fonte de identidade federada e atribuam permissões de gerenciamento. Os locatários também podem gerenciar grupos de locatários e usuários locais, a menos que o logon único (SSO) esteja em vigor para todo o sistema StorageGRID .

Diretrizes de rede

Diretrizes de rede

Use estas diretrizes para aprender sobre a arquitetura e as topologias de rede do StorageGRID e para conhecer os requisitos de configuração e provisionamento de rede.

Sobre estas instruções

Estas diretrizes fornecem informações que você pode usar para criar a infraestrutura de rede do StorageGRID antes de implantar e configurar os nós do StorageGRID . Use estas diretrizes para ajudar a garantir que a comunicação possa ocorrer entre todos os nós na grade e entre a grade e clientes e serviços externos.

Clientes externos e serviços externos precisam se conectar às redes StorageGRID para executar funções como as seguintes:

- Armazene e recupere dados de objetos
- Receber notificações por e-mail
- Acesse a interface de gerenciamento do StorageGRID (Gerenciador de Grade e Gerenciador de Locatários)
- Acesse o compartilhamento de auditoria (opcional)
- Fornecer serviços como:
 - Protocolo de Tempo de Rede (NTP)
 - Sistema de nomes de domínio (DNS)
 - Servidor de gerenciamento de chaves (KMS)

A rede StorageGRID deve ser configurada adequadamente para lidar com o tráfego para essas funções e muito mais.

Antes de começar

Configurar a rede para um sistema StorageGRID requer um alto nível de experiência com comutação Ethernet, rede TCP/IP, sub-redes, roteamento de rede e firewalls.

Antes de configurar a rede, familiarize-se com a arquitetura StorageGRID , conforme descrito em ["Saiba mais sobre o StorageGRID"](#) .

Depois de determinar quais redes StorageGRID você deseja usar e como essas redes serão configuradas, você pode instalar e configurar os nós StorageGRID seguindo as instruções apropriadas.

Instalar nós do dispositivo

- ["Instalar hardware do aparelho"](#)

Instalar nós baseados em software

- ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
- ["Instalar o StorageGRID no Ubuntu ou Debian"](#)
- ["Instalar o StorageGRID no VMware"](#)

Configurar e administrar o software StorageGRID

- ["Administrar StorageGRID"](#)
- ["Notas de lançamento"](#)

Tipos de rede StorageGRID

Os nós de grade em um sistema StorageGRID processam *tráfego de grade*, *tráfego de administrador* e *tráfego de cliente*. Você deve configurar a rede adequadamente para gerenciar esses três tipos de tráfego e fornecer controle e segurança.

Tipos de tráfego

Tipo de tráfego	Descrição	Tipo de rede
Tráfego de grade	O tráfego interno do StorageGRID que trafega entre todos os nós na grade. Todos os nós da grade devem ser capazes de se comunicar com todos os outros nós da grade nesta rede.	Rede de grade (obrigatório)
Tráfego administrativo	O tráfego usado para administração e manutenção do sistema.	Rede de administração (opcional), Rede VLAN (opcional)
Tráfego de clientes	O tráfego que trafega entre aplicativos clientes externos e a grade, incluindo todas as solicitações de armazenamento de objetos de clientes S3.	Rede de clientes (opcional), Rede VLAN (opcional)

Você pode configurar a rede das seguintes maneiras:

- Somente rede de grade
- Redes de grade e administração
- Redes de Grade e Clientes
- Redes de grade, administração e clientes

A Grid Network é obrigatória e pode gerenciar todo o tráfego da grade. As redes de administrador e cliente podem ser incluídas no momento da instalação ou adicionadas posteriormente para se adaptar às mudanças nos requisitos. Embora a Rede de Administração e a Rede de Clientes sejam opcionais, quando você usa essas redes para lidar com tráfego administrativo e de clientes, a Rede de Grade pode ser isolada e segura.

Portas internas só são acessíveis pela Grid Network. Portas externas são acessíveis de todos os tipos de rede. Essa flexibilidade oferece diversas opções para projetar uma implantação do StorageGRID e configurar filtragem de IP externo e porta em switches e firewalls. Ver "[comunicações internas do nó da rede](#)" e "[comunicações externas](#)".

Interfaces de rede

Os nós do StorageGRID são conectados a cada rede usando as seguintes interfaces específicas:

Rede	Nome da interface
Rede de grade (obrigatório)	eth0
Rede de administração (opcional)	eth1

Rede	Nome da interface
Rede de clientes (opcional)	eth2

Para obter detalhes sobre o mapeamento de portas virtuais ou físicas para interfaces de rede de nós, consulte as instruções de instalação:

Nós baseados em software

- ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
- ["Instalar o StorageGRID no Ubuntu ou Debian"](#)
- ["Instalar o StorageGRID no VMware"](#)

Nós de dispositivos

- ["Dispositivo de armazenamento SG6160"](#)
- ["Dispositivo de armazenamento SGF6112"](#)
- ["Dispositivo de armazenamento SG6000"](#)
- ["Dispositivo de armazenamento SG5800"](#)
- ["Dispositivo de armazenamento SG5700"](#)
- ["Aparelhos de serviço SG110 e SG1100"](#)
- ["Aparelhos de serviços SG100 e SG1000"](#)

Informações de rede para cada nó

Você deve configurar o seguinte para cada rede habilitada em um nó:

- Endereço IP
- Máscara de sub-rede
- Endereço IP do gateway

Você só pode configurar uma combinação de endereço IP/máscara/gateway para cada uma das três redes em cada nó da grade. Se não quiser configurar um gateway para uma rede, você deve usar o endereço IP como endereço de gateway.

Grupos de alta disponibilidade

Grupos de alta disponibilidade (HA) fornecem a capacidade de adicionar endereços IP virtuais (VIP) à interface de rede do cliente ou da grade. Para obter mais informações, consulte ["Gerenciar grupos de alta disponibilidade"](#).

Rede de grade

A Rede Grid é necessária. Ele é usado para todo o tráfego interno do StorageGRID. A Grid Network fornece conectividade entre todos os nós da grade, em todos os sites e sub-redes. Todos os nós na rede de grade devem ser capazes de se comunicar com todos os outros nós. A rede de grade pode consistir em várias sub-redes. Redes que contêm serviços de rede críticos, como NTP, também podem ser adicionadas como sub-redes de rede.



O StorageGRID não oferece suporte à tradução de endereços de rede (NAT) entre nós.

A Rede de Grade pode ser usada para todo o tráfego de administrador e todo o tráfego de cliente, mesmo que a Rede de Administrador e a Rede de Cliente estejam configuradas. O gateway da Grid Network é o gateway padrão do nó, a menos que o nó tenha a Client Network configurada.



Ao configurar a Grid Network, você deve garantir que a rede esteja protegida de clientes não confiáveis, como aqueles na Internet aberta.

Observe os seguintes requisitos e detalhes para o gateway da Grid Network:

- O gateway da rede de grade deve ser configurado se houver várias sub-redes de grade.
- O gateway da Grid Network é o gateway padrão do nó até que a configuração da grade seja concluída.
- Rotas estáticas são geradas automaticamente para todos os nós para todas as sub-redes configuradas na Lista de Sub-redes da Rede de Grade global.
- Se uma Rede Cliente for adicionada, o gateway padrão alternará do gateway da Rede Grid para o gateway da Rede Cliente quando a configuração da grade estiver concluída.

Rede de administração

A rede de administração é opcional. Quando configurado, ele pode ser usado para administração do sistema e tráfego de manutenção. A rede de administração normalmente é uma rede privada e não precisa ser roteável entre nós.

Você pode escolher quais nós da grade devem ter a Rede de Administração habilitada.

Quando você usa a Rede de Administração, o tráfego administrativo e de manutenção não precisa passar pela Rede de Grade. Os usos típicos da Rede de Administração incluem o seguinte:

- Acesso às interfaces de usuário do Grid Manager e do Tenant Manager.
- Acesso a serviços críticos, como servidores NTP, servidores DNS, servidores externos de gerenciamento de chaves (KMS) e servidores Lightweight Directory Access Protocol (LDAP).
- Acesso a logs de auditoria em nós de administração.
- Acesso ao Secure Shell Protocol (SSH) para manutenção e suporte.

A rede de administração nunca é usada para tráfego de grade interna. Um gateway de rede de administração é fornecido e permite que a rede de administração se comunique com várias sub-redes externas. No entanto, o gateway da rede de administração nunca é usado como o gateway padrão do nó.

Observe os seguintes requisitos e detalhes para o gateway da rede de administração:

- O gateway da rede de administração é necessário se as conexões forem feitas de fora da sub-rede da rede de administração ou se várias sub-redes da rede de administração forem configuradas.
- Rotas estáticas são criadas para cada sub-rede configurada na Lista de sub-redes da rede de administração do nó.

Rede de clientes

A Rede de Clientes é opcional. Quando configurado, ele é usado para fornecer acesso a serviços de grade para aplicativos clientes, como o S3. Se você planeja tornar os dados do StorageGRID acessíveis a um recurso externo (por exemplo, um Cloud Storage Pool ou o serviço de replicação StorageGRID CloudMirror), o recurso externo também pode usar a Rede do Cliente. Os nós da grade podem se comunicar com qualquer sub-rede acessível através do gateway da rede do cliente.

Você pode escolher quais nós da grade devem ter a Rede do Cliente habilitada. Nem todos os nós precisam estar na mesma Rede do Cliente, e os nós nunca se comunicarão entre si pela Rede do Cliente. A Rede do Cliente não se torna operacional até que a instalação da grade esteja concluída.

Para maior segurança, você pode especificar que a interface de rede do cliente de um nó não seja confiável para que a rede do cliente seja mais restritiva em relação às conexões permitidas. Se a interface de rede do cliente de um nó não for confiável, a interface aceitará conexões de saída, como aquelas usadas pela replicação do CloudMirror, mas aceitará somente conexões de entrada em portas que foram configuradas explicitamente como pontos de extremidade do balanceador de carga. Ver "[Gerenciar controles de firewall](#)" e "[Configurar pontos de extremidade do balanceador de carga](#)".

Quando você usa uma Rede de Cliente, o tráfego do cliente não precisa passar pela Rede de Grade. O tráfego da Grid Network pode ser separado em uma rede segura e não roteável. Os seguintes tipos de nós geralmente são configurados com uma rede de cliente:

- Nós de gateway, porque esses nós fornecem acesso ao serviço StorageGRID Load Balancer e acesso do cliente S3 à grade.
- Nós de armazenamento, porque esses nós fornecem acesso ao protocolo S3, aos pools de armazenamento em nuvem e ao serviço de replicação do CloudMirror.
- Nós de administração, para garantir que os usuários locatários possam se conectar ao Gerenciador de locatários sem precisar usar a Rede de administração.

Observe o seguinte para o gateway da rede do cliente:

- O gateway da Rede do Cliente é necessário se a Rede do Cliente estiver configurada.
- O gateway da rede do cliente se torna a rota padrão para o nó da grade quando a configuração da grade é concluída.

Redes VLAN opcionais

Conforme necessário, você pode opcionalmente usar redes LAN virtuais (VLAN) para tráfego de cliente e para alguns tipos de tráfego de administrador. O tráfego de grade, no entanto, não pode usar uma interface VLAN. O tráfego interno do StorageGRID entre os nós deve sempre usar a Grid Network na eth0.

Para dar suporte ao uso de VLANs, você deve configurar uma ou mais interfaces em um nó como interfaces de tronco no switch. Você pode configurar a interface de rede Grid (eth0) ou a interface de rede do cliente (eth2) para ser um tronco, ou pode adicionar interfaces de tronco ao nó.

Se eth0 estiver configurado como um tronco, o tráfego da Grid Network fluirá pela interface nativa do tronco, conforme configurado no switch. Da mesma forma, se eth2 estiver configurado como um tronco e a Rede do Cliente também estiver configurada no mesmo nó, a Rede do Cliente usará a VLAN nativa da porta do tronco, conforme configurada no switch.

Somente o tráfego de entrada do administrador, como o usado para tráfego SSH, Grid Manager ou Tenant Manager, é suportado em redes VLAN. O tráfego de saída, como o usado para NTP, DNS, LDAP, KMS e pools de armazenamento em nuvem, não é suportado em redes VLAN.



Interfaces VLAN podem ser adicionadas somente a nós de administração e nós de gateway. Você não pode usar uma interface VLAN para acesso de cliente ou administrador aos nós de armazenamento.

Ver "[Configurar interfaces VLAN](#)" para obter instruções e diretrizes.

As interfaces VLAN são usadas apenas em grupos HA e recebem endereços VIP no nó ativo. Ver "[Gerenciar grupos de alta disponibilidade](#)" para obter instruções e diretrizes.

Exemplos de topologia de rede

Topologia de rede em grade

A topologia de rede mais simples é criada configurando apenas a Rede de Grade.

Ao configurar a Grid Network, você estabelece o endereço IP do host, a máscara de sub-rede e o endereço IP do gateway para a interface eth0 para cada nó da grade.

Durante a configuração, você deve adicionar todas as sub-redes da Grid Network à Grid Network Subnet List (GNSL). Esta lista inclui todas as sub-redes de todos os sites e também pode incluir sub-redes externas que fornecem acesso a serviços críticos, como NTP, DNS ou LDAP.

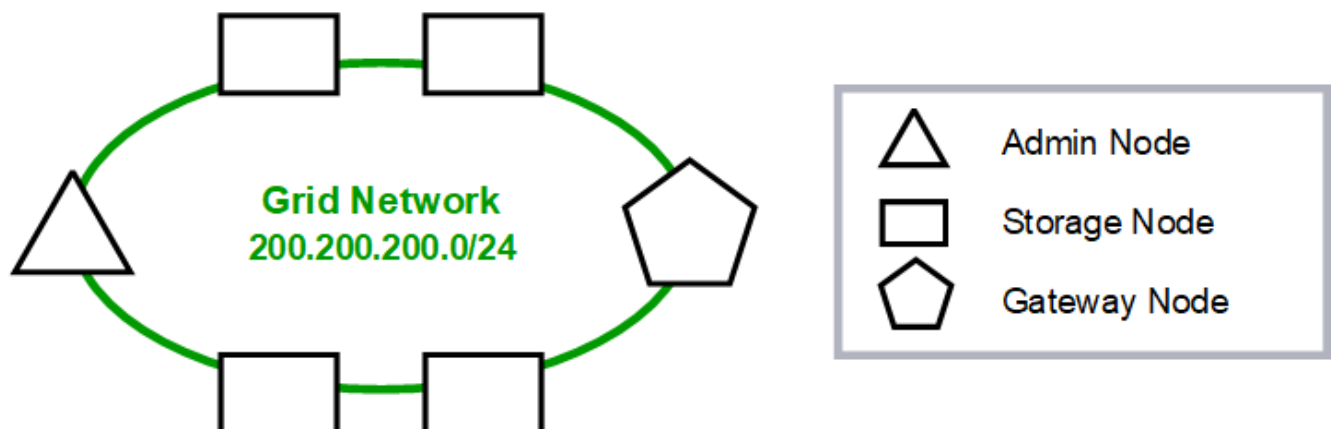
Na instalação, a interface da Grid Network aplica rotas estáticas para todas as sub-redes no GNSL e define a rota padrão do nó para o gateway da Grid Network, se houver um configurado. O GNSL não é necessário se não houver uma rede cliente e o gateway da rede Grid for a rota padrão do nó. Rotas de host para todos os outros nós na grade também são geradas.

Neste exemplo, todo o tráfego compartilha a mesma rede, incluindo o tráfego relacionado às solicitações do cliente S3 e às funções administrativas e de manutenção.



Essa topologia é apropriada para implantações de site único que não estão disponíveis externamente, implantações de teste ou de prova de conceito, ou quando um balanceador de carga de terceiros atua como limite de acesso do cliente. Sempre que possível, a Rede Grid deve ser usada 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.

Topology example: Grid Network only



*Provisioned***GNSL → 200.200.200.0/24**

Grid Network		
Nodes	IP/mask	Gateway
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	Routes	Type	From
All	0.0.0.0/0 → 200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24 → eth0	Link	Interface IP/mask

Topologia de rede de administração

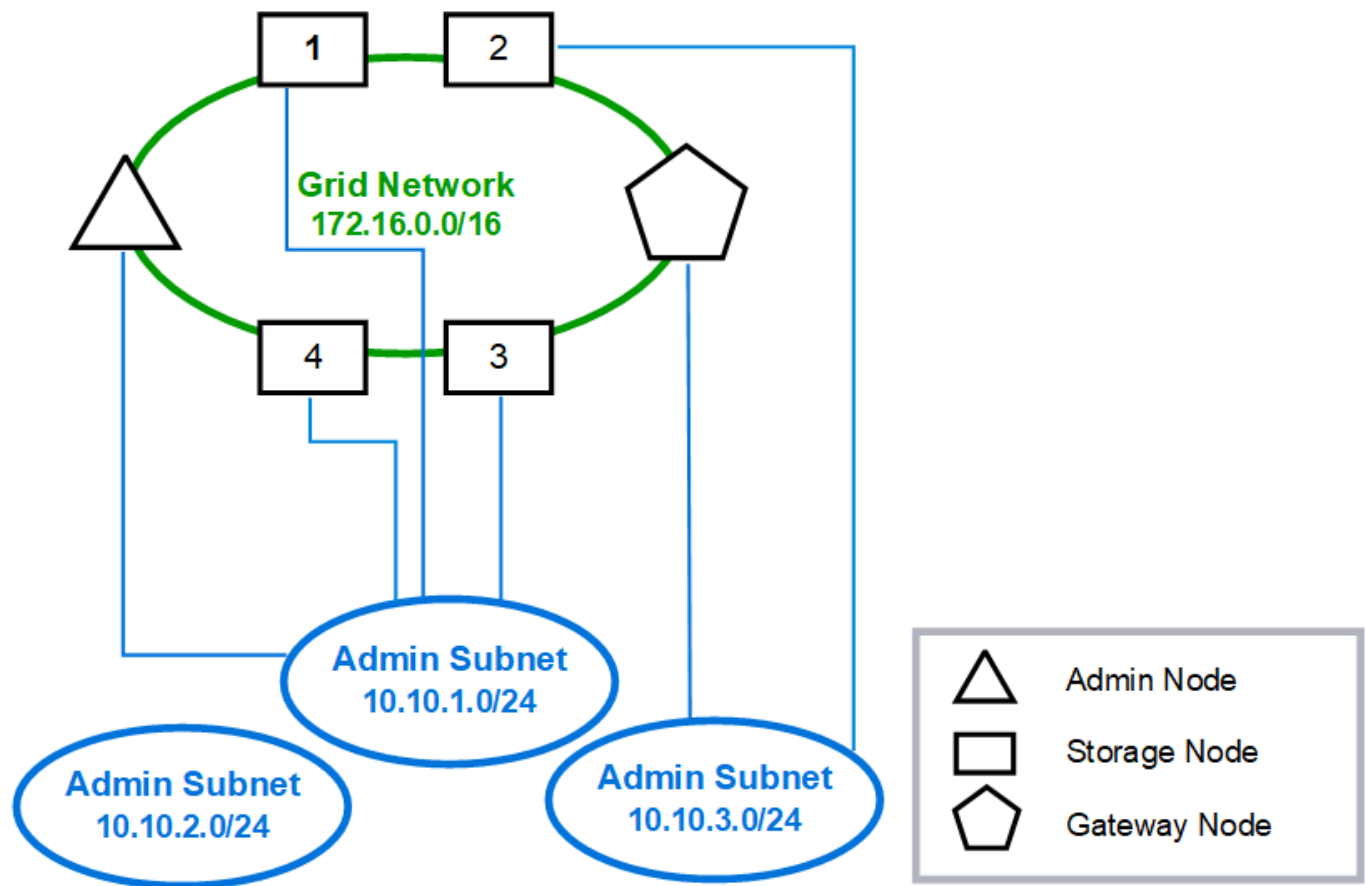
Ter uma rede de administração é opcional. Uma maneira de usar uma rede de administração e uma rede de grade é configurar uma rede de grade roteável e uma rede de administração limitada para cada nó.

Ao configurar a rede de administração, você estabelece o endereço IP do host, a máscara de sub-rede e o endereço IP do gateway para a interface eth1 para cada nó da grade.

A rede de administração pode ser exclusiva para cada nó e pode consistir em várias sub-redes. Cada nó pode ser configurado com uma Lista de Sub-redes Externas de Administração (AESL). O AESL lista as sub-redes acessíveis pela rede de administração para cada nó. O AESL também deve incluir as sub-redes de quaisquer serviços que a grade acessará pela Rede de Administração, como NTP, DNS, KMS e LDAP. Rotas estáticas são aplicadas para cada sub-rede no AESL.

Neste exemplo, a Grid Network é usada para tráfego relacionado a solicitações de clientes S3 e gerenciamento de objetos, enquanto a Admin Network é usada para funções administrativas.

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

Nodes	Grid Network		Admin Network	
	IP/mask	Gateway	IP/mask	Gateway
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated					
Nodes	Routes			Type	From
All	0.0.0.0/0	→	172.16.200.1	Default	Grid Network gateway
Admin, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	10.10.3.1	Static	AESL
	10.10.2.0/24	→	10.10.3.1	Static	AESL
	10.10.3.0/24	→	eth1	Link	Interface IP/mask

Topologia de rede do cliente

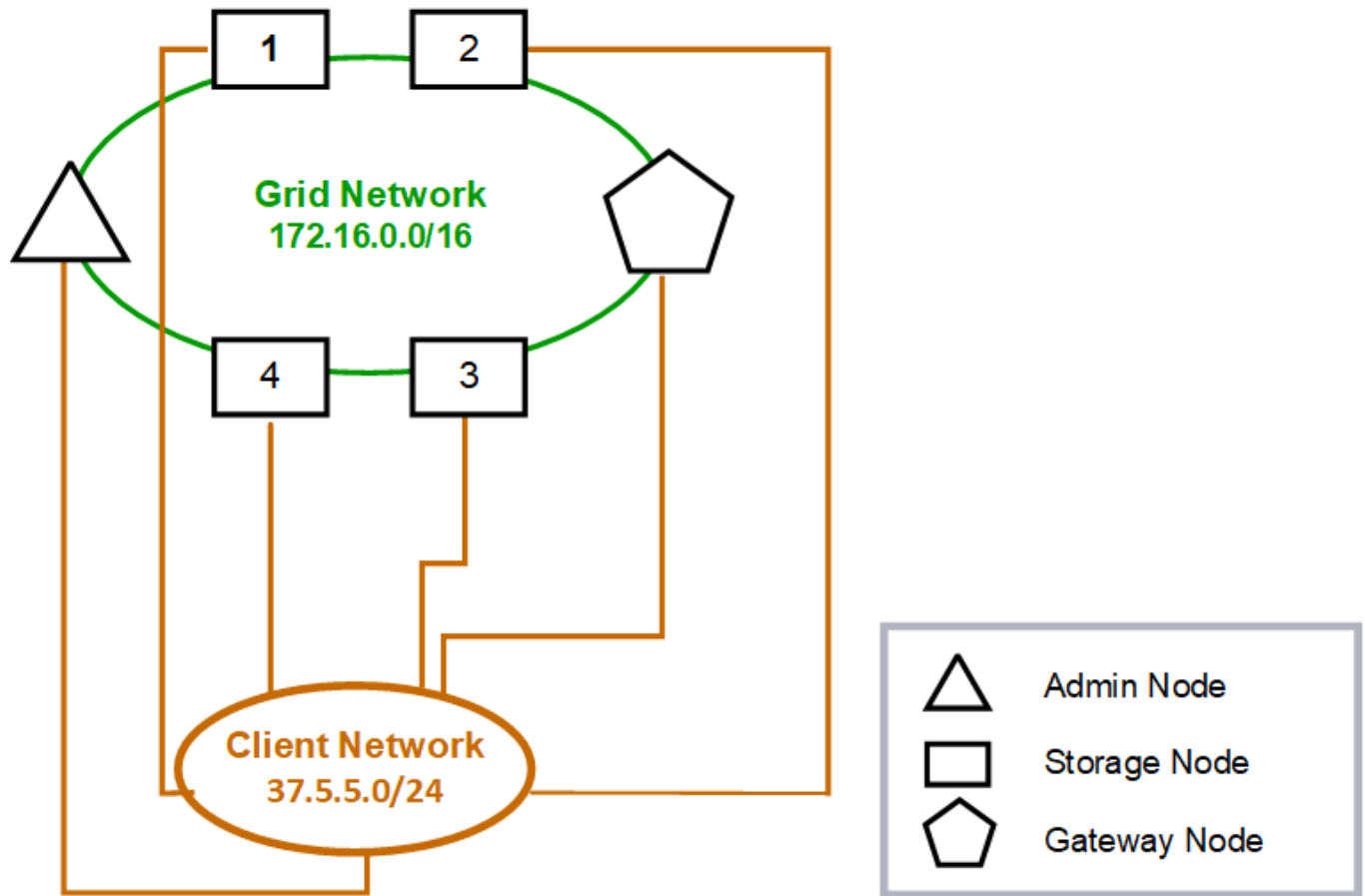
Ter uma Rede de Clientes é opcional. Usar uma rede cliente permite que o tráfego da rede cliente (por exemplo, S3) seja separado do tráfego interno da grade, o que permite que a rede da grade seja mais segura. O tráfego administrativo pode ser gerenciado pelo cliente ou pela rede de grade quando a rede de administração não estiver configurada.

Ao configurar a Rede do Cliente, você estabelece o endereço IP do host, a máscara de sub-rede e o endereço IP do Gateway para a interface eth2 do nó configurado. A Rede de Cliente de cada nó pode ser independente da Rede de Cliente de qualquer outro nó.

Se você configurar uma Rede Cliente para um nó durante a instalação, o gateway padrão do nó mudará do gateway da Rede Grid para o gateway da Rede Cliente quando a instalação estiver concluída. Se uma Rede de Cliente for adicionada posteriormente, o gateway padrão do nó alternará da mesma maneira.

Neste exemplo, a Rede do Cliente é usada para solicitações de clientes S3 e para funções administrativas, enquanto a Rede da Grade é dedicada a operações internas de gerenciamento de objetos.

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

Nodes	Grid Network	Client Network	
	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes		Type	From
All	0.0.0.0/0	→ 37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→ eth0	Link	Interface IP/mask
	37.5.5.0/24	→ eth2	Link	Interface IP/mask

Informações relacionadas

["Alterar configuração de rede do nó"](#)

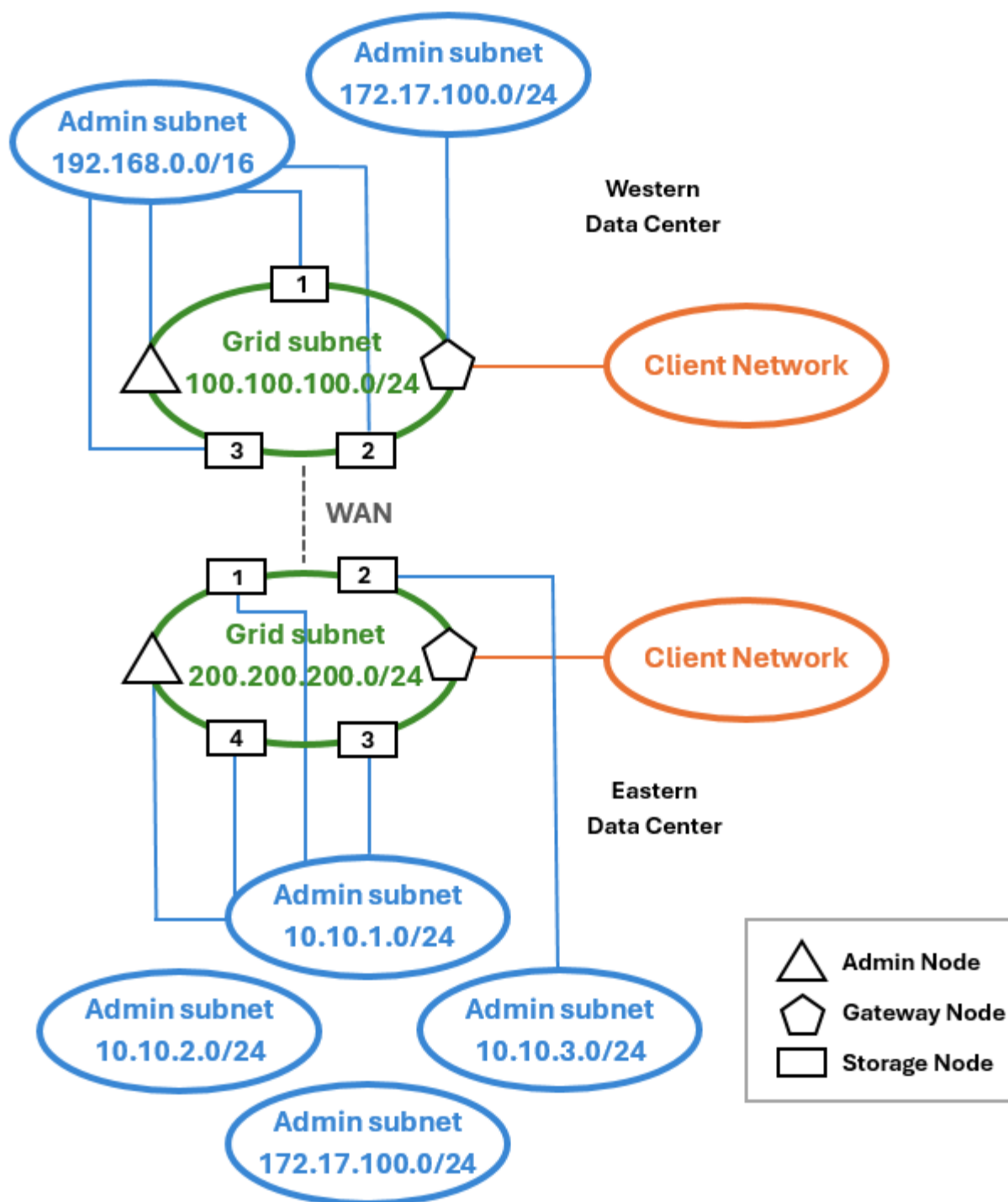
Topologia para todas as três redes

Você pode configurar todas as três redes em uma topologia de rede que consiste em uma rede de grade privada, redes de administração específicas do site e redes de clientes abertas. Usar endpoints do balanceador de carga e redes de clientes não confiáveis pode fornecer segurança adicional, se necessário.

Neste exemplo:

- A Grid Network é usada para tráfego de rede relacionado a operações internas de gerenciamento de objetos.
- A Rede de Administração é usada para tráfego relacionado a funções administrativas.
- A Rede do Cliente é usada para tráfego relacionado a solicitações de clientes S3.

Exemplo de topologia: Redes de grade, administração e clientes



Requisitos de rede

Você deve verificar se a infraestrutura e a configuração de rede atuais podem suportar o design de rede StorageGRID planejado.

Requisitos gerais de rede

Todas as implantações do StorageGRID devem ser capazes de suportar as seguintes conexões.

Essas conexões podem ocorrer por meio das redes Grid, Admin ou Client, ou das combinações dessas redes, conforme ilustrado nos exemplos de topologia de rede.

- **Conexões de gerenciamento:** Conexões de entrada de um administrador para o nó, geralmente por meio de SSH. Acesso via navegador da Web ao Grid Manager, ao Tenant Manager e ao StorageGRID Appliance Installer.
- **Conexões do servidor NTP:** Conexão UDP de saída que recebe uma resposta UDP de entrada.

Pelo menos um servidor NTP deve estar acessível ao nó de administração primário.

- **Conexões do servidor DNS:** Conexão UDP de saída que recebe uma resposta UDP de entrada.
- **Conexões do servidor LDAP/Active Directory:** Conexão TCP de saída do serviço de identidade nos nós de armazenamento.
- *** AutoSupport*:** Conexão TCP de saída dos nós de administração para `support.netapp.com` ou um proxy configurado pelo cliente.
- **Servidor de gerenciamento de chaves externo:** Conexão TCP de saída de cada nó do dispositivo com criptografia de nó habilitada.
- Conexões TCP de entrada de clientes S3.
- Solicitações de saída de serviços da plataforma StorageGRID, como replicação do CloudMirror ou de pools de armazenamento em nuvem.

Se o StorageGRID não conseguir entrar em contato com nenhum dos servidores NTP ou DNS provisionados usando as regras de roteamento padrão, ele tentará contato automaticamente em todas as redes (Grid, Admin e Cliente), desde que os endereços IP dos servidores DNS e NTP sejam especificados. Se os servidores NTP ou DNS puderem ser alcançados em qualquer rede, o StorageGRID criará automaticamente regras de roteamento adicionais para garantir que a rede seja usada para todas as tentativas futuras de conexão a ela.



Embora você possa usar essas rotas de host descobertas automaticamente, em geral você deve configurar manualmente as rotas DNS e NTP para garantir a conectividade caso a descoberta automática falhe.

Se você não estiver pronto para configurar as redes opcionais de administrador e cliente durante a implantação, poderá configurar essas redes ao aprovar os nós de grade durante as etapas de configuração. Além disso, você pode configurar essas redes após a instalação, usando a ferramenta Alterar IP (consulte "[Configurar endereços IP](#)").

Somente conexões de cliente S3 e conexões administrativas SSH, Grid Manager e Tenant Manager são suportadas em interfaces VLAN. Conexões de saída, como para servidores NTP, DNS, LDAP, AutoSupport e KMS, devem passar diretamente pelas interfaces de cliente, administrador ou rede de grade. Se a interface estiver configurada como um tronco para suportar interfaces VLAN, esse tráfego fluirá pela VLAN nativa da interface, conforme configurado no switch.

Redes de longa distância (WANs) para vários sites

Ao configurar um sistema StorageGRID com vários sites, a conexão WAN entre os sites deve ter uma largura de banda mínima de 25 Mbit/segundo em cada direção antes de contabilizar o tráfego do cliente. A replicação de dados ou codificação de eliminação entre sites, expansão de nó ou site, recuperação de nó e outras operações ou configurações exigirão largura de banda adicional.

Os requisitos mínimos reais de largura de banda da WAN dependem da atividade do cliente e do esquema de proteção do ILM. Para obter assistência na estimativa dos requisitos mínimos de largura de banda da WAN, entre em contato com seu consultor de serviços profissionais da NetApp.

Conexões para nós de administração e nós de gateway

Os nós de administração devem sempre ser protegidos de clientes não confiáveis, como aqueles na Internet aberta. Você deve garantir que nenhum cliente não confiável possa acessar qualquer nó de administração na rede Grid, na rede de administração ou na rede de clientes.

Os nós de administração e os nós de gateway que você planeja adicionar aos grupos de alta disponibilidade devem ser configurados com um endereço IP estático. Para obter mais informações, consulte ["Gerenciar grupos de alta disponibilidade"](#).

Usando tradução de endereços de rede (NAT)

Não use a tradução de endereços de rede (NAT) na Grid Network entre nós da grade ou entre sites do StorageGRID. Quando você usa endereços IPv4 privados para a Grid Network, esses endereços devem ser roteáveis diretamente de cada nó da grade em cada site. No entanto, conforme necessário, você pode usar NAT entre clientes externos e nós de grade, como para fornecer um endereço IP público para um nó de gateway. O uso de NAT para conectar um segmento de rede pública é suportado somente quando você emprega um aplicativo de tunelamento que seja transparente a todos os nós na grade, o que significa que os nós da grade não exigem conhecimento de endereços IP públicos.

Requisitos específicos da rede

Siga os requisitos para cada tipo de rede StorageGRID.

Gateways e roteadores de rede

- Se definido, o gateway para uma determinada rede deve estar dentro da sub-rede da rede específica.
- Se você configurar uma interface usando endereçamento estático, deverá especificar um endereço de gateway diferente de 0.0.0.0.
- Se você não tiver um gateway, a melhor prática é definir o endereço do gateway como o endereço IP da interface de rede.

Sub-redes



Cada rede deve ser conectada à sua própria sub-rede que não se sobreponha a nenhuma outra rede no nó.

As seguintes restrições são aplicadas pelo Grid Manager durante a implantação. Eles são fornecidos aqui para auxiliar no planejamento da rede de pré-implantação.

- A máscara de sub-rede para qualquer endereço IP de rede não pode ser 255.255.255.254 ou 255.255.255.255 (/31 ou /32 na notação CIDR).
- A sub-rede definida por um endereço IP de interface de rede e máscara de sub-rede (CIDR) não pode sobrepor a sub-rede de nenhuma outra interface configurada no mesmo nó.
- Não use sub-redes que contenham os seguintes endereços IPv4 para a Rede de Grade, Rede de Administração ou Rede de Cliente de qualquer nó:
 - 192.168.130.101
 - 192.168.131.101
 - 192.168.130.102
 - 192.168.131.102

- 198.51.100.2
- 198.51.100.4

Por exemplo, não use os seguintes intervalos de sub-rede para a Rede de Grade, Rede de Administração ou Rede de Cliente de nenhum nó:

- 192.168.130.0/24 porque este intervalo de sub-rede contém os endereços IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 porque este intervalo de sub-rede contém os endereços IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 porque este intervalo de sub-rede contém os endereços IP 198.51.100.2 e 198.51.100.4
- A sub-rede da rede de grade para cada nó deve ser incluída no GNSL.
- A sub-rede da rede de administração não pode sobrepor a sub-rede da rede de grade, a sub-rede da rede do cliente ou qualquer sub-rede no GNSL.
- As sub-redes no AESL não podem se sobrepor a nenhuma sub-rede no GNSL.
- A sub-rede da rede do cliente não pode sobrepor a sub-rede da rede da grade, a sub-rede da rede do administrador, nenhuma sub-rede no GNSL ou nenhuma sub-rede no AESL.

Rede de grade

- No momento da implantação, cada nó da grade deve ser conectado à Rede da Grade e deve ser capaz de se comunicar com o Nó de Administração principal usando a configuração de rede especificada ao implantar o nó.
- Durante as operações normais da rede, cada nó da rede deve ser capaz de se comunicar com todos os outros nós da rede na rede.



A rede Grid deve ser roteável diretamente entre cada nó. A tradução de endereços de rede (NAT) entre nós não é suportada.

- Se a rede de grade consistir em várias sub-redes, adicione-as à Lista de sub-redes da rede de grade (GNSL). Rotas estáticas são criadas em todos os nós para cada sub-rede no GNSL.
- Se a interface da Grid Network estiver configurada como um tronco para suportar interfaces VLAN, a VLAN nativa do tronco deverá ser a VLAN usada para o tráfego da Grid Network. Todos os nós da grade devem ser acessíveis pela VLAN nativa do tronco.

Rede de administração

A rede de administração é opcional. Se você planeja configurar uma rede de administração, siga estes requisitos e diretrizes.

Os usos típicos da Rede de Administração incluem conexões de gerenciamento, AutoSupport, KMS e conexões com servidores críticos, como NTP, DNS e LDAP, se essas conexões não forem fornecidas pela Rede de Grade ou Rede de Cliente.



A rede de administração e o AESL podem ser exclusivos para cada nó, desde que os serviços de rede e clientes desejados estejam acessíveis.



Você deve definir pelo menos uma sub-rede na rede de administração para habilitar conexões de entrada de sub-redes externas. Rotas estáticas são geradas automaticamente em cada nó para cada sub-rede no AESL.

Rede de clientes

A Rede de Clientes é opcional. Se você planeja configurar uma Rede de Cliente, observe as seguintes considerações.

- A Rede do Cliente foi projetada para suportar tráfego de clientes S3. Se configurado, o gateway da rede do cliente se torna o gateway padrão do nó.
- Se você usar uma rede de cliente, poderá ajudar a proteger o StorageGRID de ataques hostis aceitando tráfego de cliente de entrada somente em pontos de extremidade do balanceador de carga configurados explicitamente. Ver "[Configurar pontos de extremidade do balanceador de carga](#)".
- Se a interface de rede do cliente estiver configurada como um tronco para oferecer suporte a interfaces VLAN, considere se é necessário configurar a interface de rede do cliente (eth2). Se configurado, o tráfego da rede do cliente fluirá pela VLAN nativa do tronco, conforme configurado no switch.

Informações relacionadas

["Alterar configuração de rede do nó"](#)

Considerações de rede específicas para implantação

Implantações Linux

Para eficiência, confiabilidade e segurança, o sistema StorageGRID é executado no Linux como uma coleção de mecanismos de contêiner. A configuração de rede relacionada ao mecanismo de contêiner não é necessária em um sistema StorageGRID .

Use um dispositivo não vinculado, como um par VLAN ou Ethernet virtual (veth), para a interface de rede do contêiner. Especifique este dispositivo como a interface de rede no arquivo de configuração do nó.



Não use dispositivos de ligação ou ponte diretamente como interface de rede do contêiner. Isso pode impedir a inicialização do nó devido a um problema no kernel com o uso do macvlan com dispositivos de ligação e ponte no namespace do contêiner.

Veja as instruções de instalação para "[Red Hat Enterprise Linux](#)" ou "[Ubuntu ou Debian](#)" implantações.

Configuração de rede do host para implantações de mecanismo de contêiner

Antes de iniciar a implantação do StorageGRID em uma plataforma de mecanismo de contêiner, determine quais redes (grade, administrador, cliente) cada nó usará. Você deve garantir que a interface de rede de cada nó esteja configurada na interface de host virtual ou física correta e que cada rede tenha largura de banda suficiente.

Hosts físicos

Se você estiver usando hosts físicos para dar suporte a nós de grade:

- Certifique-se de que todos os hosts usem a mesma interface de host para cada interface de nó. Essa estratégia simplifica a configuração do host e permite a migração futura de nós.

- Obtenha um endereço IP para o próprio host físico.



Uma interface física no host pode ser usada pelo próprio host e por um ou mais nós em execução no host. Todos os endereços IP atribuídos ao host ou nós usando esta interface devem ser exclusivos. O host e o nó não podem compartilhar endereços IP.

- Abra as portas necessárias para o host.
- Se você pretende usar interfaces VLAN no StorageGRID, o host deve ter uma ou mais interfaces de tronco que forneçam acesso às VLANs desejadas. Essas interfaces podem ser passadas para o contêiner do nó como eth0, eth2 ou como interfaces adicionais. Para adicionar interfaces de tronco ou acesso, consulte o seguinte:
 - **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"](#)

Recomendações de largura de banda mínima

A tabela a seguir fornece as recomendações mínimas de largura de banda da LAN para cada tipo de nó do StorageGRID e cada tipo de rede. Você deve provisionar cada host físico ou virtual com largura de banda de rede suficiente para atender aos requisitos mínimos agregados de largura de banda para o número total e o tipo de nós StorageGRID que você planeja executar naquele host.

Tipo de nó	Tipo de rede		
	Grade	Administrador	Cliente
	Largura de banda mínima da LAN	Administrador	10 Gbps
1 Gbps	1 Gbps	Portal	10 Gbps
1 Gbps	10 Gbps	Armazenar	10 Gbps
1 Gbps	10 Gbps	Arquivo	10 Gbps



Esta tabela não inclui a largura de banda SAN, que é necessária para acessar o armazenamento compartilhado. Se estiver usando armazenamento compartilhado acessado via Ethernet (iSCSI ou FCoE), você deverá provisionar interfaces físicas separadas em cada host para fornecer largura de banda SAN suficiente. Para evitar a introdução de um gargalo, a largura de banda da SAN para um determinado host deve corresponder aproximadamente à largura de banda agregada da rede do nó de armazenamento para todos os nós de armazenamento em execução naquele host.

Use a tabela para determinar o número mínimo de interfaces de rede a serem provisionadas em cada host, com base no número e no tipo de nós StorageGRID que você planeja executar nesse host.

Por exemplo, para executar um nó de administração, um nó de gateway e um nó de armazenamento em um único host:

- Conecte as redes de grade e administração no nó de administração (requer $10 + 1 = 11$ Gbps)
- Conecte a rede e as redes do cliente no nó de gateway (requer $10 + 10 = 20$ Gbps)
- Conecte a rede de grade no nó de armazenamento (requer 10 Gbps)

Neste cenário, você deve fornecer um mínimo de $11 + 20 + 10 = 41$ Gbps de largura de banda de rede, que pode ser atendida por duas interfaces de 40 Gbps ou cinco interfaces de 10 Gbps, potencialmente agregadas em troncos e então compartilhadas por três ou mais VLANs que transportam as sub-redes Grid, Admin e Client locais para o data center físico que contém o host.

Para algumas maneiras recomendadas de configurar recursos físicos e de rede nos hosts do seu cluster StorageGRID para se preparar para a implantação do StorageGRID, consulte o seguinte:

- ["Configurar a rede do host \(Red Hat Enterprise Linux\)"](#)
- ["Configurar a rede host \(Ubuntu ou Debian\)"](#)

Rede e portas para serviços de plataforma e pools de armazenamento em nuvem

Se você planeja usar os serviços da plataforma StorageGRID ou os Cloud Storage Pools, deverá configurar a rede de grade e os firewalls para garantir que os pontos de extremidade de destino possam ser alcançados.

Rede para serviços de plataforma

Conforme descrito em ["Gerenciar serviços de plataforma para inquilinos"](#) e ["Gerenciar serviços de plataforma"](#) Os serviços de plataforma incluem serviços externos que fornecem integração de pesquisa, notificação de eventos e replicação do CloudMirror.

Os serviços de plataforma exigem acesso dos nós de armazenamento que hospedam o serviço StorageGRID ADC aos pontos de extremidade de serviço externos. Exemplos de fornecimento de acesso incluem:

- Nos nós de armazenamento com serviços ADC, configure redes de administração exclusivas com entradas AESL que roteiam para os pontos de extremidade de destino.
- Confie na rota padrão fornecida por uma Rede de Cliente. Se você usar a rota padrão, você pode usar o ["recurso de rede de cliente não confiável"](#) para restringir conexões de entrada.

Rede para pools de armazenamento em nuvem

Os pools de armazenamento em nuvem também exigem acesso dos nós de armazenamento aos endpoints fornecidos pelo serviço externo usado, como o Amazon S3 Glacier ou o armazenamento de Blobs do Microsoft Azure. Para obter informações, consulte ["O que é um pool de armazenamento em nuvem"](#).

Portas para serviços de plataforma e pools de armazenamento em nuvem

Por padrão, os serviços de plataforma e as comunicações do Cloud Storage Pool usam as seguintes portas:

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

Uma porta diferente pode ser especificada quando o ponto de extremidade é criado ou editado. Ver ["Referência de porta de rede"](#).

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.

VLANs e serviços de plataforma e pools de armazenamento em nuvem

Você não pode usar redes VLAN para serviços de plataforma ou pools de armazenamento em nuvem. Os pontos de extremidade de destino devem ser acessíveis pela rede Grid, Admin ou Client Network.

Nós de dispositivos

Você pode configurar as portas de rede nos dispositivos StorageGRID para usar os modos de vínculo de porta que atendem aos seus requisitos de taxa de transferência, redundância e failover.

As portas 10/25-GbE nos dispositivos StorageGRID podem ser configuradas no modo de vínculo fixo ou agregado para conexões com a rede de grade e a rede do cliente.

As portas de rede de administração de 1 GbE podem ser configuradas no modo independente ou de backup ativo para conexões com a rede de administração.

Veja as informações sobre os modos de ligação de porta do seu aparelho:

- ["Modos de ligação de porta \(SG6160\)"](#)
- ["Modos de ligação de porta \(SGF6112\)"](#)
- ["Modos de ligação de porta \(controlador SG6000-CN\)"](#)
- ["Modos de ligação de porta \(controlador SG5800\)"](#)
- ["Modos de ligação de porta \(controlador E5700SG\)"](#)
- ["Modos de ligação de porta \(SG110 e SG1100\)"](#)
- ["Modos de ligação de porta \(SG100 e SG1000\)"](#)

Instalação e provisionamento de rede

Você deve entender como a Rede de Grade e as Redes de Administrador e Cliente opcionais são usadas durante a implantação do nó e a configuração da grade.

Implantação inicial de um nó

Ao implantar um nó pela primeira vez, você deve anexá-lo à Rede de Grade e garantir que ele tenha acesso ao Nó de Administração principal. Se a Rede de Grade estiver isolada, você poderá configurar a Rede de Administração no Nó de Administração principal para acesso de configuração e instalação de fora da Rede de Grade.

Uma rede de grade com um gateway configurado se torna o gateway padrão para um nó durante a implantação. O gateway padrão permite que nós de grade em sub-redes separadas se comuniquem com o nó de administração principal antes que a grade seja configurada.

Se necessário, sub-redes contendo servidores NTP ou que exijam acesso ao Grid Manager ou à API também podem ser configuradas como sub-redes de grade.

Registro automático de nó com nó de administração primário

Depois que os nós são implantados, eles se registram no nó de administração principal usando a rede Grid. Você pode então usar o Grid Manager, o `configure-storagegrid.py` Script Python ou a API de instalação para configurar a grade e aprovar os nós registrados. Durante a configuração da grade, você pode configurar várias sub-redes da grade. Rotas estáticas para essas sub-redes por meio do gateway da Grid Network serão criadas em cada nó quando você concluir a configuração da grade.

Desabilitando a rede de administração ou a rede do cliente

Se você quiser desabilitar a Rede de Administração ou a Rede de Cliente, você pode remover a configuração delas durante o processo de aprovação do nó, ou você pode usar a ferramenta Alterar IP após a conclusão da instalação (veja ["Configurar endereços IP"](#)).

Diretrizes pós-instalação

Após concluir a implantação e a configuração do nó de grade, siga estas diretrizes para endereçamento DHCP e alterações na configuração de rede.

- Se o DHCP foi usado para atribuir endereços IP, configure uma reserva DHCP para cada endereço IP nas redes que estão sendo usadas.

Você só pode configurar o DHCP durante a fase de implantação. Não é possível configurar o DHCP durante a configuração.



Os nós são reinicializados quando a configuração da rede de grade é alterada pelo DHCP, o que pode causar interrupções se uma alteração de DHCP afetar vários nós ao mesmo tempo.

- Você deve usar os procedimentos Alterar IP se quiser alterar endereços IP, máscaras de sub-rede e gateways padrão para um nó de grade. Ver ["Configurar endereços IP"](#) .
- Se você fizer alterações na configuração de rede, incluindo alterações de roteamento e gateway, a conectividade do cliente com o nó de administração principal e outros nós da grade poderá ser perdida. Dependendo das alterações de rede aplicadas, pode ser necessário restabelecer essas conexões.

Referência de porta de rede

Comunicações internas do nó da rede

O firewall interno do StorageGRID permite conexões de entrada em portas específicas na Grid Network. Conexões também são aceitas em portas definidas pelos pontos de extremidade do balanceador de carga.



A NetApp recomenda que você habilite o tráfego do Protocolo de Mensagens de Controle da Internet (ICMP) entre os nós da grade. Permitir tráfego ICMP pode melhorar o desempenho de failover quando um nó de grade não pode ser alcançado.

Além do ICMP e das portas listadas na tabela, o StorageGRID usa o Virtual Router Redundancy Protocol (VRRP). VRRP é um protocolo de internet que usa o protocolo IP número 112. O StorageGRID usa VRRP somente no modo unicast. O VRRP é necessário somente se ["grupos de alta disponibilidade"](#) estão configurados.

Diretrizes para nós baseados em Linux

Se as políticas de rede corporativa restringirem o acesso a qualquer uma dessas portas, você poderá remapear as portas no momento da implantação usando um parâmetro de configuração de implantação. Para obter mais informações sobre remapeamento de portas e parâmetros de configuração de implantação, consulte:

- ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
- ["Instalar o StorageGRID no Ubuntu ou Debian"](#)

Diretrizes para nós baseados em VMware

Configure as seguintes portas somente se precisar definir restrições de firewall externas à rede VMware.

Se as políticas de rede corporativa restringirem o acesso a qualquer uma dessas portas, você poderá remapear as portas ao implantar nós usando o VMware vSphere Web Client ou usando uma definição de arquivo de configuração ao automatizar a implantação de nós de grade. Para obter mais informações sobre remapeamento de porta e parâmetros de configuração de implantação, consulte ["Instalar o StorageGRID no VMware"](#).

Diretrizes para nós de dispositivos

Se as políticas de rede corporativa restringirem o acesso a qualquer uma dessas portas, você poderá remapear as portas usando o StorageGRID Appliance Installer. Ver ["Opcional: Remapear portas de rede para o dispositivo"](#).

Portas internas do StorageGRID

Porta	TCP ou UDP	De	Para	Detalhes
22	TCP	Nó de administração primário	Todos os nós	Para procedimentos de manutenção, o nó administrativo primário deve ser capaz de se comunicar com todos os outros nós usando SSH na porta 22. Permitir tráfego SSH de outros nós é opcional.
80	TCP	Eletrodomésticos	Nó de administração primário	Usado por dispositivos StorageGRID para se comunicar com o nó de administração principal para iniciar a instalação.
123	UDP	Todos os nós	Todos os nós	Serviço de protocolo de tempo de rede. Cada nó sincroniza seu tempo com todos os outros nós usando NTP.
443	TCP	Todos os nós	Nó de administração primário	Usado para comunicar status ao nó de administração principal durante a instalação e outros procedimentos de manutenção.
1055	TCP	Todos os nós	Nó de administração primário	Tráfego interno para instalação, expansão, recuperação e outros procedimentos de manutenção.

Porta	TCP ou UDP	De	Para	Detalhes
1139	TCP	Nós de armazenamento	Nós de armazenamento	Tráfego interno entre nós de armazenamento.
1501	TCP	Todos os nós	Nós de armazenamento com ADC	Relatórios, auditoria e configuração de tráfego interno.
1502	TCP	Todos os nós	Nós de armazenamento	Tráfego interno relacionado ao S3 e Swift.
1504	TCP	Todos os nós	Nós de administração	Relatórios de serviço NMS e configuração de tráfego interno.
1505	TCP	Todos os nós	Nós de administração	Tráfego interno do serviço AMS.
1506	TCP	Todos os nós	Todos os nós	Tráfego interno de status do servidor.
1507	TCP	Todos os nós	Nós de gateway	Tráfego interno do balanceador de carga.
1508	TCP	Todos os nós	Nó de administração primário	Tráfego interno de gerenciamento de configuração.
1511	TCP	Todos os nós	Nós de armazenamento	Tráfego interno de metadados.
5353	UDP	Todos os nós	Todos os nós	Fornece o serviço DNS multicast (mDNS) usado para alterações de IP de grade completa e para descoberta do nó de administração primário durante a instalação, expansão e recuperação. Nota: A configuração desta porta é opcional.
7001	TCP	Nós de armazenamento	Nós de armazenamento	Comunicação entre clusters de nós Cassandra TLS.

Porta	TCP ou UDP	De	Para	Detalhes
7443	TCP	Todos os nós	Nó de administração primário	Tráfego interno para instalação, expansão, recuperação, outros procedimentos de manutenção e relatórios de erros.
8011	TCP	Todos os nós	Nó de administração primário	Tráfego interno para instalação, expansão, recuperação e outros procedimentos de manutenção.
8443	TCP	Nó de administração primário	Nós de dispositivos	Tráfego interno relacionado ao procedimento do modo de manutenção.
9042	TCP	Nós de armazenamento	Nós de armazenamento	Porta do cliente Cassandra.
9999	TCP	Todos os nós	Todos os nós	Tráfego interno para múltiplos serviços. Inclui procedimentos de manutenção, métricas e atualizações de rede.
10226	TCP	Nós de armazenamento	Nó de administração primário	Usado por dispositivos StorageGRID para encaminhar pacotes do AutoSupport do E-Series SANtricity System Manager para o nó de administração principal.
10342	TCP	Todos os nós	Nó de administração primário	Tráfego interno para instalação, expansão, recuperação e outros procedimentos de manutenção.
18000	TCP	Nós de administração/armazenamento	Nós de armazenamento com ADC	Tráfego interno do serviço de conta.
18001	TCP	Nós de administração/armazenamento	Nós de armazenamento com ADC	Tráfego interno da Federação de Identidade.
18002	TCP	Nós de administração/armazenamento	Nós de armazenamento	Tráfego interno de API relacionado a protocolos de objetos.

Porta	TCP ou UDP	De	Para	Detalhes
18003	TCP	Nós de administração/armazenamento	Nós de armazenamento com ADC	Tráfego interno dos serviços de plataforma.
18017	TCP	Nós de administração/armazenamento	Nós de armazenamento	Tráfego interno do serviço Data Mover para pools de armazenamento em nuvem.
18019	TCP	Todos os nós	Todos os nós	Tráfego interno do serviço de bloco para codificação de eliminação e replicação
18082	TCP	Nós de administração/armazenamento	Nós de armazenamento	Tráfego interno relacionado ao S3.
18083	TCP	Todos os nós	Nós de armazenamento	Tráfego interno relacionado ao Swift.
18086	TCP	Todos os nós	Nós de armazenamento	Tráfego interno relacionado ao serviço LDR.
18200	TCP	Nós de administração/armazenamento	Nós de armazenamento	Estatísticas adicionais sobre solicitações de clientes.
19000	TCP	Nós de administração/armazenamento	Nós de armazenamento com ADC	Tráfego interno do serviço Keystone .

Informações relacionadas

["Comunicações externas"](#)

Comunicações externas

Os clientes precisam se comunicar com os nós da grade para ingerir e recuperar conteúdo. As portas usadas dependem dos protocolos de armazenamento de objetos escolhidos. Essas portas precisam ser acessíveis ao cliente.

Acesso restrito aos portos

Se as políticas de rede corporativa restringirem o acesso a qualquer uma das portas, você poderá fazer o seguinte:

- Usar "[pontos de extremidade do balanceador de carga](#)" para permitir acesso em portas definidas pelo usuário.
- Remapeie portas ao implantar nós. No entanto, você não deve remapear os pontos de extremidade do balanceador de carga. Veja as informações sobre o remapeamento de portas para seu nó StorageGRID :
 - "[Chaves de remapeamento de porta para StorageGRID no Red Hat Enterprise Linux](#)"
 - "[Chaves de remapeamento de porta para StorageGRID no Ubuntu ou Debian](#)"
 - "[Remapear portas para StorageGRID no VMware](#)"
 - "[Opcional: Remapear portas de rede para o dispositivo](#)"

Portas usadas para comunicações externas

A tabela a seguir mostra as portas usadas para tráfego nos nós.



Esta lista não inclui portas que podem ser configuradas como "[pontos de extremidade do balanceador de carga](#)".

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
22	TCP	SSH	Laptop de serviço	Todos os nós	Acesso SSH ou console é necessário para procedimentos com etapas de console. Opcionalmente, você pode usar a porta 2022 em vez de 22.
25	TCP	SMTP	Nós de administração	Servidor de e-mail	Usado para alertas e AutoSupport baseado em e-mail. Você pode substituir a configuração de porta padrão de 25 usando a página Servidores de e-mail.
53	TCP/UDP	DNS	Todos os nós	Servidores DNS	Usado para DNS.
67	UDP	DHCP	Todos os nós	Serviço DHCP	Usado opcionalmente para dar suporte à configuração de rede baseada em DHCP. O serviço dhclient não é executado para grades configuradas estaticamente.
68	UDP	DHCP	Serviço DHCP	Todos os nós	Usado opcionalmente para dar suporte à configuração de rede baseada em DHCP. O serviço dhclient não é executado em grades que usam endereços IP estáticos.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
80	TCP	HTTP	Navegador	Nós de administração	A porta 80 redireciona para a porta 443 para a interface do usuário do nó de administração.
80	TCP	HTTP	Navegador	Eletrodomésticos	A porta 80 redireciona para a porta 8443 para o instalador do dispositivo StorageGRID .
80	TCP	HTTP	Nós de armazenamento com ADC	AWS	Usado para mensagens de serviços de plataforma enviadas para a AWS ou outros serviços externos que usam HTTP. Os locatários podem substituir a configuração padrão da porta HTTP de 80 ao criar um ponto de extremidade.
80	TCP	HTTP	Nós de armazenamento	AWS	Solicitações de pools de armazenamento em nuvem enviadas para destinos da AWS que usam HTTP. Os administradores de grade podem substituir a configuração padrão da porta HTTP de 80 ao configurar um pool de armazenamento em nuvem.
111	TCP/UDP	RPCBind	Cliente NFS	Nós de administração	Usado pela exportação de auditoria baseada em NFS (portmap). Observação: esta porta é necessária somente se a exportação de auditoria baseada em NFS estiver habilitada. Observação: O suporte para NFS foi descontinuado e será removido em uma versão futura.
123	UDP	NTP	Nós NTP primários	NTP externo	Serviço de protocolo de tempo de rede. Os nós selecionados como fontes primárias de NTP também sincronizam os horários do relógio com as fontes externas de tempo de NTP.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
161	TCP/UDP	SNMP	Cliente SNMP	Todos os nós	Usado para pesquisa SNMP. Todos os nós fornecem informações básicas; os nós administrativos também fornecem dados de alerta. O padrão é a porta UDP 161 quando configurado. Observação: esta porta só é necessária e só é aberta no firewall do nó se o SNMP estiver configurado. Se você planeja usar SNMP, pode configurar portas alternativas. Observação: Para obter informações sobre como usar SNMP com StorageGRID, entre em contato com seu representante de conta da NetApp .
162	TCP/UDP	Notificações SNMP	Todos os nós	Destinos de notificação	Notificações SNMP de saída e traps são definidas como padrão para a porta UDP 162. Observação: esta porta só é necessária se o SNMP estiver habilitado e os destinos de notificação estiverem configurados. Se você planeja usar SNMP, pode configurar portas alternativas. Observação: Para obter informações sobre como usar SNMP com StorageGRID, entre em contato com seu representante de conta da NetApp .
389	TCP/UDP	LDAP	Nós de armazenamento com ADC	Diretório Ativo/LDAP	Usado para conectar a um servidor Active Directory ou LDAP para Federação de Identidade.
443	TCP	HTTPS	Navegador	Nós de administração	Usado por navegadores da web e clientes de API de gerenciamento para acessar o Grid Manager e o Tenant Manager. Observação: 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. Consulte "Configurar controles de firewall" para configurar endereços IP privilegiados.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
443	TCP	HTTPS	Nós de administração	Diretório ativo	Usado por nós de administração que se conectam ao Active Directory se o logon único (SSO) estiver habilitado.
443	TCP	HTTPS	Nós de armazenamento com ADC	AWS	Usado para mensagens de serviços de plataforma enviadas para a AWS ou outros serviços externos que usam HTTPS. Os locatários podem substituir a configuração de porta HTTP padrão de 443 ao criar um ponto de extremidade.
443	TCP	HTTPS	Nós de armazenamento	AWS	Solicitações de pools de armazenamento em nuvem enviadas para destinos da AWS que usam HTTPS. Os administradores de grade podem substituir a configuração padrão da porta HTTPS 443 ao configurar um pool de armazenamento em nuvem.
903	TCP	NFS	Cliente NFS	Nós de administração	Usado pela exportação de auditoria baseada em NFS(<code>rpc.mountd</code>). Observação: esta porta é necessária somente se a exportação de auditoria baseada em NFS estiver habilitada. Observação: O suporte para NFS foi descontinuado e será removido em uma versão futura.
2022	TCP	SSH	Laptop de serviço	Todos os nós	Acesso SSH ou console é necessário para procedimentos com etapas de console. Opcionalmente, você pode usar a porta 22 em vez de 2022.
2049	TCP	NFS	Cliente NFS	Nós de administração	Usado pela exportação de auditoria baseada em NFS (<code>nfs</code>). Observação: esta porta é necessária somente se a exportação de auditoria baseada em NFS estiver habilitada. Observação: O suporte para NFS foi descontinuado e será removido em uma versão futura.

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
5353	UDP	mDNS	Todos os nós	Todos os nós	Fornece o serviço DNS multicast (mDNS) usado para alterações de IP de grade completa e para descoberta do nó de administração primário durante a instalação, expansão e recuperação. Nota: A configuração desta porta é opcional.
5696	TCP	KMIP	Eletrodoméstico	KMS	Tráfego externo do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP) de dispositivos configurados para criptografia de nós para o Servidor de Gerenciamento de Chaves (KMS), a menos que uma porta diferente seja especificada na página de configuração do KMS do Instalador do Dispositivo StorageGRID .
8022	TCP	SSH	Laptop de serviço	Todos os nós	O SSH na porta 8022 concede acesso ao sistema operacional base em plataformas de dispositivos e nós virtuais para suporte e solução de problemas. Esta porta não é usada para nós baseados em Linux (bare metal) e não precisa ser acessível entre nós de grade ou durante operações normais.
8443	TCP	HTTPS	Navegador	Nós de administração	Opcional. Usado por navegadores da web e clientes de API de gerenciamento para acessar o Grid Manager. Pode ser usado para separar as comunicações do Grid Manager e do Tenant Manager. Observação: 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. Consulte "Configurar controles de firewall" para configurar endereços IP privilegiados.
8443	TCP	HTTPS	Navegador	Eletrodomésticos	Usado por navegadores da web e clientes de API de gerenciamento para acessar o instalador do StorageGRID Appliance. Observação: a porta 443 redireciona para a porta 8443 para o instalador do dispositivo StorageGRID .

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
9022	TCP	SSH	Laptop de serviço	Eletrodomésticos	Concede acesso aos dispositivos StorageGRID no modo de pré-configuração para suporte e solução de problemas. Não é necessário que esta porta esteja acessível entre nós da grade ou durante operações normais.
9091	TCP	HTTPS	Serviço externo Grafana	Nós de administração	Usado por serviços externos do Grafana para acesso seguro ao serviço StorageGRID Prometheus. Observação: esta porta é necessária somente se o acesso ao Prometheus baseado em certificado estiver habilitado.
9092	TCP	Kafka	Nós de armazenamento com ADC	Aglomerado de Kafka	Usado para mensagens de serviços de plataforma enviadas a um cluster Kafka. Os locatários podem substituir a configuração de porta padrão do Kafka de 9092 ao criar um ponto de extremidade.
9443	TCP	HTTPS	Navegador	Nós de administração	Opcional. Usado por navegadores da web e clientes de API de gerenciamento para acessar o Tenant Manager. Pode ser usado para separar as comunicações do Grid Manager e do Tenant Manager.
18082	TCP	HTTPS	Clientes S3	Nós de armazenamento	Tráfego do cliente S3 diretamente para nós de armazenamento (HTTPS).
18083	TCP	HTTPS	Clientes Swift	Nós de armazenamento	Tráfego de clientes Swift diretamente para nós de armazenamento (HTTPS).
18084	TCP	HTTP	Clientes S3	Nós de armazenamento	Tráfego do cliente S3 diretamente para nós de armazenamento (HTTP).
18085	TCP	HTTP	Clientes Swift	Nós de armazenamento	Tráfego de cliente Swift diretamente para nós de armazenamento (HTTP).

Porta	TCP ou UDP	Protocolo	De	Para	Detalhes
23000-23999	TCP	HTTPS	Todos os nós na grade de origem para replicação entre grades	Nós de administração e nós de gateway na grade de destino para replicação entre grades	Este intervalo de portas é reservado para conexões de federação de rede. Ambas as grades em uma determinada conexão usam a mesma porta.

Início rápido para StorageGRID

Siga estas etapas de alto nível para configurar e usar qualquer sistema StorageGRID .

1

Aprenda, planeje e colete dados

Trabalhe com seu representante de conta NetApp para entender as opções e planejar seu novo sistema StorageGRID . Considere estes tipos de perguntas:

- Quantos dados de objetos você espera armazenar inicialmente e ao longo do tempo?
- Quantos sites você precisa?
- Quantos e quais tipos de nós você precisa em cada site?
- Quais redes StorageGRID você usará?
- Quem usará sua grade para armazenar objetos? Quais aplicativos eles usarão?
- Você tem alguma exigência especial de segurança ou armazenamento?
- Você precisa cumprir algum requisito legal ou regulatório?

Opcionalmente, trabalhe com seu consultor de serviços profissionais da NetApp para acessar a ferramenta NetApp ConfigBuilder para concluir uma pasta de trabalho de configuração para uso ao instalar e implantar seu novo sistema. Você também pode usar esta ferramenta para ajudar a automatizar a configuração de qualquer dispositivo StorageGRID . Ver ["Automatize a instalação e a configuração do dispositivo"](#) .

Análise ["Saiba mais sobre o StorageGRID"](#) e o ["Diretrizes de rede"](#) .

2

Instalar nós

Um sistema StorageGRID consiste em nós individuais baseados em hardware e software. Primeiro, instale o hardware para cada nó do dispositivo e configure cada host Linux ou VMware.

Para concluir a instalação, instale o software StorageGRID em cada dispositivo ou host de software e conecte os nós em uma grade. Durante esta etapa, você fornece nomes de sites e nós, detalhes de sub-rede e endereços IP para seus servidores NTP e DNS.

Aprenda como:

- ["Instalar hardware do aparelho"](#)
- ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
- ["Instalar o StorageGRID no Ubuntu ou Debian"](#)
- ["Instalar o StorageGRID no VMware"](#)

3

Sign in e verifique a integridade do sistema

Assim que você instalar o nó de administração principal, você poderá fazer login no Grid Manager. A partir daí, você pode revisar a integridade geral do seu novo sistema, habilitar o AutoSupport e e-mails de alerta, além de configurar nomes de domínio de endpoint S3.

Aprenda como:

- ["Sign in no Grid Manager"](#)
- ["Monitorar a saúde do sistema"](#)
- ["Configurar AutoSupport"](#)
- ["Configurar notificações por e-mail para alertas"](#)
- ["Configurar nomes de domínio de endpoint S3"](#)

4

Configurar e gerenciar

As tarefas de configuração que você precisa executar para um novo sistema StorageGRID dependem de como você usará sua grade. No mínimo, você configura o acesso ao sistema; usa os assistentes do FabricPool e do S3; e gerencia várias configurações de armazenamento e segurança.

Aprenda como:

- ["Controle de acesso ao StorageGRID"](#)
- ["Use o assistente de configuração do S3"](#)
- ["Use o assistente de configuração do FabricPool"](#)
- ["Gerenciar segurança"](#)
- ["Endurecimento do sistema"](#)

5

Configurar ILM

Você controla o posicionamento e a duração de cada objeto no seu sistema StorageGRID configurando uma política de gerenciamento do ciclo de vida das informações (ILM) que consiste em uma ou mais regras de ILM. As regras do ILM instruem o StorageGRID sobre como criar e distribuir cópias de dados de objetos e como gerenciar essas cópias ao longo do tempo.

Aprenda como: ["Gerenciar objetos com ILM"](#)

6

Usar StorageGRID

Após a conclusão da configuração inicial, as contas de locatário do StorageGRID podem usar aplicativos cliente S3 para ingerir, recuperar e excluir objetos.

Aprenda como:

- ["Use uma conta de inquilino"](#)
- ["Use a API REST do S3"](#)

7

Monitorar e solucionar problemas

Quando seu sistema estiver funcionando, você deve monitorar suas atividades regularmente e solucionar problemas e resolver quaisquer alertas. Você também pode querer configurar um servidor syslog externo, usar monitoramento SNMP ou coletar dados adicionais.

Aprenda como:

- ["Monitorar StorageGRID"](#)
- ["Solucionar problemas do StorageGRID"](#)

8

Expandir, manter e recuperar

Você pode adicionar nós ou sites para expandir a capacidade ou a funcionalidade do seu sistema. Você também pode executar vários procedimentos de manutenção para se recuperar de falhas ou para manter seu sistema StorageGRID atualizado e com desempenho eficiente.

Aprenda como:

- ["Expandir uma grade"](#)
- ["Mantenha sua grade"](#)
- ["Recuperar nós"](#)

Instalar, atualizar e corrigir o StorageGRID

Dispositivos StorageGRID

Vá para "[Documentação do dispositivo StorageGRID](#)" para aprender como instalar, configurar e manter dispositivos de armazenamento e serviços StorageGRID .

Instalar o StorageGRID no Red Hat Enterprise Linux

Início rápido para instalar o StorageGRID no Red Hat Enterprise Linux

Siga estas etapas de alto nível para instalar um nó do Red Hat Enterprise Linux (RHEL) Linux StorageGRID .

1

Preparação

- Aprenda sobre "[Arquitetura e topologia de rede do StorageGRID](#)" .
- Aprenda sobre as especificidades de "[Rede StorageGRID](#)" .
- Reúna e prepare o "[Informações e materiais necessários](#)" .
- Prepare o necessário "[CPU e RAM](#)" .
- Prover para "[requisitos de armazenamento e desempenho](#)" .
- "[Preparar os servidores Linux](#)" que hospedará seus nós StorageGRID .

2

Implantação

Implantar nós de grade. Quando você implanta nós de grade, eles são criados como parte do sistema StorageGRID e conectados a uma ou mais redes.

- Para implantar nós de grade baseados em software nos hosts que você preparou na etapa 1, use a linha de comando do Linux e "[arquivos de configuração do nó](#)" .
- Para implantar nós do dispositivo StorageGRID , siga as instruções "[Início rápido para instalação de hardware](#)" .

3

Configuração

Quando todos os nós tiverem sido implantados, use o Grid Manager para "[configurar a grade e concluir a instalação](#)" .

Automatize a instalação

Para economizar tempo e fornecer consistência, você pode automatizar a instalação do serviço de host StorageGRID e a configuração dos nós de grade.

- Use uma estrutura de orquestração padrão, como Ansible, Puppet ou Chef para automatizar:

- Instalação do RHEL
- Configuração de rede e armazenamento
- Instalação do mecanismo de contêiner e do serviço de host StorageGRID
- Implantação de nós de grade virtual

Ver ["Automatize a instalação e a configuração do serviço de host StorageGRID"](#) .

- Depois de implantar os nós da grade, ["automatizar a configuração do sistema StorageGRID"](#) usando o script de configuração Python fornecido no arquivo de instalação.
- ["Automatize a instalação e a configuração de nós de grade de dispositivos"](#)
- Se você for um desenvolvedor avançado de implantações do StorageGRID , automatize a instalação de nós de grade usando o ["instalação REST API"](#) .

Planeje e prepare a instalação no Red Hat

Informações e materiais necessários

Antes de instalar o StorageGRID, reúna e prepare as informações e os materiais necessários.

Informações necessárias

Plano de rede

Quais redes você pretende anexar a cada nó do StorageGRID . O StorageGRID oferece suporte a várias redes para separação de tráfego, segurança e conveniência administrativa.

Veja o StorageGRID ["Diretrizes de rede"](#) .

Informações de rede

Endereços IP a serem atribuídos a cada nó da grade e os endereços IP dos servidores DNS e NTP.

Servidores para nós de grade

Identifique um conjunto de servidores (físicos, virtuais ou ambos) que, em conjunto, forneçam recursos suficientes para dar suporte ao número e ao tipo de nós StorageGRID que você planeja implantar.



Se a instalação do StorageGRID não usar nós de armazenamento do dispositivo StorageGRID (hardware), você deverá usar armazenamento RAID de hardware com cache de gravação alimentado por bateria (BBWC). O StorageGRID não oferece suporte ao uso de redes de área de armazenamento virtual (vSANs), RAID de software ou nenhuma proteção RAID.

Migração de nós (se necessário)

Entenda o ["requisitos para migração de nós"](#) , se você quiser executar manutenção programada em hosts físicos sem nenhuma interrupção de serviço.

Informações relacionadas

["Ferramenta de Matriz de Interoperabilidade da NetApp"](#)

Materiais necessários

Licença NetApp StorageGRID

Você deve ter uma licença NetApp válida e assinada digitalmente.



Uma licença de não produção, que pode ser usada para testes e prova de conceito de grades, está incluída no arquivo de instalação do StorageGRID .

Arquivo de instalação do StorageGRID

["Baixe o arquivo de instalação do StorageGRID e extraia os arquivos"](#) .

Laptop de serviço

O sistema StorageGRID é instalado por meio de um laptop de serviço.

O laptop de serviço deve ter:

- Porta de rede
- Cliente SSH (por exemplo, PuTTY)
- ["Navegador da Web compatível"](#)

Documentação do StorageGRID

- ["Notas de lançamento"](#)
- ["Instruções para administrar o StorageGRID"](#)

Baixe e extraia os arquivos de instalação do StorageGRID

Você deve baixar o arquivo de instalação do StorageGRID e extrair os arquivos necessários. Opcionalmente, você pode verificar manualmente os arquivos no pacote de instalação.

Passos

1. Vá para o ["Página de downloads da NetApp para StorageGRID"](#) .
2. Selecione o botão para baixar a versão mais recente ou selecione outra versão no menu suspenso e selecione **Ir**.
3. Sign in com o nome de usuário e a senha da sua conta NetApp .
4. Se uma declaração de Cuidado/Leitura Obrigatória aparecer, leia-a e marque a caixa de seleção.



Você deve aplicar todos os hotfixes necessários após instalar a versão do StorageGRID . Para obter mais informações, consulte o ["procedimento de hotfix nas instruções de recuperação e manutenção"](#) .

5. Leia o Contrato de Licença do Usuário Final, marque a caixa de seleção e selecione **Aceitar e Continuar**.
6. Na coluna **Instalar StorageGRID**, selecione o arquivo de instalação .tgz ou .zip do Red Hat Enterprise Linux.



Selecione o .zip arquivo se você estiver executando o Windows no laptop de serviço.

7. Salve o arquivo de instalação.

8. Se você precisar verificar o arquivo de instalação:
 - a. Baixe o pacote de verificação de assinatura de código do StorageGRID . O nome do arquivo para este pacote usa o formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , onde `<version-number>` é a versão do software StorageGRID .
 - b. Siga os passos para "[verificar manualmente os arquivos de instalação](#)" .
9. Extraia os arquivos do arquivo de instalação.
10. Escolha os arquivos que você precisa.

Os arquivos necessários dependem da topologia de grade planejada e de como você implantará seu sistema StorageGRID .



Os caminhos listados na tabela são relativos ao diretório de nível superior instalado pelo arquivo de instalação extraído

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID .
	Uma licença gratuita que não fornece nenhum direito de suporte para o produto.
	Pacote RPM para instalar as imagens do nó StorageGRID nos seus hosts RHEL.
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID .
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID .
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único estiver ativado. Você também pode usar este script para integração do Ping Federate.

Caminho e nome do arquivo	Descrição
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> roteiro.
	Exemplo de função e manual do Ansible para configurar hosts RHEL para implantação de contêiner StorageGRID . Você pode personalizar a função ou o manual conforme necessário.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado usando o Active Directory ou o Ping Federate.
	Um script auxiliar chamado pelo companheiro <code>storagegrid-ssoauth-azure.py</code> Script Python para executar interações SSO com o Azure.
	Esquemas de API para StorageGRID. Observação: antes de executar uma atualização, você pode usar esses esquemas para confirmar se qualquer código que você escreveu para usar as APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID , caso você não tenha um ambiente StorageGRID não produtivo para testes de compatibilidade de atualização.

Verificar manualmente os arquivos de instalação (opcional)

Se necessário, você pode verificar manualmente os arquivos no arquivo de instalação do StorageGRID .

Antes de começar

Você tem "[baixou o pacote de verificação](#)" do "[Página de downloads da NetApp para StorageGRID](#)" .

Passos

1. Extraia os artefatos do pacote de verificação:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Certifique-se de que esses artefatos foram extraídos:

- Certificado de folha: `Leaf-Cert.pem`
- Cadeia de certificados: `CA-Int-Cert.pem`
- Cadeia de resposta de registro de data e hora: `TS-Cert.pem`
- Arquivo de soma de verificação: `sha256sum`

- Assinatura de soma de verificação: sha256sum.sig
- Arquivo de resposta de registro de data e hora: sha256sum.sig.tsr

3. Use a cadeia para verificar se o certificado em folha é válido.

Exemplo: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Saída esperada: Leaf-Cert.pem: OK

4. Se a etapa 2 falhou devido a um certificado folha expirado, use o tsr arquivo para verificar.

Exemplo: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

A produção esperada inclui: Verification: OK

5. Crie um arquivo de chave pública a partir do certificado folha.

Exemplo: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Saída esperada: *nenhuma*

6. Use a chave pública para verificar a sha256sum arquivo contra sha256sum.sig .

Exemplo: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

Saída esperada: Verified OK

7. Verifique o sha256sum conteúdo do arquivo em relação às somas de verificação recém-criadas.

Exemplo: `sha256sum -c sha256sum`

Saída esperada: <filename>: OK

<filename> é o nome do arquivo compactado que você baixou.

8. ["Conclua as etapas restantes"](#) para extrair e escolher os arquivos apropriados do arquivo de instalação.

Requisitos de software para o Red Hat Enterprise Linux

Você pode usar uma máquina virtual para hospedar qualquer tipo de nó StorageGRID .
Você precisa de uma máquina virtual para cada nó da grade.

Para instalar o StorageGRID no Red Hat Enterprise Linux (RHEL), você precisa instalar alguns pacotes de software de terceiros. Algumas distribuições Linux suportadas não contêm esses pacotes por padrão. As versões dos pacotes de software nas quais as instalações do StorageGRID são testadas incluem aquelas listadas nesta página.

Se você selecionar uma distribuição Linux e uma opção de instalação de tempo de execução de contêiner que exija qualquer um desses pacotes, e eles não forem instalados automaticamente pela distribuição Linux, instale uma das versões listadas aqui, se disponível no seu provedor ou no fornecedor de suporte para sua distribuição Linux. Caso contrário, use as versões de pacote padrão disponíveis do seu fornecedor.

Todas as opções de instalação exigem Podman ou Docker. Não instale os dois pacotes. Instale somente o pacote necessário para sua opção de instalação.



O suporte ao Docker como mecanismo de contêiner para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contêiner em uma versão futura.

Versões do Python testadas

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

Versões do Podman testadas

- 3.2.3-0
- 3.4.4+ds1
- 4.1.1-7
- 4.2.0-11
- 4.3.1+ds1-8+b1
- 4.4.1-8
- 4.4.1-12

Versões do Docker testadas



O suporte ao Docker está obsoleto e será removido em uma versão futura.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23.0.6-1
- Docker-CE 24.0.2-1
- Docker-CE 24.0.4-1
- Docker-CE 24.0.5-1
- Docker-CE 24.0.7-1
- 1,5-2

Requisitos de CPU e RAM

Antes de instalar o software StorageGRID , verifique e configure o hardware para que ele esteja pronto para suportar o sistema StorageGRID .

Cada nó StorageGRID requer os seguintes recursos mínimos:

- Núcleos de CPU: 8 por nó
- RAM: Depende da RAM total disponível e da quantidade de software não StorageGRID em execução no sistema
 - Geralmente, pelo menos 24 GB por nó e 2 a 16 GB a menos que a RAM total do sistema
 - Um mínimo de 64 GB para cada locatário que terá aproximadamente 5.000 buckets

Os recursos de nós somente de metadados baseados em software devem corresponder aos recursos de nós de armazenamento existentes. Por exemplo:

- Se o site StorageGRID existente estiver usando dispositivos SG6000 ou SG6100, os nós somente de metadados baseados em software deverão atender aos seguintes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - 8 TB SSD ou armazenamento equivalente para o banco de dados Cassandra (rangedb/0)
- Se o site StorageGRID existente estiver usando nós de armazenamento virtuais com 24 GB de RAM, CPU de 8 núcleos e 3 TB ou 4 TB de armazenamento de metadados, os nós somente de metadados baseados em software deverão usar recursos semelhantes (24 GB de RAM, CPU de 8 núcleos e 4 TB de armazenamento de metadados (rangedb/0)).

Ao adicionar um novo site StorageGRID , a capacidade total de metadados do novo site deve, no mínimo, corresponder aos sites StorageGRID existentes e os novos recursos do site devem corresponder aos nós de armazenamento nos sites StorageGRID existentes.

Certifique-se de que o número de nós StorageGRID que você planeja executar em cada host físico ou virtual não exceda o número de núcleos de CPU ou a RAM física disponível. Se os hosts não forem dedicados à execução do StorageGRID (não recomendado), considere os requisitos de recursos dos outros aplicativos.



Monitore o uso da CPU e da memória regularmente para garantir que esses recursos continuem acomodando sua carga de trabalho. Por exemplo, dobrar a alocação de RAM e CPU para nós de armazenamento virtuais forneceria recursos semelhantes aos fornecidos para nós de dispositivos StorageGRID . Além disso, se a quantidade de metadados por nó exceder 500 GB, considere aumentar a RAM por nó para 48 GB ou mais. Para obter informações sobre como gerenciar o armazenamento de metadados de objetos, aumentar a configuração do Espaço Reservado de Metadados e monitorar o uso da CPU e da memória, consulte as instruções para ["administrando"](#) , ["monitoramento"](#) , e ["atualizando"](#) StorageGRID.

Se o hyperthreading estiver habilitado nos hosts físicos subjacentes, você poderá fornecer 8 núcleos virtuais (4 núcleos físicos) por nó. Se o hyperthreading não estiver habilitado nos hosts físicos subjacentes, você deverá fornecer 8 núcleos físicos por nó.

Se você estiver usando máquinas virtuais como hosts e tiver controle sobre o tamanho e o número de VMs, use uma única VM para cada nó do StorageGRID e dimensione a VM adequadamente.

Para implantações de produção, você não deve executar vários nós de armazenamento no mesmo hardware

de armazenamento físico ou host virtual. Cada nó de armazenamento em uma única implantação do StorageGRID deve estar em seu próprio domínio de falha isolado. Você pode maximizar a durabilidade e a disponibilidade dos dados do objeto se garantir que uma única falha de hardware possa afetar apenas um único nó de armazenamento.

Veja também ["Requisitos de armazenamento e desempenho"](#) .

Requisitos de armazenamento e desempenho

Você deve entender os requisitos de armazenamento para os nós do StorageGRID para poder fornecer espaço suficiente para dar suporte à configuração inicial e à futura expansão do armazenamento.

Os nós do StorageGRID exigem três categorias lógicas de armazenamento:

- **Pool de contêineres** — Armazenamento de nível de desempenho (SAS ou SSD de 10K) para os contêineres de nós, que será atribuído ao driver de armazenamento do mecanismo de contêiner quando você instalar e configurar o mecanismo de contêiner nos hosts que darão suporte aos seus nós do StorageGRID .
- **Dados do sistema** — Armazenamento em nível de desempenho (SAS ou SSD de 10K) para armazenamento persistente por nó de dados do sistema e logs de transações, que os serviços do host StorageGRID consumirão e mapearão em nós individuais.
- **Dados de objeto** — Armazenamento em nível de desempenho (10K SAS ou SSD) e armazenamento em massa em nível de capacidade (NL-SAS/SATA) para armazenamento persistente de dados de objeto e metadados de objeto.

Você deve usar dispositivos de bloco com suporte RAID para todas as categorias de armazenamento. Discos não redundantes, SSDs ou JBODs não são suportados. Você pode usar armazenamento RAID compartilhado ou local para qualquer uma das categorias de armazenamento; no entanto, se quiser usar o recurso de migração de nós no StorageGRID, você deve armazenar dados do sistema e dados de objeto no armazenamento compartilhado. Para obter mais informações, consulte ["Requisitos de migração do contêiner de nó"](#) .

Requisitos de desempenho

O desempenho dos volumes usados para o pool de contêineres, dados do sistema e metadados de objetos impacta significativamente o desempenho geral do sistema. Você deve usar armazenamento de nível de desempenho (SAS ou SSD de 10K) para esses volumes para garantir desempenho de disco adequado em termos de latência, operações de entrada/saída por segundo (IOPS) e taxa de transferência. Você pode usar armazenamento em camadas de capacidade (NL-SAS/SATA) para armazenamento persistente de dados de objetos.

Os volumes usados para o pool de contêineres, dados do sistema e dados do objeto devem ter o cache de write-back habilitado. O cache deve estar em uma mídia protegida ou persistente.

Requisitos para hosts que usam armazenamento NetApp ONTAP

Se o nó StorageGRID usar armazenamento atribuído de um sistema NetApp ONTAP , confirme se o volume não tem 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.

Número de hosts necessários

Cada site StorageGRID requer no mínimo três nós de armazenamento.



Em uma implantação de produção, não execute mais de um nó de armazenamento em um único host físico ou virtual. Usar um host dedicado para cada nó de armazenamento fornece um domínio de falha isolado.

Outros tipos de nós, como nós de administração ou nós de gateway, podem ser implantados nos mesmos hosts ou em seus próprios hosts dedicados, conforme necessário.

Número de volumes de armazenamento para cada host

A tabela a seguir mostra o número de volumes de armazenamento (LUNs) necessários para cada host e o tamanho mínimo necessário para cada LUN, com base em quais nós serão implantados naquele host.

O tamanho máximo do LUN testado é 39 TB.



Esses números são para cada host, não para toda a grade.

Finalidade do LUN	Categoria de armazenamento	Número de LUNs	Tamanho mínimo/LUN
Piscina de armazenamento de motores de contêineres	Piscina de contêineres	1	Número total de nós × 100 GB
`/var/local` volume	Dados do sistema	1 para cada nó neste host	90 GB
Nó de armazenamento	Dados do objeto	3 para cada nó de armazenamento neste host Observação: Um nó de armazenamento baseado em software pode ter de 1 a 48 volumes de armazenamento; pelo menos 3 volumes de armazenamento são recomendados.	12 TB (4 TB/LUN) Veja Requisitos de armazenamento para nós de armazenamento para mais informações.

Finalidade do LUN	Categoria de armazenamento	Número de LUNs	Tamanho mínimo/LUN
Nó de armazenamento (somente metadados)	Metadados do objeto	1	4 TB Veja Requisitos de armazenamento para nós de armazenamento para mais informações. Observação: somente um rangedb é necessário para nós de armazenamento somente de metadados.
Logs de auditoria do nó de administração	Dados do sistema	1 para cada nó de administração neste host	200 GB
Tabelas do nó de administração	Dados do sistema	1 para cada nó de administração neste host	200 GB



Dependendo do nível de auditoria configurado, do tamanho das entradas do usuário, como o nome da chave do objeto S3, e da quantidade de dados de log de auditoria que você precisa preservar, pode ser necessário aumentar o tamanho do LUN do log de auditoria em cada nó de administração. Geralmente, uma grade gera aproximadamente 1 KB de dados de auditoria por operação S3, o que significa que um LUN de 200 GB suportaria 70 milhões de operações por dia ou 800 operações por segundo durante dois a três dias.

Espaço mínimo de armazenamento para um host

A tabela a seguir mostra o espaço mínimo de armazenamento necessário para cada tipo de nó. Você pode usar esta tabela para determinar a quantidade mínima de armazenamento que deve fornecer ao host em cada categoria de armazenamento, com base em quais nós serão implantados naquele host.



Snapshots de disco não podem ser usados para restaurar nós de grade. Em vez disso, consulte o ["recuperação de nós de grade"](#) procedimentos para cada tipo de nó.

Tipo de nó	Piscina de contêineres	Dados do sistema	Dados do objeto
Nó de armazenamento	100 GB	90 GB	4.000 GB
Nó de administração	100 GB	490 GB (3 LUNs)	<i>não aplicável</i>
Nó de gateway	100 GB	90 GB	<i>não aplicável</i>

Exemplo: Calculando os requisitos de armazenamento para um host

Suponha que você planeja implantar três nós no mesmo host: um nó de armazenamento, um nó de administração e um nó de gateway. Você deve fornecer no mínimo nove volumes de armazenamento ao host. Você precisará de no mínimo 300 GB de armazenamento de nível de desempenho para os contêineres de nós, 670 GB de armazenamento de nível de desempenho para dados do sistema e logs de transações e 12

TB de armazenamento de nível de capacidade para dados de objetos.

Tipo de nó	Finalidade do LUN	Número de LUNs	Tamanho da LUN
Nó de armazenamento	Piscina de armazenamento de motores de contêineres	1	300 GB (100 GB/nó)
Nó de armazenamento	`/var/local` volume	1	90 GB
Nó de armazenamento	Dados do objeto	3	12 TB (4 TB/LUN)
Nó de administração	`/var/local` volume	1	90 GB
Nó de administração	Logs de auditoria do nó de administração	1	200 GB
Nó de administração	Tabelas do nó de administração	1	200 GB
Nó de gateway	`/var/local` volume	1	90 GB
Total		9	Pool de contêineres: 300 GB Dados do sistema: 670 GB Dados do objeto: 12.000 GB

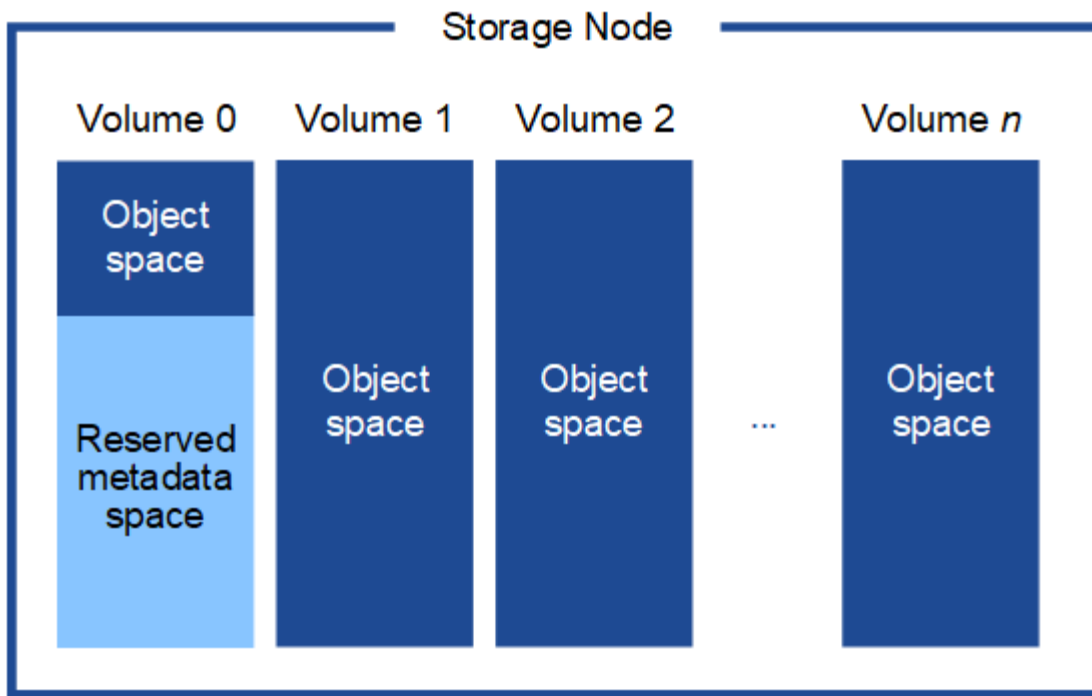
Requisitos de armazenamento para nós de armazenamento

Um nó de armazenamento baseado em software pode ter de 1 a 48 volumes de armazenamento; 3 ou mais volumes de armazenamento são recomendados. Cada volume de armazenamento deve ter 4 TB ou mais.



Um nó de armazenamento de dispositivo também pode ter até 48 volumes de armazenamento.

Conforme mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de armazenamento 0 de cada nó de armazenamento. Qualquer espaço restante no volume de armazenamento 0 e quaisquer outros volumes de armazenamento no Nó de Armazenamento são usados exclusivamente para dados de 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. As três cópias dos metadados do objeto são distribuídas uniformemente entre todos os nós de armazenamento em cada site.

Ao instalar uma grade com nós de armazenamento somente de metadados, a grade também deve conter um número mínimo de nós para armazenamento de objetos. Ver "[Tipos de nós de armazenamento](#)" para obter mais informações sobre nós de armazenamento somente de metadados.

- Para uma grade de site único, pelo menos dois nós de armazenamento são configurados para objetos e metadados.
- Para uma grade de vários sites, pelo menos um nó de armazenamento por site é configurado para objetos e metadados.

Ao atribuir espaço ao volume 0 de um novo Nó de Armazenamento, você deve garantir que haja espaço adequado para a parte desse nó de todos os metadados do objeto.

- No mínimo, você deve atribuir pelo menos 4 TB ao volume 0.



Se você usar apenas um volume de armazenamento para um Nó de Armazenamento e atribuir 4 TB ou menos ao volume, o Nó de Armazenamento poderá entrar no estado somente leitura de armazenamento na inicialização e armazenar apenas metadados de objetos.



Se você atribuir menos de 500 GB ao volume 0 (somente para uso não produtivo), 10% da capacidade do volume de armazenamento será reservada para metadados.

- Os recursos de nós somente de metadados baseados em software devem corresponder aos recursos de nós de armazenamento existentes. Por exemplo:
 - Se o site StorageGRID existente estiver usando dispositivos SG6000 ou SG6100, os nós somente de metadados baseados em software deverão atender aos seguintes requisitos mínimos:
 - 128 GB de RAM

- CPU de 8 núcleos
- 8 TB SSD ou armazenamento equivalente para o banco de dados Cassandra (rangedb/0)
- Se o site StorageGRID existente estiver usando nós de armazenamento virtuais com 24 GB de RAM, CPU de 8 núcleos e 3 TB ou 4 TB de armazenamento de metadados, os nós somente de metadados baseados em software deverão usar recursos semelhantes (24 GB de RAM, CPU de 8 núcleos e 4 TB de armazenamento de metadados (rangedb/0)).

Ao adicionar um novo site StorageGRID , a capacidade total de metadados do novo site deve, no mínimo, corresponder aos sites StorageGRID existentes e os novos recursos do site devem corresponder aos nós de armazenamento nos sites StorageGRID existentes.

- Se você estiver instalando um novo sistema (StorageGRID 11.6 ou superior) e cada nó de armazenamento tiver 128 GB ou mais de RAM, atribua 8 TB ou mais ao volume 0. Usar um valor maior para o volume 0 pode aumentar o espaço permitido para metadados em cada nó de armazenamento.
- Ao configurar diferentes nós de armazenamento para um site, use a mesma configuração para o volume 0, se possível. Se um site contiver nós de armazenamento de tamanhos diferentes, o nó de armazenamento com o menor volume 0 determinará a capacidade de metadados desse site.

Para mais detalhes, acesse "[Gerenciar armazenamento de metadados de objetos](#)".

Requisitos de migração do contêiner de nó

O recurso de migração de nós permite que você mova manualmente um nó de um host para outro. Normalmente, ambos os hosts estão no mesmo data center físico.

A migração de nós permite que você execute a manutenção do host físico sem interromper as operações da rede. Você move todos os nós do StorageGRID , um de cada vez, para outro host antes de colocar o host físico offline. A migração de nós requer apenas um curto período de inatividade para cada nó e não deve afetar a operação ou a disponibilidade dos serviços de rede.

Se você quiser usar o recurso de migração de nós do StorageGRID , sua implantação deverá atender a requisitos adicionais:

- Nomes de interface de rede consistentes em hosts em um único data center físico
- Armazenamento compartilhado para metadados do StorageGRID e volumes de repositório de objetos que podem ser acessados por todos os hosts em um único data center físico. Por exemplo, você pode usar matrizes de armazenamento NetApp E-Series.

Se você estiver usando hosts virtuais e a camada do hipervisor subjacente oferecer suporte à migração de VM, talvez seja interessante usar esse recurso em vez do recurso de migração de nós no StorageGRID. Nesse caso, você pode ignorar esses requisitos adicionais.

Antes de executar a migração ou a manutenção do hipervisor, desligue os nós corretamente. Veja as instruções para "[desligando um nó de grade](#)".

VMware Live Migration não suportado

Ao executar a instalação bare-metal em VMs VMware, o OpenStack Live Migration e o VMware live vMotion fazem com que o tempo do relógio da máquina virtual salte e não são suportados para nós de grade de nenhum tipo. Embora raros, horários incorretos podem resultar em perda de dados ou atualizações de configuração.

A migração fria é suportada. Na migração a frio, você desliga os nós do StorageGRID antes de migrá-los entre

hosts. Veja as instruções para ["desligando um nó de grade"](#) .

Nomes de interface de rede consistentes

Para mover um nó de um host para outro, o serviço de host StorageGRID precisa ter alguma confiança de que a conectividade de rede externa que o nó tem em seu local atual pode ser duplicada no novo local. Ele obtém essa confiança por meio do uso de nomes de interface de rede consistentes nos hosts.

Suponha, por exemplo, que o StorageGRID NodeA em execução no Host1 tenha sido configurado com os seguintes mapeamentos de interface:

eth0 ➔ **bond0.1001**

eth1 ➔ **bond0.1002**

eth2 ➔ **bond0.1003**

O lado esquerdo das setas corresponde às interfaces tradicionais visualizadas de dentro de um contêiner StorageGRID (ou seja, as interfaces Grid, Admin e Client Network, respectivamente). O lado direito das setas corresponde às interfaces de host reais que fornecem essas redes, que são três interfaces VLAN subordinadas ao mesmo vínculo de interface física.

Agora, suponha que você queira migrar o NodeA para o Host2. Se o Host2 também tiver interfaces denominadas bond0.1001, bond0.1002 e bond0.1003, o sistema permitirá a movimentação, supondo que as interfaces com nomes semelhantes fornecerão a mesma conectividade no Host2 que no Host1. Se o Host2 não tiver interfaces com os mesmos nomes, a movimentação não será permitida.

Existem muitas maneiras de obter uma nomenclatura de interface de rede consistente em vários hosts; consulte ["Configurando a rede host"](#) para alguns exemplos.

Armazenamento compartilhado

Para obter migrações de nós rápidas e com baixa sobrecarga, o recurso de migração de nós do StorageGRID não move fisicamente os dados dos nós. Em vez disso, a migração de nós é realizada como um par de operações de exportação e importação, da seguinte maneira:

1. Durante a operação de "exportação de nó", uma pequena quantidade de dados de estado persistentes é extraída do contêiner de nó em execução no HostA e armazenada em cache no volume de dados do sistema desse nó. Em seguida, o contêiner do nó no HostA é desinstanciado.
2. Durante a operação "importação de nó", o contêiner de nó no HostB que usa a mesma interface de rede e mapeamentos de armazenamento em bloco que estavam em vigor no HostA é instanciado. Em seguida, os dados de estado persistentes armazenados em cache são inseridos na nova instância.

Dado esse modo de operação, todos os dados do sistema e volumes de armazenamento de objetos do nó devem ser acessíveis tanto do HostA quanto do HostB para que a migração seja permitida e funcione. Além disso, eles devem ter sido mapeados no nó usando nomes que certamente fazem referência aos mesmos LUNs no HostA e no HostB.

O exemplo a seguir mostra uma solução para mapeamento de dispositivo de bloco para um nó de armazenamento StorageGRID , onde o multipathing DM está em uso nos hosts e o campo alias foi usado em `/etc/multipath.conf` para fornecer nomes de dispositivos de bloco consistentes e amigáveis disponíveis

em todos os hosts.

`/var/local` → `/dev/mapper/sgws-sn1-var-local`
`rangedb0` → `/dev/mapper/sgws-sn1-rangedb0`
`rangedb1` → `/dev/mapper/sgws-sn1-rangedb1`
`rangedb2` → `/dev/mapper/sgws-sn1-rangedb2`
`rangedb3` → `/dev/mapper/sgws-sn1-rangedb3`

Preparar os anfitriões (Red Hat)

Como as configurações de todo o host mudam durante a instalação

Em sistemas bare metal, o StorageGRID faz algumas alterações em todo o host `sysctl` configurações.

As seguintes alterações são feitas:

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
```

```

# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

```



```
# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Instalar Linux

Você deve instalar o StorageGRID em todos os hosts de grade do Red Hat Enterprise Linux. Para obter uma lista de versões suportadas, use a NetApp Interoperability Matrix Tool.

Antes de começar

Certifique-se de que seu sistema operacional atenda aos requisitos mínimos de versão do kernel do StorageGRID, conforme listado abaixo. Use o comando `uname -r` para obter a versão do kernel do seu sistema operacional ou consulte o fornecedor do seu sistema operacional.

Versão do Red Hat Enterprise Linux	Versão mínima do kernel	Nome do pacote do kernel
8.8 (obsoleto)	4.18.0-477.10.1.el8_8.x86_64	kernel-4.18.0-477.10.1.el8_8.x86_64
8,10	4.18.0-553.el8_10.x86_64	kernel-4.18.0-553.el8_10.x86_64
9.0 (obsoleto)	5.14.0-70.22.1.el9_0.x86_64	kernel-5.14.0-70.22.1.el9_0.x86_64
9.2 (obsoleto)	5.14.0-284.11.1.el9_2.x86_64	kernel-5.14.0-284.11.1.el9_2.x86_64
9,4	5.14.0-427.18.1.el9_4.x86_64	kernel-5.14.0-427.18.1.el9_4.x86_64
9,6	5.14.0-570.18.1.el9_6.x86_64	kernel-5.14.0-570.18.1.el9_6.x86_64

Passos

1. Instale o Linux em todos os hosts de grade físicos ou virtuais de acordo com as instruções do distribuidor ou seu procedimento padrão.



Se você estiver usando o instalador padrão do Linux, selecione a configuração de software "nó de computação", se disponível, ou o ambiente base "instalação mínima". Não instale nenhum ambiente de área de trabalho gráfico.

2. Certifique-se de que todos os hosts tenham acesso aos repositórios de pacotes, incluindo o canal Extras.

Você pode precisar desses pacotes adicionais mais tarde neste procedimento de instalação.

3. Se a troca estiver habilitada:

- a. Execute o seguinte comando: `$ sudo swapoff --all`
- b. Remova todas as entradas de swap de `/etc/fstab` para persistir as configurações.



Não desabilitar completamente a troca pode reduzir severamente o desempenho.

Configurar a rede do host (Red Hat Enterprise Linux)

Após concluir a instalação do Linux em seus hosts, talvez seja necessário executar alguma configuração adicional para preparar um conjunto de interfaces de rede em cada host que sejam adequadas para mapeamento nos nós do StorageGRID que você implantará posteriormente.

Antes de começar

- Você revisou o ["Diretrizes de rede StorageGRID"](#) .
- Você revisou as informações sobre ["requisitos de migração do contêiner de nó"](#) .
- Se você estiver usando hosts virtuais, você leu [o considerações e recomendações para clonagem de endereços MAC](#) antes de configurar a rede host.



Se estiver usando VMs como hosts, você deve selecionar VMXNET 3 como o adaptador de rede virtual. O adaptador de rede VMware E1000 causou problemas de conectividade com contêineres StorageGRID implantados em determinadas distribuições do Linux.

Sobre esta tarefa

Os nós da grade devem ser capazes de acessar a Rede da Grade e, opcionalmente, as Redes de Administração e Cliente. Você fornece esse acesso criando mapeamentos que associam a interface física do host às interfaces virtuais de cada nó da grade. Ao criar interfaces de host, use nomes amigáveis para facilitar a implantação em todos os hosts e permitir a migração.

A mesma interface pode ser compartilhada entre o host e um ou mais nós. Por exemplo, você pode usar a mesma interface para acesso ao host e acesso à rede de administração do nó, para facilitar a manutenção do host e do nó. Embora a mesma interface possa ser compartilhada entre o host e nós individuais, todos devem ter endereços IP diferentes. Endereços IP não podem ser compartilhados entre nós ou entre o host e qualquer nó.

Você pode usar a mesma interface de rede do host para fornecer a interface Grid Network para todos os nós StorageGRID no host; você pode usar uma interface de rede do host diferente para cada nó; ou pode fazer algo intermediário. No entanto, normalmente você não forneceria a mesma interface de rede de host que as interfaces de rede de grade e de administração para um único nó, ou como a interface de rede de grade para um nó e a interface de rede de cliente para outro.

Você pode concluir esta tarefa de muitas maneiras. Por exemplo, se seus hosts forem máquinas virtuais e você estiver implantando um ou dois nós StorageGRID para cada host, poderá criar o número correto de interfaces de rede no hipervisor e usar um mapeamento 1 para 1. Se você estiver implantando vários nós em hosts bare metal para uso em produção, poderá aproveitar o suporte da pilha de rede Linux para VLAN e LACP para tolerância a falhas e compartilhamento de largura de banda. As seções a seguir fornecem abordagens detalhadas para ambos os exemplos. Você não precisa usar nenhum desses exemplos; você pode usar qualquer abordagem que atenda às suas necessidades.



Não use dispositivos de ligação ou ponte diretamente como interface de rede do contêiner. Isso pode impedir a inicialização do nó causada por um problema de kernel com o uso de MACVLAN com dispositivos de ligação e ponte no namespace do contêiner. Em vez disso, use um dispositivo sem vínculo, como um par VLAN ou Ethernet virtual (veth). Especifique este dispositivo como a interface de rede no arquivo de configuração do nó.

Informações relacionadas

["Criando arquivos de configuração de nó"](#)

Considerações e recomendações para clonagem de endereços MAC

A clonagem de endereço MAC faz com que o contêiner use o endereço MAC do host, e o host use o endereço MAC de um endereço especificado por você ou de um gerado aleatoriamente. Você deve usar a clonagem de endereço MAC para evitar o uso de configurações de rede em modo promíscuo.

Habilitando a clonagem de MAC

Em certos ambientes, a segurança pode ser aprimorada por meio da clonagem de endereços MAC, pois ela permite que você use uma NIC virtual dedicada para a rede de administração, a rede de grade e a rede de cliente. Fazer com que o contêiner use o endereço MAC da NIC dedicada no host permite que você evite o uso de configurações de rede em modo promíscuo.



A clonagem de endereço MAC deve ser usada com instalações de servidores virtuais e pode não funcionar corretamente com todas as configurações de dispositivos físicos.



Se um nó não iniciar devido a uma interface de destino de clonagem de MAC estar ocupada, talvez seja necessário definir o link como "inativo" antes de iniciar o nó. Além disso, é possível que o ambiente virtual impeça a clonagem de MAC em uma interface de rede enquanto o link estiver ativo. Se um nó não conseguir definir o endereço MAC e iniciar devido a uma interface estar ocupada, definir o link como "inativo" antes de iniciar o nó pode resolver o problema.

A clonagem de endereço MAC é desabilitada por padrão e deve ser definida pelas chaves de configuração do nó. Você deve habilitá-lo ao instalar o StorageGRID.

Existe uma chave para cada rede:

- ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC
- GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC
- CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Definir a chave como "true" faz com que o contêiner use o endereço MAC da NIC do host. Além disso, o host usará o endereço MAC da rede de contêineres especificada. Por padrão, o endereço do contêiner é um endereço gerado aleatoriamente, mas se você tiver definido um usando o `_NETWORK_MAC` chave de configuração do nó, esse endereço é usado em seu lugar. O host e o contêiner sempre terão endereços MAC diferentes.



Habilitar a clonagem de MAC em um host virtual sem também habilitar o modo promíscuo no hipervisor pode fazer com que a rede do host Linux que usa a interface do host pare de funcionar.

Casos de uso de clonagem de MAC

Há dois casos de uso a serem considerados com a clonagem de MAC:

- Clonagem de MAC não habilitada: Quando o `_CLONE_MAC` a chave no arquivo de configuração do nó não estiver definida ou definida como "false", o host usará o MAC da NIC do host e o contêiner terá um MAC

gerado StorageGRID, a menos que um MAC seja especificado no `_NETWORK_MAC` chave. Se um endereço for definido no `_NETWORK_MAC` chave, o contêiner terá o endereço especificado na `_NETWORK_MAC` chave. Esta configuração de chaves requer o uso do modo promíscuo.

- Clonagem de MAC habilitada: Quando o `_CLONE_MAC` a chave no arquivo de configuração do nó for definida como "true", o contêiner usa o MAC da NIC do host e o host usa um MAC gerado StorageGRID, a menos que um MAC seja especificado no `_NETWORK_MAC` chave. Se um endereço for definido no `_NETWORK_MAC` chave, o host usa o endereço especificado em vez de um gerado. Nesta configuração de chaves, você não deve usar o modo promíscuo.



Se você não quiser usar a clonagem de endereço MAC e preferir permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes daqueles atribuídos pelo hipervisor, certifique-se de que as propriedades de segurança nos níveis de switch virtual e grupo de portas estejam definidas como **Aceitar** para Modo Promíscuo, Alterações de Endereço MAC e Transmissões Falsificadas. Os valores definidos no switch virtual podem ser substituídos pelos valores no nível do grupo de portas, portanto, certifique-se de que as configurações sejam as mesmas em ambos os locais.

Para habilitar a clonagem de MAC, consulte o "[instruções para criar arquivos de configuração de nó](#)".

Exemplo de clonagem de MAC

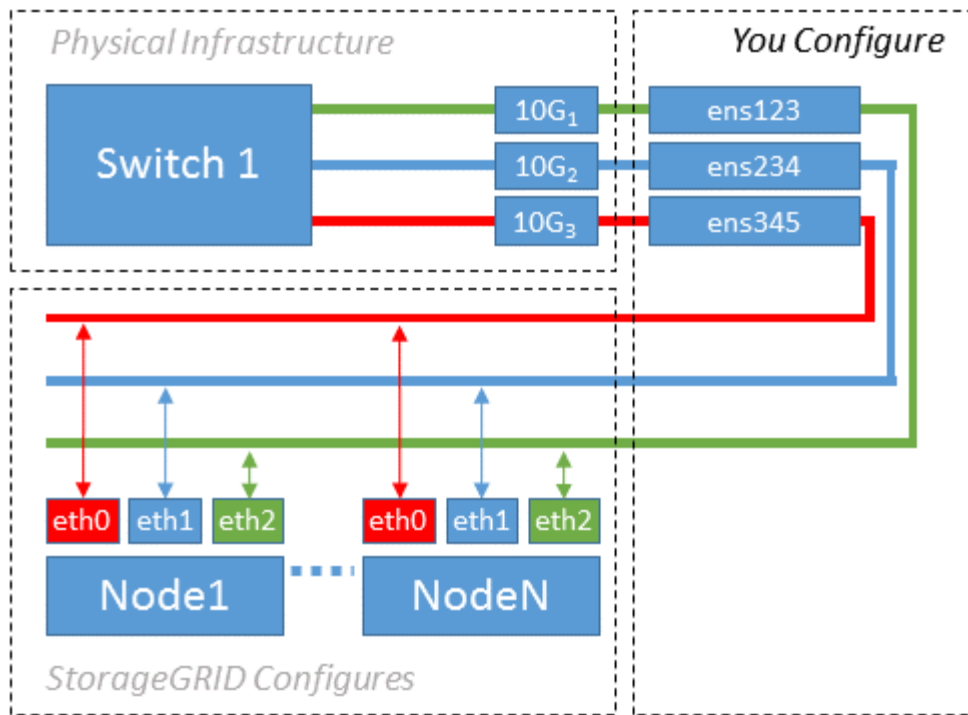
Exemplo de clonagem de MAC habilitada com um host com endereço MAC de 11:22:33:44:55:66 para a interface `ens256` e as seguintes chaves no arquivo de configuração do nó:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Resultado: o MAC do host para `ens256` é `b2:9c:02:c2:27:10` e o MAC da rede de administração é `11:22:33:44:55:66`

Exemplo 1: mapeamento 1 para 1 para NICs físicas ou virtuais

O Exemplo 1 descreve um mapeamento de interface física simples que requer pouca ou nenhuma configuração do lado do host.



O sistema operacional Linux cria o `ensXYZ` interfaces automaticamente durante a instalação ou inicialização, ou quando as interfaces são adicionadas a quente. Nenhuma configuração é necessária além de garantir que as interfaces estejam definidas para serem ativadas automaticamente após a inicialização. Você tem que determinar qual `ensXYZ` corresponde a qual rede StorageGRID (Grid, Admin ou Client) para que você possa fornecer os mapeamentos corretos posteriormente no processo de configuração.

Observe que a figura mostra vários nós StorageGRID ; no entanto, você normalmente usaria essa configuração para VMs de nó único.

Se o Switch 1 for um switch físico, você deverá configurar as portas conectadas às interfaces 10G1 a 10G3 para o modo de acesso e colocá-las nas VLANs apropriadas.

Exemplo 2: VLANs transportando vínculo LACP

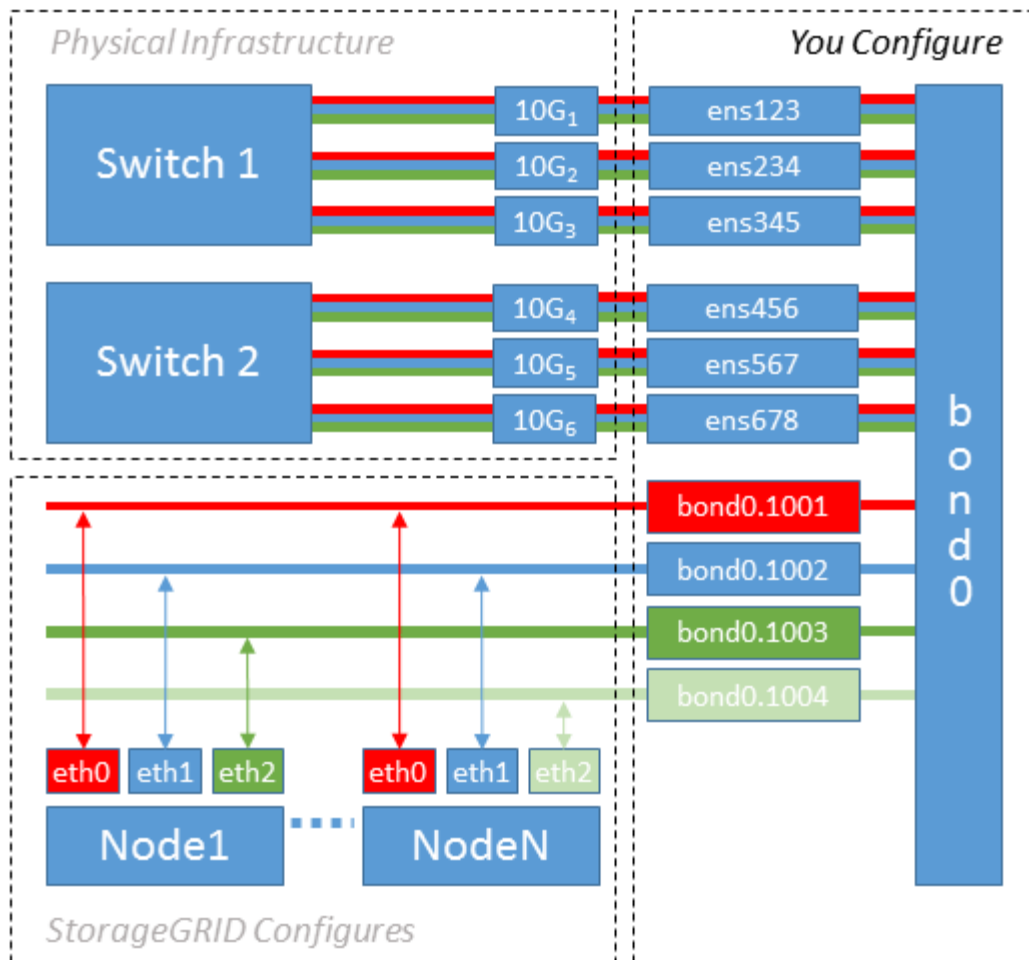
Sobre esta tarefa

O Exemplo 2 pressupõe que você esteja familiarizado com a vinculação de interfaces de rede e com a criação de interfaces VLAN na distribuição Linux que está usando.

O Exemplo 2 descreve um esquema genérico e flexível baseado em VLAN que facilita o compartilhamento de toda a largura de banda de rede disponível entre todos os nós em um único host. Este exemplo é particularmente aplicável a hosts bare metal.

Para entender este exemplo, suponha que você tenha três sub-redes separadas para as redes Grid, Admin e Client em cada data center. As sub-redes estão em VLANs separadas (1001, 1002 e 1003) e são apresentadas ao host em uma porta de tronco vinculada ao LACP (`bond0`). Você configuraria três interfaces VLAN no bond: `bond0.1001`, `bond0.1002` e `bond0.1003`.

Se você precisar de VLANs e sub-redes separadas para redes de nós no mesmo host, poderá adicionar interfaces de VLAN no vínculo e mapeá-las no host (mostrado como `bond0.1004` na ilustração).



Passos

1. Agregue todas as interfaces de rede física que serão usadas para conectividade de rede StorageGRID em um único vínculo LACP.

Use o mesmo nome para o vínculo em todos os hosts. Por exemplo, `bond0`.

2. Crie interfaces VLAN que usem esse vínculo como seu "dispositivo físico" associado, usando a convenção de nomenclatura de interface VLAN padrão `physdev-name.VLAN ID`.

Observe que as etapas 1 e 2 exigem configuração apropriada nos switches de borda que terminam as outras extremidades dos links de rede. As portas do switch de borda também devem ser agregadas em um canal de porta LACP, configuradas como um tronco e autorizadas a passar todas as VLANs necessárias.

São fornecidos arquivos de configuração de interface de exemplo para este esquema de configuração de rede por host.

Informações relacionadas

["Exemplo /etc/sysconfig/network-scripts"](#)

Configurar armazenamento do host

Você deve alocar volumes de armazenamento em bloco para cada host.

Antes de começar

Você revisou os seguintes tópicos, que fornecem as informações necessárias para realizar esta tarefa:

- ["Requisitos de armazenamento e desempenho"](#)
- ["Requisitos de migração do contêiner de nó"](#)

Sobre esta tarefa

Ao alocar volumes de armazenamento em bloco (LUNs) para hosts, use as tabelas em "Requisitos de armazenamento" para determinar o seguinte:

- Número de volumes necessários para cada host (com base no número e nos tipos de nós que serão implantados naquele host)
- Categoria de armazenamento para cada volume (ou seja, Dados do Sistema ou Dados do Objeto)
- Tamanho de cada volume

Você usará essas informações, bem como o nome persistente atribuído pelo Linux a cada volume físico ao implantar nós StorageGRID no host.



Você não precisa particionar, formatar ou montar nenhum desses volumes; você só precisa garantir que eles estejam visíveis para os hosts.



Somente um LUN de dados de objeto é necessário para nós de armazenamento somente de metadados.

Evite usar arquivos de dispositivos especiais "brutos" (`/dev/sdb`, por exemplo) ao compor sua lista de nomes de volumes. Esses arquivos podem mudar durante as reinicializações do host, o que afetará a operação correta do sistema. Se você estiver usando iSCSI LUNs e Device Mapper Multipathing, considere usar aliases multipath no `/dev/mapper` diretório, especialmente se sua topologia SAN incluir caminhos de rede redundantes para o armazenamento compartilhado. Alternativamente, você pode usar os softlinks criados pelo sistema em `/dev/disk/by-path/` para seus nomes de dispositivos persistentes.

Por exemplo:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Os resultados serão diferentes para cada instalação.

Atribua nomes amigáveis a cada um desses volumes de armazenamento em bloco para simplificar a instalação inicial do StorageGRID e os procedimentos futuros de manutenção. Se você estiver usando o driver multipath do mapeador de dispositivos para acesso redundante a volumes de armazenamento compartilhado, poderá usar o `alias` campo em seu `/etc/multipath.conf` arquivo.

Por exemplo:


```

multipaths {
    multipath {
        wwid 3600a09800059d6df00005df2573c2c30
        alias docker-storage-volume-hostA
    }
    multipath {
        wwid 3600a09800059d6df00005df3573c2c30
        alias sgws-adml-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df4573c2c30
        alias sgws-adml-audit-logs
    }
    multipath {
        wwid 3600a09800059d6df00005df5573c2c30
        alias sgws-adml-tables
    }
    multipath {
        wwid 3600a09800059d6df00005df6573c2c30
        alias sgws-gw1-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df7573c2c30
        alias sgws-sn1-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df7573c2c30
        alias sgws-sn1-rangedb-0
    }
    ...
}

```

Usar o campo de alias dessa forma faz com que os aliases apareçam como dispositivos de bloco no /dev/mapper diretório no host, permitindo que você especifique um nome amigável e facilmente validado sempre que uma operação de configuração ou manutenção exigir a especificação de um volume de armazenamento em bloco.



Se você estiver configurando o armazenamento compartilhado para oferecer suporte à migração de nós do StorageGRID e usar o Device Mapper Multipathing, você pode criar e instalar um /etc/multipath.conf em todos os hosts co-localizados. Apenas certifique-se de usar um volume de armazenamento de mecanismo de contêiner diferente em cada host. Usar aliases e incluir o nome do host de destino no alias para cada LUN de volume de armazenamento do mecanismo de contêiner tornará isso fácil de lembrar e é recomendado.



O suporte ao Docker como mecanismo de contêiner para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contêiner em uma versão futura.

Informações relacionadas

["Configurar o volume de armazenamento do mecanismo de contêiner"](#)

Configurar o volume de armazenamento do mecanismo de contêiner

Antes de instalar o mecanismo de contêiner (Docker ou Podman), talvez seja necessário formatar o volume de armazenamento e montá-lo.



O suporte ao Docker como mecanismo de contêiner para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contêiner em uma versão futura.

Sobre esta tarefa

Você pode pular essas etapas se planeja usar o armazenamento local para o volume de armazenamento do Docker ou Podman e tiver espaço suficiente disponível na partição do host que contém `/var/lib/docker` para Docker e `/var/lib/containers` para Podman.



O Podman é suportado apenas no Red Hat Enterprise Linux (RHEL).

Passos

1. Crie um sistema de arquivos no volume de armazenamento do mecanismo de contêiner:

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

2. Monte o volume de armazenamento do mecanismo do contêiner:

- Para Docker:

```
sudo mkdir -p /var/lib/docker
sudo mount container-storage-volume-device /var/lib/docker
```

- Para Podman:

```
sudo mkdir -p /var/lib/containers
sudo mount container-storage-volume-device /var/lib/containers
```

3. Adicione uma entrada para container-storage-volume-device em `/etc/fstab`.

Esta etapa garante que o volume de armazenamento será remontado automaticamente após a reinicialização do host.

Instalar o Docker

O sistema StorageGRID é executado no Red Hat Enterprise Linux como uma coleção de contêineres. Se você escolheu usar o mecanismo de contêiner do Docker, siga estas etapas para instalar o Docker. De outra forma, [instalar Podman](#).

Passos

1. Instale o Docker seguindo as instruções para sua distribuição Linux.



Se o Docker não estiver incluído na sua distribuição Linux, você poderá baixá-lo do site do Docker.

2. Certifique-se de que o Docker foi habilitado e iniciado executando os dois comandos a seguir:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Confirme se você instalou a versão esperada do Docker digitando o seguinte:

```
sudo docker version
```

As versões do cliente e do servidor devem ser 1.11.0 ou posterior.

Instalar Podman

O sistema StorageGRID é executado no Red Hat Enterprise Linux como uma coleção de contêineres. Se você escolheu usar o mecanismo de contêiner Podman, siga estas etapas para instalar o Podman. De outra forma, [instalar Docker](#).



O Podman é suportado apenas no Red Hat Enterprise Linux (RHEL).

Passos

1. Instale o Podman e o Podman-Docker seguindo as instruções para sua distribuição Linux.



Você também deve instalar o pacote Podman-Docker ao instalar o Podman.

2. Confirme se você instalou a versão esperada do Podman e do Podman-Docker digitando o seguinte:

```
sudo docker version
```



O pacote Podman-Docker permite que você use comandos do Docker.

As versões do Cliente e do Servidor devem ser 3.2.3 ou posterior.

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

Instalar serviços de host do StorageGRID

Use o pacote RPM do StorageGRID para instalar os serviços de host do StorageGRID .

Sobre esta tarefa

Estas instruções descrevem como instalar os serviços de host dos pacotes RPM. Como alternativa, você pode usar os metadados do repositório DNF incluídos no arquivo de instalação para instalar os pacotes RPM remotamente. Consulte as instruções do repositório DNF para seu sistema operacional Linux.

Passos

1. Copie os pacotes RPM do StorageGRID para cada um dos seus hosts ou disponibilize-os no armazenamento compartilhado.

Por exemplo, coloque-os no `/tmp` diretório, para que você possa usar o comando de exemplo na próxima etapa.

2. Efetue login em cada host como root ou usando uma conta com permissão sudo e execute os seguintes comandos na ordem especificada:

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-  
version-SHA.rpm
```

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-  
version-SHA.rpm
```



Você deve instalar o pacote Imagens primeiro e o pacote Serviço depois.



Se você colocou os pacotes em um diretório diferente de `/tmp` , modifique o comando para refletir o caminho que você usou.

Automatize a instalação do StorageGRID no Red Hat Enterprise Linux

Você pode automatizar a instalação do serviço de host StorageGRID e a configuração dos nós da grade.

Automatizar a implantação pode ser útil em qualquer um dos seguintes casos:

- Você já usa uma estrutura de orquestração padrão, como Ansible, Puppet ou Chef, para implantar e configurar hosts físicos ou virtuais.

- Você pretende implantar várias instâncias do StorageGRID .
- Você está implantando uma instância StorageGRID grande e complexa.

O serviço de host StorageGRID é instalado por um pacote e controlado por arquivos de configuração. Você pode criar os arquivos de configuração usando um destes métodos:

- ["Crie os arquivos de configuração"](#) interativamente durante uma instalação manual.
- Prepare os arquivos de configuração com antecedência (ou programaticamente) para permitir a instalação automatizada usando estruturas de orquestração padrão, conforme descrito neste artigo.

O StorageGRID fornece scripts Python opcionais para automatizar a configuração de dispositivos StorageGRID e de todo o sistema StorageGRID (a "grade"). Você pode usar esses scripts diretamente ou inspecioná-los para aprender como usá-los. ["API REST de instalação do StorageGRID"](#) em ferramentas de implantação e configuração de grade que você mesmo desenvolve.

Automatize a instalação e a configuração do serviço de host StorageGRID

Você pode automatizar a instalação do serviço de host StorageGRID usando estruturas de orquestração padrão, como Ansible, Puppet, Chef, Fabric ou SaltStack.

O serviço de host StorageGRID é empacotado em um RPM e é controlado por arquivos de configuração que você pode preparar com antecedência (ou programaticamente) para permitir a instalação automatizada. Se você já usa uma estrutura de orquestração padrão para instalar e configurar o RHEL, adicionar o StorageGRID aos seus playbooks ou receitas deve ser simples.

Veja o exemplo de função e manual do Ansible no `/extras` pasta fornecida com o arquivo de instalação. O manual do Ansible mostra como o `storagegrid` A função prepara o host e instala o StorageGRID nos servidores de destino. Você pode personalizar a função ou o manual conforme necessário.



O manual de exemplo não inclui as etapas necessárias para criar dispositivos de rede antes de iniciar o serviço de host StorageGRID . Adicione estas etapas antes de finalizar e usar o manual.

Você pode automatizar todas as etapas de preparação dos hosts e implantação de nós de grade virtual.

Exemplo de função e manual do Ansible

Exemplo de função e manual do Ansible são fornecidos com o arquivo de instalação no `/extras` pasta. O manual do Ansible mostra como o `storagegrid` A função prepara os hosts e instala o StorageGRID nos servidores de destino. Você pode personalizar a função ou o manual conforme necessário.

As tarefas de instalação fornecidas `storagegrid` exemplo de função use o `ansible.builtin.dnf` módulo para executar a instalação a partir dos arquivos RPM locais ou de um repositório Yum remoto. Se o módulo não estiver disponível ou não for compatível, talvez seja necessário editar as tarefas Ansible apropriadas nos seguintes arquivos para usá-lo `yum` ou `ansible.builtin.yum` módulo:

- `roles/storagegrid/tasks/rhel_install_from_repo.yml`
- `roles/storagegrid/tasks/rhel_install_from_local.yml`

Automatize a configuração do StorageGRID

Após implantar os nós da grade, você pode automatizar a configuração do sistema StorageGRID .

Antes de começar

- Você sabe a localização dos seguintes arquivos do arquivo de instalação.

Nome do arquivo	Descrição
configurar-storagegrid.py	Script Python usado para automatizar a configuração
configurar-storagegrid.sample.json	Arquivo de configuração de exemplo para uso com o script
configurar-storagegrid.blank.json	Arquivo de configuração em branco para uso com o script

- Você criou um `configure-storagegrid.json` arquivo de configuração. Para criar este arquivo, você pode modificar o arquivo de configuração de exemplo(`configure-storagegrid.sample.json`) ou o arquivo de configuração em branco(`configure-storagegrid.blank.json`).

Sobre esta tarefa

Você pode usar o `configure-storagegrid.py` Script Python e o `configure-storagegrid.json` arquivo de configuração para automatizar a configuração do seu sistema StorageGRID .



Você também pode configurar o sistema usando o Grid Manager ou a API de instalação.

Passos

1. Faça login na máquina Linux que você está usando para executar o script Python.
2. Mude para o diretório onde você extraiu o arquivo de instalação.

Por exemplo:

```
cd StorageGRID-Webscale-version/platform
```

onde `platform` é `debs` , `rpms` , ou `vsphere` .

3. Execute o script Python e use o arquivo de configuração que você criou.

Por exemplo:

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Resultado

Um pacote de recuperação .zip O arquivo é gerado durante o processo de configuração e é baixado para o diretório onde você está executando o processo de instalação e configuração. Você deve fazer backup do

arquivo do pacote de recuperação para poder recuperar o sistema StorageGRID se um ou mais nós da grade falharem. Por exemplo, copie-o para um local de rede seguro e com backup e para um local de armazenamento em nuvem seguro.



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 .

Se você especificou que senhas aleatórias seriam geradas, abra o `Passwords.txt` arquivo e procure as senhas necessárias para acessar seu sistema StorageGRID .

```
#####
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####      ./sgws-recovery-package-994078-rev1.zip      #####
#####   Safeguard this file as it will be needed in case of a   #####
#####               StorageGRID node recovery.               #####
#####
```

Seu sistema StorageGRID estará instalado e configurado quando uma mensagem de confirmação for exibida.

```
StorageGRID has been configured and installed.
```

Informações relacionadas

["Instalação REST API"](#)

Implantar nós de grade virtual (Red Hat)

Criar arquivos de configuração de nó para implantações do Red Hat Enterprise Linux

Os arquivos de configuração de nó são pequenos arquivos de texto que fornecem as informações que o serviço de host StorageGRID precisa para iniciar um nó e conectá-lo à rede apropriada e aos recursos de armazenamento em bloco. Os arquivos de configuração de nós são usados para nós virtuais e não para nós de dispositivos.

Localização dos arquivos de configuração do nó

Coloque o arquivo de configuração para cada nó StorageGRID no `/etc/storagegrid/nodes` diretório no host onde o nó será executado. Por exemplo, se você planeja executar um nó de administração, um nó de gateway e um nó de armazenamento no HostA, você deve colocar três arquivos de configuração de nó em `/etc/storagegrid/nodes` no HostA.

Você pode criar os arquivos de configuração diretamente em cada host usando um editor de texto, como vim ou nano, ou pode criá-los em outro lugar e movê-los para cada host.

Nomenclatura de arquivos de configuração de nó

Os nomes dos arquivos de configuração são significativos. O formato é `node-name.conf` , onde `node-name` é um nome que você atribui ao nó. Este nome aparece no instalador do StorageGRID e é usado para operações de manutenção de nós, como migração de nós.

Os nomes dos nós devem seguir estas regras:

- Deve ser único
- Deve começar com uma letra
- Pode conter os caracteres de A a Z e de a a z
- Pode conter os números de 0 a 9
- Pode conter um ou mais hífens (-)
- Não deve ter mais de 32 caracteres, sem incluir o `.conf` extensão

Quaisquer arquivos em `/etc/storagegrid/nodes` que não seguem essas convenções de nomenclatura não serão analisados pelo serviço host.

Se você tiver uma topologia multisite planejada para sua grade, um esquema típico de nomenclatura de nós pode ser:

`site-nodetype-nodenumbers.conf`

Por exemplo, você pode usar `dc1-adm1.conf` para o primeiro nó de administração no Data Center 1 e `dc2-sn3.conf` para o terceiro nó de armazenamento no Data Center 2. No entanto, você pode usar qualquer esquema que desejar, desde que todos os nomes de nós sigam as regras de nomenclatura.

Conteúdo de um arquivo de configuração de nó

Um arquivo de configuração contém pares chave/valor, com uma chave e um valor por linha. Para cada par chave/valor, siga estas regras:

- A chave e o valor devem ser separados por um sinal de igual(=) e espaço em branco opcional.
- As chaves não podem conter espaços.
- Os valores podem conter espaços incorporados.
- Qualquer espaço em branco à esquerda ou à direita será ignorado.

A tabela a seguir define os valores para todas as chaves suportadas. Cada tecla tem uma das seguintes designações:

- **Obrigatório:** Obrigatório para cada nó ou para os tipos de nó especificados
- **Melhor prática:** Opcional, embora recomendado
- **Opcional:** Opcional para todos os nós

Chaves de rede de administração

IP_ADMIN

Valor	Designação
Endereço IPv4 da rede de grade do nó administrativo primário da grade à qual esse nó pertence. Use o mesmo valor especificado para GRID_NETWORK_IP para o nó de grade com NODE_TYPE = VM_Admin_Node e ADMIN_ROLE = Primary. Se você omitir esse parâmetro, o nó tentará descobrir um nó de administração primário usando mDNS. "Como os nós da grade descobrem o nó administrativo principal" Observação: Este valor é ignorado e pode ser proibido no nó de administração primário.	Melhores práticas

CONFIGURAÇÃO_DE_ADMINISTRAÇÃO

Valor	Designação
DHCP, ESTÁTICO ou DESATIVADO	Opcional

ADMIN_REDE_ESL

Valor	Designação
Lista separada por vírgulas de sub-redes em notação CIDR com as quais este nó deve se comunicar usando o gateway da rede de administração. Exemplo: 172.16.0.0/21, 172.17.0.0/21	Opcional

GATEWAY_DE_REDE_ADMINISTRATIVA

Valor	Designação
Endereço IPv4 do gateway da rede de administração local para este nó. Deve estar na sub-rede definida por ADMIN_NETWORK_IP e ADMIN_NETWORK_MASK. Este valor é ignorado para redes configuradas por DHCP. Exemplos: 1.1.1.1 10.224.4.81	Obrigatório se ADMIN_NETWORK_ESL é especificado. Caso contrário, é opcional.

IP_DE_REDE_ADMINISTRATIVA

Valor	Designação
Endereço IPv4 deste nó na rede de administração. Esta chave só é necessária quando ADMIN_NETWORK_CONFIG = STATIC; não a especifique para outros valores.	Obrigatório quando ADMIN_NETWORK_CONFIG = STATIC.
Exemplos:	Caso contrário, é opcional.
1.1.1.1	
10.224.4.81	

ADMIN_REDE_MAC

Valor	Designação
O endereço MAC da interface de rede de administração no contêiner.	Opcional
Este campo é opcional. Se omitido, um endereço MAC será gerado automaticamente.	
Deve ter 6 pares de dígitos hexadecimais separados por dois pontos.	
Exemplo: b2:9c:02:c2:27:10	

MÁSCARA_DE_REDE_ADMINISTRATIVA

Valor	Designação
Máscara de rede IPv4 para este nó, na rede de administração. Especifique esta chave quando ADMIN_NETWORK_CONFIG = STATIC; não a especifique para outros valores.	Obrigatório se ADMIN_NETWORK_IP for especificado e ADMIN_NETWORK_CONFIG = STATIC.
Exemplos:	Caso contrário, é opcional.
255.255.255.0	
255.255.248.0	

MTU_DE_REDE_ADMINISTRATIVA

Valor	Designação
A unidade máxima de transmissão (MTU) para este nó na rede de administração. Não especifique se ADMIN_NETWORK_CONFIG = DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 será usado. Se você quiser usar quadros jumbo, defina a MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão. IMPORTANTE: O valor da MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conectado. Caso contrário, podem ocorrer problemas de desempenho da rede ou perda de pacotes. Exemplos: 1500 8192	Opcional

ADMIN_REDE_ALVO

Valor	Designação
Nome do dispositivo host que você usará para acesso à rede de administração pelo nó StorageGRID . Somente nomes de interface de rede são suportados. Normalmente, você usa um nome de interface diferente do que foi especificado para GRID_NETWORK_TARGET ou CLIENT_NETWORK_TARGET. Observação: Não use dispositivos de ligação ou ponte como alvo de rede. Configure uma VLAN (ou outra interface virtual) sobre o dispositivo de ligação ou use um par de ponte e Ethernet virtual (veth). Melhor prática: especifique um valor mesmo que este nó não tenha inicialmente um endereço IP de rede de administração. Depois, você pode adicionar um endereço IP de rede de administração, sem precisar reconfigurar o nó no host. Exemplos: bond0.1002 ens256	Melhores práticas

TIPO_DE_ALVO_DE_REDE_ADMINISTRATIVA

Valor	Designação
Interface (Este é o único valor suportado.)	Opcional

TIPO_DE_ALVO_DE_REDE_ADMINISTRAÇÃO_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou falso Defina a chave como "true" para fazer com que o contêiner StorageGRID use o endereço MAC da interface de destino do host na rede de administração. Melhores práticas: Em redes onde o modo promíscuo seria necessário, use a chave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Para mais detalhes sobre clonagem de MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Melhores práticas

FUNÇÃO_ADMINISTRATIVA

Valor	Designação
Primário ou não primário Esta chave só é necessária quando NODE_TYPE = VM_Admin_Node; não a especifique para outros tipos de nó.	Obrigatório quando NODE_TYPE = VM_Admin_Node Caso contrário, é opcional.

Bloquear chaves do dispositivo

LOGS_DE_AUDITORIA_DE_DISPOSITIVO_DE_BLOCO

Valor	Designação
Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento persistente de logs de auditoria. Exemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-audit-logs</pre>	Obrigatório para nós com NODE_TYPE = VM_Admin_Node. Não especifique isso para outros tipos de nós.

BLOCK_DEVICE_RANGEDB_nnn

Valor	Designação
Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento de objetos persistentes. Esta chave só é necessária para nós com NODE_TYPE = VM_Storage_Node; não a especifique para outros tipos de nós. Somente BLOCK_DEVICE_RANGEDB_000 é necessário; o restante é opcional. O dispositivo de bloco especificado para BLOCK_DEVICE_RANGEDB_000 deve ter pelo menos 4 TB; os outros podem ser menores. Não deixe lacunas. Se você especificar BLOCK_DEVICE_RANGEDB_005, também deverá especificar BLOCK_DEVICE_RANGEDB_004. Observação: para compatibilidade com implantações existentes, chaves de dois dígitos são suportadas para nós atualizados. Exemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-rangedb-000</pre>	Obrigatório: BLOCK_DEVICE_RANGEDB_000 Opcional: BLOCK_DEVICE_RANGEDB_001 BLOCK_DEVICE_RANGEDB_002 BLOCK_DEVICE_RANGEDB_003 BLOCK_DEVICE_RANGEDB_004 BLOCK_DEVICE_RANGEDB_005 BLOCK_DEVICE_RANGEDB_006 BLOCK_DEVICE_RANGEDB_007 BLOCK_DEVICE_RANGEDB_008 BLOCK_DEVICE_RANGEDB_009 BLOCK_DEVICE_RANGEDB_010 BLOCK_DEVICE_RANGEDB_011 BLOCK_DEVICE_RANGEDB_012 BLOCK_DEVICE_RANGEDB_013 BLOCK_DEVICE_RANGEDB_014 BLOCK_DEVICE_RANGEDB_015

TABELAS_DE_DISPOSITIVOS_DE_BLOCO

Valor	Designação
Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento persistente de tabelas de banco de dados. Esta chave só é necessária para nós com NODE_TYPE = VM_Admin_Node; não a especifique para outros tipos de nós. Exemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-tables</pre>	Obrigatório

BLOCO_DISPOSITIVO_VAR_LOCAL

Valor	Designação
Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para seu /var/local armazenamento persistente. Exemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-var-local</pre>	Obrigatório

Chaves de rede do cliente

CONFIGURAÇÃO_DE_REDE_DO_CLIENTE

Valor	Designação
DHCP, ESTÁTICO ou DESATIVADO	Opcional

GATEWAY_DE_REDE_DO_CLIENTE

Valor	Designação

Endereço IPv4 do gateway da rede do cliente local para este nó, que deve estar na sub-rede definida por CLIENT_NETWORK_IP e CLIENT_NETWORK_MASK. Este valor é ignorado para redes configuradas por DHCP. Exemplos: 1.1.1.1 10.224.4.81	Opcional

IP_DE_REDE_DO_CLIENTE

Valor	Designação
Endereço IPv4 deste nó na rede do cliente. Esta chave só é necessária quando CLIENT_NETWORK_CONFIG = STATIC; não a especifique para outros valores. Exemplos: 1.1.1.1 10.224.4.81	Obrigatório quando CLIENT_NETWORK_CONFIG = STATIC Caso contrário, é opcional.

CLIENTE_REDE_MAC

Valor	Designação
O endereço MAC da interface de rede do cliente no contêiner. Este campo é opcional. Se omitido, um endereço MAC será gerado automaticamente. Deve ter 6 pares de dígitos hexadecimais separados por dois pontos. Exemplo: b2:9c:02:c2:27:20	Opcional

MÁSCARA_DE_REDE_DO_CLIENTE

Valor	Designação
Máscara de rede IPv4 para este nó na rede do cliente. Especifique esta chave quando CLIENT_NETWORK_CONFIG = STATIC; não a especifique para outros valores. Exemplos: 255.255.255.0 255.255.248.0	Obrigatório se CLIENT_NETWORK_IP for especificado e CLIENT_NETWORK_CONFIG = STATIC Caso contrário, é opcional.

MTU_DE_REDE_DO_CLIENTE

Valor	Designação
A unidade máxima de transmissão (MTU) para este nó na rede do cliente. Não especifique se CLIENT_NETWORK_CONFIG = DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 será usado. Se você quiser usar quadros jumbo, defina a MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão. IMPORTANTE: O valor da MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conectado. Caso contrário, podem ocorrer problemas de desempenho da rede ou perda de pacotes. Exemplos: 1500 8192	Opcional

CLIENTE_REDE_ALVO

Valor	Designação
Nome do dispositivo host que você usará para acesso à rede do cliente pelo nó StorageGRID . Somente nomes de interface de rede são suportados. Normalmente, você usa um nome de interface diferente do que foi especificado para GRID_NETWORK_TARGET ou ADMIN_NETWORK_TARGET. Observação: Não use dispositivos de ligação ou ponte como alvo de rede. Configure uma VLAN (ou outra interface virtual) sobre o dispositivo de ligação ou use um par de ponte e Ethernet virtual (veth). Melhor prática: especifique um valor mesmo que este nó não tenha inicialmente um endereço IP de rede do cliente. Depois, você pode adicionar um endereço IP de rede do cliente, sem precisar reconfigurar o nó no host. Exemplos: bond0.1003 ens423	Melhores práticas

TIPO_DE_ALVO_DE_REDE_DO_CLIENTE

Valor	Designação
Interface (Este é o único valor suportado.)	Opcional

CLIENTE_REDE_TIPO_DE_ALVO_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou falso Defina a chave como "true" para fazer com que o contêiner StorageGRID use o endereço MAC da interface de destino do host na rede do cliente. Melhores práticas: Em redes onde o modo promíscuo seria necessário, use a chave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Para mais detalhes sobre clonagem de MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Melhores práticas

Chaves de rede de grade

CONFIGURAÇÃO_DE_REDE_DE_GRADE

Valor	Designação
ESTÁTICO ou DHCP O padrão é STATIC se não for especificado.	Melhores práticas

GATEWAY_DE_REDE_DE_GRADE

Valor	Designação
Endereço IPv4 do gateway da Grid Network local para este nó, que deve estar na sub-rede definida por GRID_NETWORK_IP e GRID_NETWORK_MASK. Este valor é ignorado para redes configuradas por DHCP. Se a Grid Network for uma única sub-rede sem gateway, use o endereço de gateway padrão para a sub-rede (XYZ1) ou o valor GRID_NETWORK_IP deste nó; qualquer valor simplificará possíveis expansões futuras da Grid Network.	Obrigatório

IP_DE_REDE_DE_GRID

Valor	Designação
Endereço IPv4 deste nó na Rede Grid. Esta chave só é necessária quando GRID_NETWORK_CONFIG = STATIC; não a especifique para outros valores. Exemplos: 1.1.1.1 10.224.4.81	Obrigatório quando GRID_NETWORK_CONFIG = STATIC Caso contrário, é opcional.

GRID_REDE_MAC

Valor	Designação
O endereço MAC da interface da Grid Network no contêiner. Deve ter 6 pares de dígitos hexadecimais separados por dois pontos. Exemplo: b2:9c:02:c2:27:30	Opcional Se omitido, um endereço MAC será gerado automaticamente.

MÁSCARA_DE_REDE_DE_GRADE

Valor	Designação
Máscara de rede IPv4 para este nó na rede Grid. Especifique esta chave quando GRID_NETWORK_CONFIG = STATIC; não a especifique para outros valores. Exemplos: 255.255.255.0 255.255.248.0	Obrigatório quando GRID_NETWORK_IP é especificado e GRID_NETWORK_CONFIG = STATIC. Caso contrário, é opcional.

MTU_DE_REDE_DE_GRADE

Valor	Designação
A unidade máxima de transmissão (MTU) para este nó na rede de grade. Não especifique se GRID_NETWORK_CONFIG = DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 será usado. Se você quiser usar quadros jumbo, defina a MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão. IMPORTANTE: O valor da MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conectado. Caso contrário, podem ocorrer problemas de desempenho da rede ou perda de pacotes. IMPORTANTE: Para o melhor desempenho da rede, todos os nós devem ser configurados com valores de MTU semelhantes em suas interfaces de rede de grade. O alerta Incompatibilidade de MTU da rede de grade é acionado se houver uma diferença significativa nas configurações de MTU da rede de grade em nós individuais. Os valores de MTU não precisam ser os mesmos para todos os tipos de rede. Exemplos: 1500 8192	Opcional

ALVO_DA_REDE_DE_GRID

Valor	Designação
Nome do dispositivo host que você usará para acesso à Grid Network pelo nó StorageGRID . Somente nomes de interface de rede são suportados. Normalmente, você usa um nome de interface diferente do que foi especificado para ADMIN_NETWORK_TARGET ou CLIENT_NETWORK_TARGET. Observação: Não use dispositivos de ligação ou ponte como alvo de rede. Configure uma VLAN (ou outra interface virtual) sobre o dispositivo de ligação ou use um par de ponte e Ethernet virtual (veth). Exemplos: bond0.1001 ens192	Obrigatório

TIPO_DE_ALVO_DE_REDE_DE_GRID

Valor	Designação
Interface (Este é o único valor suportado.)	Opcional

TIPO_DE_ALVO_DE_REDE_DE_GRID_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou falso Defina o valor da chave como "true" para fazer com que o contêiner StorageGRID use o endereço MAC da interface de destino do host na Grid Network. Melhores práticas: Em redes onde o modo promíscuo seria necessário, use a chave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Para mais detalhes sobre clonagem de MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Melhores práticas

Chave de senha de instalação (temporária)

HASH_DE_SENHA_TEMPORÁRIA_PERSONALIZADA

Valor	Designação
Para o nó de administração principal, defina uma senha temporária padrão para a API de instalação do StorageGRID durante a instalação. Observação: Defina uma senha de instalação somente no nó de administração principal. Se você tentar definir uma senha em outro tipo de nó, a validação do arquivo de configuração do nó falhará. Definir esse valor não terá efeito quando a instalação estiver concluída. Se esta chave for omitida, por padrão nenhuma senha temporária será definida. Como alternativa, você pode definir uma senha temporária usando a API de instalação do StorageGRID . Deve ser um <code>crypt()</code> Hash de senha SHA-512 com formato <code>\$6\$<salt>\$<password hash></code> para uma senha de pelo menos 8 e não mais que 32 caracteres. Este hash pode ser gerado usando ferramentas CLI, como o <code>openssl passwd</code> comando no modo SHA-512.	Melhores práticas

Chave de interfaces

INTERFACE_ALVO_nnnn

Valor	Designação
Nome e descrição opcional para uma interface extra que você deseja adicionar a este nó. Você pode adicionar várias interfaces extras a cada nó. Para <i>nnnn</i>, especifique um número exclusivo para cada entrada <code>INTERFACE_TARGET</code> que você está adicionando. Para o valor, especifique o nome da interface física no host bare-metal. Em seguida, opcionalmente, adicione uma vírgula e forneça uma descrição da interface, que é exibida na página de interfaces de VLAN e na página de grupos de HA. Exemplo: <code>INTERFACE_TARGET_0001=ens256, Trunk</code> Se você adicionar uma interface de tronco, deverá configurar uma interface VLAN no StorageGRID. Se você adicionar uma interface de acesso, poderá adicioná-la diretamente a um grupo HA; não precisará configurar uma interface VLAN.	Opcional

Chave de RAM máxima

MÁXIMA_RAM

Valor	Designação
A quantidade máxima de RAM que este nó pode consumir. Se esta chave for omitida, o nó não terá restrições de memória. Ao definir este campo para um nó de nível de produção, especifique um valor que seja pelo menos 24 GB e 16 a 32 GB menor que a RAM total do sistema. Observação: O valor de RAM afeta o espaço real reservado de metadados de um nó. Veja o "descrição do que é Espaço Reservado de Metadados". O formato para este campo é <i>numberunit</i>, onde <i>unit</i> pode ser <i>b</i>, <i>k</i>, <i>m</i>, ou <i>g</i>. Exemplos: 24g 38654705664b Observação: Se você quiser usar esta opção, deverá habilitar o suporte do kernel para cgroups de memória.	Opcional

Chaves de tipo de nó

TIPO_NÓ

Valor	Designação
Tipo de nó: - Nó_Administrador_VM - Nó_de_armazenamento_VM - Nó_de_arquivo_VM - Gateway de API da VM	Obrigatório

TIPO_DE_ARMAZENAMENTO

Valor	Designação
Define o tipo de objetos que um nó de armazenamento contém. Para obter mais informações, consulte "Tipos de nós de armazenamento" . Esta chave só é necessária para nós com NODE_TYPE = VM_Storage_Node; não a especifique para outros tipos de nós. Tipos de armazenamento: • combinado • dados • metadados Observação: se o STORAGE_TYPE não for especificado, o tipo de nó de armazenamento será definido como combinado (dados e metadados) por padrão.	Opcional

Chaves de remapeamento de portas

PORTA_REMAPARAR

Valor	Designação
Remapeia qualquer porta usada por um nó para comunicações internas do nó da grade ou comunicações externas. O remapeamento de portas é necessário se as políticas de rede corporativa restringirem uma ou mais portas usadas pelo StorageGRID, conforme descrito em "Comunicações internas do nó da rede" ou "Comunicações externas" . IMPORTANTE: Não remapeie as portas que você planeja usar para configurar os pontos de extremidade do balanceador de carga. Observação: se somente PORT_REMAP estiver definido, o mapeamento especificado será usado para comunicações de entrada e saída. Se PORT_REMAP_INBOUND também for especificado, PORT_REMAP se aplicará somente às comunicações de saída. O formato utilizado é: <i>network type/protocol/default port used by grid node/new port</i> , onde <i>network type</i> é grade, administrador ou cliente e <i>protocol</i> é tcp ou udp. Exemplo: PORT_REMAP = client/tcp/18082/443 Você também pode remapear várias portas usando uma lista separada por vírgulas. Exemplo: PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80	Opcional

PORTA_REMAPAR_ENTRADA

Valor	Designação
Remapeia as comunicações de entrada para a porta especificada. Se você especificar <code>PORT_REMAP_INBOUND</code>, mas não especificar um valor para <code>PORT_REMAP</code>, as comunicações de saída para a porta permanecerão inalteradas. IMPORTANTE: Não remapeie as portas que você planeja usar para configurar os pontos de extremidade do balanceador de carga. O formato utilizado é: <i>network type/protocol/remapped port/default port used by grid node</i>, onde <i>network type</i> é grade, administrador ou cliente e <i>protocol</i> é tcp ou udp. Exemplo: <code>PORT_REMAP_INBOUND = grid/tcp/3022/22</code> Você também pode remapear várias portas de entrada usando uma lista separada por vírgulas. Exemplo: <code>PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22</code>	Opcional

Como os nós da grade descobrem o nó administrativo principal

Os nós de grade se comunicam com o nó de administração principal para configuração e gerenciamento. Cada nó da grade deve saber o endereço IP do nó administrativo primário na rede da grade.

Para garantir que um nó de grade possa acessar o nó de administração principal, você pode fazer o seguinte ao implantar o nó:

- Você pode usar o parâmetro `ADMIN_IP` para inserir manualmente o endereço IP do nó de administração principal.
- Você pode omitir o parâmetro `ADMIN_IP` para que o nó da grade descubra o valor automaticamente. A descoberta automática é especialmente útil quando a Grid Network usa DHCP para atribuir o endereço IP ao nó administrativo primário.

A descoberta automática do nó de administração primário é realizada usando um sistema de nomes de domínio multicast (mDNS). Quando o nó de administração primário é iniciado pela primeira vez, ele publica seu endereço IP usando mDNS. Outros nós na mesma sub-rede podem então consultar o endereço IP e adquiri-lo automaticamente. Entretanto, como o tráfego IP multicast normalmente não é roteável entre sub-redes, os nós em outras sub-redes não podem adquirir o endereço IP do nó administrativo principal diretamente.

Se você usar a descoberta automática:



- Você deve incluir a configuração `ADMIN_IP` para pelo menos um nó de grade em qualquer sub-rede à qual o nó de administração primário não esteja diretamente conectado. Este nó de grade publicará então o endereço IP do nó de administração principal para que outros nós na sub-rede o descubram com o mDNS.
- Certifique-se de que sua infraestrutura de rede suporte a passagem de tráfego IP multicast dentro de uma sub-rede.

Arquivos de configuração de nó de exemplo

Você pode usar os arquivos de configuração de nó de exemplo para ajudar a configurar os arquivos de configuração de nó para seu sistema StorageGRID . Os exemplos mostram arquivos de configuração de nós para todos os tipos de nós de grade.

Para a maioria dos nós, você pode adicionar informações de endereçamento de rede de administrador e cliente (IP, máscara, gateway e assim por diante) ao configurar a grade usando o Grid Manager ou a API de instalação. A exceção é o nó de administração principal. Se você quiser navegar até o IP da rede de administração do nó de administração primário para concluir a configuração da grade (porque a rede de grade não é roteada, por exemplo), você deve configurar a conexão da rede de administração para o nó de administração primário no arquivo de configuração do nó. Isso é mostrado no exemplo.



Nos exemplos, o destino Rede do Cliente foi configurado como uma prática recomendada, embora a Rede do Cliente esteja desabilitada por padrão.

Exemplo para nó de administração primário

Exemplo de nome de arquivo: `/etc/storagegrid/nodes/dcl-adm1.conf`

Exemplo de conteúdo do arquivo:

```

NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adml-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adml-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adml-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21

```

Exemplo para nó de armazenamento

Exemplo de nome de arquivo: /etc/storagegrid/nodes/dc1-sn1.conf

Exemplo de conteúdo do arquivo:

```

NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

```

Exemplo para nó de gateway

Exemplo de nome de arquivo: /etc/storagegrid/nodes/dc1-gw1.conf

Exemplo de conteúdo do arquivo:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemplo para um nó de administração não primário

Exemplo de nome de arquivo: /etc/storagegrid/nodes/dcl-adm2.conf

Exemplo de conteúdo do arquivo:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dcl-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dcl-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Validar a configuração do StorageGRID

Após criar os arquivos de configuração em /etc/storagegrid/nodes para cada um dos seus nós StorageGRID , você deve validar o conteúdo desses arquivos.

Para validar o conteúdo dos arquivos de configuração, execute o seguinte comando em cada host:

```
sudo storagegrid node validate all
```

Se os arquivos estiverem corretos, a saída mostrará **PASSED** para cada arquivo de configuração, conforme mostrado no exemplo.



Ao usar apenas um LUN em nós somente de metadados, você poderá receber uma mensagem de aviso que pode ser ignorada.

```
Checking for misnamed node configuration files... PASSED
Checking configuration file for node dcl-adm1... PASSED
Checking configuration file for node dcl-gw1... PASSED
Checking configuration file for node dcl-sn1... PASSED
Checking configuration file for node dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes... PASSED
```



Para uma instalação automatizada, você pode suprimir esta saída usando o `-q` ou `--quiet` opções no `storagegrid` comando (por exemplo, `storagegrid --quiet...`). Se você suprimir a saída, o comando terá um valor de saída diferente de zero se algum aviso ou erro de configuração for detectado.

Se os arquivos de configuração estiverem incorretos, os problemas serão mostrados como **AVISO** e **ERRO**, conforme mostrado no exemplo. Se algum erro de configuração for encontrado, você deverá corrigi-lo antes de continuar com a instalação.

```

Checking for misnamed node configuration files...
WARNING: ignoring /etc/storagegrid/nodes/dcl-adml
WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adml...
ERROR: NODE_TYPE = VM_Foo_Node
      VM_Foo_Node is not a valid node type.  See *.conf.sample
ERROR: ADMIN_ROLE = Foo
      Foo is not a valid admin role.  See *.conf.sample
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
      /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dcl-gw1...
ERROR: GRID_NETWORK_TARGET = bond0.1001
      bond0.1001 is not a valid interface.  See `ip link show`
ERROR: GRID_NETWORK_IP = 10.1.3
      10.1.3 is not a valid IPv4 address
ERROR: GRID_NETWORK_MASK = 255.248.255.0
      255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dcl-sn1...
ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
      10.2.0.1 is not on the local subnet
ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
      Could not parse subnet list
Checking configuration file for node dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes...
ERROR: GRID_NETWORK_IP = 10.1.0.4
      dcl-sn2 and dcl-sn3 have the same GRID_NETWORK_IP
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_RANGEDB_00

```

Inicie o serviço do host StorageGRID

Para iniciar seus nós StorageGRID e garantir que eles reiniciem após uma reinicialização do host, você deve habilitar e iniciar o serviço do host StorageGRID .

Passos

1. Execute os seguintes comandos em cada host:

```

sudo systemctl enable storagegrid
sudo systemctl start storagegrid

```

2. Execute o seguinte comando para garantir que a implantação esteja em andamento:

```
sudo storagegrid node status node-name
```

3. Se algum nó retornar o status "Não em execução" ou "Parado", execute o seguinte comando:

```
sudo storagegrid node start node-name
```

4. Se você habilitou e iniciou o serviço de host StorageGRID anteriormente (ou se não tiver certeza se o serviço foi habilitado e iniciado), execute também o seguinte comando:

```
sudo systemctl reload-or-restart storagegrid
```

Configurar a grade e concluir a instalação (Red Hat)

Navegue até o Gerenciador de Grade

Use o Grid Manager para definir todas as informações necessárias para configurar seu sistema StorageGRID .

Antes de começar

O nó de administração principal deve ser implantado e ter concluído a sequência de inicialização inicial.

Passos

1. Abra seu navegador e navegue até:

```
https://primary_admin_node_ip
```

Alternativamente, você pode acessar o Grid Manager na porta 8443:

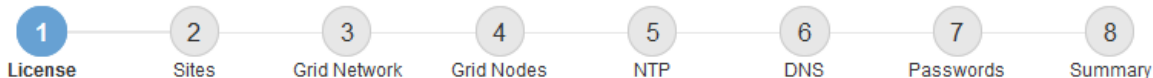
```
https://primary_admin_node_ip:8443
```

Você pode usar o endereço IP do nó de administração primário na rede Grid ou na rede de administração, conforme apropriado para sua configuração de rede.

2. Gerencie uma senha temporária do instalador conforme necessário:
 - Se uma senha já tiver sido definida usando um desses métodos, digite a senha para prosseguir.
 - Um usuário definiu a senha ao acessar o instalador anteriormente
 - A senha foi importada automaticamente do arquivo de configuração do nó em `/etc/storagegrid/nodes/<node_name>.conf`
 - Se uma senha não tiver sido definida, opcionalmente defina uma senha para proteger o instalador do StorageGRID .
3. Selecione ***Instalar um sistema StorageGRID ***.

A página usada para configurar um sistema StorageGRID é exibida.

Install



License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Browse

Especifique as informações da licença StorageGRID

Você deve especificar o nome do seu sistema StorageGRID e carregar o arquivo de licença fornecido pela NetApp.

Passos

1. Na página Licença, insira um nome significativo para seu sistema StorageGRID no campo **Nome da grade**.

Após a instalação, o nome é exibido no topo do menu Nós.

2. Selecione **Procurar**, localize o arquivo de licença do NetApp(*NLF-unique-id.txt*) e selecione **Abrir**.

O arquivo de licença é validado e o número de série é exibido.



O arquivo de instalação do StorageGRID inclui uma licença gratuita que não fornece nenhum direito de suporte para o produto. Você pode atualizar para uma licença que ofereça suporte após a instalação.

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File NLF-959007-Internal.txt

License Serial Number

3. Selecione **Avançar**.

Adicionar sites

Você deve criar pelo menos um site ao instalar o StorageGRID. Você pode criar sites adicionais para aumentar a confiabilidade e a capacidade de armazenamento do seu sistema StorageGRID.

Passos

1. Na página Sites, insira o **Nome do Site**.
2. Para adicionar outros sites, clique no sinal de mais ao lado da última entrada do site e digite o nome na nova caixa de texto **Nome do site**.

Adicione quantos sites adicionais forem necessários para sua topologia de grade. Você pode adicionar até 16 sites.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top is a blue header with 'NetApp® StorageGRID®' and a 'Help' dropdown. Below the header is a progress bar with eight steps: 1. License, 2. Sites (highlighted in blue), 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. Below the progress bar, the 'Sites' section is displayed. It contains two paragraphs of text explaining single-site and multi-site deployments. Below the text are two input fields for 'Site Name'. The first field is labeled 'Site Name 1' and contains the text 'Raleigh', with a red 'x' icon to its right. The second field is labeled 'Site Name 2' and contains the text 'Atlanta', with a '+ x' icon to its right.

3. Clique em **Avançar**.

Especificar sub-redes da rede de grade

Você deve especificar as sub-redes que são usadas na Grid Network.

Sobre esta tarefa

As entradas de sub-rede incluem as sub-redes da Grid Network para cada site no seu sistema StorageGRID, juntamente com quaisquer sub-redes que precisam ser acessadas por meio da Grid Network.

Se você tiver várias sub-redes de grade, o gateway da Rede de Grade será necessário. Todas as sub-redes de grade especificadas devem ser acessíveis por meio deste gateway.

Passos

1. Especifique o endereço de rede CIDR para pelo menos uma rede de grade na caixa de texto **Sub-rede 1**.
2. Clique no sinal de mais ao lado da última entrada para adicionar uma entrada de rede adicional. Você deve especificar todas as sub-redes para todos os sites na Grid Network.
 - Se você já tiver implantado pelo menos um nó, clique em **Descobrir sub-redes de redes de grade** para preencher automaticamente a Lista de sub-redes de redes de grade com as sub-redes relatadas

pelos nós de grade que foram registrados no Gerenciador de grade.

- Você deve adicionar manualmente quaisquer sub-redes para NTP, DNS, LDAP ou outros servidores externos acessados pelo gateway da Grid Network.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 **Grid Network** 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.

Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1 +

3. Clique em **Avançar**.

Aprovar nós de grade pendentes

Você deve aprovar cada nó de grade antes que ele possa ingressar no sistema StorageGRID .

Antes de começar

Você implantou todos os nós de grade do dispositivo virtual e StorageGRID .



É mais eficiente executar uma única instalação de todos os nós, em vez de instalar alguns nós agora e outros depois.

Passos

1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade que você implantou.



Se um nó de grade estiver faltando, confirme se ele foi implantado com sucesso e se tem o IP de rede de grade correto do nó de administração primário definido para ADMIN_IP.

2. Selecione o botão de opção ao lado de um nó pendente que você deseja aprovar.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve		✖ Remove		Search		
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address	
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21	

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit		Reset		✖ Remove		Search	
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address	
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21	
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21	
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21	
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21	
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21	

3. Clique em **Aprovar**.

4. Em Configurações gerais, modifique as configurações das seguintes propriedades, conforme necessário:

- **Site:** O nome do sistema do site para este nó de grade.
- **Nome:** O nome do sistema para o nó. O nome padrão é o nome que você especificou quando configurou o nó.

Os nomes do sistema são necessários para operações internas do StorageGRID e não podem ser alterados após a conclusão da instalação. No entanto, durante esta etapa do processo de instalação, você pode alterar os nomes do sistema conforme necessário.

- **Função NTP:** A função do Protocolo de Tempo de Rede (NTP) do nó da grade. As opções são **Automático**, **Principal** e **Cliente**. Selecionar **Automático** atribui a função Primária aos Nós de Administração, Nós de Armazenamento com serviços ADC, Nós de Gateway e quaisquer nós de grade que tenham endereços IP não estáticos. Todos os outros nós da grade recebem a função Cliente.



Certifique-se de que pelo menos dois nós em cada site possam acessar pelo menos quatro fontes NTP externas. Se apenas um nó em um site puder alcançar as fontes NTP, ocorrerão problemas de tempo se esse nó ficar inativo. Além disso, designar dois nós por site como fontes primárias de NTP garante um tempo preciso se um site estiver isolado do restante da rede.

- **Tipo de armazenamento** (somente nós de armazenamento): especifique que um novo nó de armazenamento seja usado exclusivamente para dados, metadados ou ambos. As opções são **Dados e metadados** ("combinados"), **Somente dados** e **Somente metadados**.



Ver "[Tipos de nós de armazenamento](#)" para obter informações sobre os requisitos para esses tipos de nós.

- **Serviço ADC** (somente nós de armazenamento): selecione **Automático** para permitir que o sistema determine se o nó requer o serviço Controlador de Domínio Administrativo (ADC). O serviço ADC monitora a localização e a disponibilidade dos serviços de rede. Pelo menos três nós de armazenamento em cada site devem incluir o serviço ADC. Não é possível adicionar o serviço ADC a um nó depois que ele for implantado.

5. Em Grid Network, modifique as configurações das seguintes propriedades conforme necessário:

- **Endereço IPv4 (CIDR)**: O endereço de rede CIDR para a interface Grid Network (eth0 dentro do contêiner). Por exemplo: 192.168.1.234/21
- **Gateway**: O gateway da Grid Network. Por exemplo: 192.168.0.1

O gateway é necessário se houver várias sub-redes de grade.



Se você selecionou DHCP para a configuração da Grid Network e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não esteja em um pool de endereços DHCP.

6. Se você quiser configurar a Rede de Administração para o nó da grade, adicione ou atualize as configurações na seção Rede de Administração, conforme necessário.

Insira as sub-redes de destino das rotas fora desta interface na caixa de texto **Sub-redes (CIDR)**. Se houver várias sub-redes de administração, o gateway de administração será necessário.



Se você selecionou DHCP para a configuração da rede de administração e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não esteja em um pool de endereços DHCP.

Dispositivos: Para um dispositivo StorageGRID, se a Rede de administração não foi configurada durante a instalação inicial usando o Instalador do dispositivo StorageGRID, ela não poderá ser configurada nesta caixa de diálogo Gerenciador de grade. Em vez disso, você deve seguir estes passos:

- a. Reinicie o dispositivo: No Instalador do Dispositivo, selecione **Avançado > Reinicializar**.

A reinicialização pode levar vários minutos.

- b. Selecione **Configurar rede > Configuração de link** e habilite as redes apropriadas.
- c. Selecione **Configurar rede > Configuração de IP** e configure as redes habilitadas.
- d. Retorne à página inicial e clique em **Iniciar instalação**.

- e. No Grid Manager: se o nó estiver listado na tabela Nós aprovados, remova-o.
- f. Remova o nó da tabela Nós Pendentes.
- g. Aguarde até que o nó reapareça na lista de Nós Pendentes.
- h. Confirme se você pode configurar as redes apropriadas. Eles já devem estar preenchidos com as informações que você forneceu na página Configuração de IP do Instalador do Appliance.

Para obter informações adicionais, consulte as instruções de instalação do modelo do seu aparelho.

7. Se você quiser configurar a Rede do Cliente para o nó da grade, adicione ou atualize as configurações na seção Rede do Cliente, conforme necessário. Se a Rede do Cliente estiver configurada, o gateway será necessário e se tornará o gateway padrão para o nó após a instalação.



Se você selecionou DHCP para a configuração da rede do cliente e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não esteja em um pool de endereços DHCP.

Dispositivos: Para um dispositivo StorageGRID , se a Rede do Cliente não foi configurada durante a instalação inicial usando o Instalador do Dispositivo StorageGRID , ela não poderá ser configurada nesta caixa de diálogo Gerenciador de Grade. Em vez disso, você deve seguir estes passos:

- a. Reinicie o dispositivo: No Instalador do Dispositivo, selecione **Avançado > Reinicializar**.

A reinicialização pode levar vários minutos.

- b. Selecione **Configurar rede > Configuração de link** e habilite as redes apropriadas.
- c. Selecione **Configurar rede > Configuração de IP** e configure as redes habilitadas.
- d. Retorne à página inicial e clique em **Iniciar instalação**.
- e. No Grid Manager: se o nó estiver listado na tabela Nós aprovados, remova-o.
- f. Remova o nó da tabela Nós Pendentes.
- g. Aguarde até que o nó reapareça na lista de Nós Pendentes.
- h. Confirme se você pode configurar as redes apropriadas. Eles já devem estar preenchidos com as informações que você forneceu na página Configuração de IP do Instalador do Appliance.

Para obter informações adicionais, consulte as instruções de instalação do seu aparelho.

8. Clique em **Salvar**.

A entrada do nó da grade é movida para a lista de nós aprovados.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
☐	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

9. Repita essas etapas para cada nó de grade pendente que você deseja aprovar.

Você deve aprovar todos os nós que deseja na grade. No entanto, você pode retornar a esta página a qualquer momento antes de clicar em **Instalar** na página Resumo. Você pode modificar as propriedades de um nó de grade aprovado selecionando seu botão de opção e clicando em **Editar**.

10. Quando terminar de aprovar os nós da grade, clique em **Avançar**.

Especificar informações do servidor Network Time Protocol

Você deve especificar as informações de configuração do Network Time Protocol (NTP) para o sistema StorageGRID, para que as operações executadas em servidores separados possam ser mantidas sincronizadas.

Sobre esta tarefa

Você deve especificar endereços IPv4 para os servidores NTP.

Você deve especificar servidores NTP externos. Os servidores NTP especificados devem usar o protocolo NTP.

Você deve especificar quatro referências de servidor NTP do Stratum 3 ou superior para evitar problemas com desvio de tempo.



Ao especificar a origem NTP externa para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft para uso em ambientes de alta precisão, como o StorageGRID.

["Limite de suporte para configurar o serviço Windows Time para ambientes de alta precisão"](#)

Os servidores NTP externos são usados pelos nós aos quais você atribuiu anteriormente funções NTP primárias.



Certifique-se de que pelo menos dois nós em cada site possam acessar pelo menos quatro fontes NTP externas. Se apenas um nó em um site puder alcançar as fontes NTP, ocorrerão problemas de tempo se esse nó ficar inativo. Além disso, designar dois nós por site como fontes primárias de NTP garante um tempo preciso se um site estiver isolado do restante da rede.

Passos

1. Especifique os endereços IPv4 para pelo menos quatro servidores NTP nas caixas de texto **Servidor 1** a **Servidor 4**.
2. Se necessário, selecione o sinal de mais ao lado da última entrada para adicionar entradas de servidor adicionais.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Network Time Protocol

Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.

Server 1

10.60.248.183

Server 2

10.227.204.142

Server 3

10.235.48.111

Server 4

0.0.0.0

+

3. Selecione **Avançar**.

Especificar informações do servidor DNS

Você deve especificar informações de DNS para seu sistema StorageGRID para poder acessar servidores externos usando nomes de host em vez de endereços IP.

Sobre esta tarefa

Especificando ["Informações do servidor DNS"](#) permite que você use nomes de host de nomes de domínio totalmente qualificados (FQDN) em vez de endereços IP para notificações por e-mail e AutoSupport.

Para garantir a operação correta, especifique dois ou três servidores DNS. Se você especificar mais de três, é possível que apenas três sejam usados devido a limitações conhecidas do sistema operacional em algumas plataformas. Se você tiver restrições de roteamento em seu ambiente, você pode ["personalizar a lista de servidores DNS"](#) para nós individuais (normalmente todos os nós em um site) usar um conjunto diferente de até três servidores DNS.

Se possível, use servidores DNS que cada site possa acessar localmente para garantir que um site isolado possa resolver os FQDNs para destinos externos.

Passos

1. Especifique o endereço IPv4 para pelo menos um servidor DNS na caixa de texto **Servidor 1**.
2. Se necessário, selecione o sinal de mais ao lado da última entrada para adicionar entradas de servidor adicionais.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" dropdown. Below the header is a navigation bar with "Install" and a progress indicator showing eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (highlighted in blue), 7. Passwords, and 8. Summary. Below the progress bar, the "Domain Name Service" section is visible. It contains a text box with instructions: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport." Below this, there are two input fields for DNS servers. "Server 1" has the IP address "10.224.223.130" and a red "X" icon to its right. "Server 2" has the IP address "10.224.223.136" and a red "X" icon to its right. A red "+" icon is located between the two input fields, indicating that more servers can be added.

A melhor prática é especificar pelo menos dois servidores DNS. Você pode especificar até seis servidores DNS.

3. Selecione **Avançar**.

Especifique as senhas do sistema StorageGRID

Como parte da instalação do seu sistema StorageGRID, você precisa inserir as senhas que serão usadas para proteger seu sistema e executar tarefas de manutenção.

Sobre esta tarefa

Use a página Instalar senhas para especificar a senha de provisionamento e a senha do usuário root de gerenciamento da grade.

- A senha de provisionamento é usada como uma chave de criptografia e não é armazenada pelo sistema StorageGRID .
- Você deve ter a senha de provisionamento para os procedimentos de instalação, expansão e manutenção, incluindo o download do Pacote de Recuperação. Portanto, é importante que você armazene a senha de provisionamento em um local seguro.
- Você pode alterar a senha de provisionamento no Grid Manager se tiver a atual.
- A senha do usuário root de gerenciamento de grade pode ser alterada usando o Grid Manager.
- As senhas do console de linha de comando e SSH geradas aleatoriamente são armazenadas no `Passwords.txt` arquivo no Pacote de Recuperação.

Passos

1. Em **Provisioning Passphrase**, insira a senha de provisionamento que será necessária para fazer alterações na topologia de grade do seu sistema StorageGRID .

Armazene a senha de provisionamento em um local seguro.



Se, após a conclusão da instalação, você quiser alterar a senha de provisionamento posteriormente, poderá usar o Grid Manager. Selecione **CONFIGURAÇÃO > Controle de acesso > Senhas de grade**.

2. Em **Confirmar senha de provisionamento**, digite novamente a senha de provisionamento para confirmá-la.
3. Em **Senha do usuário raiz do Grid Management**, insira a senha a ser usada para acessar o Grid Manager como usuário "root".

Guarde a senha em um local seguro.

4. Em **Confirmar senha do usuário raiz**, digite novamente a senha do Grid Manager para confirmá-la.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning Passphrase

.....

Confirm Provisioning Passphrase

.....

Grid Management Root User Password

.....

Confirm Root User Password

.....

☒ Create random command line passwords.

- Se você estiver instalando uma grade para fins de prova de conceito ou demonstração, opcionalmente desmarque a caixa de seleção **Criar senhas aleatórias de linha de comando**.

Para implantações de produção, senhas aleatórias devem sempre ser usadas por motivos de segurança. Desmarque **Criar senhas aleatórias de linha de comando** apenas para grades de demonstração se quiser usar senhas padrão para acessar nós de grade a partir da linha de comando usando a conta "root" ou "admin".



Você será solicitado a baixar o arquivo do pacote de recuperação(sgws-recovery-package-id-revision.zip) depois de clicar em **Instalar** na página Resumo. Você deve "[baixar este arquivo](#)" para concluir a instalação. As senhas necessárias para acessar o sistema são armazenadas no Passwords.txt arquivo, contido no arquivo Recovery Package.

- Clique em **Avançar**.

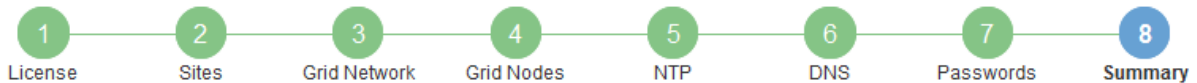
Revise sua configuração e conclua a instalação

Você deve revisar cuidadosamente as informações de configuração inseridas para garantir que a instalação seja concluída com sucesso.

Passos

- Veja a página **Resumo**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1	dc1-g1	dc1-s1
	dc1-s2	dc1-s3	NetApp-SGA

2. Verifique se todas as informações de configuração da grade estão corretas. Use os links Modificar na página Resumo para voltar e corrigir quaisquer erros.
3. Clique em **Instalar**.



Se um nó estiver configurado para usar a Rede do Cliente, o gateway padrão para esse nó muda da Rede de Grade para a Rede do Cliente quando você clica em **Instalar**. Se você perder a conectividade, certifique-se de estar acessando o nó de administração principal por meio de uma sub-rede acessível. Ver "[Diretrizes de rede](#)" para mais detalhes.

4. Clique em **Baixar pacote de recuperação**.

Quando a instalação avança até o ponto em que a topologia da grade é definida, você é solicitado a baixar o arquivo do pacote de recuperação(.zip) e confirme se você consegue acessar com sucesso o conteúdo deste arquivo. Você deve baixar o arquivo do pacote de recuperação para poder recuperar o sistema StorageGRID se um ou mais nós da grade falharem. A instalação continua em segundo plano, mas você não poderá concluir a instalação e acessar o sistema StorageGRID até baixar e verificar este arquivo.

5. Verifique se você pode extrair o conteúdo do .zip arquivo e salve-o em 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 .

6. Marque a caixa de seleção **Eu baixei e verifiquei com sucesso o arquivo do pacote de recuperação** e clique em **Avançar**.

Se a instalação ainda estiver em andamento, a página de status será exibida. Esta página indica o progresso da instalação de cada nó da grade.

Installation Status

If necessary, you may [Download the Recovery Package](#) file again.

Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage	IT
dc1-adm1		Site1		172.16.4.215/21			Starting services	
dc1-g1		Site1		172.16.4.216/21			Complete	
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers	
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed	
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed	

Quando o estágio Concluído for atingido para todos os nós da grade, a página de login do Gerenciador de Grade será exibida.

7. Sign in no Grid Manager usando o usuário "root" e a senha que você especificou durante a instalação.

Diretrizes pós-instalação

Após concluir a implantação e a configuração do nó de grade, siga estas diretrizes para endereçamento DHCP e alterações na configuração de rede.

- Se o DHCP foi usado para atribuir endereços IP, configure uma reserva DHCP para cada endereço IP nas redes que estão sendo usadas.

Você só pode configurar o DHCP durante a fase de implantação. Não é possível configurar o DHCP durante a configuração.



Os nós são reinicializados quando a configuração da rede de grade é alterada pelo DHCP, o que pode causar interrupções se uma alteração de DHCP afetar vários nós ao mesmo tempo.

- Você deve usar os procedimentos Alterar IP se quiser alterar endereços IP, máscaras de sub-rede e gateways padrão para um nó de grade. Ver "[Configurar endereços IP](#)".
- Se você fizer alterações na configuração de rede, incluindo alterações de roteamento e gateway, a conectividade do cliente com o nó de administração principal e outros nós da grade poderá ser perdida. Dependendo das alterações de rede aplicadas, pode ser necessário restabelecer essas conexões.

Instalação REST API

O StorageGRID fornece a API de instalação do StorageGRID para executar tarefas de instalação.

A API usa a plataforma de API de código aberto Swagger para fornecer a documentação da API. O Swagger permite que desenvolvedores e não desenvolvedores interajam com a API em uma interface de usuário que ilustra como a API responde a parâmetros e opções. Esta documentação pressupõe que você esteja familiarizado com tecnologias web padrão e o formato de dados JSON.



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.

Cada comando da API REST inclui a URL da API, uma ação HTTP, quaisquer parâmetros de URL obrigatórios ou opcionais e uma resposta de API esperada.

API de instalação do StorageGRID

A API de instalação do StorageGRID só estará disponível quando você estiver configurando inicialmente seu sistema StorageGRID e se precisar executar uma recuperação do nó de administração primário. A API de instalação pode ser acessada via HTTPS a partir do Grid Manager.

Para acessar a documentação da API, vá para a página de instalação no nó de administração principal e selecione **Ajuda > Documentação da API** na barra de menu.

A API de instalação do StorageGRID inclui as seguintes seções:

- **config** — Operações relacionadas ao lançamento do produto e versões da API. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **grid** — Operações de configuração em nível de grade. Você pode obter e atualizar as configurações da grade, incluindo detalhes da grade, sub-redes da rede da grade, senhas da grade e endereços IP dos servidores NTP e DNS.
- **nodes** — Operações de configuração em nível de nó. Você pode recuperar uma lista de nós de grade, excluir um nó de grade, configurar um nó de grade, visualizar um nó de grade e redefinir a configuração de um nó de grade.
- **provisão** — Operações de provisionamento. Você pode iniciar a operação de provisionamento e visualizar o status da operação de provisionamento.
- **recuperação** — Operações de recuperação do nó de administração principal. Você pode redefinir informações, carregar o Pacote de Recuperação, iniciar a recuperação e visualizar o status da operação de recuperação.
- **recovery-package** — Operações para baixar o pacote de recuperação.
- **sites** — Operações de configuração em nível de site. Você pode criar, visualizar, excluir e modificar um site.
- **temporary-password** — Operações na senha temporária para proteger a mgmt-api durante a instalação.

Para onde ir a seguir

Após concluir a instalação, execute as tarefas de integração e configuração necessárias. Você pode executar as tarefas opcionais conforme necessário.

Tarefas necessárias

- "[Criar uma conta de inquilino](#)" para o protocolo do cliente S3 que será usado para armazenar objetos no seu sistema StorageGRID .
- "[Acesso ao sistema de controle](#)" configurando grupos e contas de usuários. Opcionalmente, você pode "[configurar uma fonte de identidade federada](#)" (como Active Directory ou OpenLDAP), para que você possa importar grupos de administração e usuários. Ou você pode "[criar grupos e usuários locais](#)".
- Integrar e testar o "[S3 API](#)" aplicativos cliente que você usará para carregar objetos no seu sistema

StorageGRID .

- ["Configurar as regras de gerenciamento do ciclo de vida das informações \(ILM\) e a política de ILM"](#) que você deseja usar para proteger dados de objetos.
- Se sua instalação incluir nós de armazenamento de dispositivos, use o SANtricity OS para concluir as seguintes tarefas:
 - Conecte-se a cada dispositivo StorageGRID .
 - Verifique o recebimento dos dados do AutoSupport .

Ver ["Configurar hardware"](#) .

- Revise e siga o ["Diretrizes de reforço do sistema StorageGRID"](#) para eliminar riscos de segurança.
- ["Configurar notificações por e-mail para alertas do sistema"](#) .

Tarefas opcionais

- ["Atualizar endereços IP dos nós da grade"](#) se eles mudaram desde que você planejou sua implantação e gerou o Pacote de Recuperação.
- ["Configurar criptografia de armazenamento"](#), se necessário.
- ["Configurar compactação de armazenamento"](#) para reduzir o tamanho dos objetos armazenados, se necessário.
- ["Configurar interfaces VLAN"](#) para isolar e particionar o tráfego de rede, se necessário.
- ["Configurar grupos de alta disponibilidade"](#) para melhorar a disponibilidade de conexão para o Grid Manager, o Tenant Manager e os clientes S3, se necessário.
- ["Configurar pontos de extremidade do balanceador de carga"](#) para conectividade do cliente S3, se necessário.

Solucionar problemas de instalação

Caso ocorra algum problema durante a instalação do seu sistema StorageGRID , você pode acessar os arquivos de log da instalação. O suporte técnico também pode precisar usar os arquivos de log de instalação para resolver problemas.

Os seguintes arquivos de log de instalação estão disponíveis no contêiner que está executando cada nó:

- `/var/local/log/install.log` (encontrado em todos os nós da grade)
- `/var/local/log/gdu-server.log` (encontrado no nó de administração principal)

Os seguintes arquivos de log de instalação estão disponíveis no host:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

Para saber como acessar os arquivos de log, consulte ["Coletar arquivos de log e dados do sistema"](#) .

Informações relacionadas

["Solucionar problemas de um sistema StorageGRID"](#)

Exemplo /etc/sysconfig/network-scripts

Você pode usar os arquivos de exemplo para agregar quatro interfaces físicas do Linux em um único vínculo LACP e, em seguida, estabelecer três interfaces VLAN subtendendo o vínculo para uso como interfaces de rede StorageGRID Grid, Admin e Client.

Interfaces físicas

Observe que os switches nas outras extremidades dos links também devem tratar as quatro portas como um único tronco LACP ou canal de porta e devem passar pelo menos as três VLANs referenciadas com tags.

/etc/sysconfig/network-scripts/ifcfg-ens160

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens192

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens224

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

Interface de ligação

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

Interfaces VLAN

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Instalar o StorageGRID no Ubuntu ou Debian

Início rápido para instalar o StorageGRID no Ubuntu ou Debian

Siga estas etapas de alto nível para instalar um nó StorageGRID do Ubuntu ou Debian.

1

Preparação

- Aprenda sobre "[Arquitetura e topologia de rede do StorageGRID](#)".
- Aprenda sobre as especificidades de "[Rede StorageGRID](#)".
- Reúna e prepare o "[Informações e materiais necessários](#)".
- Prepare o necessário "[CPU e RAM](#)".
- Prover para "[requisitos de armazenamento e desempenho](#)".
- "[Preparar os servidores Linux](#)" que hospedará seus nós StorageGRID.

2

Implantação

Implantar nós de grade. Quando você implanta nós de grade, eles são criados como parte do sistema StorageGRID e conectados a uma ou mais redes.

- Para implantar nós de grade baseados em software nos hosts que você preparou na etapa 1, use a linha de comando do Linux e "[arquivos de configuração do nó](#)".
- Para implantar nós do dispositivo StorageGRID, siga as instruções "[Início rápido para instalação de hardware](#)".

3

Configuração

Quando todos os nós tiverem sido implantados, use o Grid Manager para "[configurar a grade e concluir a instalação](#)".

Automatize a instalação

Para economizar tempo e fornecer consistência, você pode automatizar a instalação do serviço de host StorageGRID e a configuração dos nós de grade.

- Use uma estrutura de orquestração padrão, como Ansible, Puppet ou Chef para automatizar:
 - Instalação do Ubuntu ou Debian
 - Configuração de rede e armazenamento
 - Instalação do mecanismo de contêiner e do serviço de host StorageGRID
 - Implantação de nós de grade virtual

Ver "[Automatize a instalação e a configuração do serviço de host StorageGRID](#)".

- Depois de implantar os nós da grade, "[automatizar a configuração do sistema StorageGRID](#)" usando o script de configuração Python fornecido no arquivo de instalação.
- "[Automatize a instalação e a configuração de nós de grade de dispositivos](#)"
- Se você for um desenvolvedor avançado de implantações do StorageGRID, automatize a instalação de nós de grade usando o "[instalação REST API](#)".

Planeje e prepare a instalação no Ubuntu ou Debian

Informações e materiais necessários

Antes de instalar o StorageGRID, reúna e prepare as informações e os materiais necessários.

Informações necessárias

Plano de rede

Quais redes você pretende anexar a cada nó do StorageGRID. O StorageGRID oferece suporte a várias redes para separação de tráfego, segurança e conveniência administrativa.

Veja o StorageGRID "[Diretrizes de rede](#)".

Informações de rede

Endereços IP a serem atribuídos a cada nó da grade e os endereços IP dos servidores DNS e NTP.

Servidores para nós de grade

Identifique um conjunto de servidores (físicos, virtuais ou ambos) que, em conjunto, forneçam recursos suficientes para dar suporte ao número e ao tipo de nós StorageGRID que você planeja implantar.



Se a instalação do StorageGRID não usar nós de armazenamento do dispositivo StorageGRID (hardware), você deverá usar armazenamento RAID de hardware com cache de gravação alimentado por bateria (BBWC). O StorageGRID não oferece suporte ao uso de redes de área de armazenamento virtual (vSANs), RAID de software ou nenhuma proteção RAID.

Migração de nós (se necessário)

Entenda o ["requisitos para migração de nós"](#), se você quiser executar manutenção programada em hosts físicos sem nenhuma interrupção de serviço.

Informações relacionadas

["Ferramenta de Matriz de Interoperabilidade da NetApp"](#)

Materiais necessários

Licença NetApp StorageGRID

Você deve ter uma licença NetApp válida e assinada digitalmente.



Uma licença de não produção, que pode ser usada para testes e prova de conceito de grades, está incluída no arquivo de instalação do StorageGRID.

Arquivo de instalação do StorageGRID

["Baixe o arquivo de instalação do StorageGRID e extraia os arquivos"](#).

Laptop de serviço

O sistema StorageGRID é instalado por meio de um laptop de serviço.

O laptop de serviço deve ter:

- Porta de rede
- Cliente SSH (por exemplo, PuTTY)
- ["Navegador da Web compatível"](#)

Documentação do StorageGRID

- ["Notas de lançamento"](#)
- ["Instruções para administrar o StorageGRID"](#)

Baixe e extraia os arquivos de instalação do StorageGRID

Você deve baixar o arquivo de instalação do StorageGRID e extrair os arquivos necessários. Opcionalmente, você pode verificar manualmente os arquivos no pacote de instalação.

Passos

1. Vá para o ["Página de downloads da NetApp para StorageGRID"](#).

2. Selecione o botão para baixar a versão mais recente ou selecione outra versão no menu suspenso e selecione **Ir**.
3. Sign in com o nome de usuário e a senha da sua conta NetApp .
4. Se uma declaração de Cuidado/Leitura Obrigatória aparecer, leia-a e marque a caixa de seleção.



Você deve aplicar todos os hotfixes necessários após instalar a versão do StorageGRID . Para mais informações, consulte o "[procedimento de hotfix nas instruções de recuperação e manutenção](#)".

5. Leia o Contrato de Licença do Usuário Final, marque a caixa de seleção e selecione **Aceitar e Continuar**.
6. Na coluna **Instalar StorageGRID**, selecione o arquivo de instalação .tgz ou .zip para Ubuntu ou Debian.



Selecione o .zip arquivo se você estiver executando o Windows no laptop de serviço.

7. Salve o arquivo de instalação.
8. Se você precisar verificar o arquivo de instalação:
 - a. Baixe o pacote de verificação de assinatura de código do StorageGRID . O nome do arquivo para este pacote usa o formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , onde <version-number> é a versão do software StorageGRID .
 - b. Siga os passos para "[verificar manualmente os arquivos de instalação](#)".
9. Extraia os arquivos do arquivo de instalação.
10. Escolha os arquivos que você precisa.

Os arquivos necessários dependem da topologia de grade planejada e de como você implantará seu sistema StorageGRID .



Os caminhos listados na tabela são relativos ao diretório de nível superior instalado pelo arquivo de instalação extraído.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID .
	Um arquivo de licença NetApp não produtivo que você pode usar para testes e implantações de prova de conceito.
	Pacote DEB para instalar as imagens do nó StorageGRID em hosts Ubuntu ou Debian.
	Soma de verificação MD5 para o arquivo <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .

Caminho e nome do arquivo	Descrição
	Pacote DEB para instalar o serviço de host StorageGRID em hosts Ubuntu ou Debian.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID .
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID .
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único estiver ativado. Você também pode usar este script para integração do Ping Federate.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> roteiro.
	Exemplo de função e manual do Ansible para configurar hosts Ubuntu ou Debian para implantação de contêiner StorageGRID . Você pode personalizar a função ou o manual conforme necessário.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado usando o Active Directory ou o Ping Federate.
	Um script auxiliar chamado pelo companheiro <code>storagegrid-ssoauth-azure.py</code> Script Python para executar interações SSO com o Azure.
	Esquemas de API para StorageGRID. Observação: antes de executar uma atualização, você pode usar esses esquemas para confirmar se qualquer código que você escreveu para usar as APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID , caso você não tenha um ambiente StorageGRID não produtivo para testes de compatibilidade de atualização.

Verificar manualmente os arquivos de instalação (opcional)

Se necessário, você pode verificar manualmente os arquivos no arquivo de instalação do StorageGRID .

Antes de começar

Você tem "[baixou o pacote de verificação](#)" do "[Página de downloads da NetApp para StorageGRID](#)".

Passos

1. Extraia os artefatos do pacote de verificação:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Certifique-se de que esses artefatos foram extraídos:

- Certificado de folha: Leaf-Cert.pem
- Cadeia de certificados: CA-Int-Cert.pem
- Cadeia de resposta de registro de data e hora: TS-Cert.pem
- Arquivo de soma de verificação: sha256sum
- Assinatura de soma de verificação: sha256sum.sig
- Arquivo de resposta de registro de data e hora: sha256sum.sig.tsr

3. Use a cadeia para verificar se o certificado em folha é válido.

Exemplo: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Saída esperada: Leaf-Cert.pem: OK

4. Se a etapa 2 falhou devido a um certificado folha expirado, use o tsr arquivo para verificar.

Exemplo: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

A produção esperada inclui: Verification: OK

5. Crie um arquivo de chave pública a partir do certificado folha.

Exemplo: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Saída esperada: *nenhuma*

6. Use a chave pública para verificar a sha256sum arquivo contra sha256sum.sig .

Exemplo: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

Saída esperada: Verified OK

7. Verifique o sha256sum conteúdo do arquivo em relação às somas de verificação recém-criadas.

Exemplo: `sha256sum -c sha256sum`

Saída esperada: `<filename>`: OK

`<filename>` é o nome do arquivo compactado que você baixou.

8. ["Conclua as etapas restantes"](#) para extrair e escolher os arquivos de instalação apropriados.

Requisitos de software para Ubuntu e Debian

Você pode usar uma máquina virtual para hospedar qualquer tipo de nó StorageGRID . Você precisa de uma máquina virtual para cada nó da grade.

Para instalar o StorageGRID no Ubuntu ou Debian, você precisa instalar alguns pacotes de software de terceiros. Algumas distribuições Linux suportadas não contêm esses pacotes por padrão. As versões dos pacotes de software nas quais as instalações do StorageGRID são testadas incluem aquelas listadas nesta página.

Se você selecionar uma distribuição Linux e uma opção de instalação de tempo de execução de contêiner que exija qualquer um desses pacotes, e eles não forem instalados automaticamente pela distribuição Linux, instale uma das versões listadas aqui, se disponível no seu provedor ou no fornecedor de suporte para sua distribuição Linux. Caso contrário, use as versões de pacote padrão disponíveis do seu fornecedor.

Todas as opções de instalação exigem Podman ou Docker. Não instale os dois pacotes. Instale somente o pacote necessário para sua opção de instalação.



O suporte ao Docker como mecanismo de contêiner para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contêiner em uma versão futura.

Versões do Python testadas

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

Versões do Podman testadas

- 3.2.3-0
- 3.4.4+ds1
- 4.1.1-7
- 4.2.0-11

- 4.3.1+ds1-8+b1
- 4.4.1-8
- 4.4.1-12

Versões do Docker testadas



O suporte ao Docker está obsoleto e será removido em uma versão futura.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23.0.6-1
- Docker-CE 24.0.2-1
- Docker-CE 24.0.4-1
- Docker-CE 24.0.5-1
- Docker-CE 24.0.7-1
- 1,5-2

Requisitos de CPU e RAM

Antes de instalar o software StorageGRID , verifique e configure o hardware para que ele esteja pronto para suportar o sistema StorageGRID .

Cada nó StorageGRID requer os seguintes recursos mínimos:

- Núcleos de CPU: 8 por nó
- RAM: Depende da RAM total disponível e da quantidade de software não StorageGRID em execução no sistema
 - Geralmente, pelo menos 24 GB por nó e 2 a 16 GB a menos que a RAM total do sistema
 - Um mínimo de 64 GB para cada locatário que terá aproximadamente 5.000 buckets

Os recursos de nós somente de metadados baseados em software devem corresponder aos recursos de nós de armazenamento existentes. Por exemplo:

- Se o site StorageGRID existente estiver usando dispositivos SG6000 ou SG6100, os nós somente de metadados baseados em software deverão atender aos seguintes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - 8 TB SSD ou armazenamento equivalente para o banco de dados Cassandra (rangedb/0)
- Se o site StorageGRID existente estiver usando nós de armazenamento virtuais com 24 GB de RAM, CPU de 8 núcleos e 3 TB ou 4 TB de armazenamento de metadados, os nós somente de metadados baseados em software deverão usar recursos semelhantes (24 GB de RAM, CPU de 8 núcleos e 4 TB de armazenamento de metadados (rangedb/0)).

Ao adicionar um novo site StorageGRID , a capacidade total de metadados do novo site deve, no mínimo, corresponder aos sites StorageGRID existentes e os novos recursos do site devem corresponder aos nós de armazenamento nos sites StorageGRID existentes.

Certifique-se de que o número de nós StorageGRID que você planeja executar em cada host físico ou virtual não exceda o número de núcleos de CPU ou a RAM física disponível. Se os hosts não forem dedicados à execução do StorageGRID (não recomendado), considere os requisitos de recursos dos outros aplicativos.



Monitore o uso da CPU e da memória regularmente para garantir que esses recursos continuem acomodando sua carga de trabalho. Por exemplo, dobrar a alocação de RAM e CPU para nós de armazenamento virtuais forneceria recursos semelhantes aos fornecidos para nós de dispositivos StorageGRID. Além disso, se a quantidade de metadados por nó exceder 500 GB, considere aumentar a RAM por nó para 48 GB ou mais. Para obter informações sobre como gerenciar o armazenamento de metadados de objetos, aumentar a configuração do Espaço Reservado de Metadados e monitorar o uso da CPU e da memória, consulte as instruções para ["administrando"](#), ["monitoramento"](#), e ["atualizando"](#) StorageGRID.

Se o hyperthreading estiver habilitado nos hosts físicos subjacentes, você poderá fornecer 8 núcleos virtuais (4 núcleos físicos) por nó. Se o hyperthreading não estiver habilitado nos hosts físicos subjacentes, você deverá fornecer 8 núcleos físicos por nó.

Se você estiver usando máquinas virtuais como hosts e tiver controle sobre o tamanho e o número de VMs, use uma única VM para cada nó do StorageGRID e dimensione a VM adequadamente.

Para implantações de produção, você não deve executar vários nós de armazenamento no mesmo hardware de armazenamento físico ou host virtual. Cada nó de armazenamento em uma única implantação do StorageGRID deve estar em seu próprio domínio de falha isolado. Você pode maximizar a durabilidade e a disponibilidade dos dados do objeto se garantir que uma única falha de hardware possa afetar apenas um único nó de armazenamento.

Veja também ["Requisitos de armazenamento e desempenho"](#).

Requisitos de armazenamento e desempenho

Você deve entender os requisitos de armazenamento para os nós do StorageGRID para poder fornecer espaço suficiente para dar suporte à configuração inicial e à futura expansão do armazenamento.

Os nós do StorageGRID exigem três categorias lógicas de armazenamento:

- **Pool de contêineres** — Armazenamento de nível de desempenho (SAS ou SSD de 10K) para os contêineres de nós, que serão atribuídos ao driver de armazenamento do Docker quando você instalar e configurar o Docker nos hosts que darão suporte aos seus nós do StorageGRID.
- **Dados do sistema** — Armazenamento em nível de desempenho (SAS ou SSD de 10K) para armazenamento persistente por nó de dados do sistema e logs de transações, que os serviços do host StorageGRID consumirão e mapearão em nós individuais.
- **Dados de objeto** — Armazenamento em nível de desempenho (10K SAS ou SSD) e armazenamento em massa em nível de capacidade (NL-SAS/SATA) para armazenamento persistente de dados de objeto e metadados de objeto.

Você deve usar dispositivos de bloco com suporte RAID para todas as categorias de armazenamento. Discos não redundantes, SSDs ou JBODs não são suportados. Você pode usar armazenamento RAID compartilhado ou local para qualquer uma das categorias de armazenamento; no entanto, se quiser usar o recurso de migração de nós no StorageGRID, você deve armazenar dados do sistema e dados de objeto no armazenamento compartilhado. Para obter mais informações, consulte ["Requisitos de migração do contêiner de nó"](#).

Requisitos de desempenho

O desempenho dos volumes usados para o pool de contêineres, dados do sistema e metadados de objetos impacta significativamente o desempenho geral do sistema. Você deve usar armazenamento de nível de desempenho (SAS ou SSD de 10K) para esses volumes para garantir desempenho de disco adequado em termos de latência, operações de entrada/saída por segundo (IOPS) e taxa de transferência. Você pode usar armazenamento em camadas de capacidade (NL-SAS/SATA) para armazenamento persistente de dados de objetos.

Os volumes usados para o pool de contêineres, dados do sistema e dados do objeto devem ter o cache de write-back habilitado. O cache deve estar em uma mídia protegida ou persistente.

Requisitos para hosts que usam armazenamento NetApp ONTAP

Se o nó StorageGRID usar armazenamento atribuído de um sistema NetApp ONTAP, confirme se o volume não tem 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.

Número de hosts necessários

Cada site StorageGRID requer no mínimo três nós de armazenamento.



Em uma implantação de produção, não execute mais de um nó de armazenamento em um único host físico ou virtual. Usar um host dedicado para cada nó de armazenamento fornece um domínio de falha isolado.

Outros tipos de nós, como nós de administração ou nós de gateway, podem ser implantados nos mesmos hosts ou em seus próprios hosts dedicados, conforme necessário.

Número de volumes de armazenamento para cada host

A tabela a seguir mostra o número de volumes de armazenamento (LUNs) necessários para cada host e o tamanho mínimo necessário para cada LUN, com base em quais nós serão implantados naquele host.

O tamanho máximo do LUN testado é 39 TB.



Esses números são para cada host, não para toda a grade.

Finalidade do LUN	Categoria de armazenamento	Número de LUNs	Tamanho mínimo/LUN
Piscina de armazenamento de motores de contêineres	Piscina de contêineres	1	Número total de nós × 100 GB

Finalidade do LUN	Categoria de armazenamento	Número de LUNs	Tamanho mínimo/LUN
`/var/local` volume	Dados do sistema	1 para cada nó neste host	90 GB
Nó de armazenamento	Dados do objeto	3 para cada nó de armazenamento neste host Observação: Um nó de armazenamento baseado em software pode ter de 1 a 48 volumes de armazenamento; pelo menos 3 volumes de armazenamento são recomendados.	12 TB (4 TB/LUN) Veja Requisitos de armazenamento para nós de armazenamento para mais informações.
Nó de armazenamento (somente metadados)	Metadados do objeto	1	4 TB Veja Requisitos de armazenamento para nós de armazenamento para mais informações. Observação: somente um rangedb é necessário para nós de armazenamento somente de metadados.
Logs de auditoria do nó de administração	Dados do sistema	1 para cada nó de administração neste host	200 GB
Tabelas do nó de administração	Dados do sistema	1 para cada nó de administração neste host	200 GB



Dependendo do nível de auditoria configurado, do tamanho das entradas do usuário, como o nome da chave do objeto S3, e da quantidade de dados de log de auditoria que você precisa preservar, pode ser necessário aumentar o tamanho do LUN do log de auditoria em cada nó de administração. Geralmente, uma grade gera aproximadamente 1 KB de dados de auditoria por operação S3, o que significa que um LUN de 200 GB suportaria 70 milhões de operações por dia ou 800 operações por segundo durante dois a três dias.

Espaço mínimo de armazenamento para um host

A tabela a seguir mostra o espaço mínimo de armazenamento necessário para cada tipo de nó. Você pode usar esta tabela para determinar a quantidade mínima de armazenamento que deve fornecer ao host em cada categoria de armazenamento, com base em quais nós serão implantados naquele host.



Snapshots de disco não podem ser usados para restaurar nós de grade. Em vez disso, consulte o "[recuperação de nós de grade](#)" procedimentos para cada tipo de nó.

Tipo de nó	Piscina de contêineres	Dados do sistema	Dados do objeto
Nó de armazenamento	100 GB	90 GB	4.000 GB
Nó de administração	100 GB	490 GB (3 LUNs)	<i>não aplicável</i>
Nó de gateway	100 GB	90 GB	<i>não aplicável</i>

Exemplo: Calculando os requisitos de armazenamento para um host

Suponha que você planeja implantar três nós no mesmo host: um nó de armazenamento, um nó de administração e um nó de gateway. Você deve fornecer no mínimo nove volumes de armazenamento ao host. Você precisará de no mínimo 300 GB de armazenamento de nível de desempenho para os contêineres de nós, 670 GB de armazenamento de nível de desempenho para dados do sistema e logs de transações e 12 TB de armazenamento de nível de capacidade para dados de objetos.

Tipo de nó	Finalidade do LUN	Número de LUNs	Tamanho da LUN
Nó de armazenamento	Pool de armazenamento do Docker	1	300 GB (100 GB/nó)
Nó de armazenamento	`/var/local` volume	1	90 GB
Nó de armazenamento	Dados do objeto	3	12 TB (4 TB/LUN)
Nó de administração	`/var/local` volume	1	90 GB
Nó de administração	Logs de auditoria do nó de administração	1	200 GB
Nó de administração	Tabelas do nó de administração	1	200 GB
Nó de gateway	`/var/local` volume	1	90 GB
Total		9	Pool de contêineres: 300 GB Dados do sistema: 670 GB Dados do objeto: 12.000 GB

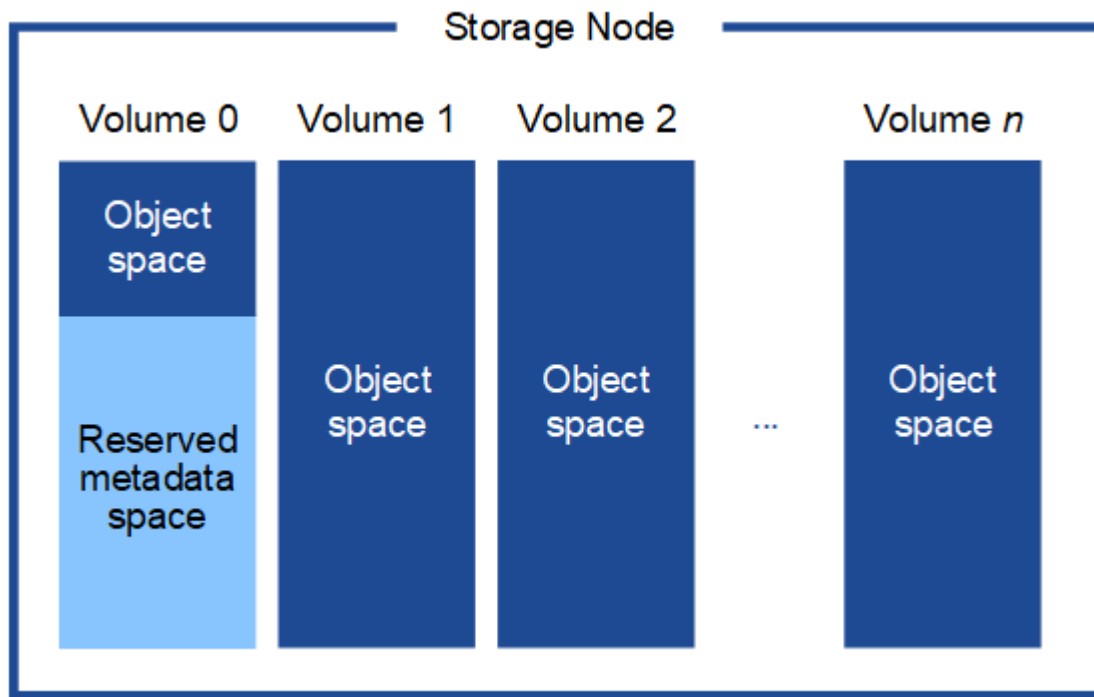
Requisitos de armazenamento para nós de armazenamento

Um nó de armazenamento baseado em software pode ter de 1 a 48 volumes de armazenamento; 3 ou mais volumes de armazenamento são recomendados. Cada volume de armazenamento deve ter 4 TB ou mais.



Um nó de armazenamento de dispositivo também pode ter até 48 volumes de armazenamento.

Conforme mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de armazenamento 0 de cada nó de armazenamento. Qualquer espaço restante no volume de armazenamento 0 e quaisquer outros volumes de armazenamento no Nó de Armazenamento são usados exclusivamente para dados de 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. As três cópias dos metadados do objeto são distribuídas uniformemente entre todos os nós de armazenamento em cada site.

Ao instalar uma grade com nós de armazenamento somente de metadados, a grade também deve conter um número mínimo de nós para armazenamento de objetos. Ver "[Tipos de nós de armazenamento](#)" para obter mais informações sobre nós de armazenamento somente de metadados.

- Para uma grade de site único, pelo menos dois nós de armazenamento são configurados para objetos e metadados.
- Para uma grade de vários sites, pelo menos um nó de armazenamento por site é configurado para objetos e metadados.

Ao atribuir espaço ao volume 0 de um novo Nó de Armazenamento, você deve garantir que haja espaço adequado para a parte desse nó de todos os metadados do objeto.

- No mínimo, você deve atribuir pelo menos 4 TB ao volume 0.



Se você usar apenas um volume de armazenamento para um Nó de Armazenamento e atribuir 4 TB ou menos ao volume, o Nó de Armazenamento poderá entrar no estado somente leitura de armazenamento na inicialização e armazenar apenas metadados de objetos.



Se você atribuir menos de 500 GB ao volume 0 (somente para uso não produtivo), 10% da capacidade do volume de armazenamento será reservada para metadados.

- Os recursos de nós somente de metadados baseados em software devem corresponder aos recursos de nós de armazenamento existentes. Por exemplo:
 - Se o site StorageGRID existente estiver usando dispositivos SG6000 ou SG6100, os nós somente de metadados baseados em software deverão atender aos seguintes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - 8 TB SSD ou armazenamento equivalente para o banco de dados Cassandra (rangedb/0)
 - Se o site StorageGRID existente estiver usando nós de armazenamento virtuais com 24 GB de RAM, CPU de 8 núcleos e 3 TB ou 4 TB de armazenamento de metadados, os nós somente de metadados baseados em software deverão usar recursos semelhantes (24 GB de RAM, CPU de 8 núcleos e 4 TB de armazenamento de metadados (rangedb/0)).

Ao adicionar um novo site StorageGRID, a capacidade total de metadados do novo site deve, no mínimo, corresponder aos sites StorageGRID existentes e os novos recursos do site devem corresponder aos nós de armazenamento nos sites StorageGRID existentes.

- Se você estiver instalando um novo sistema (StorageGRID 11.6 ou superior) e cada nó de armazenamento tiver 128 GB ou mais de RAM, atribua 8 TB ou mais ao volume 0. Usar um valor maior para o volume 0 pode aumentar o espaço permitido para metadados em cada nó de armazenamento.
- Ao configurar diferentes nós de armazenamento para um site, use a mesma configuração para o volume 0, se possível. Se um site contiver nós de armazenamento de tamanhos diferentes, o nó de armazenamento com o menor volume 0 determinará a capacidade de metadados desse site.

Para mais detalhes, acesse "[Gerenciar armazenamento de metadados de objetos](#)".

Requisitos de migração do contêiner de nó

O recurso de migração de nós permite que você mova manualmente um nó de um host para outro. Normalmente, ambos os hosts estão no mesmo data center físico.

A migração de nós permite que você execute a manutenção do host físico sem interromper as operações da rede. Você move todos os nós do StorageGRID, um de cada vez, para outro host antes de colocar o host físico offline. A migração de nós requer apenas um curto período de inatividade para cada nó e não deve afetar a operação ou a disponibilidade dos serviços de rede.

Se você quiser usar o recurso de migração de nós do StorageGRID, sua implantação deverá atender a requisitos adicionais:

- Nomes de interface de rede consistentes em hosts em um único data center físico
- Armazenamento compartilhado para metadados do StorageGRID e volumes de repositório de objetos que podem ser acessados por todos os hosts em um único data center físico. Por exemplo, você pode usar matrizes de armazenamento NetApp E-Series.

Se você estiver usando hosts virtuais e a camada do hipervisor subjacente oferecer suporte à migração de VM, talvez seja interessante usar esse recurso em vez do recurso de migração de nós no StorageGRID. Nesse caso, você pode ignorar esses requisitos adicionais.

Antes de executar a migração ou a manutenção do hipervisor, desligue os nós corretamente. Veja as

instruções para ["desligando um nó de grade"](#) .

VMware Live Migration não suportado

Ao executar a instalação bare-metal em VMs VMware, o OpenStack Live Migration e o VMware live vMotion fazem com que o tempo do relógio da máquina virtual salte e não são suportados para nós de grade de nenhum tipo. Embora raros, horários incorretos podem resultar em perda de dados ou atualizações de configuração.

A migração fria é suportada. Na migração a frio, você desliga os nós do StorageGRID antes de migrá-los entre hosts. Veja as instruções para ["desligando um nó de grade"](#) .

Nomes de interface de rede consistentes

Para mover um nó de um host para outro, o serviço de host StorageGRID precisa ter alguma confiança de que a conectividade de rede externa que o nó tem em seu local atual pode ser duplicada no novo local. Ele obtém essa confiança por meio do uso de nomes de interface de rede consistentes nos hosts.

Suponha, por exemplo, que o StorageGRID NodeA em execução no Host1 tenha sido configurado com os seguintes mapeamentos de interface:

eth0 → bond0.1001

eth1 → bond0.1002

eth2 → bond0.1003

O lado esquerdo das setas corresponde às interfaces tradicionais visualizadas de dentro de um contêiner StorageGRID (ou seja, as interfaces Grid, Admin e Client Network, respectivamente). O lado direito das setas corresponde às interfaces de host reais que fornecem essas redes, que são três interfaces VLAN subordinadas ao mesmo vínculo de interface física.

Agora, suponha que você queira migrar o NodeA para o Host2. Se o Host2 também tiver interfaces denominadas bond0.1001, bond0.1002 e bond0.1003, o sistema permitirá a movimentação, supondo que as interfaces com nomes semelhantes fornecerão a mesma conectividade no Host2 que no Host1. Se o Host2 não tiver interfaces com os mesmos nomes, a movimentação não será permitida.

Existem muitas maneiras de obter uma nomenclatura de interface de rede consistente em vários hosts; consulte ["Configurar a rede do host"](#) para alguns exemplos.

Armazenamento compartilhado

Para obter migrações de nós rápidas e com baixa sobrecarga, o recurso de migração de nós do StorageGRID não move fisicamente os dados dos nós. Em vez disso, a migração de nós é realizada como um par de operações de exportação e importação, da seguinte maneira:

Passos

1. Durante a operação de "exportação de nó", uma pequena quantidade de dados de estado persistentes é extraída do contêiner de nó em execução no HostA e armazenada em cache no volume de dados do sistema desse nó. Em seguida, o contêiner do nó no HostA é desinstanciado.
2. Durante a operação "importação de nó", o contêiner de nó no HostB que usa a mesma interface de rede e

mapeamentos de armazenamento em bloco que estavam em vigor no HostA é instanciado. Em seguida, os dados de estado persistentes armazenados em cache são inseridos na nova instância.

Dado esse modo de operação, todos os dados do sistema e volumes de armazenamento de objetos do nó devem ser acessíveis tanto do HostA quanto do HostB para que a migração seja permitida e funcione. Além disso, eles devem ter sido mapeados no nó usando nomes que certamente fazem referência aos mesmos LUNs no HostA e no HostB.

O exemplo a seguir mostra uma solução para mapeamento de dispositivo de bloco para um nó de armazenamento StorageGRID , onde o multipathing DM está em uso nos hosts e o campo alias foi usado em `/etc/multipath.conf` para fornecer nomes de dispositivos de bloco consistentes e amigáveis disponíveis em todos os hosts.

```
/var/local    → /dev/mapper/sgws-sn1-var-local
rangedb0     → /dev/mapper/sgws-sn1-rangedb0
rangedb1     → /dev/mapper/sgws-sn1-rangedb1
rangedb2     → /dev/mapper/sgws-sn1-rangedb2
rangedb3     → /dev/mapper/sgws-sn1-rangedb3
```

Preparar os hosts (Ubuntu ou Debian)

Como as configurações de todo o host mudam durante a instalação

Em sistemas bare metal, o StorageGRID faz algumas alterações em todo o host `sysctl` configurações.

As seguintes alterações são feitas:

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
```

```

more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536

```



```

net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096

```

Instalar Linux

Você deve instalar o StorageGRID em todos os hosts de grade Ubuntu ou Debian. Para obter uma lista de versões suportadas, use a NetApp Interoperability Matrix Tool.

Antes de começar

Certifique-se de que seu sistema operacional atenda aos requisitos mínimos de versão do kernel do StorageGRID, conforme listado abaixo. Use o comando `uname -r` para obter a versão do kernel do seu sistema operacional ou consulte o fornecedor do seu sistema operacional.

Observação: O suporte para as versões 18.04 e 20.04 do Ubuntu foi descontinuado e será removido em uma versão futura.

Versão do Ubuntu	Versão mínima do kernel	Nome do pacote do kernel
18.04.6 (obsoleto)	5.4.0-150-genérico	linux-image-5.4.0-150-generic/bionic-updates,bionic-security, agora 5.4.0-150.167~18.04.1
20.04.5 (obsoleto)	5.4.0-131-genérico	linux-image-5.4.0-131-generic/focal-updates, agora 5.4.0-131.147
22.04.1	5.15.0-47-genérico	linux-image-5.15.0-47-generic/jammy-updates,jammy-security, agora 5.15.0-47.51
24,04	6.8.0-31-genérico	linux-image-6.8.0-31-generic/noble, agora 6.8.0-31.31

Observação: O suporte para o Debian versão 11 foi descontinuado e será removido em uma versão futura.

Versão Debian	Versão mínima do kernel	Nome do pacote do kernel
11 (obsoleto)	5.10.0-18-amd64	linux-image-5.10.0-18-amd64/stable, agora 5.10.150-1

Versão Debian	Versão mínima do kernel	Nome do pacote do kernel
12	6.1.0-9-amd64	linux-image-6.1.0-9-amd64/stable, agora 6.1.27-1

Passos

1. Instale o Linux em todos os hosts de grade físicos ou virtuais de acordo com as instruções do distribuidor ou seu procedimento padrão.



Não instale nenhum ambiente de área de trabalho gráfico. Ao instalar o Ubuntu, você deve selecionar **utilitários padrão do sistema**. É recomendável selecionar **Servidor OpenSSH** para habilitar o acesso SSH aos seus hosts Ubuntu. Todas as outras opções podem permanecer desmarcadas.

2. Certifique-se de que todos os hosts tenham acesso aos repositórios de pacotes do Ubuntu ou Debian.
3. Se a troca estiver habilitada:
 - a. Execute o seguinte comando: `$ sudo swapoff --all`
 - b. Remova todas as entradas de swap de `/etc/fstab` para persistir as configurações.



Não desabilitar completamente a troca pode reduzir severamente o desempenho.

Entenda a instalação do perfil do AppArmor

Se você estiver operando em um ambiente Ubuntu autoimplantado e usando o sistema de controle de acesso obrigatório AppArmor, os perfis do AppArmor associados aos pacotes que você instala no sistema base podem ser bloqueados pelos pacotes correspondentes instalados com StorageGRID.

Por padrão, os perfis do AppArmor são instalados para pacotes que você instala no sistema operacional base. Quando você executa esses pacotes do contêiner do sistema StorageGRID, os perfis do AppArmor são bloqueados. Os pacotes base DHCP, MySQL, NTP e tcdump entram em conflito com o AppArmor, e outros pacotes base também podem entrar em conflito.

Você tem duas opções para lidar com perfis do AppArmor:

- Desabilite perfis individuais para os pacotes instalados no sistema base que se sobrepõem aos pacotes no contêiner do sistema StorageGRID. Quando você desabilita perfis individuais, uma entrada aparece nos arquivos de log do StorageGRID indicando que o AppArmor está habilitado.

Use os seguintes comandos:

```
sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
```

Exemplo:

```
sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/  
sudo apparmor_parser -R /etc/apparmor.d/bin.ping
```

- Desabilite o AppArmor completamente. Para o Ubuntu 9.10 ou posterior, siga as instruções na comunidade online do Ubuntu: "[Desativar AppArmor](#)". Desabilitar completamente o AppArmor pode não ser possível em versões mais recentes do Ubuntu.

Depois de desabilitar o AppArmor, nenhuma entrada indicando que o AppArmor está habilitado aparecerá nos arquivos de log do StorageGRID.

Configurar a rede host (Ubuntu ou Debian)

Após concluir a instalação do Linux em seus hosts, talvez seja necessário executar alguma configuração adicional para preparar um conjunto de interfaces de rede em cada host que sejam adequadas para mapeamento nos nós do StorageGRID que você implantará posteriormente.

Antes de começar

- Você revisou o "[Diretrizes de rede StorageGRID](#)".
- Você revisou as informações sobre "[requisitos de migração do contêiner de nó](#)".
- Se você estiver usando hosts virtuais, você leu [oconsiderações e recomendações para clonagem de endereços MAC](#) antes de configurar a rede host.



Se estiver usando VMs como hosts, você deve selecionar VMXNET 3 como o adaptador de rede virtual. O adaptador de rede VMware E1000 causou problemas de conectividade com contêineres StorageGRID implantados em determinadas distribuições do Linux.

Sobre esta tarefa

Os nós da grade devem ser capazes de acessar a Rede da Grade e, opcionalmente, as Redes de Administração e Cliente. Você fornece esse acesso criando mapeamentos que associam a interface física do host às interfaces virtuais de cada nó da grade. Ao criar interfaces de host, use nomes amigáveis para facilitar a implantação em todos os hosts e permitir a migração.

A mesma interface pode ser compartilhada entre o host e um ou mais nós. Por exemplo, você pode usar a mesma interface para acesso ao host e acesso à rede de administração do nó, para facilitar a manutenção do host e do nó. Embora a mesma interface possa ser compartilhada entre o host e nós individuais, todos devem ter endereços IP diferentes. Endereços IP não podem ser compartilhados entre nós ou entre o host e qualquer nó.

Você pode usar a mesma interface de rede do host para fornecer a interface Grid Network para todos os nós StorageGRID no host; você pode usar uma interface de rede do host diferente para cada nó; ou pode fazer algo intermediário. No entanto, normalmente você não forneceria a mesma interface de rede de host que as interfaces de rede de grade e de administração para um único nó, ou como a interface de rede de grade para um nó e a interface de rede de cliente para outro.

Você pode concluir esta tarefa de muitas maneiras. Por exemplo, se seus hosts forem máquinas virtuais e você estiver implantando um ou dois nós StorageGRID para cada host, poderá criar o número correto de interfaces de rede no hipervisor e usar um mapeamento 1 para 1. Se você estiver implantando vários nós em hosts bare metal para uso em produção, poderá aproveitar o suporte da pilha de rede Linux para VLAN e

LACP para tolerância a falhas e compartilhamento de largura de banda. As seções a seguir fornecem abordagens detalhadas para ambos os exemplos. Você não precisa usar nenhum desses exemplos; você pode usar qualquer abordagem que atenda às suas necessidades.



Não use dispositivos de ligação ou ponte diretamente como interface de rede do contêiner. Isso pode impedir a inicialização do nó causada por um problema de kernel com o uso de MACVLAN com dispositivos de ligação e ponte no namespace do contêiner. Em vez disso, use um dispositivo sem vínculo, como um par VLAN ou Ethernet virtual (veth). Especifique este dispositivo como a interface de rede no arquivo de configuração do nó.

Considerações e recomendações para clonagem de endereços MAC

A clonagem de endereço MAC faz com que o contêiner use o endereço MAC do host, e o host use o endereço MAC de um endereço especificado por você ou de um gerado aleatoriamente. Você deve usar a clonagem de endereço MAC para evitar o uso de configurações de rede em modo promíscuo.

Habilitando a clonagem de MAC

Em certos ambientes, a segurança pode ser aprimorada por meio da clonagem de endereços MAC, pois ela permite que você use uma NIC virtual dedicada para a rede de administração, a rede de grade e a rede de cliente. Fazer com que o contêiner use o endereço MAC da NIC dedicada no host permite que você evite o uso de configurações de rede em modo promíscuo.



A clonagem de endereço MAC deve ser usada com instalações de servidores virtuais e pode não funcionar corretamente com todas as configurações de dispositivos físicos.



Se um nó não iniciar devido a uma interface de destino de clonagem de MAC estar ocupada, talvez seja necessário definir o link como "inativo" antes de iniciar o nó. Além disso, é possível que o ambiente virtual impeça a clonagem de MAC em uma interface de rede enquanto o link estiver ativo. Se um nó não conseguir definir o endereço MAC e iniciar devido a uma interface estar ocupada, definir o link como "inativo" antes de iniciar o nó pode resolver o problema.

A clonagem de endereço MAC é desabilitada por padrão e deve ser definida pelas chaves de configuração do nó. Você deve habilitá-lo ao instalar o StorageGRID.

Existe uma chave para cada rede:

- ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC
- GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC
- CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Definir a chave como "true" faz com que o contêiner use o endereço MAC da NIC do host. Além disso, o host usará o endereço MAC da rede de contêineres especificada. Por padrão, o endereço do contêiner é um endereço gerado aleatoriamente, mas se você tiver definido um usando o `_NETWORK_MAC` chave de configuração do nó, esse endereço é usado em seu lugar. O host e o contêiner sempre terão endereços MAC diferentes.



Habilitar a clonagem de MAC em um host virtual sem também habilitar o modo promíscuo no hipervisor pode fazer com que a rede do host Linux que usa a interface do host pare de funcionar.

Casos de uso de clonagem de MAC

Há dois casos de uso a serem considerados com a clonagem de MAC:

- **Clonagem de MAC não habilitada:** Quando o `_CLONE_MAC` a chave no arquivo de configuração do nó não estiver definida ou definida como "false", o host usará o MAC da NIC do host e o contêiner terá um MAC gerado StorageGRID, a menos que um MAC seja especificado no `_NETWORK_MAC` chave. Se um endereço for definido no `_NETWORK_MAC` chave, o contêiner terá o endereço especificado na `_NETWORK_MAC` chave. Esta configuração de chaves requer o uso do modo promíscuo.
- **Clonagem de MAC habilitada:** Quando o `_CLONE_MAC` a chave no arquivo de configuração do nó for definida como "true", o contêiner usa o MAC da NIC do host e o host usa um MAC gerado StorageGRID, a menos que um MAC seja especificado no `_NETWORK_MAC` chave. Se um endereço for definido no `_NETWORK_MAC` chave, o host usa o endereço especificado em vez de um gerado. Nesta configuração de chaves, você não deve usar o modo promíscuo.



Se você não quiser usar a clonagem de endereço MAC e preferir permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes daqueles atribuídos pelo hipervisor, certifique-se de que as propriedades de segurança nos níveis de switch virtual e grupo de portas estejam definidas como **Aceitar** para Modo Promíscuo, Alterações de Endereço MAC e Transmissões Falsificadas. Os valores definidos no switch virtual podem ser substituídos pelos valores no nível do grupo de portas, portanto, certifique-se de que as configurações sejam as mesmas em ambos os locais.

Para habilitar a clonagem de MAC, consulte o "[instruções para criar arquivos de configuração de nó](#)".

Exemplo de clonagem de MAC

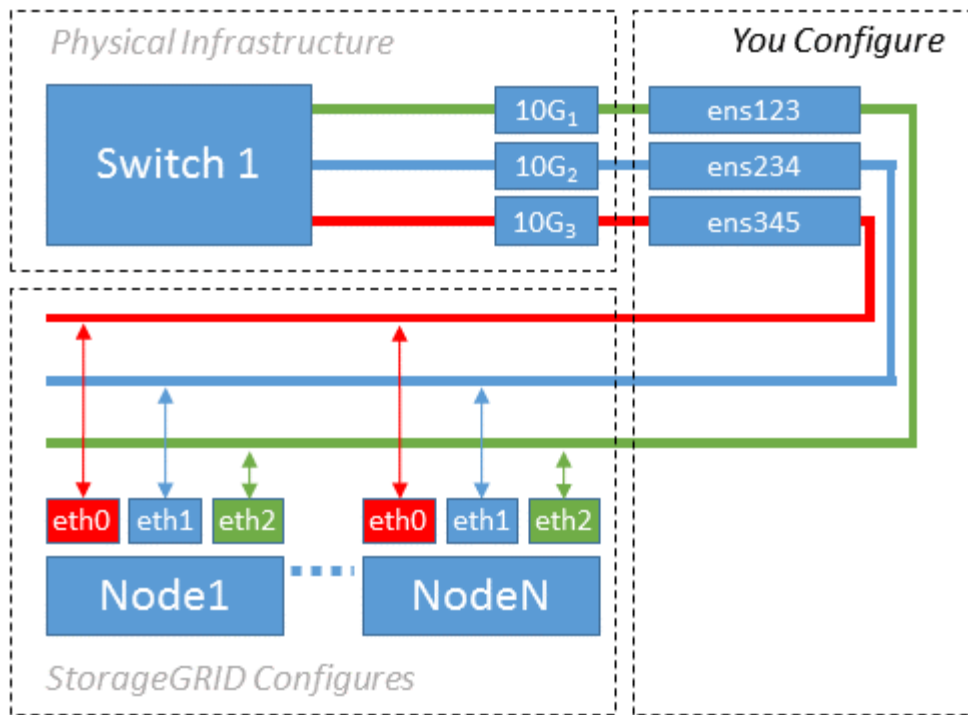
Exemplo de clonagem de MAC habilitada com um host com endereço MAC de 11:22:33:44:55:66 para a interface ens256 e as seguintes chaves no arquivo de configuração do nó:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Resultado: o MAC do host para ens256 é b2:9c:02:c2:27:10 e o MAC da rede de administração é 11:22:33:44:55:66

Exemplo 1: mapeamento 1 para 1 para NICs físicas ou virtuais

O Exemplo 1 descreve um mapeamento de interface física simples que requer pouca ou nenhuma configuração do lado do host.



O sistema operacional Linux cria as interfaces ensXYZ automaticamente durante a instalação ou inicialização, ou quando as interfaces são adicionadas a quente. Nenhuma configuração é necessária além de garantir que as interfaces estejam definidas para serem ativadas automaticamente após a inicialização. Você precisa determinar qual ensXYZ corresponde a qual rede StorageGRID (Grid, Admin ou Cliente) para poder fornecer os mapeamentos corretos posteriormente no processo de configuração.

Observe que a figura mostra vários nós StorageGRID ; no entanto, você normalmente usaria essa configuração para VMs de nó único.

Se o Switch 1 for um switch físico, você deverá configurar as portas conectadas às interfaces 10G₁ a 10G₃ para o modo de acesso e colocá-las nas VLANs apropriadas.

Exemplo 2: VLANs transportando vínculo LACP

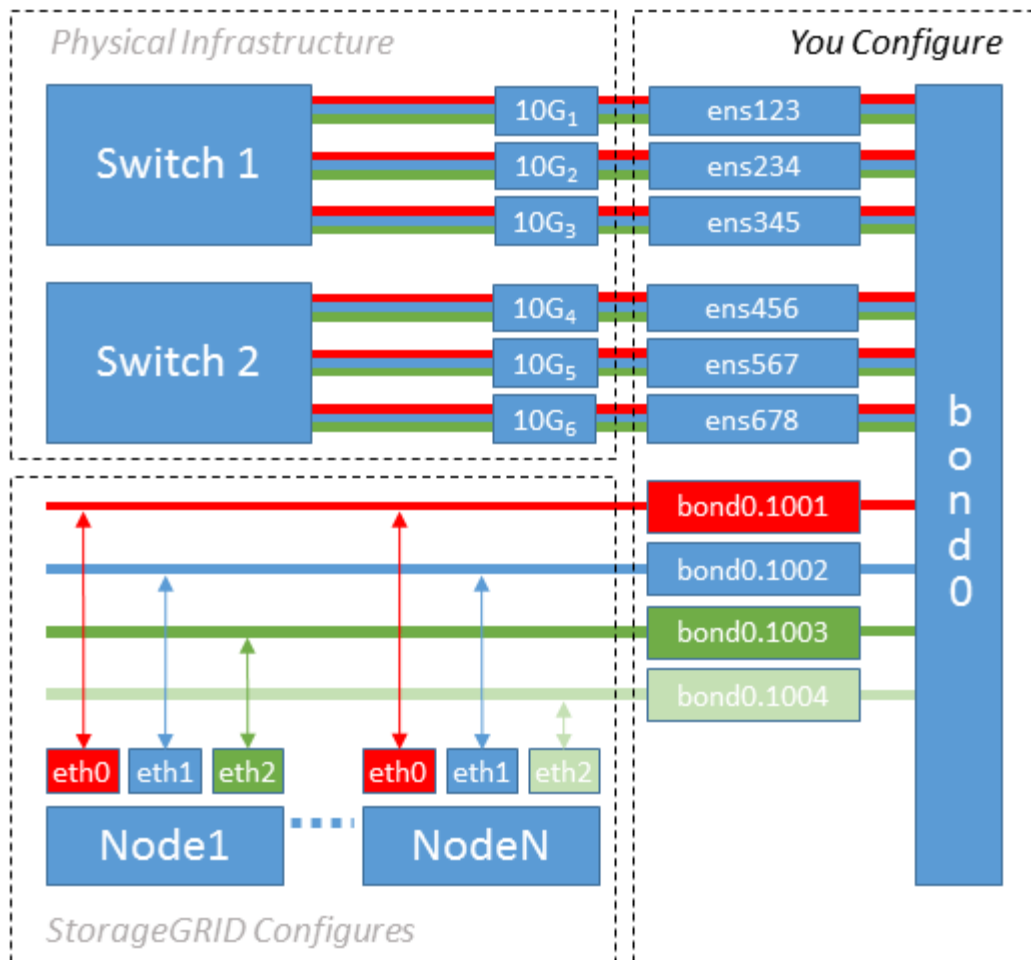
O Exemplo 2 pressupõe que você esteja familiarizado com a vinculação de interfaces de rede e com a criação de interfaces VLAN na distribuição Linux que está usando.

Sobre esta tarefa

O Exemplo 2 descreve um esquema genérico e flexível baseado em VLAN que facilita o compartilhamento de toda a largura de banda de rede disponível entre todos os nós em um único host. Este exemplo é particularmente aplicável a hosts bare metal.

Para entender este exemplo, suponha que você tenha três sub-redes separadas para as redes Grid, Admin e Client em cada data center. As sub-redes estão em VLANs separadas (1001, 1002 e 1003) e são apresentadas ao host em uma porta de tronco vinculada ao LACP (bond0). Você configuraria três interfaces VLAN no bond: bond0.1001, bond0.1002 e bond0.1003.

Se você precisar de VLANs e sub-redes separadas para redes de nós no mesmo host, poderá adicionar interfaces de VLAN no vínculo e mapeá-las no host (mostrado como bond0.1004 na ilustração).



Passos

1. Agregue todas as interfaces de rede física que serão usadas para conectividade de rede StorageGRID em um único vínculo LACP.

Use o mesmo nome para o vínculo em todos os hosts, por exemplo, bond0.

2. Crie interfaces VLAN que usem esse vínculo como seu "dispositivo físico" associado, usando a convenção de nomenclatura de interface VLAN padrão `physdev-name.VLAN ID`.

Observe que as etapas 1 e 2 exigem configuração apropriada nos switches de borda que terminam as outras extremidades dos links de rede. As portas do switch de borda também devem ser agregadas em um canal de porta LACP, configuradas como um tronco e autorizadas a passar todas as VLANs necessárias.

São fornecidos arquivos de configuração de interface de exemplo para este esquema de configuração de rede por host.

Informações relacionadas

["Exemplo /etc/network/interfaces"](#)

Configurar armazenamento do host

Você deve alocar volumes de armazenamento em bloco para cada host.

Antes de começar

Você revisou os seguintes tópicos, que fornecem as informações necessárias para realizar esta tarefa:

- ["Requisitos de armazenamento e desempenho"](#)
- ["Requisitos de migração do contêiner de nó"](#)

Sobre esta tarefa

Ao alocar volumes de armazenamento em bloco (LUNs) para hosts, use as tabelas em "Requisitos de armazenamento" para determinar o seguinte:

- Número de volumes necessários para cada host (com base no número e nos tipos de nós que serão implantados naquele host)
- Categoria de armazenamento para cada volume (ou seja, Dados do Sistema ou Dados do Objeto)
- Tamanho de cada volume

Você usará essas informações, bem como o nome persistente atribuído pelo Linux a cada volume físico ao implantar nós StorageGRID no host.



Você não precisa particionar, formatar ou montar nenhum desses volumes; você só precisa garantir que eles estejam visíveis para os hosts.



Somente um LUN de dados de objeto é necessário para nós de armazenamento somente de metadados.

Evite usar arquivos de dispositivos especiais "brutos" (`/dev/sdb`, por exemplo) ao compor sua lista de nomes de volumes. Esses arquivos podem mudar durante as reinicializações do host, o que afetará a operação correta do sistema. Se você estiver usando iSCSI LUNs e Device Mapper Multipathing, considere usar aliases multipath no `/dev/mapper` diretório, especialmente se sua topologia SAN incluir caminhos de rede redundantes para o armazenamento compartilhado. Alternativamente, você pode usar os softlinks criados pelo sistema em `/dev/disk/by-path/` para seus nomes de dispositivos persistentes.

Por exemplo:


```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root 9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Os resultados serão diferentes para cada instalação.

Atribua nomes amigáveis a cada um desses volumes de armazenamento em bloco para simplificar a instalação inicial do StorageGRID e os procedimentos futuros de manutenção. Se você estiver usando o driver multipath do mapeador de dispositivos para acesso redundante a volumes de armazenamento compartilhado, poderá usar o `alias` campo em seu `/etc/multipath.conf` arquivo.

Por exemplo:

```

multipaths {
    multipath {
        wwid 3600a09800059d6df00005df2573c2c30
        alias docker-storage-volume-hostA
    }
    multipath {
        wwid 3600a09800059d6df00005df3573c2c30
        alias sgws-adml-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df4573c2c30
        alias sgws-adml-audit-logs
    }
    multipath {
        wwid 3600a09800059d6df00005df5573c2c30
        alias sgws-adml-tables
    }
    multipath {
        wwid 3600a09800059d6df00005df6573c2c30
        alias sgws-gw1-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df7573c2c30
        alias sgws-sn1-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df7573c2c30
        alias sgws-sn1-rangedb-0
    }
    ...
}

```

Usar o campo de alias dessa forma faz com que os aliases apareçam como dispositivos de bloco no `/dev/mapper` diretório no host, permitindo que você especifique um nome amigável e facilmente validado sempre que uma operação de configuração ou manutenção exigir a especificação de um volume de armazenamento em bloco.

Se você estiver configurando o armazenamento compartilhado para oferecer suporte à migração de nós do StorageGRID e usar o Device Mapper Multipathing, você pode criar e instalar um `/etc/multipath.conf` em todos os hosts co-localizados. Apenas certifique-se de usar um volume de armazenamento do Docker diferente em cada host. Usar aliases e incluir o nome do host de destino no alias para cada LUN de volume de armazenamento do Docker tornará isso fácil de lembrar e é recomendado.



O suporte ao Docker como mecanismo de contêiner para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contêiner em uma versão futura.

Informações relacionadas

- ["Requisitos de armazenamento e desempenho"](#)
- ["Requisitos de migração do contêiner de nó"](#)

Configurar o volume de armazenamento do mecanismo de contêiner

Antes de instalar o mecanismo de contêiner (Docker ou Podman), talvez seja necessário formatar o volume de armazenamento e montá-lo.



O suporte ao Docker como mecanismo de contêiner para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contêiner em uma versão futura.

Sobre esta tarefa

Você pode pular essas etapas se planeja usar armazenamento local para o volume de armazenamento do Docker e tiver espaço suficiente disponível na partição do host que contém `/var/lib`.

Passos

1. Crie um sistema de arquivos no volume de armazenamento do Docker:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Monte o volume de armazenamento do Docker:

```
sudo mkdir -p /var/lib/docker  
sudo mount docker-storage-volume-device /var/lib/docker
```

3. Adicione uma entrada para docker-storage-volume-device em `/etc/fstab`.

Esta etapa garante que o volume de armazenamento será remontado automaticamente após a reinicialização do host.

Instalar o Docker

O sistema StorageGRID é executado no Linux como uma coleção de contêineres Docker. Antes de instalar o StorageGRID, você deve instalar o Docker.



O suporte ao Docker como mecanismo de contêiner para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contêiner em uma versão futura.

Passos

1. Instale o Docker seguindo as instruções para sua distribuição Linux.



Se o Docker não estiver incluído na sua distribuição Linux, você poderá baixá-lo do site do Docker.

2. Certifique-se de que o Docker foi habilitado e iniciado executando os dois comandos a seguir:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Confirme se você instalou a versão esperada do Docker digitando o seguinte:

```
sudo docker version
```

As versões do cliente e do servidor devem ser 1.11.0 ou posterior.

Informações relacionadas

["Configurar armazenamento do host"](#)

Instalar serviços de host do StorageGRID

Use o pacote StorageGRID DEB para instalar os serviços do host StorageGRID .

Sobre esta tarefa

Estas instruções descrevem como instalar os serviços de host dos pacotes DEB. Como alternativa, você pode usar os metadados do repositório APT incluídos no arquivo de instalação para instalar os pacotes DEB remotamente. Consulte as instruções do repositório APT para seu sistema operacional Linux.

Passos

1. Copie os pacotes DEB do StorageGRID para cada um dos seus hosts ou disponibilize-os no armazenamento compartilhado.

Por exemplo, coloque-os no `/tmp` diretório, para que você possa usar o comando de exemplo na próxima etapa.

2. Efetue login em cada host como root ou usando uma conta com permissão sudo e execute os seguintes comandos.

Você deve instalar o `images` pacote primeiro, e o `service` pacote segundo. Se você colocou os pacotes em um diretório diferente de `/tmp` , modifique o comando para refletir o caminho que você usou.

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```



O Python 2,7 já deve estar instalado antes que os pacotes StorageGRID possam ser instalados. O `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` o comando falhará até que você o faça.

Automatize a instalação (Ubuntu ou Debian)

Você pode automatizar a instalação do serviço de host StorageGRID e a configuração dos nós da grade.

Sobre esta tarefa

Automatizar a implantação pode ser útil em qualquer um dos seguintes casos:

- Você já usa uma estrutura de orquestração padrão, como Ansible, Puppet ou Chef, para implantar e configurar hosts físicos ou virtuais.
- Você pretende implantar várias instâncias do StorageGRID .
- Você está implantando uma instância StorageGRID grande e complexa.

O serviço de host StorageGRID é instalado por um pacote e controlado por arquivos de configuração que podem ser criados interativamente durante uma instalação manual ou preparados com antecedência (ou programaticamente) para permitir a instalação automatizada usando estruturas de orquestração padrão. O StorageGRID fornece scripts Python opcionais para automatizar a configuração de dispositivos StorageGRID e de todo o sistema StorageGRID (a "grade"). Você pode usar esses scripts diretamente ou inspecioná-los para aprender como usar a API REST de instalação do StorageGRID em ferramentas de implantação e configuração de grade que você mesmo desenvolve.

Automatize a instalação e a configuração do serviço de host StorageGRID

Você pode automatizar a instalação do serviço de host StorageGRID usando estruturas de orquestração padrão, como Ansible, Puppet, Chef, Fabric ou SaltStack.

O serviço de host StorageGRID é empacotado em um DEB e é controlado por arquivos de configuração que podem ser preparados com antecedência (ou programaticamente) para permitir a instalação automatizada. Se você já usa uma estrutura de orquestração padrão para instalar e configurar o Ubuntu ou Debian, adicionar o StorageGRID aos seus playbooks ou receitas deve ser simples.

Você pode automatizar estas tarefas:

1. Instalando Linux
2. Configurando o Linux
3. Configurando interfaces de rede do host para atender aos requisitos do StorageGRID
4. Configurando o armazenamento do host para atender aos requisitos do StorageGRID
5. Instalando o Docker
6. Instalando o serviço de host StorageGRID
7. Criando arquivos de configuração de nó StorageGRID em `/etc/storagegrid/nodes`
8. Validando arquivos de configuração do nó StorageGRID
9. Iniciando o serviço do host StorageGRID

Exemplo de função e manual do Ansible

Exemplo de função e manual do Ansible são fornecidos com o arquivo de instalação no `/extras` pasta. O manual do Ansible mostra como o `storagegrid` A função prepara os hosts e instala o StorageGRID nos servidores de destino. Você pode personalizar a função ou o manual conforme necessário.

Automatize a configuração do StorageGRID

Após implantar os nós da grade, você pode automatizar a configuração do sistema StorageGRID .

Antes de começar

- Você sabe a localização dos seguintes arquivos do arquivo de instalação.

Nome do arquivo	Descrição
configurar-storagegrid.py	Script Python usado para automatizar a configuração
configurar-storagegrid.sample.json	Arquivo de configuração de exemplo para uso com o script
configurar-storagegrid.blank.json	Arquivo de configuração em branco para uso com o script

- Você criou um `configure-storagegrid.json` arquivo de configuração. Para criar este arquivo, você pode modificar o arquivo de configuração de exemplo(`configure-storagegrid.sample.json`) ou o arquivo de configuração em branco(`configure-storagegrid.blank.json`).

Sobre esta tarefa

Você pode usar o `configure-storagegrid.py` Script Python e o `configure-storagegrid.json` arquivo de configuração para automatizar a configuração do seu sistema StorageGRID .



Você também pode configurar o sistema usando o Grid Manager ou a API de instalação.

Passos

1. Faça login na máquina Linux que você está usando para executar o script Python.
2. Mude para o diretório onde você extraiu o arquivo de instalação.

Por exemplo:

```
cd StorageGRID-Webscale-version/platform
```

onde `platform` é `debs` , `rpms` , ou `vsphere` .

3. Execute o script Python e use o arquivo de configuração que você criou.

Por exemplo:

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Resultado

Um pacote de recuperação .zip O arquivo é gerado durante o processo de configuração e é baixado para o diretório onde você está executando o processo de instalação e configuração. Você deve fazer backup do

arquivo do pacote de recuperação para poder recuperar o sistema StorageGRID se um ou mais nós da grade falharem. Por exemplo, copie-o para um local de rede seguro e com backup e para um local de armazenamento em nuvem seguro.



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 .

Se você especificou que senhas aleatórias devem ser geradas, abra o `Passwords.txt` arquivo e procure as senhas necessárias para acessar seu sistema StorageGRID .

```
#####
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####      ./sgws-recovery-package-994078-rev1.zip      #####
#####   Safeguard this file as it will be needed in case of a   #####
#####               StorageGRID node recovery.               #####
#####
```

Seu sistema StorageGRID estará instalado e configurado quando uma mensagem de confirmação for exibida.

```
StorageGRID has been configured and installed.
```

Informações relacionadas

["Instalação REST API"](#)

Implantar nós de grade virtual (Ubuntu ou Debian)

Crie arquivos de configuração de nó para implantações do Ubuntu ou Debian

Os arquivos de configuração de nó são pequenos arquivos de texto que fornecem as informações que o serviço de host StorageGRID precisa para iniciar um nó e conectá-lo à rede apropriada e aos recursos de armazenamento em bloco. Os arquivos de configuração de nós são usados para nós virtuais e não para nós de dispositivos.

Localização dos arquivos de configuração do nó

Coloque o arquivo de configuração para cada nó StorageGRID no `/etc/storagegrid/nodes` diretório no host onde o nó será executado. Por exemplo, se você planeja executar um nó de administração, um nó de gateway e um nó de armazenamento no HostA, você deve colocar três arquivos de configuração de nó em `/etc/storagegrid/nodes` no HostA.

Você pode criar os arquivos de configuração diretamente em cada host usando um editor de texto, como vim ou nano, ou pode criá-los em outro lugar e movê-los para cada host.

Nomenclatura de arquivos de configuração de nó

Os nomes dos arquivos de configuração são significativos. O formato é `node-name.conf` , onde `node-name` é um nome que você atribui ao nó. Este nome aparece no instalador do StorageGRID e é usado para operações de manutenção de nós, como migração de nós.

Os nomes dos nós devem seguir estas regras:

- Deve ser único
- Deve começar com uma letra
- Pode conter os caracteres de A a Z e de a a z
- Pode conter os números de 0 a 9
- Pode conter um ou mais hífens (-)
- Não deve ter mais de 32 caracteres, sem incluir o `.conf` extensão

Quaisquer arquivos em `/etc/storagegrid/nodes` que não seguem essas convenções de nomenclatura não serão analisados pelo serviço host.

Se você tiver uma topologia multisite planejada para sua grade, um esquema típico de nomenclatura de nós pode ser:

`site-nodetype-nodenumbers.conf`

Por exemplo, você pode usar `dc1-adm1.conf` para o primeiro nó de administração no Data Center 1 e `dc2-sn3.conf` para o terceiro nó de armazenamento no Data Center 2. No entanto, você pode usar qualquer esquema que desejar, desde que todos os nomes de nós sigam as regras de nomenclatura.

Conteúdo de um arquivo de configuração de nó

Um arquivo de configuração contém pares chave/valor, com uma chave e um valor por linha. Para cada par chave/valor, siga estas regras:

- A chave e o valor devem ser separados por um sinal de igual(=) e espaço em branco opcional.
- As chaves não podem conter espaços.
- Os valores podem conter espaços incorporados.
- Qualquer espaço em branco à esquerda ou à direita será ignorado.

A tabela a seguir define os valores para todas as chaves suportadas. Cada tecla tem uma das seguintes designações:

- **Obrigatório:** Obrigatório para cada nó ou para os tipos de nó especificados
- **Melhor prática:** Opcional, embora recomendado
- **Opcional:** Opcional para todos os nós

Chaves de rede de administração

IP_ADMIN

Valor	Designação
Endereço IPv4 da rede de grade do nó administrativo primário da grade à qual esse nó pertence. Use o mesmo valor especificado para GRID_NETWORK_IP para o nó de grade com NODE_TYPE = VM_Admin_Node e ADMIN_ROLE = Primary. Se você omitir esse parâmetro, o nó tentará descobrir um nó de administração primário usando mDNS. "Como os nós da grade descobrem o nó administrativo principal" Observação: Este valor é ignorado e pode ser proibido no nó de administração primário.	Melhores práticas

CONFIGURAÇÃO_DE_ADMINISTRAÇÃO

Valor	Designação
DHCP, ESTÁTICO ou DESATIVADO	Opcional

ADMIN_REDE_ESL

Valor	Designação
Lista separada por vírgulas de sub-redes em notação CIDR com as quais este nó deve se comunicar usando o gateway da rede de administração. Exemplo: 172.16.0.0/21, 172.17.0.0/21	Opcional

GATEWAY_DE_REDE_ADMINISTRATIVA

Valor	Designação
Endereço IPv4 do gateway da rede de administração local para este nó. Deve estar na sub-rede definida por ADMIN_NETWORK_IP e ADMIN_NETWORK_MASK. Este valor é ignorado para redes configuradas por DHCP. Exemplos: 1.1.1.1 10.224.4.81	Obrigatório se ADMIN_NETWORK_ESL é especificado. Caso contrário, é opcional.

IP_DE_REDE_ADMINISTRATIVA

Valor	Designação
Endereço IPv4 deste nó na rede de administração. Esta chave só é necessária quando ADMIN_NETWORK_CONFIG = STATIC; não a especifique para outros valores.	Obrigatório quando ADMIN_NETWORK_CONFIG = STATIC.
Exemplos:	Caso contrário, é opcional.
1.1.1.1	
10.224.4.81	

ADMIN_REDE_MAC

Valor	Designação
O endereço MAC da interface de rede de administração no contêiner.	Opcional
Este campo é opcional. Se omitido, um endereço MAC será gerado automaticamente.	
Deve ter 6 pares de dígitos hexadecimais separados por dois pontos.	
Exemplo: b2:9c:02:c2:27:10	

MÁSCARA_DE_REDE_ADMINISTRATIVA

Valor	Designação
Máscara de rede IPv4 para este nó, na rede de administração. Especifique esta chave quando ADMIN_NETWORK_CONFIG = STATIC; não a especifique para outros valores.	Obrigatório se ADMIN_NETWORK_IP for especificado e ADMIN_NETWORK_CONFIG = STATIC.
Exemplos:	Caso contrário, é opcional.
255.255.255.0	
255.255.248.0	

MTU_DE_REDE_ADMINISTRATIVA

Valor	Designação
A unidade máxima de transmissão (MTU) para este nó na rede de administração. Não especifique se ADMIN_NETWORK_CONFIG = DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 será usado. Se você quiser usar quadros jumbo, defina a MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão. IMPORTANTE: O valor da MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conectado. Caso contrário, podem ocorrer problemas de desempenho da rede ou perda de pacotes. Exemplos: 1500 8192	Opcional

ADMIN_REDE_ALVO

Valor	Designação
Nome do dispositivo host que você usará para acesso à rede de administração pelo nó StorageGRID . Somente nomes de interface de rede são suportados. Normalmente, você usa um nome de interface diferente do que foi especificado para GRID_NETWORK_TARGET ou CLIENT_NETWORK_TARGET. Observação: Não use dispositivos de ligação ou ponte como alvo de rede. Configure uma VLAN (ou outra interface virtual) sobre o dispositivo de ligação ou use um par de ponte e Ethernet virtual (veth). Melhor prática: especifique um valor mesmo que este nó não tenha inicialmente um endereço IP de rede de administração. Depois, você pode adicionar um endereço IP de rede de administração, sem precisar reconfigurar o nó no host. Exemplos: bond0.1002 ens256	Melhores práticas

TIPO_DE_ALVO_DE_REDE_ADMINISTRATIVA

Valor	Designação
Interface (Este é o único valor suportado.)	Opcional

TIPO_DE_ALVO_DE_REDE_ADMINISTRAÇÃO_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou falso Defina a chave como "true" para fazer com que o contêiner StorageGRID use o endereço MAC da interface de destino do host na rede de administração. Melhores práticas: Em redes onde o modo promíscuo seria necessário, use a chave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Para mais detalhes sobre clonagem de MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Melhores práticas

FUNÇÃO_ADMINISTRATIVA

Valor	Designação
Primário ou não primário Esta chave só é necessária quando NODE_TYPE = VM_Admin_Node; não a especifique para outros tipos de nó.	Obrigatório quando NODE_TYPE = VM_Admin_Node Caso contrário, é opcional.

Bloquear chaves do dispositivo

LOGS_DE_AUDITORIA_DE_DISPOSITIVO_DE_BLOCO

Valor	Designação
Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento persistente de logs de auditoria. Exemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-audit-logs</pre>	Obrigatório para nós com NODE_TYPE = VM_Admin_Node. Não especifique isso para outros tipos de nós.

BLOCK_DEVICE_RANGEDB_nnn

Valor	Designação
Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento de objetos persistentes. Esta chave só é necessária para nós com NODE_TYPE = VM_Storage_Node; não a especifique para outros tipos de nós. Somente BLOCK_DEVICE_RANGEDB_000 é necessário; o restante é opcional. O dispositivo de bloco especificado para BLOCK_DEVICE_RANGEDB_000 deve ter pelo menos 4 TB; os outros podem ser menores. Não deixe lacunas. Se você especificar BLOCK_DEVICE_RANGEDB_005, também deverá especificar BLOCK_DEVICE_RANGEDB_004. Observação: para compatibilidade com implantações existentes, chaves de dois dígitos são suportadas para nós atualizados. Exemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-rangedb-000</pre>	Obrigatório: BLOCK_DEVICE_RANGEDB_000 Opcional: BLOCK_DEVICE_RANGEDB_001 BLOCK_DEVICE_RANGEDB_002 BLOCK_DEVICE_RANGEDB_003 BLOCK_DEVICE_RANGEDB_004 BLOCK_DEVICE_RANGEDB_005 BLOCK_DEVICE_RANGEDB_006 BLOCK_DEVICE_RANGEDB_007 BLOCK_DEVICE_RANGEDB_008 BLOCK_DEVICE_RANGEDB_009 BLOCK_DEVICE_RANGEDB_010 BLOCK_DEVICE_RANGEDB_011 BLOCK_DEVICE_RANGEDB_012 BLOCK_DEVICE_RANGEDB_013 BLOCK_DEVICE_RANGEDB_014 BLOCK_DEVICE_RANGEDB_015

TABELAS_DE_DISPOSITIVOS_DE_BLOCO

Valor	Designação
Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para armazenamento persistente de tabelas de banco de dados. Esta chave só é necessária para nós com NODE_TYPE = VM_Admin_Node; não a especifique para outros tipos de nós. Exemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-tables</pre>	Obrigatório

BLOCO_DISPOSITIVO_VAR_LOCAL

Valor	Designação
Caminho e nome do arquivo especial do dispositivo de bloco que este nó usará para seu /var/local armazenamento persistente. Exemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-var-local</pre>	Obrigatório

Chaves de rede do cliente

CONFIGURAÇÃO_DE_REDE_DO_CLIENTE

Valor	Designação
DHCP, ESTÁTICO ou DESATIVADO	Opcional

GATEWAY_DE_REDE_DO_CLIENTE

Valor	Designação

Endereço IPv4 do gateway da rede do cliente local para este nó, que deve estar na sub-rede definida por CLIENT_NETWORK_IP e CLIENT_NETWORK_MASK. Este valor é ignorado para redes configuradas por DHCP. Exemplos: 1.1.1.1 10.224.4.81	Opcional

IP_DE_REDE_DO_CLIENTE

Valor	Designação
Endereço IPv4 deste nó na rede do cliente. Esta chave só é necessária quando CLIENT_NETWORK_CONFIG = STATIC; não a especifique para outros valores. Exemplos: 1.1.1.1 10.224.4.81	Obrigatório quando CLIENT_NETWORK_CONFIG = STATIC Caso contrário, é opcional.

CLIENTE_REDE_MAC

Valor	Designação
O endereço MAC da interface de rede do cliente no contêiner. Este campo é opcional. Se omitido, um endereço MAC será gerado automaticamente. Deve ter 6 pares de dígitos hexadecimais separados por dois pontos. Exemplo: b2:9c:02:c2:27:20	Opcional

MÁSCARA_DE_REDE_DO_CLIENTE

Valor	Designação
Máscara de rede IPv4 para este nó na rede do cliente. Especifique esta chave quando CLIENT_NETWORK_CONFIG = STATIC; não a especifique para outros valores. Exemplos: 255.255.255.0 255.255.248.0	Obrigatório se CLIENT_NETWORK_IP for especificado e CLIENT_NETWORK_CONFIG = STATIC Caso contrário, é opcional.

MTU_DE_REDE_DO_CLIENTE

Valor	Designação
A unidade máxima de transmissão (MTU) para este nó na rede do cliente. Não especifique se CLIENT_NETWORK_CONFIG = DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 será usado. Se você quiser usar quadros jumbo, defina a MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão. IMPORTANTE: O valor da MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conectado. Caso contrário, podem ocorrer problemas de desempenho da rede ou perda de pacotes. Exemplos: 1500 8192	Opcional

CLIENTE_REDE_ALVO

Valor	Designação
Nome do dispositivo host que você usará para acesso à rede do cliente pelo nó StorageGRID . Somente nomes de interface de rede são suportados. Normalmente, você usa um nome de interface diferente do que foi especificado para GRID_NETWORK_TARGET ou ADMIN_NETWORK_TARGET. Observação: Não use dispositivos de ligação ou ponte como alvo de rede. Configure uma VLAN (ou outra interface virtual) sobre o dispositivo de ligação ou use um par de ponte e Ethernet virtual (veth). Melhor prática: especifique um valor mesmo que este nó não tenha inicialmente um endereço IP de rede do cliente. Depois, você pode adicionar um endereço IP de rede do cliente, sem precisar reconfigurar o nó no host. Exemplos: bond0.1003 ens423	Melhores práticas

TIPO_DE_ALVO_DE_REDE_DO_CLIENTE

Valor	Designação
Interface (Este é o único valor suportado.)	Opcional

CLIENTE_REDE_TIPO_DE_ALVO_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou falso Defina a chave como "true" para fazer com que o contêiner StorageGRID use o endereço MAC da interface de destino do host na rede do cliente. Melhores práticas: Em redes onde o modo promíscuo seria necessário, use a chave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Para mais detalhes sobre clonagem de MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Melhores práticas

Chaves de rede de grade

CONFIGURAÇÃO_DE_REDE_DE_GRADE

Valor	Designação
ESTÁTICO ou DHCP O padrão é STATIC se não for especificado.	Melhores práticas

GATEWAY_DE_REDE_DE_GRADE

Valor	Designação
Endereço IPv4 do gateway da Grid Network local para este nó, que deve estar na sub-rede definida por GRID_NETWORK_IP e GRID_NETWORK_MASK. Este valor é ignorado para redes configuradas por DHCP. Se a Grid Network for uma única sub-rede sem gateway, use o endereço de gateway padrão para a sub-rede (XYZ1) ou o valor GRID_NETWORK_IP deste nó; qualquer valor simplificará possíveis expansões futuras da Grid Network.	Obrigatório

IP_DE_REDE_DE_GRID

Valor	Designação
Endereço IPv4 deste nó na Rede Grid. Esta chave só é necessária quando GRID_NETWORK_CONFIG = STATIC; não a especifique para outros valores. Exemplos: 1.1.1.1 10.224.4.81	Obrigatório quando GRID_NETWORK_CONFIG = STATIC Caso contrário, é opcional.

GRID_REDE_MAC

Valor	Designação
O endereço MAC da interface da Grid Network no contêiner. Deve ter 6 pares de dígitos hexadecimais separados por dois pontos. Exemplo: b2:9c:02:c2:27:30	Opcional Se omitido, um endereço MAC será gerado automaticamente.

MÁSCARA_DE_REDE_DE_GRADE

Valor	Designação
Máscara de rede IPv4 para este nó na rede Grid. Especifique esta chave quando GRID_NETWORK_CONFIG = STATIC; não a especifique para outros valores. Exemplos: 255.255.255.0 255.255.248.0	Obrigatório quando GRID_NETWORK_IP é especificado e GRID_NETWORK_CONFIG = STATIC. Caso contrário, é opcional.

MTU_DE_REDE_DE_GRADE

Valor	Designação
A unidade máxima de transmissão (MTU) para este nó na rede de grade. Não especifique se GRID_NETWORK_CONFIG = DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1500 será usado. Se você quiser usar quadros jumbo, defina a MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão. IMPORTANTE: O valor da MTU da rede deve corresponder ao valor configurado na porta do switch à qual o nó está conectado. Caso contrário, podem ocorrer problemas de desempenho da rede ou perda de pacotes. IMPORTANTE: Para o melhor desempenho da rede, todos os nós devem ser configurados com valores de MTU semelhantes em suas interfaces de rede de grade. O alerta Incompatibilidade de MTU da rede de grade é acionado se houver uma diferença significativa nas configurações de MTU da rede de grade em nós individuais. Os valores de MTU não precisam ser os mesmos para todos os tipos de rede. Exemplos: 1500 8192	Opcional

ALVO_DA_REDE_DE_GRID

Valor	Designação
Nome do dispositivo host que você usará para acesso à Grid Network pelo nó StorageGRID . Somente nomes de interface de rede são suportados. Normalmente, você usa um nome de interface diferente do que foi especificado para ADMIN_NETWORK_TARGET ou CLIENT_NETWORK_TARGET. Observação: Não use dispositivos de ligação ou ponte como alvo de rede. Configure uma VLAN (ou outra interface virtual) sobre o dispositivo de ligação ou use um par de ponte e Ethernet virtual (veth). Exemplos: bond0.1001 ens192	Obrigatório

TIPO_DE_ALVO_DE_REDE_DE_GRID

Valor	Designação
Interface (Este é o único valor suportado.)	Opcional

TIPO_DE_ALVO_DE_REDE_DE_GRID_INTERFACE_CLONE_MAC

Valor	Designação
Verdadeiro ou falso Defina o valor da chave como "true" para fazer com que o contêiner StorageGRID use o endereço MAC da interface de destino do host na Grid Network. Melhores práticas: Em redes onde o modo promíscuo seria necessário, use a chave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Para mais detalhes sobre clonagem de MAC: • "Considerações e recomendações para clonagem de endereços MAC (Red Hat Enterprise Linux)" • "Considerações e recomendações para clonagem de endereços MAC (Ubuntu ou Debian)"	Melhores práticas

Chave de senha de instalação (temporária)

HASH_DE_SENHA_TEMPORÁRIA_PERSONALIZADA

Valor	Designação
Para o nó de administração principal, defina uma senha temporária padrão para a API de instalação do StorageGRID durante a instalação. Observação: Defina uma senha de instalação somente no nó de administração principal. Se você tentar definir uma senha em outro tipo de nó, a validação do arquivo de configuração do nó falhará. Definir esse valor não terá efeito quando a instalação estiver concluída. Se esta chave for omitida, por padrão nenhuma senha temporária será definida. Como alternativa, você pode definir uma senha temporária usando a API de instalação do StorageGRID . Deve ser um <code>crypt()</code> Hash de senha SHA-512 com formato <code>\$6\$<salt>\$<password hash></code> para uma senha de pelo menos 8 e não mais que 32 caracteres. Este hash pode ser gerado usando ferramentas CLI, como o <code>openssl passwd</code> comando no modo SHA-512.	Melhores práticas

Chave de interfaces

INTERFACE_ALVO_nnnn

Valor	Designação
Nome e descrição opcional para uma interface extra que você deseja adicionar a este nó. Você pode adicionar várias interfaces extras a cada nó. Para <i>nnnn</i>, especifique um número exclusivo para cada entrada <code>INTERFACE_TARGET</code> que você está adicionando. Para o valor, especifique o nome da interface física no host bare-metal. Em seguida, opcionalmente, adicione uma vírgula e forneça uma descrição da interface, que é exibida na página de interfaces de VLAN e na página de grupos de HA. Exemplo: <code>INTERFACE_TARGET_0001=ens256, Trunk</code> Se você adicionar uma interface de tronco, deverá configurar uma interface VLAN no StorageGRID. Se você adicionar uma interface de acesso, poderá adicioná-la diretamente a um grupo HA; não precisará configurar uma interface VLAN.	Opcional

Chave de RAM máxima

MÁXIMA_RAM

Valor	Designação
A quantidade máxima de RAM que este nó pode consumir. Se esta chave for omitida, o nó não terá restrições de memória. Ao definir este campo para um nó de nível de produção, especifique um valor que seja pelo menos 24 GB e 16 a 32 GB menor que a RAM total do sistema. Observação: O valor de RAM afeta o espaço real reservado de metadados de um nó. Veja o "descrição do que é Espaço Reservado de Metadados". O formato para este campo é <i>numberunit</i>, onde <i>unit</i> pode ser <i>b</i>, <i>k</i>, <i>m</i>, ou <i>g</i>. Exemplos: 24g 38654705664b Observação: Se você quiser usar esta opção, deverá habilitar o suporte do kernel para cgroups de memória.	Opcional

Chaves de tipo de nó

TIPO_NÓ

Valor	Designação
Tipo de nó: • Nó_Administrador_VM • Nó_de_armazenamento_VM • Nó_de_arquivo_VM • Gateway de API da VM	Obrigatório

TIPO_DE_ARMAZENAMENTO

Valor	Designação
Define o tipo de objetos que um nó de armazenamento contém. Para obter mais informações, consulte "Tipos de nós de armazenamento" . Esta chave só é necessária para nós com NODE_TYPE = VM_Storage_Node; não a especifique para outros tipos de nós. Tipos de armazenamento: • combinado • dados • metadados Observação: se o STORAGE_TYPE não for especificado, o tipo de nó de armazenamento será definido como combinado (dados e metadados) por padrão.	Opcional

Chaves de remapeamento de portas

PORTA_REMAPARAR

Valor	Designação
Remapeia qualquer porta usada por um nó para comunicações internas do nó da grade ou comunicações externas. O remapeamento de portas é necessário se as políticas de rede corporativa restringirem uma ou mais portas usadas pelo StorageGRID, conforme descrito em "Comunicações internas do nó da rede" ou "Comunicações externas" . IMPORTANTE: Não remapeie as portas que você planeja usar para configurar os pontos de extremidade do balanceador de carga. Observação: se somente PORT_REMAP estiver definido, o mapeamento especificado será usado para comunicações de entrada e saída. Se PORT_REMAP_INBOUND também for especificado, PORT_REMAP se aplicará somente às comunicações de saída. O formato utilizado é: <i>network type/protocol/default port used by grid node/new port</i> , onde <i>network type</i> é grade, administrador ou cliente e <i>protocol</i> é tcp ou udp. Exemplo: PORT_REMAP = client/tcp/18082/443 Você também pode remapear várias portas usando uma lista separada por vírgulas. Exemplo: PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80	Opcional

PORTA_REMAPAR_ENTRADA

Valor	Designação
Remapeia as comunicações de entrada para a porta especificada. Se você especificar <code>PORT_REMAP_INBOUND</code>, mas não especificar um valor para <code>PORT_REMAP</code>, as comunicações de saída para a porta permanecerão inalteradas. IMPORTANTE: Não remapeie as portas que você planeja usar para configurar os pontos de extremidade do balanceador de carga. O formato utilizado é: <i>network type/protocol/remapped port /default port used by grid node</i>, onde <i>network type</i> é grade, administrador ou cliente e <i>protocol</i> é tcp ou udp. Exemplo: <code>PORT_REMAP_INBOUND = grid/tcp/3022/22</code> Você também pode remapear várias portas de entrada usando uma lista separada por vírgulas. Exemplo: <code>PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22</code>	Opcional

Como os nós da grade descobrem o nó administrativo principal

Os nós de grade se comunicam com o nó de administração principal para configuração e gerenciamento. Cada nó da grade deve saber o endereço IP do nó administrativo primário na rede da grade.

Para garantir que um nó de grade possa acessar o nó de administração principal, você pode fazer o seguinte ao implantar o nó:

- Você pode usar o parâmetro `ADMIN_IP` para inserir manualmente o endereço IP do nó de administração principal.
- Você pode omitir o parâmetro `ADMIN_IP` para que o nó da grade descubra o valor automaticamente. A descoberta automática é especialmente útil quando a Grid Network usa DHCP para atribuir o endereço IP ao nó administrativo primário.

A descoberta automática do nó de administração primário é realizada usando um sistema de nomes de domínio multicast (mDNS). Quando o nó de administração primário é iniciado pela primeira vez, ele publica seu endereço IP usando mDNS. Outros nós na mesma sub-rede podem então consultar o endereço IP e adquiri-lo automaticamente. Entretanto, como o tráfego IP multicast normalmente não é roteável entre sub-redes, os nós em outras sub-redes não podem adquirir o endereço IP do nó administrativo principal diretamente.

Se você usar a descoberta automática:



- Você deve incluir a configuração `ADMIN_IP` para pelo menos um nó de grade em qualquer sub-rede à qual o nó de administração primário não esteja diretamente conectado. Este nó de grade publicará então o endereço IP do nó de administração principal para que outros nós na sub-rede o descubram com o mDNS.
- Certifique-se de que sua infraestrutura de rede suporte a passagem de tráfego IP multicast dentro de uma sub-rede.

Arquivos de configuração de nó de exemplo

Você pode usar os arquivos de configuração de nó de exemplo para ajudar a configurar os arquivos de configuração de nó para seu sistema StorageGRID . Os exemplos mostram arquivos de configuração de nós para todos os tipos de nós de grade.

Para a maioria dos nós, você pode adicionar informações de endereçamento de rede de administrador e cliente (IP, máscara, gateway e assim por diante) ao configurar a grade usando o Grid Manager ou a API de instalação. A exceção é o nó de administração principal. Se você quiser navegar até o IP da rede de administração do nó de administração primário para concluir a configuração da grade (porque a rede de grade não é roteada, por exemplo), você deve configurar a conexão da rede de administração para o nó de administração primário no arquivo de configuração do nó. Isso é mostrado no exemplo.



Nos exemplos, o destino Rede do Cliente foi configurado como uma prática recomendada, embora a Rede do Cliente esteja desabilitada por padrão.

Exemplo para nó de administração primário

Exemplo de nome de arquivo: `/etc/storagegrid/nodes/dcl-adm1.conf`

Exemplo de conteúdo do arquivo:

```

NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adml-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adml-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adml-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21

```

Exemplo para nó de armazenamento

Exemplo de nome de arquivo: /etc/storagegrid/nodes/dc1-sn1.conf

Exemplo de conteúdo do arquivo:

```

NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

```

Exemplo para nó de gateway

Exemplo de nome de arquivo: /etc/storagegrid/nodes/dc1-gw1.conf

Exemplo de conteúdo do arquivo:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemplo para um nó de administração não primário

Exemplo de nome de arquivo: /etc/storagegrid/nodes/dcl-adm2.conf

Exemplo de conteúdo do arquivo:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dcl-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dcl-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Validar a configuração do StorageGRID

Após criar os arquivos de configuração em /etc/storagegrid/nodes para cada um dos seus nós StorageGRID , você deve validar o conteúdo desses arquivos.

Para validar o conteúdo dos arquivos de configuração, execute o seguinte comando em cada host:

```
sudo storagegrid node validate all
```

Se os arquivos estiverem corretos, a saída mostrará **PASSED** para cada arquivo de configuração, conforme mostrado no exemplo.



Ao usar apenas um LUN em nós somente de metadados, você poderá receber uma mensagem de aviso que pode ser ignorada.

```
Checking for misnamed node configuration files... PASSED
Checking configuration file for node dcl-adm1... PASSED
Checking configuration file for node dcl-gw1... PASSED
Checking configuration file for node dcl-sn1... PASSED
Checking configuration file for node dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes... PASSED
```



Para uma instalação automatizada, você pode suprimir esta saída usando o `-q` ou `--quiet` opções no `storagegrid` comando (por exemplo, `storagegrid --quiet...`). Se você suprimir a saída, o comando terá um valor de saída diferente de zero se algum aviso ou erro de configuração for detectado.

Se os arquivos de configuração estiverem incorretos, os problemas serão mostrados como **AVISO** e **ERRO**, conforme mostrado no exemplo. Se algum erro de configuração for encontrado, você deverá corrigi-lo antes de continuar com a instalação.

```

Checking for misnamed node configuration files...
WARNING: ignoring /etc/storagegrid/nodes/dcl-adml
WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adml...
ERROR: NODE_TYPE = VM_Foo_Node
      VM_Foo_Node is not a valid node type.  See *.conf.sample
ERROR: ADMIN_ROLE = Foo
      Foo is not a valid admin role.  See *.conf.sample
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
      /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dcl-gw1...
ERROR: GRID_NETWORK_TARGET = bond0.1001
      bond0.1001 is not a valid interface.  See `ip link show`
ERROR: GRID_NETWORK_IP = 10.1.3
      10.1.3 is not a valid IPv4 address
ERROR: GRID_NETWORK_MASK = 255.248.255.0
      255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dcl-sn1...
ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
      10.2.0.1 is not on the local subnet
ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
      Could not parse subnet list
Checking configuration file for node dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes...
ERROR: GRID_NETWORK_IP = 10.1.0.4
      dcl-sn2 and dcl-sn3 have the same GRID_NETWORK_IP
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_RANGEDB_00

```

Inicie o serviço do host StorageGRID

Para iniciar seus nós StorageGRID e garantir que eles reiniciem após uma reinicialização do host, você deve habilitar e iniciar o serviço do host StorageGRID .

Passos

1. Execute os seguintes comandos em cada host:

```

sudo systemctl enable storagegrid
sudo systemctl start storagegrid

```

2. Execute o seguinte comando para garantir que a implantação esteja em andamento:

```
sudo storagegrid node status node-name
```

3. Se algum nó retornar o status "Não em execução" ou "Parado", execute o seguinte comando:

```
sudo storagegrid node start node-name
```

4. Se você habilitou e iniciou o serviço de host StorageGRID anteriormente (ou se não tiver certeza se o serviço foi habilitado e iniciado), execute também o seguinte comando:

```
sudo systemctl reload-or-restart storagegrid
```

Configurar a grade e concluir a instalação (Ubuntu ou Debian)

Navegue até o Gerenciador de Grade

Use o Grid Manager para definir todas as informações necessárias para configurar seu sistema StorageGRID .

Antes de começar

O nó de administração principal deve ser implantado e ter concluído a sequência de inicialização inicial.

Passos

1. Abra seu navegador e navegue até:

```
https://primary_admin_node_ip
```

Alternativamente, você pode acessar o Grid Manager na porta 8443:

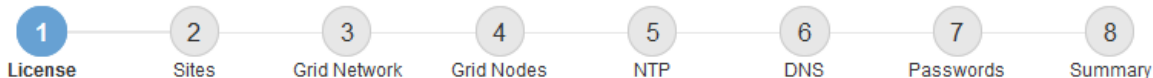
```
https://primary_admin_node_ip:8443
```

Você pode usar o endereço IP do nó de administração primário na rede Grid ou na rede de administração, conforme apropriado para sua configuração de rede.

2. Gerencie uma senha temporária do instalador conforme necessário:
 - Se uma senha já tiver sido definida usando um desses métodos, digite a senha para prosseguir.
 - Um usuário definiu a senha ao acessar o instalador anteriormente
 - A senha foi importada automaticamente do arquivo de configuração do nó em `/etc/storagegrid/nodes/<node_name>.conf`
 - Se uma senha não tiver sido definida, opcionalmente defina uma senha para proteger o instalador do StorageGRID .
3. Selecione ***Instalar um sistema StorageGRID ***.

A página usada para configurar um sistema StorageGRID é exibida.

Install



License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Browse

Especifique as informações da licença StorageGRID

Você deve especificar o nome do seu sistema StorageGRID e carregar o arquivo de licença fornecido pela NetApp.

Passos

1. Na página Licença, insira um nome significativo para seu sistema StorageGRID no campo **Nome da grade**.

Após a instalação, o nome é exibido no topo do menu Nós.

2. Selecione **Procurar**, localize o arquivo de licença do NetApp(*NLF-unique-id.txt*) e selecione **Abrir**.

O arquivo de licença é validado e o número de série é exibido.



O arquivo de instalação do StorageGRID inclui uma licença gratuita que não fornece nenhum direito de suporte para o produto. Você pode atualizar para uma licença que ofereça suporte após a instalação.

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File NLF-959007-Internal.txt

License Serial Number

3. Selecione **Avançar**.

Adicionar sites

Você deve criar pelo menos um site ao instalar o StorageGRID. Você pode criar sites adicionais para aumentar a confiabilidade e a capacidade de armazenamento do seu sistema StorageGRID.

Passos

1. Na página Sites, insira o **Nome do Site**.
2. Para adicionar outros sites, clique no sinal de mais ao lado da última entrada do site e digite o nome na nova caixa de texto **Nome do site**.

Adicione quantos sites adicionais forem necessários para sua topologia de grade. Você pode adicionar até 16 sites.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top is a blue header with 'NetApp® StorageGRID®' and a 'Help' dropdown. Below the header is a progress bar with eight steps: 1. License, 2. Sites (highlighted in blue), 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. Below the progress bar, the 'Sites' section is displayed. It contains two paragraphs of text explaining single-site and multi-site deployments. Below the text are two input fields for 'Site Name'. The first field is labeled 'Site Name 1' and contains the text 'Raleigh', with a red 'x' icon to its right. The second field is labeled 'Site Name 2' and contains the text 'Atlanta', with a '+ x' icon to its right.

3. Clique em **Avançar**.

Especificar sub-redes da rede de grade

Você deve especificar as sub-redes que são usadas na Grid Network.

Sobre esta tarefa

As entradas de sub-rede incluem as sub-redes da Grid Network para cada site no seu sistema StorageGRID, juntamente com quaisquer sub-redes que precisam ser acessadas por meio da Grid Network.

Se você tiver várias sub-redes de grade, o gateway da Rede de Grade será necessário. Todas as sub-redes de grade especificadas devem ser acessíveis por meio deste gateway.

Passos

1. Especifique o endereço de rede CIDR para pelo menos uma rede de grade na caixa de texto **Sub-rede 1**.
2. Clique no sinal de mais ao lado da última entrada para adicionar uma entrada de rede adicional. Você deve especificar todas as sub-redes para todos os sites na Grid Network.
 - Se você já tiver implantado pelo menos um nó, clique em **Descobrir sub-redes de redes de grade** para preencher automaticamente a Lista de sub-redes de redes de grade com as sub-redes relatadas

pelos nós de grade que foram registrados no Gerenciador de grade.

- Você deve adicionar manualmente quaisquer sub-redes para NTP, DNS, LDAP ou outros servidores externos acessados pelo gateway da Grid Network.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.

Note:

 You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1

172.16.0.0/21

+

Discover Grid Network subnets

3. Clique em **Avançar**.

Aprovar nós de grade pendentes

Você deve aprovar cada nó de grade antes que ele possa ingressar no sistema StorageGRID .

Antes de começar

Você implantou todos os nós de grade do dispositivo virtual e StorageGRID .



É mais eficiente executar uma única instalação de todos os nós, em vez de instalar alguns nós agora e outros depois.

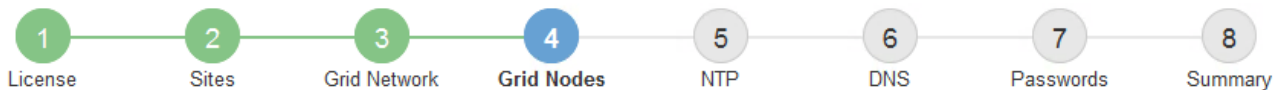
Passos

1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade que você implantou.



Se um nó de grade estiver faltando, confirme se ele foi implantado com sucesso e se tem o IP de rede de grade correto do nó de administração primário definido para ADMIN_IP.

2. Selecione o botão de opção ao lado de um nó pendente que você deseja aprovar.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve ✕ Remove		Search				
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address	
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21	

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit Reset ✕ Remove		Search				
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21

3. Clique em **Aprovar**.

4. Em Configurações gerais, modifique as configurações das seguintes propriedades, conforme necessário:

- **Site:** O nome do sistema do site para este nó de grade.
- **Nome:** O nome do sistema para o nó. O nome padrão é o nome que você especificou quando configurou o nó.

Os nomes do sistema são necessários para operações internas do StorageGRID e não podem ser alterados após a conclusão da instalação. No entanto, durante esta etapa do processo de instalação, você pode alterar os nomes do sistema conforme necessário.

- **Função NTP:** A função do Protocolo de Tempo de Rede (NTP) do nó da grade. As opções são **Automático**, **Principal** e **Cliente**. Selecionar **Automático** atribui a função Primária aos Nós de Administração, Nós de Armazenamento com serviços ADC, Nós de Gateway e quaisquer nós de grade que tenham endereços IP não estáticos. Todos os outros nós da grade recebem a função Cliente.



Certifique-se de que pelo menos dois nós em cada site possam acessar pelo menos quatro fontes NTP externas. Se apenas um nó em um site puder alcançar as fontes NTP, ocorrerão problemas de tempo se esse nó ficar inativo. Além disso, designar dois nós por site como fontes primárias de NTP garante um tempo preciso se um site estiver isolado do restante da rede.

- **Tipo de armazenamento** (somente nós de armazenamento): especifique que um novo nó de armazenamento seja usado exclusivamente para dados, metadados ou ambos. As opções são **Dados e metadados** ("combinados"), **Somente dados** e **Somente metadados**.



Ver "[Tipos de nós de armazenamento](#)" para obter informações sobre os requisitos para esses tipos de nós.

- **Serviço ADC** (somente nós de armazenamento): selecione **Automático** para permitir que o sistema determine se o nó requer o serviço Controlador de Domínio Administrativo (ADC). O serviço ADC monitora a localização e a disponibilidade dos serviços de rede. Pelo menos três nós de armazenamento em cada site devem incluir o serviço ADC. Não é possível adicionar o serviço ADC a um nó depois que ele for implantado.

5. Em Grid Network, modifique as configurações das seguintes propriedades conforme necessário:

- **Endereço IPv4 (CIDR)**: O endereço de rede CIDR para a interface Grid Network (eth0 dentro do contêiner). Por exemplo: 192.168.1.234/21
- **Gateway**: O gateway da Grid Network. Por exemplo: 192.168.0.1

O gateway é necessário se houver várias sub-redes de grade.



Se você selecionou DHCP para a configuração da Grid Network e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não esteja em um pool de endereços DHCP.

6. Se você quiser configurar a Rede de Administração para o nó da grade, adicione ou atualize as configurações na seção Rede de Administração, conforme necessário.

Insira as sub-redes de destino das rotas fora desta interface na caixa de texto **Sub-redes (CIDR)**. Se houver várias sub-redes de administração, o gateway de administração será necessário.



Se você selecionou DHCP para a configuração da rede de administração e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não esteja em um pool de endereços DHCP.

Dispositivos: Para um dispositivo StorageGRID, se a Rede de administração não foi configurada durante a instalação inicial usando o Instalador do dispositivo StorageGRID, ela não poderá ser configurada nesta caixa de diálogo Gerenciador de grade. Em vez disso, você deve seguir estes passos:

- Reinicie o dispositivo: No Instalador do Dispositivo, selecione **Avançado > Reinicializar**.

A reinicialização pode levar vários minutos.

- Selecione **Configurar rede > Configuração de link** e habilite as redes apropriadas.
- Selecione **Configurar rede > Configuração de IP** e configure as redes habilitadas.
- Retorne à página inicial e clique em **Iniciar instalação**.

- e. No Grid Manager: se o nó estiver listado na tabela Nós aprovados, remova-o.
- f. Remova o nó da tabela Nós Pendentes.
- g. Aguarde até que o nó reapareça na lista de Nós Pendentes.
- h. Confirme se você pode configurar as redes apropriadas. Eles já devem estar preenchidos com as informações que você forneceu na página Configuração de IP do Instalador do Appliance.

Para obter informações adicionais, consulte o "[Início rápido para instalação de hardware](#)" para localizar instruções para seu aparelho.

7. Se você quiser configurar a Rede do Cliente para o nó da grade, adicione ou atualize as configurações na seção Rede do Cliente, conforme necessário. Se a Rede do Cliente estiver configurada, o gateway será necessário e se tornará o gateway padrão para o nó após a instalação.



Se você selecionou DHCP para a configuração da rede do cliente e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não esteja em um pool de endereços DHCP.

Dispositivos: Para um dispositivo StorageGRID , se a Rede do Cliente não foi configurada durante a instalação inicial usando o Instalador do Dispositivo StorageGRID , ela não poderá ser configurada nesta caixa de diálogo Gerenciador de Grade. Em vez disso, você deve seguir estes passos:

- a. Reinicie o dispositivo: No Instalador do Dispositivo, selecione **Avançado > Reinicializar**.

A reinicialização pode levar vários minutos.

- b. Selecione **Configurar rede > Configuração de link** e habilite as redes apropriadas.
- c. Selecione **Configurar rede > Configuração de IP** e configure as redes habilitadas.
- d. Retorne à página inicial e clique em **Iniciar instalação**.
- e. No Grid Manager: se o nó estiver listado na tabela Nós aprovados, remova-o.
- f. Remova o nó da tabela Nós Pendentes.
- g. Aguarde até que o nó reapareça na lista de Nós Pendentes.
- h. Confirme se você pode configurar as redes apropriadas. Eles já devem estar preenchidos com as informações que você forneceu na página Configuração de IP do Instalador do Appliance.

Para saber como instalar dispositivos StorageGRID , consulte o "[Início rápido para instalação de hardware](#)" para localizar instruções para seu aparelho.

8. Clique em **Salvar**.

A entrada do nó da grade é movida para a lista de nós aprovados.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve

✖ Remove

Search

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit

Reset

✖ Remove

Search

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
☐	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

9. Repita essas etapas para cada nó de grade pendente que você deseja aprovar.

Você deve aprovar todos os nós que deseja na grade. No entanto, você pode retornar a esta página a qualquer momento antes de clicar em **Instalar** na página Resumo. Você pode modificar as propriedades de um nó de grade aprovado selecionando seu botão de opção e clicando em **Editar**.

10. Quando terminar de aprovar os nós da grade, clique em **Avançar**.

Especificar informações do servidor Network Time Protocol

Você deve especificar as informações de configuração do Network Time Protocol (NTP) para o sistema StorageGRID , para que as operações executadas em servidores separados possam ser mantidas sincronizadas.

Sobre esta tarefa

Você deve especificar endereços IPv4 para os servidores NTP.

Você deve especificar servidores NTP externos. Os servidores NTP especificados devem usar o protocolo NTP.

Você deve especificar quatro referências de servidor NTP do Stratum 3 ou superior para evitar problemas com desvio de tempo.



Ao especificar a origem NTP externa para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft para uso em ambientes de alta precisão, como o StorageGRID.

["Limite de suporte para configurar o serviço Windows Time para ambientes de alta precisão"](#)

Os servidores NTP externos são usados pelos nós aos quais você atribuiu anteriormente funções NTP primárias.



Certifique-se de que pelo menos dois nós em cada site possam acessar pelo menos quatro fontes NTP externas. Se apenas um nó em um site puder alcançar as fontes NTP, ocorrerão problemas de tempo se esse nó ficar inativo. Além disso, designar dois nós por site como fontes primárias de NTP garante um tempo preciso se um site estiver isolado do restante da rede.

Passos

1. Especifique os endereços IPv4 para pelo menos quatro servidores NTP nas caixas de texto **Servidor 1** a **Servidor 4**.
2. Se necessário, selecione o sinal de mais ao lado da última entrada para adicionar entradas de servidor adicionais.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Network Time Protocol

Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.

Server 1

10.60.248.183

Server 2

10.227.204.142

Server 3

10.235.48.111

Server 4

0.0.0.0

+

3. Selecione **Avançar**.

Informações relacionadas

["Diretrizes de rede"](#)

Especificar informações do servidor DNS

Você deve especificar informações de DNS para seu sistema StorageGRID para poder acessar servidores externos usando nomes de host em vez de endereços IP.

Sobre esta tarefa

Especificando ["Informações do servidor DNS"](#) permite que você use nomes de host de nomes de domínio totalmente qualificados (FQDN) em vez de endereços IP para notificações por e-mail e AutoSupport.

Para garantir a operação correta, especifique dois ou três servidores DNS. Se você especificar mais de três, é possível que apenas três sejam usados devido a limitações conhecidas do sistema operacional em algumas plataformas. Se você tiver restrições de roteamento em seu ambiente, você pode ["personalizar a lista de servidores DNS"](#) para nós individuais (normalmente todos os nós em um site) usar um conjunto diferente de até três servidores DNS.

Se possível, use servidores DNS que cada site possa acessar localmente para garantir que um site isolado possa resolver os FQDNs para destinos externos.

Passos

1. Especifique o endereço IPv4 para pelo menos um servidor DNS na caixa de texto **Servidor 1**.
2. Se necessário, selecione o sinal de mais ao lado da última entrada para adicionar entradas de servidor adicionais.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" dropdown. Below the header is a navigation bar with "Install" and a progress indicator showing steps 1 through 8: License, Sites, Grid Network, Grid Nodes, NTP, DNS (highlighted in blue), Passwords, and Summary. The main content area is titled "Domain Name Service" and contains instructions: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport." Below this, there are two input fields for DNS servers. "Server 1" has the IP address "10.224.223.130" and a red "X" icon to its right. "Server 2" has the IP address "10.224.223.136" and a red plus sign icon to its right.

A melhor prática é especificar pelo menos dois servidores DNS. Você pode especificar até seis servidores DNS.

3. Selecione **Avançar**.

Especifique as senhas do sistema StorageGRID

Como parte da instalação do seu sistema StorageGRID, você precisa inserir as senhas que serão usadas para proteger seu sistema e executar tarefas de manutenção.

Sobre esta tarefa

Use a página Instalar senhas para especificar a senha de provisionamento e a senha do usuário root de gerenciamento da grade.

- A senha de provisionamento é usada como uma chave de criptografia e não é armazenada pelo sistema StorageGRID .
- Você deve ter a senha de provisionamento para os procedimentos de instalação, expansão e manutenção, incluindo o download do Pacote de Recuperação. Portanto, é importante que você armazene a senha de provisionamento em um local seguro.
- Você pode alterar a senha de provisionamento no Grid Manager se tiver a atual.
- A senha do usuário root de gerenciamento de grade pode ser alterada usando o Grid Manager.
- As senhas do console de linha de comando e SSH geradas aleatoriamente são armazenadas no `Passwords.txt` arquivo no Pacote de Recuperação.

Passos

1. Em **Provisioning Passphrase**, insira a senha de provisionamento que será necessária para fazer alterações na topologia de grade do seu sistema StorageGRID .

Armazene a senha de provisionamento em um local seguro.



Se, após a conclusão da instalação, você quiser alterar a senha de provisionamento posteriormente, poderá usar o Grid Manager. Selecione **CONFIGURAÇÃO > Controle de acesso > Senhas de grade**.

2. Em **Confirmar senha de provisionamento**, digite novamente a senha de provisionamento para confirmá-la.
3. Em **Senha do usuário raiz do Grid Management**, insira a senha a ser usada para acessar o Grid Manager como usuário "root".

Guarde a senha em um local seguro.

4. Em **Confirmar senha do usuário raiz**, digite novamente a senha do Grid Manager para confirmá-la.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning Passphrase

.....

Confirm Provisioning Passphrase

.....

Grid Management Root User Password

.....

Confirm Root User Password

.....

☒ Create random command line passwords.

- Se você estiver instalando uma grade para fins de prova de conceito ou demonstração, opcionalmente desmarque a caixa de seleção **Criar senhas aleatórias de linha de comando**.

Para implantações de produção, senhas aleatórias devem sempre ser usadas por motivos de segurança. Desmarque **Criar senhas aleatórias de linha de comando** apenas para grades de demonstração se quiser usar senhas padrão para acessar nós de grade a partir da linha de comando usando a conta "root" ou "admin".



Você será solicitado a baixar o arquivo do pacote de recuperação(sgws-recovery-package-id-revision.zip) depois de clicar em **Instalar** na página Resumo. Você deve "[baixar este arquivo](#)" para concluir a instalação. As senhas necessárias para acessar o sistema são armazenadas no Passwords.txt arquivo, contido no arquivo Recovery Package.

- Clique em **Avançar**.

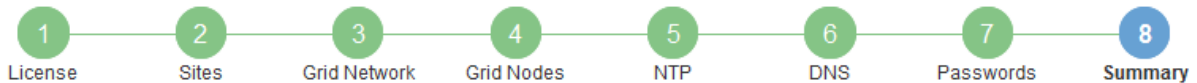
Revise sua configuração e conclua a instalação

Você deve revisar cuidadosamente as informações de configuração inseridas para garantir que a instalação seja concluída com sucesso.

Passos

- Veja a página **Resumo**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1	dc1-g1	dc1-s1
	dc1-s2	dc1-s3	NetApp-SGA

- Verifique se todas as informações de configuração da grade estão corretas. Use os links Modificar na página Resumo para voltar e corrigir quaisquer erros.
- Clique em **Instalar**.



Se um nó estiver configurado para usar a Rede do Cliente, o gateway padrão para esse nó muda da Rede de Grade para a Rede do Cliente quando você clica em **Instalar**. Se você perder a conectividade, certifique-se de estar acessando o nó de administração principal por meio de uma sub-rede acessível. Ver "[Diretrizes de rede](#)" para mais detalhes.

- Clique em **Baixar pacote de recuperação**.

Quando a instalação avança até o ponto em que a topologia da grade é definida, você é solicitado a baixar o arquivo do pacote de recuperação(.zip) e confirme se você consegue acessar com sucesso o conteúdo deste arquivo. Você deve baixar o arquivo do pacote de recuperação para poder recuperar o sistema StorageGRID se um ou mais nós da grade falharem. A instalação continua em segundo plano, mas você não poderá concluir a instalação e acessar o sistema StorageGRID até baixar e verificar este arquivo.

- Verifique se você pode extrair o conteúdo do .zip arquivo e salve-o em 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 .

6. Marque a caixa de seleção **Eu baixei e verifiquei com sucesso o arquivo do pacote de recuperação** e clique em **Avançar**.

Se a instalação ainda estiver em andamento, a página de status será exibida. Esta página indica o progresso da instalação de cada nó da grade.

Installation Status

If necessary, you may [Download the Recovery Package](#) file again.

Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage	IT
dc1-adm1		Site1		172.16.4.215/21			Starting services	
dc1-g1		Site1		172.16.4.216/21			Complete	
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers	
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed	
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed	

Quando o estágio Concluído for atingido para todos os nós da grade, a página de login do Gerenciador de Grade será exibida.

7. Sign in no Grid Manager usando o usuário "root" e a senha que você especificou durante a instalação.

Diretrizes pós-instalação

Após concluir a implantação e a configuração do nó de grade, siga estas diretrizes para endereçamento DHCP e alterações na configuração de rede.

- Se o DHCP foi usado para atribuir endereços IP, configure uma reserva DHCP para cada endereço IP nas redes que estão sendo usadas.

Você só pode configurar o DHCP durante a fase de implantação. Não é possível configurar o DHCP durante a configuração.



Os nós são reinicializados quando a configuração da rede de grade é alterada pelo DHCP, o que pode causar interrupções se uma alteração de DHCP afetar vários nós ao mesmo tempo.

- Você deve usar os procedimentos Alterar IP se quiser alterar endereços IP, máscaras de sub-rede e gateways padrão para um nó de grade. Ver "[Configurar endereços IP](#)".
- Se você fizer alterações na configuração de rede, incluindo alterações de roteamento e gateway, a conectividade do cliente com o nó de administração principal e outros nós da grade poderá ser perdida. Dependendo das alterações de rede aplicadas, pode ser necessário restabelecer essas conexões.

Instalação REST API

O StorageGRID fornece a API de instalação do StorageGRID para executar tarefas de instalação.

A API usa a plataforma de API de código aberto Swagger para fornecer a documentação da API. O Swagger permite que desenvolvedores e não desenvolvedores interajam com a API em uma interface de usuário que ilustra como a API responde a parâmetros e opções. Esta documentação pressupõe que você esteja familiarizado com tecnologias web padrão e o formato de dados JSON.



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.

Cada comando da API REST inclui a URL da API, uma ação HTTP, quaisquer parâmetros de URL obrigatórios ou opcionais e uma resposta de API esperada.

API de instalação do StorageGRID

A API de instalação do StorageGRID só estará disponível quando você estiver configurando inicialmente seu sistema StorageGRID e se precisar executar uma recuperação do nó de administração primário. A API de instalação pode ser acessada via HTTPS a partir do Grid Manager.

Para acessar a documentação da API, vá para a página de instalação no nó de administração principal e selecione **Ajuda > Documentação da API** na barra de menu.

A API de instalação do StorageGRID inclui as seguintes seções:

- **config** — Operações relacionadas ao lançamento do produto e versões da API. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **grid** — Operações de configuração em nível de grade. Você pode obter e atualizar as configurações da grade, incluindo detalhes da grade, sub-redes da rede da grade, senhas da grade e endereços IP dos servidores NTP e DNS.
- **nodes** — Operações de configuração em nível de nó. Você pode recuperar uma lista de nós de grade, excluir um nó de grade, configurar um nó de grade, visualizar um nó de grade e redefinir a configuração de um nó de grade.
- **provisão** — Operações de provisionamento. Você pode iniciar a operação de provisionamento e visualizar o status da operação de provisionamento.
- **recuperação** — Operações de recuperação do nó de administração principal. Você pode redefinir informações, carregar o Pacote de Recuperação, iniciar a recuperação e visualizar o status da operação de recuperação.
- **recovery-package** — Operações para baixar o pacote de recuperação.
- **sites** — Operações de configuração em nível de site. Você pode criar, visualizar, excluir e modificar um site.
- **temporary-password** — Operações na senha temporária para proteger a mgmt-api durante a instalação.

Informações relacionadas

["Automatizando a instalação"](#)

Para onde ir a seguir

Após concluir a instalação, execute as tarefas de integração e configuração necessárias. Você pode executar as tarefas opcionais conforme necessário.

Tarefas necessárias

- ["Criar uma conta de inquilino"](#) para o protocolo do cliente S3 que será usado para armazenar objetos no seu sistema StorageGRID .
- ["Acesso ao sistema de controle"](#) configurando grupos e contas de usuários. Opcionalmente, você

pode [configurar uma fonte de identidade federada](#) (como Active Directory ou OpenLDAP), para que você possa importar grupos de administração e usuários. Ou você pode [criar grupos e usuários locais](#) .

- Integrar e testar o ["S3 API"](#) aplicativos cliente que você usará para carregar objetos no seu sistema StorageGRID .
- ["Configurar as regras de gerenciamento do ciclo de vida das informações \(ILM\) e a política de ILM"](#) que você deseja usar para proteger dados de objetos.
- Se sua instalação incluir nós de armazenamento de dispositivos, use o SANtricity OS para concluir as seguintes tarefas:
 - Conecte-se a cada dispositivo StorageGRID .
 - Verifique o recebimento dos dados do AutoSupport .

Ver ["Configurar hardware"](#) .

- Revise e siga o ["Diretrizes de reforço do sistema StorageGRID"](#) para eliminar riscos de segurança.
- ["Configurar notificações por e-mail para alertas do sistema"](#) .

Tarefas opcionais

- ["Atualizar endereços IP dos nós da grade"](#) se eles mudaram desde que você planejou sua implantação e gerou o Pacote de Recuperação.
- ["Configurar criptografia de armazenamento"](#), se necessário.
- ["Configurar compactação de armazenamento"](#) para reduzir o tamanho dos objetos armazenados, se necessário.
- ["Configurar interfaces VLAN"](#) para isolar e particionar o tráfego de rede, se necessário.
- ["Configurar grupos de alta disponibilidade"](#) para melhorar a disponibilidade de conexão para o Grid Manager, o Tenant Manager e os clientes S3, se necessário.
- ["Configurar pontos de extremidade do balanceador de carga"](#) para conectividade do cliente S3, se necessário.

Solucionar problemas de instalação

Caso ocorra algum problema durante a instalação do seu sistema StorageGRID , você pode acessar os arquivos de log da instalação. O suporte técnico também pode precisar usar os arquivos de log de instalação para resolver problemas.

Os seguintes arquivos de log de instalação estão disponíveis no contêiner que está executando cada nó:

- `/var/local/log/install.log` (encontrado em todos os nós da grade)
- `/var/local/log/gdu-server.log` (encontrado no nó de administração principal)

Os seguintes arquivos de log de instalação estão disponíveis no host:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/<node-name>.log`

Para saber como acessar os arquivos de log, consulte ["Coletar arquivos de log e dados do sistema"](#) .

Informações relacionadas

Exemplo /etc/network/interfaces

O /etc/network/interfaces O arquivo inclui três seções, que definem as interfaces físicas, a interface de vínculo e as interfaces VLAN. Você pode combinar as três seções de exemplo em um único arquivo, que agregará quatro interfaces físicas do Linux em um único vínculo LACP e, em seguida, estabelecerá três interfaces VLAN subtendendo o vínculo para uso como interfaces de rede StorageGRID Grid, Admin e Client.

Interfaces físicas

Observe que os switches nas outras extremidades dos links também devem tratar as quatro portas como um único tronco LACP ou canal de porta e devem passar pelo menos as três VLANs referenciadas com tags.

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

Interface de ligação

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

Interfaces VLAN

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

Instalar o StorageGRID no VMware

Início rápido para instalar o StorageGRID no VMware

Siga estas etapas de alto nível para instalar um nó VMware StorageGRID .

1

Preparação

- Aprenda sobre ["Arquitetura e topologia de rede do StorageGRID"](#) .
- Aprenda sobre as especificidades de ["Rede StorageGRID"](#) .
- Reúna e prepare o ["Informações e materiais necessários"](#) .
- Instalar e configurar ["VMware vSphere Hypervisor, vCenter e hosts ESX"](#) .
- Prepare o necessário ["CPU e RAM"](#) .
- Prover para ["requisitos de armazenamento e desempenho"](#) .

2

Implantação

Implantar nós de grade. Quando você implanta nós de grade, eles são criados como parte do sistema

StorageGRID e conectados a uma ou mais redes.

- Use o VMware vSphere Web Client, um arquivo .vmdk e um conjunto de modelos de arquivo .ovf para ["implantar os nós baseados em software como máquinas virtuais \(VMs\)"](#) nos servidores que você preparou na etapa 1.
- Para implantar nós do dispositivo StorageGRID , siga as instruções ["Início rápido para instalação de hardware"](#) .

3

Configuração

Quando todos os nós tiverem sido implantados, use o Grid Manager para ["configurar a grade e concluir a instalação"](#) .

Automatize a instalação

Para economizar tempo e fornecer consistência, você pode automatizar a implantação e a configuração dos nós da grade e a configuração do sistema StorageGRID .

- ["Automatize a implantação de nós de grade usando VMware vSphere"](#) .
- Depois de implantar os nós da grade, ["automatizar a configuração do sistema StorageGRID"](#) usando o script de configuração Python fornecido no arquivo de instalação.
- ["Automatize a instalação e a configuração de nós de grade de dispositivos"](#)
- Se você for um desenvolvedor avançado de implantações do StorageGRID , automatize a instalação de nós de grade usando o ["instalação REST API"](#) .

Planeje e prepare a instalação no VMware

Informações e materiais necessários

Antes de instalar o StorageGRID, reúna e prepare as informações e os materiais necessários.

Informações necessárias

Plano de rede

Quais redes você pretende anexar a cada nó do StorageGRID . O StorageGRID oferece suporte a várias redes para separação de tráfego, segurança e conveniência administrativa.

Veja o StorageGRID ["Diretrizes de rede"](#) .

Informações de rede

Endereços IP a serem atribuídos a cada nó da grade e os endereços IP dos servidores DNS e NTP.

Servidores para nós de grade

Identifique um conjunto de servidores (físicos, virtuais ou ambos) que, em conjunto, forneçam recursos suficientes para dar suporte ao número e ao tipo de nós StorageGRID que você planeja implantar.



Se a instalação do StorageGRID não usar nós de armazenamento do dispositivo StorageGRID (hardware), você deverá usar armazenamento RAID de hardware com cache de gravação alimentado por bateria (BBWC). O StorageGRID não oferece suporte ao uso de redes de área de armazenamento virtual (vSANs), RAID de software ou nenhuma proteção RAID.

Informações relacionadas

["Ferramenta de Matriz de Interoperabilidade da NetApp"](#)

Materiais necessários

Licença NetApp StorageGRID

Você deve ter uma licença NetApp válida e assinada digitalmente.



Uma licença de não produção, que pode ser usada para testes e prova de conceito de grades, está incluída no arquivo de instalação do StorageGRID .

Arquivo de instalação do StorageGRID

["Baixe o arquivo de instalação do StorageGRID e extraia os arquivos"](#) .

Laptop de serviço

O sistema StorageGRID é instalado por meio de um laptop de serviço.

O laptop de serviço deve ter:

- Porta de rede
- Cliente SSH (por exemplo, PuTTY)
- ["Navegador da Web compatível"](#)

Documentação do StorageGRID

- ["Notas de lançamento"](#)
- ["Instruções para administrar o StorageGRID"](#)

Baixe e extraia os arquivos de instalação do StorageGRID

Você deve baixar os arquivos de instalação do StorageGRID e extrair os arquivos. Opcionalmente, você pode verificar manualmente os arquivos no pacote de instalação.

Passos

1. Vá para o ["Página de downloads da NetApp para StorageGRID"](#) .
2. Selecione o botão para baixar a versão mais recente ou selecione outra versão no menu suspenso e selecione **Ir**.
3. Sign in com o nome de usuário e a senha da sua conta NetApp .
4. Se uma declaração de Cuidado/Leitura Obrigatória aparecer, leia-a e marque a caixa de seleção.



Você deve aplicar todos os hotfixes necessários após instalar a versão do StorageGRID . Para mais informações, consulte o ["procedimento de hotfix nas instruções de recuperação e manutenção"](#)

5. Leia o Contrato de Licença do Usuário Final, marque a caixa de seleção e selecione **Aceitar e Continuar**.
6. Na coluna **Instalar StorageGRID**, selecione o arquivo de instalação .tgz ou .zip para o VMware.



Use o .zip arquivo se você estiver executando o Windows no laptop de serviço.

7. Salve o arquivo de instalação.
8. Se você precisar verificar o arquivo de instalação:
 - a. Baixe o pacote de verificação de assinatura de código do StorageGRID . O nome do arquivo para este pacote usa o formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , onde <version-number> é a versão do software StorageGRID .
 - b. Siga os passos para "[verificar manualmente os arquivos de instalação](#)" .
9. Extraia os arquivos do arquivo de instalação.
10. Escolha os arquivos que você precisa.

Os arquivos necessários dependem da topologia de grade planejada e de como você implantará seu sistema StorageGRID .



Os caminhos listados na tabela são relativos ao diretório de nível superior instalado pelo arquivo de instalação extraído.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID .
	Uma licença gratuita que não fornece nenhum direito de suporte para o produto.
	O arquivo de disco da máquina virtual que é usado como modelo para criar máquinas virtuais de nós de grade.
	O arquivo de modelo do Open Virtualization Format(.ovf) e arquivo de manifesto(.mf) para implantar o nó de administração primário.
	O arquivo de modelo(.ovf) e arquivo de manifesto(.mf) para implantar nós administrativos não primários.
	O arquivo de modelo(.ovf) e arquivo de manifesto(.mf) para implantar nós de gateway.

Caminho e nome do arquivo	Descrição
	O arquivo de modelo(<code>.ovf</code>) e arquivo de manifesto(<code>.mf</code>) para implantar nós de armazenamento baseados em máquina virtual.
Ferramenta de script de implantação	Descrição
	Um script de shell Bash usado para automatizar a implantação de nós de grade virtual.
	Um exemplo de arquivo de configuração para uso com o <code>deploy-vsphere-ovftool.sh</code> roteiro.
	Um script Python usado para automatizar a configuração de um sistema StorageGRID .
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID .
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado. Você também pode usar este script para integração do Ping Federate.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado usando o Active Directory ou o Ping Federate.
	Um script auxiliar chamado pelo companheiro <code>storagegrid-ssoauth-azure.py</code> Script Python para executar interações SSO com o Azure.

Caminho e nome do arquivo	Descrição
	Esquemas de API para StorageGRID. Observação: antes de executar uma atualização, você pode usar esses esquemas para confirmar se qualquer código que você escreveu para usar as APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID , caso você não tenha um ambiente StorageGRID não produtivo para testes de compatibilidade de atualização.

Verificar manualmente os arquivos de instalação (opcional)

Se necessário, você pode verificar manualmente os arquivos no arquivo de instalação do StorageGRID .

Antes de começar

Você tem ["baixou o pacote de verificação"](#) do ["Página de downloads da NetApp para StorageGRID"](#) .

Passos

1. Extraia os artefatos do pacote de verificação:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Certifique-se de que esses artefatos foram extraídos:

- Certificado de folha: Leaf-Cert.pem
- Cadeia de certificados: CA-Int-Cert.pem
- Cadeia de resposta de registro de data e hora: TS-Cert.pem
- Arquivo de soma de verificação: sha256sum
- Assinatura de soma de verificação: sha256sum.sig
- Arquivo de resposta de registro de data e hora: sha256sum.sig.tsr

3. Use a cadeia para verificar se o certificado em folha é válido.

Exemplo: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Saída esperada: Leaf-Cert.pem: OK

4. Se a etapa 2 falhou devido a um certificado folha expirado, use o tsr arquivo para verificar.

Exemplo: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

A produção esperada inclui: Verification: OK

5. Crie um arquivo de chave pública a partir do certificado folha.

Exemplo: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Saída esperada: *nenhuma*

6. Use a chave pública para verificar a sha256sum arquivo contra sha256sum.sig .

Exemplo: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

Saída esperada: Verified OK

7. Verifique o sha256sum conteúdo do arquivo em relação às somas de verificação recém-criadas.

Exemplo: `sha256sum -c sha256sum`

Saída esperada: `<filename>: OK`

`<filename>` é o nome do arquivo compactado que você baixou.

8. ["Conclua as etapas restantes"](#) para extrair e escolher os arquivos de instalação apropriados.

Requisitos de software para VMware

Você pode usar uma máquina virtual para hospedar qualquer tipo de nó StorageGRID .
Você precisa de uma máquina virtual para cada nó da grade.

Hipervisor VMware vSphere

Você deve instalar o VMware vSphere Hypervisor em um servidor físico preparado. O hardware deve ser configurado corretamente (incluindo versões de firmware e configurações de BIOS) antes de instalar o software VMware.

- Configure a rede no hipervisor conforme necessário para dar suporte à rede do sistema StorageGRID que você está instalando.

["Diretrizes de rede"](#)

- Certifique-se de que o armazenamento de dados seja grande o suficiente para as máquinas virtuais e os discos virtuais necessários para hospedar os nós da grade.
- Se você criar mais de um armazenamento de dados, nomeie cada armazenamento de dados para que você possa identificar facilmente qual armazenamento de dados usar para cada nó de grade ao criar máquinas virtuais.

Requisitos de configuração do host ESX



Você deve configurar corretamente o protocolo de tempo de rede (NTP) em cada host ESX. Se o horário do host estiver incorreto, poderão ocorrer efeitos negativos, incluindo perda de dados.

Requisitos de configuração do VMware

Você deve instalar e configurar o VMware vSphere e o vCenter antes de implantar os nós do StorageGRID .

Para versões suportadas do software VMware vSphere Hypervisor e VMware vCenter Server, consulte o ["Ferramenta de Matriz de Interoperabilidade da NetApp"](#) .

Para saber as etapas necessárias para instalar esses produtos VMware, consulte a documentação da VMware.

Requisitos de CPU e RAM

Antes de instalar o software StorageGRID , verifique e configure o hardware para que ele esteja pronto para suportar o sistema StorageGRID .

Cada nó StorageGRID requer os seguintes recursos mínimos:

- Núcleos de CPU: 8 por nó
- RAM: Depende da RAM total disponível e da quantidade de software não StorageGRID em execução no sistema
 - Geralmente, pelo menos 24 GB por nó e 2 a 16 GB a menos que a RAM total do sistema
 - Um mínimo de 64 GB para cada locatário que terá aproximadamente 5.000 buckets

Os recursos de nós somente de metadados baseados em software devem corresponder aos recursos de nós de armazenamento existentes. Por exemplo:

- Se o site StorageGRID existente estiver usando dispositivos SG6000 ou SG6100, os nós somente de metadados baseados em software deverão atender aos seguintes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - 8 TB SSD ou armazenamento equivalente para o banco de dados Cassandra (rangedb/0)
- Se o site StorageGRID existente estiver usando nós de armazenamento virtuais com 24 GB de RAM, CPU de 8 núcleos e 3 TB ou 4 TB de armazenamento de metadados, os nós somente de metadados baseados em software deverão usar recursos semelhantes (24 GB de RAM, CPU de 8 núcleos e 4 TB de armazenamento de metadados (rangedb/0)).

Ao adicionar um novo site StorageGRID , a capacidade total de metadados do novo site deve, no mínimo, corresponder aos sites StorageGRID existentes e os novos recursos do site devem corresponder aos nós de armazenamento nos sites StorageGRID existentes.

O VMware suporta um nó por máquina virtual. Certifique-se de que o nó StorageGRID não exceda a RAM física disponível. Cada máquina virtual deve ser dedicada à execução do StorageGRID.



Monitore o uso da CPU e da memória regularmente para garantir que esses recursos continuem acomodando sua carga de trabalho. Por exemplo, dobrar a alocação de RAM e CPU para nós de armazenamento virtuais forneceria recursos semelhantes aos fornecidos para nós de dispositivos StorageGRID . Além disso, se a quantidade de metadados por nó exceder 500 GB, considere aumentar a RAM por nó para 48 GB ou mais. Para obter informações sobre como gerenciar o armazenamento de metadados de objetos, aumentar a configuração do Espaço Reservado de Metadados e monitorar o uso da CPU e da memória, consulte as instruções para ["administrando"](#) , ["monitoramento"](#) , e ["atualizando"](#) StorageGRID.

Se o hyperthreading estiver habilitado nos hosts físicos subjacentes, você poderá fornecer 8 núcleos virtuais (4 núcleos físicos) por nó. Se o hyperthreading não estiver habilitado nos hosts físicos subjacentes, você deverá fornecer 8 núcleos físicos por nó.

Se você estiver usando máquinas virtuais como hosts e tiver controle sobre o tamanho e o número de VMs, use uma única VM para cada nó do StorageGRID e dimensione a VM adequadamente.

Veja também ["Requisitos de armazenamento e desempenho"](#) .

Requisitos de armazenamento e desempenho

Você deve entender os requisitos de armazenamento e desempenho para nós StorageGRID hospedados por máquinas virtuais, para que possa fornecer espaço suficiente para dar suporte à configuração inicial e à futura expansão de armazenamento.

Requisitos de desempenho

O desempenho do volume do sistema operacional e do primeiro volume de armazenamento impacta significativamente o desempenho geral do sistema. Certifique-se de que eles forneçam desempenho de disco adequado em termos de latência, operações de entrada/saída por segundo (IOPS) e taxa de transferência.

Todos os nós do StorageGRID exigem que a unidade do sistema operacional e todos os volumes de armazenamento tenham o cache de write-back habilitado. O cache deve estar em uma mídia protegida ou persistente.

Requisitos para máquinas virtuais que usam armazenamento NetApp ONTAP

Se você estiver implantando um nó StorageGRID como uma máquina virtual com armazenamento atribuído de um sistema NetApp ONTAP , terá confirmado que o volume não tem uma política de camadas FabricPool habilitada. Por exemplo, se um nó StorageGRID estiver sendo executado como uma máquina virtual em um host VMware, certifique-se de que o volume que faz o backup do armazenamento de dados para o nó 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.

Número de máquinas virtuais necessárias

Cada site StorageGRID requer no mínimo três nós de armazenamento.

Requisitos de armazenamento por tipo de nó

Em um ambiente de produção, as máquinas virtuais para nós StorageGRID devem atender a requisitos diferentes, dependendo dos tipos de nós.



Snapshots de disco não podem ser usados para restaurar nós de grade. Em vez disso, consulte o ["recuperação de nós de grade"](#) procedimentos para cada tipo de nó.

Tipo de nó	Armazenar
Nó de administração	100 GB LUN para SO LUN de 200 GB para tabelas de nó de administração LUN de 200 GB para log de auditoria do nó de administração

Tipo de nó	Armazenar
Nó de armazenamento	100 GB LUN para SO 3 LUNs para cada nó de armazenamento neste host Observação: Um nó de armazenamento pode ter de 1 a 16 LUNs de armazenamento; pelo menos 3 LUNs de armazenamento são recomendados. Tamanho mínimo por LUN: 4 TB Tamanho máximo do LUN testado: 39 TB.
Nó de armazenamento (somente metadados)	100 GB LUN para SO 1 LUN Tamanho mínimo por LUN: 4 TB Tamanho máximo do LUN testado: 39 TB. Observação: somente um rangedb é necessário para nós de armazenamento somente de metadados.
Nó de gateway	100 GB LUN para SO



Dependendo do nível de auditoria configurado, do tamanho das entradas do usuário, como o nome da chave do objeto S3, e da quantidade de dados de log de auditoria que você precisa preservar, pode ser necessário aumentar o tamanho do LUN do log de auditoria em cada nó de administração. Geralmente, uma grade gera aproximadamente 1 KB de dados de auditoria por operação S3, o que significa que um LUN de 200 GB suportaria 70 milhões de operações por dia ou 800 operações por segundo durante dois a três dias.

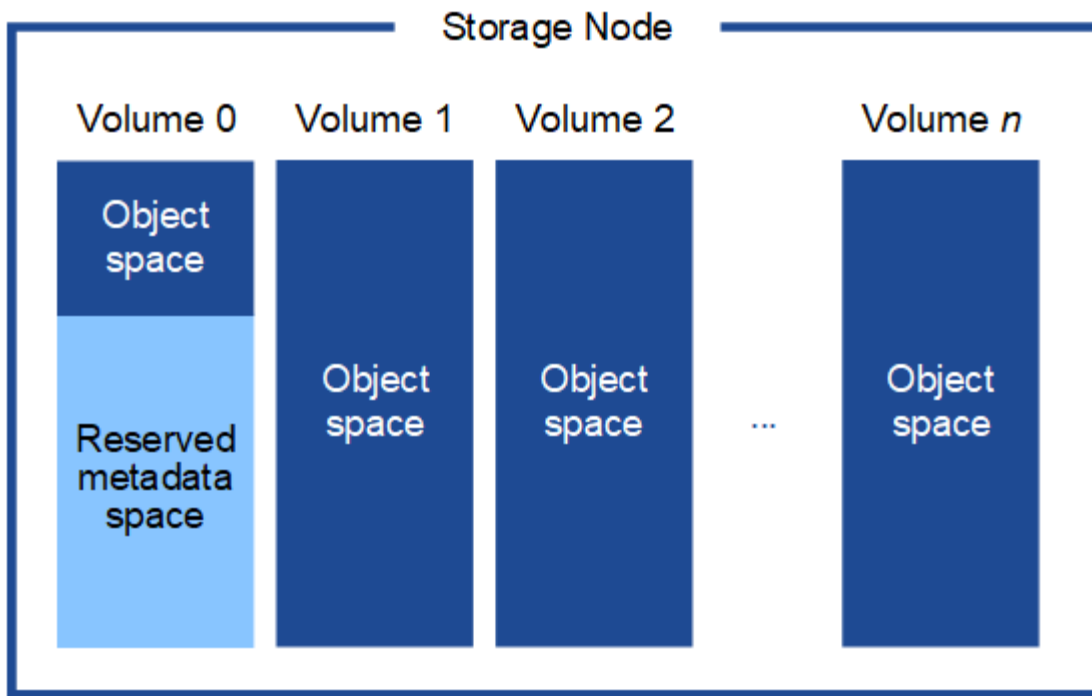
Requisitos de armazenamento para nós de armazenamento

Um nó de armazenamento baseado em software pode ter de 1 a 16 volumes de armazenamento; 3 ou mais volumes de armazenamento são recomendados. Cada volume de armazenamento deve ter 4 TB ou mais.



Um nó de armazenamento de dispositivo também pode ter até 48 volumes de armazenamento.

Conforme mostrado na figura, o StorageGRID reserva espaço para metadados de objetos no volume de armazenamento 0 de cada nó de armazenamento. Qualquer espaço restante no volume de armazenamento 0 e quaisquer outros volumes de armazenamento no Nó de Armazenamento são usados exclusivamente para dados de 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. As três cópias dos metadados do objeto são distribuídas uniformemente entre todos os nós de armazenamento em cada site.

Ao instalar uma grade com nós de armazenamento somente de metadados, a grade também deve conter um número mínimo de nós para armazenamento de objetos. Ver "[Tipos de nós de armazenamento](#)" para obter mais informações sobre nós de armazenamento somente de metadados.

- Para uma grade de site único, pelo menos dois nós de armazenamento são configurados para objetos e metadados.
- Para uma grade de vários sites, pelo menos um nó de armazenamento por site é configurado para objetos e metadados.

Ao atribuir espaço ao volume 0 de um novo Nó de Armazenamento, você deve garantir que haja espaço adequado para a parte desse nó de todos os metadados do objeto.

- No mínimo, você deve atribuir pelo menos 4 TB ao volume 0.



Se você usar apenas um volume de armazenamento para um Nó de Armazenamento e atribuir 4 TB ou menos ao volume, o Nó de Armazenamento poderá entrar no estado somente leitura de armazenamento na inicialização e armazenar apenas metadados de objetos.



Se você atribuir menos de 500 GB ao volume 0 (somente para uso não produtivo), 10% da capacidade do volume de armazenamento será reservada para metadados.

- Os recursos de nós somente de metadados baseados em software devem corresponder aos recursos de nós de armazenamento existentes. Por exemplo:
 - Se o site StorageGRID existente estiver usando dispositivos SG6000 ou SG6100, os nós somente de metadados baseados em software deverão atender aos seguintes requisitos mínimos:
 - 128 GB de RAM

- CPU de 8 núcleos
- 8 TB SSD ou armazenamento equivalente para o banco de dados Cassandra (rangedb/0)
- Se o site StorageGRID existente estiver usando nós de armazenamento virtuais com 24 GB de RAM, CPU de 8 núcleos e 3 TB ou 4 TB de armazenamento de metadados, os nós somente de metadados baseados em software deverão usar recursos semelhantes (24 GB de RAM, CPU de 8 núcleos e 4 TB de armazenamento de metadados (rangedb/0)).

Ao adicionar um novo site StorageGRID, a capacidade total de metadados do novo site deve, no mínimo, corresponder aos sites StorageGRID existentes e os novos recursos do site devem corresponder aos nós de armazenamento nos sites StorageGRID existentes.

- Se você estiver instalando um novo sistema (StorageGRID 11.6 ou superior) e cada nó de armazenamento tiver 128 GB ou mais de RAM, atribua 8 TB ou mais ao volume 0. Usar um valor maior para o volume 0 pode aumentar o espaço permitido para metadados em cada nó de armazenamento.
- Ao configurar diferentes nós de armazenamento para um site, use a mesma configuração para o volume 0, se possível. Se um site contiver nós de armazenamento de tamanhos diferentes, o nó de armazenamento com o menor volume 0 determinará a capacidade de metadados desse site.

Para mais detalhes, acesse "[Gerenciar armazenamento de metadados de objetos](#)".

Automatize a instalação (VMware)

Você pode usar a VMware OVF Tool para automatizar a implantação de nós de grade. Você também pode automatizar a configuração do StorageGRID.

Automatizar a implantação de nós de grade

Use a ferramenta VMware OVF para automatizar a implantação de nós de grade.

Antes de começar

- Você tem acesso a um sistema Linux/Unix com Bash 3.2 ou posterior.
- Você tem VMware vSphere com vCenter
- Você tem o VMware OVF Tool 4.1 instalado e configurado corretamente.
- Você sabe o nome de usuário e a senha para acessar o VMware vSphere usando a ferramenta OVF
- Você tem permissões suficientes para implantar VMs de arquivos OVF e ligá-las, além de permissões para criar volumes adicionais para anexar às VMs. Veja o `ovftool` documentação para mais detalhes.
- Você conhece a URL da infraestrutura virtual (VI) para o local no vSphere onde deseja implantar as máquinas virtuais StorageGRID. Essa URL normalmente será um vApp ou um pool de recursos. Por exemplo: `vi://vcenter.example.com/vi/sgws`



Você pode usar o VMware `ovftool` utilitário para determinar este valor (veja o `ovftool` documentação para detalhes).



Se você estiver implantando em um vApp, as máquinas virtuais não iniciarão automaticamente na primeira vez e você deverá ligá-las manualmente.

- Você coletou todas as informações necessárias para o arquivo de configuração de implantação. Ver "[Colete informações sobre seu ambiente de implantação](#)" para obter informações.

- Você tem acesso aos seguintes arquivos do arquivo de instalação do VMware para StorageGRID:

Nome do arquivo	Descrição
NetApp-SG-versão-SHA.vmdk	O arquivo de disco da máquina virtual que é usado como modelo para criar máquinas virtuais de nós de grade. Nota: Este arquivo deve estar na mesma pasta que o <code>.ovf</code> e <code>.mf</code> arquivos.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	O arquivo de modelo do Open Virtualization Format(<code>.ovf</code>) e arquivo de manifesto(<code>.mf</code>) para implantar o nó de administração primário.
vsphere-não-primário-admin.ovf vsphere-não-primário-admin.mf	O arquivo de modelo(<code>.ovf</code>) e arquivo de manifesto(<code>.mf</code>) para implantar nós administrativos não primários.
vsphere-gateway.ovf vsphere-gateway.mf	O arquivo de modelo(<code>.ovf</code>) e arquivo de manifesto(<code>.mf</code>) para implantar nós de gateway.
vsphere-storage.ovf vsphere-storage.mf	O arquivo de modelo(<code>.ovf</code>) e arquivo de manifesto(<code>.mf</code>) para implantar nós de armazenamento baseados em máquina virtual.
implantar-vsphere-ovftool.sh	O script de shell Bash usado para automatizar a implantação de nós de grade virtual.
implantar-vsphere-ovftool-sample.ini	O arquivo de configuração de exemplo para uso com o <code>deploy-vsphere-ovftool.sh</code> roteiro.

Defina o arquivo de configuração para sua implantação

Você especifica as informações necessárias para implantar nós de grade virtual para StorageGRID em um arquivo de configuração, que é usado pelo `deploy-vsphere-ovftool.sh` Script Bash. Você pode modificar um arquivo de configuração de exemplo para não precisar criar o arquivo do zero.

Passos

1. Faça uma cópia do arquivo de configuração de exemplo(`deploy-vsphere-ovftool.sample.ini`). Salve o novo arquivo como `deploy-vsphere-ovftool.ini` no mesmo diretório que `deploy-vsphere-ovftool.sh`.
2. Abrir `deploy-vsphere-ovftool.ini`.
3. Insira todas as informações necessárias para implantar nós de grade virtual do VMware.

Ver [Configurações do arquivo de configuração](#) para obter informações.
4. Depois de inserir e verificar todas as informações necessárias, salve e feche o arquivo.

Configurações do arquivo de configuração

O `deploy-vsphere-ovftool.ini` O arquivo de configuração contém as configurações necessárias para implantar nós de grade virtual.

O arquivo de configuração primeiro lista os parâmetros globais e, em seguida, lista os parâmetros específicos do nó em seções definidas pelo nome do nó. Quando o arquivo é usado:

- *Parâmetros globais* são aplicados a todos os nós da grade.
- *Parâmetros específicos do nó* substituem parâmetros globais.

Parâmetros globais

Os parâmetros globais são aplicados a todos os nós da grade, a menos que sejam substituídos por configurações em seções individuais. Coloque os parâmetros que se aplicam a vários nós na seção de parâmetros globais e, em seguida, substitua essas configurações conforme necessário nas seções para nós individuais.

- **OVFTOOL_ARGUMENTS:** Você pode especificar `OVFTOOL_ARGUMENTS` como configurações globais ou pode aplicar argumentos individualmente a nós específicos. Por exemplo:

```
OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
--datastore='datastore_name'
```

Você pode usar o `--powerOffTarget` e `--overwrite` opções para desligar e substituir máquinas virtuais existentes.



Você deve implantar nós em diferentes armazenamentos de dados e especificar `OVFTOOL_ARGUMENTS` para cada nó, em vez de globalmente.

- **FONTE:** O caminho para o modelo de máquina virtual `StorageGRID(.vmdk)` arquivo e o `.ovf` e `.mf` arquivos para nós de grade individuais. O padrão é o diretório atual.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **TARGET:** A URL da infraestrutura virtual VMware vSphere (vi) para o local onde o `StorageGRID` será implantado. Por exemplo:

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_NETWORK_CONFIG:** O método usado para adquirir endereços IP, `ESTÁTICOS` ou `DHCP`. O padrão é `ESTÁTICO`. Se todos ou a maioria dos nós usarem o mesmo método para adquirir endereços IP, você pode especificar esse método aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
GRID_NETWORK_CONFIG = STATIC
```

- **GRID_NETWORK_TARGET:** O nome de uma rede VMware existente a ser usada para a Grid Network. Se todos ou a maioria dos nós usarem o mesmo nome de rede, você pode especificá-lo aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
GRID_NETWORK_TARGET = SG Admin Network
```

- **GRID_NETWORK_MASK:** A máscara de rede para a Rede Grid. Se todos ou a maioria dos nós usarem a mesma máscara de rede, você pode especificá-la aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY:** O gateway de rede para a Rede Grid. Se todos ou a maioria dos nós usarem o mesmo gateway de rede, você pode especificá-lo aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU:** Opcional. A unidade máxima de transmissão (MTU) na rede elétrica. Se especificado, o valor deve estar entre 1280 e 9216. Por exemplo:

```
GRID_NETWORK_MTU = 9000
```

Se omitido, 1400 será usado.

Se você quiser usar quadros jumbo, defina a MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão.



O valor de MTU da rede deve corresponder ao valor configurado na porta do switch virtual no vSphere ao qual o nó está conectado. Caso contrário, podem ocorrer problemas de desempenho da rede ou perda de pacotes.



Para obter o melhor desempenho da rede, todos os nós devem ser configurados com valores de MTU semelhantes em suas interfaces de rede de grade. O alerta **Incompatibilidade de MTU da rede de grade** é acionado se houver uma diferença significativa nas configurações de MTU da rede de grade em nós individuais. Os valores de MTU não precisam ser os mesmos para todos os tipos de rede.

- **ADMIN_NETWORK_CONFIG:** O método usado para adquirir endereços IP, DESATIVADO, ESTÁTICO ou DHCP. O padrão é DESATIVADO. Se todos ou a maioria dos nós usarem o mesmo método para adquirir endereços IP, você pode especificar esse método aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET:** O nome de uma rede VMware existente a ser usada para a Rede de Administração. Esta configuração é necessária, a menos que a Rede de Administração esteja desabilitada. Se todos ou a maioria dos nós usarem o mesmo nome de rede, você pode especificá-lo aqui. Ao contrário da Grid Network, todos os nós não precisam estar conectados à mesma Admin Network. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- **ADMIN_NETWORK_MASK:** A máscara de rede para a rede de administração. Esta configuração é necessária se você estiver usando endereçamento IP estático. Se todos ou a maioria dos nós usarem a mesma máscara de rede, você pode especificá-la aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY:** O gateway de rede para a rede de administração. Esta configuração é necessária se você estiver usando endereçamento IP estático e especificar sub-redes externas na configuração ADMIN_NETWORK_ESL. (Ou seja, não é necessário se ADMIN_NETWORK_ESL estiver vazio.) Se todos ou a maioria dos nós usarem o mesmo gateway de rede, você pode especificá-lo aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL:** A lista de sub-redes externas (rotas) para a Rede de Administração, especificada como uma lista separada por vírgulas de destinos de rotas CIDR. Se todos ou a maioria dos nós usarem a mesma lista de sub-redes externas, você poderá especificá-la aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU:** Opcional. A unidade máxima de transmissão (MTU) na rede de administração. Não especifique se ADMIN_NETWORK_CONFIG = DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1400 será usado. Se você quiser usar quadros jumbo, defina a MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão. Se todos ou a maioria dos nós usarem a mesma MTU para a Rede de Administração, você pode especificá-la aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG:** O método usado para adquirir endereços IP, DESATIVADO, ESTÁTICO ou DHCP. O padrão é DESATIVADO. Se todos ou a maioria dos nós usarem o mesmo método para adquirir endereços IP, você pode especificar esse método aqui. Você pode então substituir a configuração

global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET:** O nome de uma rede VMware existente a ser usada para a Rede do Cliente. Esta configuração é necessária, a menos que a Rede do Cliente esteja desabilitada. Se todos ou a maioria dos nós usarem o mesmo nome de rede, você pode especificá-lo aqui. Ao contrário da Rede Grid, todos os nós não precisam estar conectados à mesma Rede Cliente. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- **CLIENT_NETWORK_MASK:** A máscara de rede para a rede do cliente. Esta configuração é necessária se você estiver usando endereçamento IP estático. Se todos ou a maioria dos nós usarem a mesma máscara de rede, você pode especificá-la aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY:** O gateway de rede para a Rede do Cliente. Esta configuração é necessária se você estiver usando endereçamento IP estático. Se todos ou a maioria dos nós usarem o mesmo gateway de rede, você pode especificá-lo aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU:** Opcional. A unidade máxima de transmissão (MTU) na rede do cliente. Não especifique se CLIENT_NETWORK_CONFIG = DHCP. Se especificado, o valor deve estar entre 1280 e 9216. Se omitido, 1400 será usado. Se você quiser usar quadros jumbo, defina a MTU para um valor adequado para quadros jumbo, como 9000. Caso contrário, mantenha o valor padrão. Se todos ou a maioria dos nós usarem a mesma MTU para a Rede do Cliente, você pode especificá-la aqui. Você pode então substituir a configuração global especificando configurações diferentes para um ou mais nós individuais. Por exemplo:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAP:** Remapeia qualquer porta usada por um nó para comunicações internas do nó da grade ou comunicações externas. O remapeamento de portas é necessário se as políticas de rede corporativa restringirem uma ou mais portas usadas pelo StorageGRID. Para obter a lista de portas usadas pelo StorageGRID, consulte comunicações internas do nó da grade e comunicações externas em "[Diretrizes de rede](#)".



Não remapeie as portas que você planeja usar para configurar os pontos de extremidade do balanceador de carga.



Se somente `PORT_REMAP` estiver definido, o mapeamento especificado será usado para comunicações de entrada e saída. Se `PORT_REMAP_INBOUND` também for especificado, `PORT_REMAP` se aplicará somente às comunicações de saída.

O formato utilizado é: *network type/protocol/default port used by grid node/new port*, onde o tipo de rede é *grade*, *administrador* ou *cliente*, e o protocolo é *tcp* ou *udp*.

Por exemplo:

```
PORT_REMAP = client/tcp/18082/443
```

Se usado sozinho, este exemplo de configuração mapeia simetricamente as comunicações de entrada e saída do nó da grade da porta 18082 para a porta 443. Se usado em conjunto com `PORT_REMAP_INBOUND`, esta configuração de exemplo mapeia as comunicações de saída da porta 18082 para a porta 443.

Você também pode remapear várias portas usando uma lista separada por vírgulas.

Por exemplo:

```
PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
```

- **PORT_REMAP_INBOUND:** Remapeia as comunicações de entrada para a porta especificada. Se você especificar `PORT_REMAP_INBOUND`, mas não especificar um valor para `PORT_REMAP`, as comunicações de saída para a porta permanecerão inalteradas.



Não remapeie as portas que você planeja usar para configurar os pontos de extremidade do balanceador de carga.

O formato utilizado é: *network type/protocol/_default port used by grid node/new port*, onde o tipo de rede é *grade*, *administrador* ou *cliente*, e o protocolo é *tcp* ou *udp*.

Por exemplo:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

Este exemplo pega o tráfego enviado para a porta 443 para passar por um firewall interno e o direciona para a porta 18082, onde o nó da grade está escutando solicitações S3.

Você também pode remapear várias portas de entrada usando uma lista separada por vírgulas.

Por exemplo:

```
PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
```

- **TEMPORARY_PASSWORD_TYPE:** O tipo de senha de instalação temporária a ser usada ao acessar o console da VM ou a API de instalação do StorageGRID, ou usar SSH, antes que o nó ingresse na grade.



Se todos ou a maioria dos nós usarem o mesmo tipo de senha de instalação temporária, especifique o tipo na seção de parâmetros globais. Então, opcionalmente, use uma configuração diferente para um nó individual. Por exemplo, se você selecionar **Usar senha personalizada** globalmente, poderá usar **CUSTOM_TEMPORARY_PASSWORD=<senha>** para definir a senha para cada nó.

TEMPORARY_PASSWORD_TYPE pode ser um dos seguintes:

- **Usar nome do nó:** O nome do nó é usado como senha de instalação temporária e fornece acesso ao console da VM, à API de instalação do StorageGRID e ao SSH.
- **Desabilitar senha:** Nenhuma senha de instalação temporária será usada. Se você precisar acessar a VM para depurar problemas de instalação, consulte ["Solucionar problemas de instalação"](#).
- **Usar senha personalizada:** O valor fornecido com **CUSTOM_TEMPORARY_PASSWORD=<password>** é usado como senha de instalação temporária e fornece acesso ao console da VM, à API de instalação do StorageGRID e ao SSH.



Opcionalmente, você pode omitir o parâmetro **TEMPORARY_PASSWORD_TYPE** e especificar apenas **CUSTOM_TEMPORARY_PASSWORD=<password>**.

- **CUSTOM_TEMPORARY_PASSWORD=<senha>** Opcional. A senha temporária a ser usada durante a instalação ao acessar o console da VM, a API de instalação do StorageGRID e o SSH. Ignorado se **TEMPORARY_PASSWORD_TYPE** estiver definido como **Usar nome do nó** ou **Desativar senha**.

Parâmetros específicos do nó

Cada nó está em sua própria seção do arquivo de configuração. Cada nó requer as seguintes configurações:

- O cabeçalho da seção define o nome do nó que será exibido no Grid Manager. Você pode substituir esse valor especificando o parâmetro opcional **NODE_NAME** para o nó.
- **NODE_TYPE:** VM_Admin_Node, VM_Storage_Node ou VM_API_Gateway_Node
- **STORAGE_TYPE:** combinado, dados ou metadados. Este parâmetro opcional para nós de armazenamento assume como padrão o valor combinado (dados e metadados) se não for especificado. Para obter mais informações, consulte ["Tipos de nós de armazenamento"](#).
- **GRID_NETWORK_IP:** O endereço IP do nó na rede Grid.
- **ADMIN_NETWORK_IP:** O endereço IP do nó na rede de administração. Obrigatório somente se o nó estiver conectado à rede de administração e **ADMIN_NETWORK_CONFIG** estiver definido como **STATIC**.
- **CLIENT_NETWORK_IP:** O endereço IP do nó na rede do cliente. Obrigatório somente se o nó estiver conectado à rede do cliente e **CLIENT_NETWORK_CONFIG** para este nó estiver definido como **STATIC**.
- **ADMIN_IP:** O endereço IP do nó de administração primário na rede Grid. Use o valor especificado como **GRID_NETWORK_IP** para o nó de administração primário. Se você omitir esse parâmetro, o nó tentará descobrir o IP do nó de administração primário usando o mDNS. Para obter mais informações, consulte ["Como os nós da grade descobrem o nó administrativo principal"](#).



O parâmetro **ADMIN_IP** é ignorado para o nó de administração primário.

- Quaisquer parâmetros que não foram definidos globalmente. Por exemplo, se um nó estiver anexado à Rede de Administração e você não tiver especificado os parâmetros **ADMIN_NETWORK** globalmente, será necessário especificá-los para o nó.

Nó de administração primário

As seguintes configurações adicionais são necessárias para o nó de administração principal:

- **TIPO_NÓ:** Nó_Administrador_VM
- **ADMIN_ROLE:** Primário

Esta entrada de exemplo é para um nó de administração primário que está em todas as três redes:

```
[DC1-ADM1]
ADMIN_ROLE = Primary
NODE_TYPE = VM_Admin_Node
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd

GRID_NETWORK_IP = 10.1.0.2
ADMIN_NETWORK_IP = 10.3.0.2
CLIENT_NETWORK_IP = 10.4.0.2
```

A seguinte configuração adicional é opcional para o nó de administração principal:

- **DISCO:** Por padrão, os nós de administração recebem dois discos rígidos adicionais de 200 GB para auditoria e uso de banco de dados. Você pode aumentar essas configurações usando o parâmetro DISK. Por exemplo:

```
DISK = INSTANCES=2, CAPACITY=300
```



Para nós de administração, INSTÂNCIAS deve sempre ser igual a 2.

Nó de armazenamento

A seguinte configuração adicional é necessária para nós de armazenamento:

- **TIPO_NÓ:** Nó_de_armazenamento_VM

Esta entrada de exemplo é para um nó de armazenamento que está nas redes de grade e de administração, mas não na rede do cliente. Este nó usa a configuração ADMIN_IP para especificar o endereço IP do nó de administração principal na rede Grid.

```
[DC1-S1]
NODE_TYPE = VM_Storage_Node

GRID_NETWORK_IP = 10.1.0.3
ADMIN_NETWORK_IP = 10.3.0.3

ADMIN_IP = 10.1.0.2
```

Este segundo exemplo de entrada é para um nó de armazenamento em uma rede de cliente onde a política de rede corporativa do cliente declara que um aplicativo cliente S3 só tem permissão para acessar o nó de armazenamento usando a porta 80 ou 443. O arquivo de configuração de exemplo usa `PORT_REMAP` para permitir que o nó de armazenamento envie e receba mensagens S3 na porta 443.

```
[DC2-S1]
NODE_TYPE = VM_Storage_Node

GRID_NETWORK_IP = 10.1.1.3
CLIENT_NETWORK_IP = 10.4.1.3
PORT_REMAP = client/tcp/18082/443

ADMIN_IP = 10.1.0.2
```

O último exemplo cria um remapeamento simétrico para o tráfego SSH da porta 22 para a porta 3022, mas define explicitamente os valores para o tráfego de entrada e saída.

```
[DC1-S3]
NODE_TYPE = VM_Storage_Node

GRID_NETWORK_IP = 10.1.1.3

PORT_REMAP = grid/tcp/22/3022
PORT_REMAP_INBOUND = grid/tcp/3022/22

ADMIN_IP = 10.1.0.2
```

As seguintes configurações adicionais são opcionais para nós de armazenamento:

- **DISCO:** Por padrão, os nós de armazenamento recebem três discos de 4 TB para uso do RangeDB. Você pode aumentar essas configurações com o parâmetro `DISK`. Por exemplo:

```
DISK = INSTANCES=16, CAPACITY=4096
```

- **TIPO_DE_ARMAZENAMENTO:** Por padrão, todos os novos Nós de Armazenamento são configurados para armazenar dados de objetos e metadados, conhecidos como Nó de Armazenamento *combinado*. Você pode alterar o tipo de nó de armazenamento para armazenar somente dados ou metadados com o parâmetro `STORAGE_TYPE`. Por exemplo:

```
STORAGE_TYPE = data
```

Nó de gateway

A seguinte configuração adicional é necessária para nós de gateway:

- **TIPO_NÓ:** VM_API_Gateway

Esta entrada de exemplo é para um nó de gateway de exemplo em todas as três redes. Neste exemplo, nenhum parâmetro de rede do cliente foi especificado na seção global do arquivo de configuração, portanto, eles devem ser especificados para o nó:

```
[DC1-G1]
NODE_TYPE = VM_API_Gateway

GRID_NETWORK_IP = 10.1.0.5
ADMIN_NETWORK_IP = 10.3.0.5

CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_TARGET = SG Client Network
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.4.0.1
CLIENT_NETWORK_IP = 10.4.0.5

ADMIN_IP = 10.1.0.2
```

Nó de administração não primário

As seguintes configurações adicionais são necessárias para nós administrativos não primários:

- **TIPO_NÓ:** Nó_Administrador_VM
- **ADMIN_ROLE:** Não primário

Esta entrada de exemplo é para um nó de administração não primário que não está na rede do cliente:

```
[DC2-ADM1]
ADMIN_ROLE = Non-Primary
NODE_TYPE = VM_Admin_Node

GRID_NETWORK_TARGET = SG Grid Network
GRID_NETWORK_IP = 10.1.0.6
ADMIN_NETWORK_IP = 10.3.0.6

ADMIN_IP = 10.1.0.2
```

A seguinte configuração adicional é opcional para nós administrativos não primários:

- **DISCO:** Por padrão, os nós de administração recebem dois discos rígidos adicionais de 200 GB para auditoria e uso de banco de dados. Você pode aumentar essas configurações usando o parâmetro DISK. Por exemplo:

```
DISK = INSTANCES=2, CAPACITY=300
```



Para nós de administração, INSTÂNCIAS deve sempre ser igual a 2.

Execute o script Bash

Você pode usar o `deploy-vsphere-ovftool.sh` Script Bash e o arquivo de configuração `deploy-vsphere-ovftool.ini` que você modificou para automatizar a implantação de nós StorageGRID no VMware vSphere.

Antes de começar

Você criou um arquivo de configuração `deploy-vsphere-ovftool.ini` para seu ambiente.

Você pode usar a ajuda disponível com o script Bash inserindo os comandos de ajuda (`-h/--help`). Por exemplo:

```
./deploy-vsphere-ovftool.sh -h
```

ou

```
./deploy-vsphere-ovftool.sh --help
```

Passos

1. Efetue login na máquina Linux que você está usando para executar o script Bash.
2. Mude para o diretório onde você extraiu o arquivo de instalação.

Por exemplo:

```
cd StorageGRID-Webscale-version/vsphere
```

3. Para implantar todos os nós da grade, execute o script Bash com as opções apropriadas para seu ambiente.

Por exemplo:

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-vsphere-ovftool.ini
```

4. Se um nó de grade não puder ser implantado devido a um erro, resolva o erro e execute novamente o script Bash somente para esse nó.

Por exemplo:

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd --single -node="DC1-S3" ./deploy-vsphere-ovftool.ini
```

A implantação é concluída quando o status de cada nó é "Aprovado".

```
Deployment Summary
+-----+-----+-----+
| node           | attempts | status           |
+-----+-----+-----+
| DC1-ADM1       | 1        | Passed           |
| DC1-G1         | 1        | Passed           |
| DC1-S1         | 1        | Passed           |
| DC1-S2         | 1        | Passed           |
| DC1-S3         | 1        | Passed           |
+-----+-----+-----+
```

Automatize a configuração do StorageGRID

Após implantar os nós da grade, você pode automatizar a configuração do sistema StorageGRID .

Antes de começar

- Você sabe a localização dos seguintes arquivos do arquivo de instalação.

Nome do arquivo	Descrição
configurar-storagegrid.py	Script Python usado para automatizar a configuração
configurar-storagegrid.sample.json	Arquivo de configuração de exemplo para uso com o script
configurar-storagegrid.blank.json	Arquivo de configuração em branco para uso com o script

- Você criou um `configure-storagegrid.json` arquivo de configuração. Para criar este arquivo, você pode modificar o arquivo de configuração de exemplo(`configure-storagegrid.sample.json`) ou o arquivo de configuração em branco(`configure-storagegrid.blank.json`).

Você pode usar o `configure-storagegrid.py` Script Python e o `configure-storagegrid.json` arquivo de configuração de grade para automatizar a configuração do seu sistema StorageGRID .



Você também pode configurar o sistema usando o Grid Manager ou a API de instalação.

Passos

1. Faça login na máquina Linux que você está usando para executar o script Python.
2. Mude para o diretório onde você extraiu o arquivo de instalação.

Por exemplo:

```
cd StorageGRID-Webscale-version/platform
```

onde `platform` é `debs`, `rpms` ou `vsphere`.

3. Execute o script Python e use o arquivo de configuração que você criou.

Por exemplo:

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Resultado

Um pacote de recuperação `.zip` O arquivo é gerado durante o processo de configuração e é baixado para o diretório onde você está executando o processo de instalação e configuração. Você deve fazer backup do arquivo do pacote de recuperação para poder recuperar o sistema StorageGRID se um ou mais nós da grade falharem. Por exemplo, copie-o para um local de rede seguro e com backup e para um local de armazenamento em nuvem seguro.



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 .

Se você especificou que senhas aleatórias devem ser geradas, abra o `Passwords.txt` arquivo e procure as senhas necessárias para acessar seu sistema StorageGRID .

```
#####
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####      ./sgws-recovery-package-994078-rev1.zip      #####
#####   Safeguard this file as it will be needed in case of a   #####
#####               StorageGRID node recovery.               #####
#####
```

Seu sistema StorageGRID estará instalado e configurado quando uma mensagem de confirmação for exibida.

```
StorageGRID has been configured and installed.
```

Informações relacionadas

- ["Navegue até o Gerenciador de Grade"](#)
- ["Instalação REST API"](#)

Implantar nós de grade de máquina virtual (VMware)

Colete informações sobre seu ambiente de implantação

Antes de implantar nós de grade, você deve coletar informações sobre sua configuração de rede e ambiente VMware.



É mais eficiente executar uma única instalação de todos os nós, em vez de instalar alguns nós agora e outros depois.

Informações sobre VMware

Você deve acessar o ambiente de implantação e coletar informações sobre o ambiente VMware; as redes que foram criadas para as redes Grid, Admin e Client; e os tipos de volume de armazenamento que você planeja usar para os nós de armazenamento.

Você deve coletar informações sobre seu ambiente VMware, incluindo o seguinte:

- O nome de usuário e a senha de uma conta do VMware vSphere que tenha permissões apropriadas para concluir a implantação.
- Informações de configuração de host, armazenamento de dados e rede para cada máquina virtual do nó StorageGRID .



O VMware live vMotion faz com que o tempo do relógio da máquina virtual salte e não é compatível com nós de grade de nenhum tipo. Embora raros, horários incorretos podem resultar em perda de dados ou atualizações de configuração.

Informações da rede de grade

Você deve coletar informações sobre a rede VMware criada para a StorageGRID Grid Network (obrigatório), incluindo:

- O nome da rede.
- O método usado para atribuir endereços IP, estáticos ou DHCP.
 - Se você estiver usando endereços IP estáticos, os detalhes de rede necessários para cada nó da grade (endereço IP, gateway, máscara de rede).
 - Se você estiver usando DHCP, o endereço IP do nó de administração primário na rede de grade. Ver ["Como os nós da grade descobrem o nó administrativo principal"](#) para maiores informações.

Informações da rede de administração

Para nós que serão conectados à Rede de Administração StorageGRID opcional, você deve coletar informações sobre a rede VMware criada para esta rede, incluindo:

- O nome da rede.
- O método usado para atribuir endereços IP, estáticos ou DHCP.
 - Se você estiver usando endereços IP estáticos, os detalhes de rede necessários para cada nó da grade (endereço IP, gateway, máscara de rede).
 - Se você estiver usando DHCP, o endereço IP do nó de administração primário na rede de grade. Ver ["Como os nós da grade descobrem o nó administrativo principal"](#) para maiores informações.
- A lista de sub-redes externas (ESL) para a rede de administração.

Informações da rede do cliente

Para nós que serão conectados à Rede de Cliente StorageGRID opcional, você deve coletar informações sobre a rede VMware criada para esta rede, incluindo:

- O nome da rede.
- O método usado para atribuir endereços IP, estáticos ou DHCP.
- Se você estiver usando endereços IP estáticos, os detalhes de rede necessários para cada nó da grade (endereço IP, gateway, máscara de rede).

Informações sobre interfaces adicionais

Opcionalmente, você pode adicionar interfaces de tronco ou de acesso à VM no vCenter depois de instalar o nó. Por exemplo, você pode querer adicionar uma interface de tronco a um nó de administração ou gateway, para poder usar interfaces de 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).

As interfaces adicionadas são exibidas na página de interfaces de VLAN e na página de grupos de HA no Grid Manager.

- Se você adicionar uma interface de tronco, configure uma ou mais interfaces VLAN para cada nova interface pai. Ver ["configurar interfaces VLAN"](#) .
- Se você adicionar uma interface de acesso, deverá adicioná-la diretamente aos grupos de HA. Ver ["configurar grupos de alta disponibilidade"](#) .

Volumes de armazenamento para nós de armazenamento virtuais

Você deve coletar as seguintes informações para nós de armazenamento baseados em máquina virtual:

- O número e o tamanho dos volumes de armazenamento (LUNs de armazenamento) que você planeja adicionar. Consulte ["Requisitos de armazenamento e desempenho"](#) .

Informações de configuração da grade

Você deve coletar informações para configurar sua grade:

- Licença de rede
- Endereços IP do servidor Network Time Protocol (NTP)
- Endereços IP do servidor DNS

Como os nós da grade descobrem o nó administrativo principal

Os nós de grade se comunicam com o nó de administração principal para configuração e gerenciamento. Cada nó da grade deve saber o endereço IP do nó administrativo primário na rede da grade.

Para garantir que um nó de grade possa acessar o nó de administração principal, você pode fazer o seguinte ao implantar o nó:

- Você pode usar o parâmetro ADMIN_IP para inserir manualmente o endereço IP do nó de administração principal.
- Você pode omitir o parâmetro ADMIN_IP para que o nó da grade descubra o valor automaticamente. A descoberta automática é especialmente útil quando a Grid Network usa DHCP para atribuir o endereço IP ao nó administrativo primário.

A descoberta automática do nó de administração primário é realizada usando um sistema de nomes de domínio multicast (mDNS). Quando o nó de administração primário é iniciado pela primeira vez, ele publica

seu endereço IP usando mDNS. Outros nós na mesma sub-rede podem então consultar o endereço IP e adquiri-lo automaticamente. Entretanto, como o tráfego IP multicast normalmente não é roteável entre sub-redes, os nós em outras sub-redes não podem adquirir o endereço IP do nó administrativo principal diretamente.

Se você usar a descoberta automática:



- Você deve incluir a configuração ADMIN_IP para pelo menos um nó de grade em qualquer sub-rede à qual o nó de administração primário não esteja diretamente conectado. Este nó de grade publicará então o endereço IP do nó de administração principal para que outros nós na sub-rede o descubram com o mDNS.
- Certifique-se de que sua infraestrutura de rede suporte a passagem de tráfego IP multicast dentro de uma sub-rede.

Implantar um nó StorageGRID como uma máquina virtual

Use o VMware vSphere Web Client para implantar cada nó de grade como uma máquina virtual. Durante a implantação, cada nó de grade é criado e conectado a uma ou mais redes StorageGRID .

Se você precisar implantar qualquer nó de armazenamento do dispositivo StorageGRID , consulte ["Implantar nó de armazenamento do dispositivo"](#) .

Opcionalmente, você pode remapear as portas do nó ou aumentar as configurações de CPU ou memória do nó antes de ligá-lo.

Antes de começar

- Você revisou como ["planejar e preparar para a instalação"](#) , e você entende os requisitos de software, CPU e RAM, além de armazenamento e desempenho.
- Você está familiarizado com o VMware vSphere Hypervisor e tem experiência na implantação de máquinas virtuais neste ambiente.



O `open-vm-tools` pacote, uma implementação de código aberto semelhante ao VMware Tools, está incluído na máquina virtual StorageGRID . Você não precisa instalar o VMware Tools manualmente.

- Você baixou e extraiu a versão correta do arquivo de instalação do StorageGRID para o VMware.



Se você estiver implantando o novo nó como parte de uma operação de expansão ou recuperação, deverá usar a versão do StorageGRID que está atualmente em execução na grade.

- Você tem o disco da máquina virtual StorageGRID(`.vmdk`) arquivo:

```
NetApp-SG-version-SHA.vmdk
```

- Você tem o `.ovf` e `.mf` arquivos para cada tipo de nó de grade que você está implantando:

Nome do arquivo	Descrição
vsphere-primary-admin.ovf vsphere-primary-admin.mf	O arquivo de modelo e o arquivo de manifesto para o nó de administração primário.
vsphere-não-primário-admin.ovf vsphere-não-primário-admin.mf	O arquivo de modelo e o arquivo de manifesto para um nó de administração não primário.
vsphere-storage.ovf vsphere-storage.mf	O arquivo de modelo e o arquivo de manifesto para um nó de armazenamento.
vsphere-gateway.ovf vsphere-gateway.mf	O arquivo de modelo e o arquivo de manifesto para um nó de gateway.

- O .vdmk , .ovf , e .mf os arquivos estão todos no mesmo diretório.
- Você tem um plano para minimizar os domínios de falha. Por exemplo, você não deve implantar todos os nós de gateway em um único host vSphere ESXi.



Em uma implantação de produção, não execute mais de um nó de armazenamento em uma única máquina virtual. Não execute várias máquinas virtuais no mesmo host ESXi se isso criar um problema de domínio de falha inaceitável.

- Se você estiver implantando um nó como parte de uma operação de expansão ou recuperação, você terá a ["instruções para expandir um sistema StorageGRID"](#) ou o ["instruções de recuperação e manutenção"](#) .
- Se você estiver implantando um nó StorageGRID como uma máquina virtual com armazenamento atribuído de um sistema NetApp ONTAP , terá confirmado que o volume não tem uma política de camadas FabricPool habilitada. Por exemplo, se um nó StorageGRID estiver sendo executado como uma máquina virtual em um host VMware, certifique-se de que o volume que faz o backup do armazenamento de dados para o nó 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.

Sobre esta tarefa

Siga estas instruções para implantar inicialmente nós VMware, adicionar um novo nó VMware em uma expansão ou substituir um nó VMware como parte de uma operação de recuperação. Exceto conforme indicado nas etapas, o procedimento de implantação do nó é o mesmo para todos os tipos de nó, incluindo nós de administração, nós de armazenamento e nós de gateway.

Se você estiver instalando um novo sistema StorageGRID :

- Você pode implantar nós em qualquer ordem.
- Você deve garantir que cada máquina virtual possa se conectar ao nó de administração principal pela rede Grid.
- Você deve implantar todos os nós da grade antes de configurá-la.

Se você estiver executando uma operação de expansão ou recuperação:

- Você deve garantir que a nova máquina virtual possa se conectar a todos os outros nós na Grid Network.

Se você precisar remapear qualquer uma das portas do nó, não ligue o novo nó até que a configuração de remapeamento de porta esteja concluída.

Passos

1. Usando o VCenter, implante um modelo OVF.

Se você especificar uma URL, aponte para uma pasta que contém os seguintes arquivos. Caso contrário, selecione cada um desses arquivos em um diretório local.

```
NetApp-SG-version-SHA.vmdk  
vsphere-node.ovf  
vsphere-node.mf
```

Por exemplo, se este for o primeiro nó que você está implantando, use estes arquivos para implantar o nó de administração principal do seu sistema StorageGRID :

```
NetApp-SG-version-SHA.vmdk  
vsphere-primary-admin.ovf  
vsphere-primary-admin.mf
```

2. Forneça um nome para a máquina virtual.

A prática padrão é usar o mesmo nome para a máquina virtual e para o nó da grade.

3. Coloque a máquina virtual no vApp ou pool de recursos apropriado.
4. Se você estiver implantando o nó de administração principal, leia e aceite o Contrato de licença do usuário final.

Dependendo da sua versão do vCenter, a ordem das etapas irá variar para aceitar o Contrato de Licença do Usuário Final, especificar o nome da máquina virtual e selecionar um armazenamento de dados.

5. Selecione o armazenamento para a máquina virtual.

Se você estiver implantando um nó como parte de uma operação de recuperação, siga as instruções em [etapa de recuperação de armazenamento](#) para adicionar novos discos virtuais, reconectar discos rígidos virtuais do nó de grade com falha ou ambos.

Ao implantar um nó de armazenamento, use 3 ou mais volumes de armazenamento, com cada volume de armazenamento tendo 4 TB ou mais. Você deve atribuir pelo menos 4 TB ao volume 0.



O arquivo .ovf do nó de armazenamento define vários VMDKs para armazenamento. A menos que esses VMDKs atendam aos seus requisitos de armazenamento, você deve removê-los e atribuir VMDKs ou RDMs apropriados para armazenamento antes de ligar o nó. Os VMDKs são mais comumente usados em ambientes VMware e são mais fáceis de gerenciar, enquanto os RDMs podem fornecer melhor desempenho para cargas de trabalho que usam tamanhos de objetos maiores (por exemplo, maiores que 100 MB).



Algumas instalações do StorageGRID podem usar volumes de armazenamento maiores e mais ativos do que cargas de trabalho virtualizadas típicas. Pode ser necessário ajustar alguns parâmetros do hipervisor, como `MaxAddressableSpaceTB` , para atingir o desempenho ideal. Se você encontrar baixo desempenho, entre em contato com seu recurso de suporte de virtualização para determinar se seu ambiente pode se beneficiar do ajuste de configuração específico da carga de trabalho.

6. Selecione redes.

Determine quais redes StorageGRID o nó usará selecionando uma rede de destino para cada rede de origem.

- A Rede Grid é necessária. Você deve selecionar uma rede de destino no ambiente vSphere. + 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. Todos os nós na rede de grade devem ser capazes de se comunicar com todos os outros nós.
- Se você usar a Rede de administração, selecione uma rede de destino diferente no ambiente vSphere. Se você não usar a Rede de administração, selecione o mesmo destino que você selecionou para a Rede de grade.
- Se você usar a Rede do Cliente, selecione uma rede de destino diferente no ambiente vSphere. Se você não usar a Rede do Cliente, selecione o mesmo destino que você selecionou para a Rede da Grade.
- Se você usar uma rede de administrador ou cliente, os nós não precisam estar nas mesmas redes de administrador ou cliente.

7. Para **Personalizar modelo**, configure as propriedades do nó StorageGRID necessárias.

a. Digite o **Nome do nó**.



Se estiver recuperando um nó de grade, você deverá inserir o nome do nó que está recuperando.

b. Use o menu suspenso **Senha de instalação temporária** para especificar uma senha de instalação temporária, para que você possa acessar o console da VM ou a API de instalação do StorageGRID , ou usar SSH, antes que o novo nó se junte à grade.



A senha de instalação temporária é usada somente durante a instalação do nó. Depois que um nó for adicionado à grade, você pode acessá-lo usando o "[senha do console do nó](#)" , que está listado no `Passwords.txt` arquivo no Pacote de Recuperação.

- **Usar nome do nó:** O valor fornecido para o campo **Nome do nó** é usado como senha de instalação temporária.
 - **Usar senha personalizada:** Uma senha personalizada é usada como senha de instalação temporária.
 - **Desabilitar senha:** Nenhuma senha de instalação temporária será usada. Se você precisar acessar a VM para depurar problemas de instalação, consulte "[Solucionar problemas de instalação](#)" .
- c. Se você selecionou **Usar senha personalizada**, especifique a senha de instalação temporária que deseja usar no campo **Senha personalizada**.
- d. Na seção **Rede de grade (eth0)**, selecione ESTÁTICO ou DHCP para a **Configuração de IP da rede**

de grade.

- Se você selecionar **ESTÁTICO**, insira o **IP da rede de grade**, a **Máscara da rede de grade**, o **Gateway da rede de grade** e a **MTU da rede de grade**.
 - Se você selecionar **DHCP**, o **IP da rede Grid**, a **Máscara da rede Grid** e o **Gateway da rede Grid** serão atribuídos automaticamente.
- e. No campo **IP do administrador primário**, insira o endereço IP do nó de administração primário da rede de grade.



Esta etapa não se aplica se o nó que você está implantando for o nó de administração principal.

Se você omitir o endereço IP do nó de administração primário, o endereço IP será descoberto automaticamente se o nó de administração primário, ou pelo menos um outro nó de grade com **ADMIN_IP** configurado, estiver presente na mesma sub-rede. No entanto, é recomendável definir o endereço IP do nó de administração principal aqui.

- a. Na seção **Rede de administração (eth1)**, selecione **ESTÁTICO**, **DHCP** ou **DESATIVADO** para a **Configuração de IP da rede de administração**.
- Se você não quiser usar a Rede de Administração, selecione **DESATIVADO** e digite **0.0.0.0** para o IP da Rede de Administração. Você pode deixar os outros campos em branco.
 - Se você selecionar **ESTÁTICO**, insira o **IP da rede de administração**, a **Máscara da rede de administração**, o **Gateway da rede de administração** e a **MTU da rede de administração**.
 - Se você selecionar **ESTÁTICO**, entre na **Lista de sub-redes externas da rede de administração**. Você também deve configurar um gateway.
 - Se você selecionar **DHCP**, o **IP da rede de administração**, a **Máscara de rede de administração** e o **Gateway da rede de administração** serão atribuídos automaticamente.
- b. Na seção **Rede do cliente (eth2)**, selecione **ESTÁTICO**, **DHCP** ou **DESATIVADO** para a **Configuração de IP da rede do cliente**.
- Se você não quiser usar a Rede do Cliente, selecione **DESATIVADO** e digite **0.0.0.0** para o IP da Rede do Cliente. Você pode deixar os outros campos em branco.
 - Se você selecionar **ESTÁTICO**, insira o **IP da rede do cliente**, a **Máscara da rede do cliente**, o **Gateway da rede do cliente** e a **MTU da rede do cliente**.
 - Se você selecionar **DHCP**, o **IP da rede do cliente**, a **Máscara da rede do cliente** e o **Gateway da rede do cliente** serão atribuídos automaticamente.

8. Revise a configuração da máquina virtual e faça as alterações necessárias.
9. Quando estiver pronto para concluir, selecione **Concluir** para iniciar o upload da máquina virtual.
10. Se você implantou este nó como parte de uma operação de recuperação e esta não for uma recuperação de nó completo, execute estas etapas após a conclusão da implantação:
- a. Clique com o botão direito do mouse na máquina virtual e selecione **Editar configurações**.
 - b. Selecione cada disco rígido virtual padrão que foi designado para armazenamento e selecione **Remover**.
 - c. Dependendo das circunstâncias de recuperação de dados, adicione novos discos virtuais de acordo com seus requisitos de armazenamento, reconecte quaisquer discos rígidos virtuais preservados do nó de grade com falha removido anteriormente, ou ambos.

Observe as seguintes diretrizes importantes:

- Se você estiver adicionando novos discos, deverá usar o mesmo tipo de dispositivo de armazenamento que estava em uso antes da recuperação do nó.
- O arquivo .ovf do nó de armazenamento define vários VMDKs para armazenamento. A menos que esses VMDKs atendam aos seus requisitos de armazenamento, você deve removê-los e atribuir VMDKs ou RDMs apropriados para armazenamento antes de ligar o nó. Os VMDKs são mais comumente usados em ambientes VMware e são mais fáceis de gerenciar, enquanto os RDMs podem fornecer melhor desempenho para cargas de trabalho que usam tamanhos de objetos maiores (por exemplo, maiores que 100 MB).

11. Se você precisar remapear as portas usadas por este nó, siga estas etapas.

Pode ser necessário remapear uma porta se suas políticas de rede corporativa restringirem o acesso a uma ou mais portas usadas pelo StorageGRID. Veja o "[diretrizes de rede](#)" para as portas usadas pelo StorageGRID.



Não remapeie as portas usadas nos pontos de extremidade do balanceador de carga.

- Selecione a nova VM.
- Na guia Configurar, selecione **Configurações > Opções do vApp**. A localização de **Opções do vApp** depende da versão do vCenter.
- Na tabela **Propriedades**, localize PORT_REMAP_INBOUND e PORT_REMAP.
- Para mapear simetricamente as comunicações de entrada e saída de uma porta, selecione **PORT_REMAP**.



Se somente PORT_REMAP estiver definido, o mapeamento especificado se aplicará às comunicações de entrada e saída. Se PORT_REMAP_INBOUND também for especificado, PORT_REMAP se aplicará somente às comunicações de saída.

- Selecione **Definir valor**.
- Digite o mapeamento da porta:

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

<network type> é grade, administrador ou cliente e <protocol> é tcp ou udp.

Por exemplo, para remapear o tráfego SSH da porta 22 para a porta 3022, digite:

```
client/tcp/22/3022
```

Você pode remapear várias portas usando uma lista separada por vírgulas.

Por exemplo:

```
client/tcp/18082/443, client/tcp/18083/80
```

- Selecione **OK**.

- Para especificar a porta usada para comunicações de entrada no nó, selecione **PORT_REMAP_INBOUND**.



Se você especificar PORT_REMAP_INBOUND e não especificar um valor para PORT_REMAP, as comunicações de saída para a porta permanecerão inalteradas.

- i. Selecione **Definir valor**.
- ii. Digite o mapeamento da porta:

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port  
used by grid node>
```

<network type>`é grade, administrador ou cliente e `<protocol> é tcp ou udp.

Por exemplo, para remapear o tráfego SSH de entrada enviado para a porta 3022 para que seja recebido na porta 22 pelo nó da grade, insira o seguinte:

```
client/tcp/3022/22
```

Você pode remapear várias portas de entrada usando uma lista separada por vírgulas.

Por exemplo:

```
grid/tcp/3022/22, admin/tcp/3022/22
```

- i. Selecione **OK**

12. Se você quiser aumentar a CPU ou a memória do nó em relação às configurações padrão:
 - a. Clique com o botão direito do mouse na máquina virtual e selecione **Editar configurações**.
 - b. Altere o número de CPUs ou a quantidade de memória conforme necessário.

Defina a **Reserva de Memória** para o mesmo tamanho da **Memória** alocada para a máquina virtual.

- c. Selecione **OK**.

13. Ligue a máquina virtual.

Depois que você terminar

Se você implantou este nó como parte de um procedimento de expansão ou recuperação, retorne a essas instruções para concluir o procedimento.

Configurar a grade e concluir a instalação (VMware)

Navegue até o Gerenciador de Grade

Use o Grid Manager para definir todas as informações necessárias para configurar seu sistema StorageGRID .

Antes de começar

O nó de administração principal deve ser implantado e ter concluído a sequência de inicialização inicial.

Passos

1. Abra seu navegador e navegue até:

```
https://primary_admin_node_ip
```

Alternativamente, você pode acessar o Grid Manager na porta 8443:

```
https://primary_admin_node_ip:8443
```

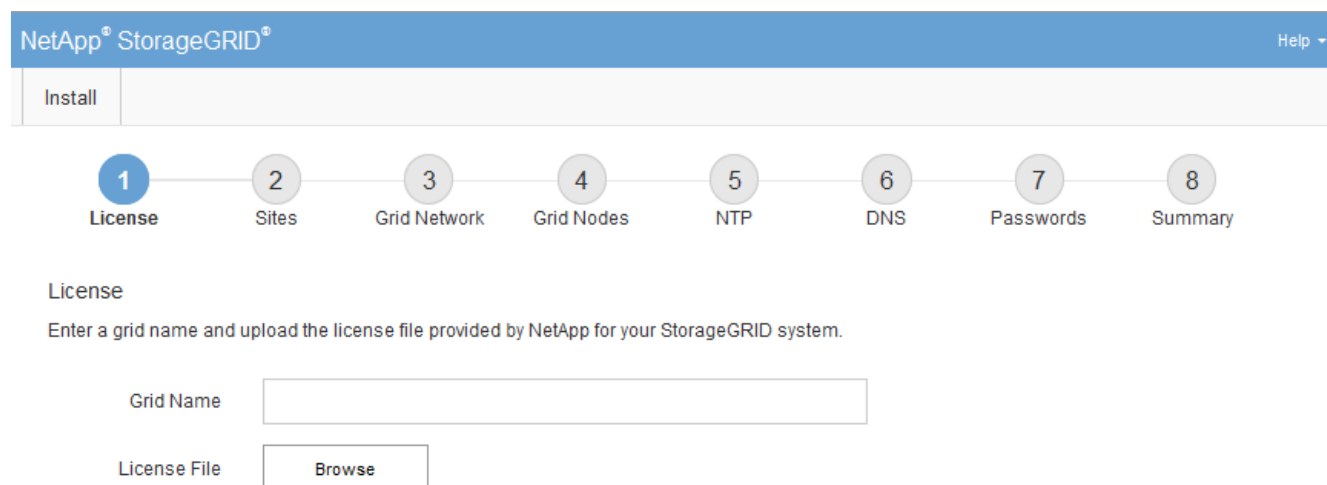

Você pode usar o endereço IP do nó de administração primário na rede Grid ou na rede de administração, conforme apropriado para sua configuração de rede. Talvez seja necessário usar a opção de segurança/avançado no seu navegador para navegar até um certificado não confiável.

2. Gerencie uma senha temporária do instalador conforme necessário:

- Se uma senha já tiver sido definida usando um desses métodos, digite a senha para prosseguir.
 - Um usuário definiu a senha ao acessar o instalador anteriormente
 - A senha SSH/console foi importada automaticamente das propriedades do OVF
- Se uma senha não tiver sido definida, opcionalmente defina uma senha para proteger o instalador do StorageGRID .

3. Selecione *Instalar um sistema StorageGRID* .

A página usada para configurar uma grade StorageGRID é exibida.



Especifique as informações da licença StorageGRID

Você deve especificar o nome do seu sistema StorageGRID e carregar o arquivo de licença fornecido pela NetApp.

Passos

1. Na página Licença, insira um nome significativo para seu sistema StorageGRID no campo **Nome da grade**.

Após a instalação, o nome é exibido no topo do menu Nós.

2. Selecione **Procurar**, localize o arquivo de licença do NetApp(*NLF-unique-id.txt*) e selecione **Abrir**.

O arquivo de licença é validado e o número de série é exibido.



O arquivo de instalação do StorageGRID inclui uma licença gratuita que não fornece nenhum direito de suporte para o produto. Você pode atualizar para uma licença que ofereça suporte após a instalação.

1 License **2** Sites **3** Grid Network **4** Grid Nodes **5** NTP **6** DNS **7** Passwords **8** Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name:

License File: NLF-959007-Internal.txt

License Serial Number:

3. Selecione **Avançar**.

Adicionar sites

Você deve criar pelo menos um site ao instalar o StorageGRID. Você pode criar sites adicionais para aumentar a confiabilidade e a capacidade de armazenamento do seu sistema StorageGRID .

Passos

1. Na página Sites, insira o **Nome do Site**.
2. Para adicionar outros sites, clique no sinal de mais ao lado da última entrada do site e digite o nome na nova caixa de texto **Nome do site**.

Adicione quantos sites adicionais forem necessários para sua topologia de grade. Você pode adicionar até 16 sites.

NetApp® StorageGRID® Help ▾

Install

1 License **2** Sites **3** Grid Network **4** Grid Nodes **5** NTP **6** DNS **7** Passwords **8** Summary

Sites

In a single-site deployment, infrastructure and operations are centralized in one site.

In a multi-site deployment, infrastructure can be distributed asymmetrically across sites, and proportional to the needs of each site. Typically, sites are located in geographically different locations. Having multiple sites also allows the use of distributed replication and erasure coding for increased availability and resiliency.

Site Name 1:

Site Name 2:

3. Clique em **Avançar**.

Especificar sub-redes da rede de grade

Você deve especificar as sub-redes que são usadas na Grid Network.

Sobre esta tarefa

As entradas de sub-rede incluem as sub-redes da Grid Network para cada site no seu sistema StorageGRID , juntamente com quaisquer sub-redes que precisam ser acessadas por meio da Grid Network.

Se você tiver várias sub-redes de grade, o gateway da Rede de Grade será necessário. Todas as sub-redes de grade especificadas devem ser acessíveis por meio deste gateway.

Passos

1. Especifique o endereço de rede CIDR para pelo menos uma rede de grade na caixa de texto **Sub-rede 1**.
2. Clique no sinal de mais ao lado da última entrada para adicionar uma entrada de rede adicional. Você deve especificar todas as sub-redes para todos os sites na Grid Network.
 - Se você já tiver implantado pelo menos um nó, clique em **Descobrir sub-redes de redes de grade** para preencher automaticamente a Lista de sub-redes de redes de grade com as sub-redes relacionadas pelos nós de grade que foram registrados no Gerenciador de grade.
 - Você deve adicionar manualmente quaisquer sub-redes para NTP, DNS, LDAP ou outros servidores externos acessados pelo gateway da Grid Network.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with 'NetApp® StorageGRID®' and a 'Help' dropdown. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network (current step), 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. The 'Grid Network' step is highlighted with a blue circle. Below the progress bar, the 'Grid Network' section is displayed. It contains a text box for 'Subnet 1' with the value '172.16.0.0/21' and a plus sign icon to its right. Below this, there is a button labeled 'Discover Grid Network subnets'.

3. Clique em **Avançar**.

Aprovar nós de grade pendentes

Você deve aprovar cada nó de grade antes que ele possa ingressar no sistema StorageGRID .

Antes de começar

Você implantou todos os nós de grade do dispositivo virtual e StorageGRID .



É mais eficiente executar uma única instalação de todos os nós, em vez de instalar alguns nós agora e outros depois.

Passos

1. Revise a lista de nós pendentes e confirme se ela mostra todos os nós de grade que você implantou.



Se um nó de grade estiver faltando, confirme se ele foi implantado com sucesso e se tem o IP de rede de grade correto do nó de administração primário definido para ADMIN_IP.

2. Selecione o botão de opção ao lado de um nó pendente que você deseja aprovar.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve

✕ Remove

Search

Q

	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21

◀

▶

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit

Reset

✕ Remove

Search

Q

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21

◀

▶

3. Clique em **Aprovar**.
4. Em Configurações gerais, modifique as configurações das seguintes propriedades, conforme necessário:
- **Site:** O nome do sistema do site para este nó de grade.
 - **Nome:** O nome do sistema para o nó. O nome padrão é o nome que você especificou quando configurou o nó.

Os nomes do sistema são necessários para operações internas do StorageGRID e não podem ser alterados após a conclusão da instalação. No entanto, durante esta etapa do processo de instalação, você pode alterar os nomes do sistema conforme necessário.



Para um nó VMware, você pode alterar o nome aqui, mas esta ação não alterará o nome da máquina virtual no vSphere.

- **Função NTP:** A função do Protocolo de Tempo de Rede (NTP) do nó da grade. As opções são **Automático**, **Principal** e **Cliente**. Selecionar **Automático** atribui a função Primária aos Nós de Administração, Nós de Armazenamento com serviços ADC, Nós de Gateway e quaisquer nós de grade que tenham endereços IP não estáticos. Todos os outros nós da grade recebem a função Cliente.



Certifique-se de que pelo menos dois nós em cada site possam acessar pelo menos quatro fontes NTP externas. Se apenas um nó em um site puder alcançar as fontes NTP, ocorrerão problemas de tempo se esse nó ficar inativo. Além disso, designar dois nós por site como fontes primárias de NTP garante um tempo preciso se um site estiver isolado do restante da rede.

- **Tipo de armazenamento** (somente nós de armazenamento): especifique que um novo nó de armazenamento seja usado exclusivamente para dados, metadados ou ambos. As opções são **Dados e metadados** ("combinados"), **Somente dados** e **Somente metadados**.



Ver "[Tipos de nós de armazenamento](#)" para obter informações sobre os requisitos para esses tipos de nós.

- **Serviço ADC** (somente nós de armazenamento): selecione **Automático** para permitir que o sistema determine se o nó requer o serviço Controlador de Domínio Administrativo (ADC). O serviço ADC monitora a localização e a disponibilidade dos serviços de rede. Pelo menos três nós de armazenamento em cada site devem incluir o serviço ADC. Não é possível adicionar o serviço ADC a um nó depois que ele for implantado.

5. Em Grid Network, modifique as configurações das seguintes propriedades conforme necessário:

- **Endereço IPv4 (CIDR):** O endereço de rede CIDR para a interface Grid Network (eth0 dentro do contêiner). Por exemplo: 192.168.1.234/21
- **Gateway:** O gateway da Grid Network. Por exemplo: 192.168.0.1



O gateway é necessário se houver várias sub-redes de grade.



Se você selecionou DHCP para a configuração da Grid Network e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não esteja em um pool de endereços DHCP.

6. Se você quiser configurar a Rede de Administração para o nó da grade, adicione ou atualize as configurações na seção Rede de Administração, conforme necessário.

Insira as sub-redes de destino das rotas fora desta interface na caixa de texto **Sub-redes (CIDR)**. Se houver várias sub-redes de administração, o gateway de administração será necessário.



Se você selecionou DHCP para a configuração da rede de administração e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não esteja em um pool de endereços DHCP.

Dispositivos: Para um dispositivo StorageGRID, se a Rede de administração não foi configurada durante a instalação inicial usando o Instalador do dispositivo StorageGRID, ela não poderá ser configurada nesta

caixa de diálogo Gerenciador de grade. Em vez disso, você deve seguir estes passos:

- a. Reinicie o dispositivo: No Instalador do Dispositivo, selecione **Avançado > Reinicializar**.

A reinicialização pode levar vários minutos.

- b. Selecione **Configurar rede > Configuração de link** e habilite as redes apropriadas.
- c. Selecione **Configurar rede > Configuração de IP** e configure as redes habilitadas.
- d. Retorne à página inicial e clique em **Iniciar instalação**.
- e. No Grid Manager: se o nó estiver listado na tabela Nós aprovados, remova-o.
- f. Remova o nó da tabela Nós Pendentes.
- g. Aguarde até que o nó reapareça na lista de Nós Pendentes.
- h. Confirme se você pode configurar as redes apropriadas. Eles já devem estar preenchidos com as informações que você forneceu na página Configuração de IP do Instalador do Appliance.

Para obter informações adicionais, consulte o "[Início rápido para instalação de hardware](#)" para localizar instruções para seu aparelho.

7. Se você quiser configurar a Rede do Cliente para o nó da grade, adicione ou atualize as configurações na seção Rede do Cliente, conforme necessário. Se a Rede do Cliente estiver configurada, o gateway será necessário e se tornará o gateway padrão para o nó após a instalação.



Se você selecionou DHCP para a configuração da rede do cliente e alterar o valor aqui, o novo valor será configurado como um endereço estático no nó. Você deve certificar-se de que o endereço IP configurado não esteja em um pool de endereços DHCP.

Dispositivos: Para um dispositivo StorageGRID, se a Rede do Cliente não foi configurada durante a instalação inicial usando o Instalador do Dispositivo StorageGRID, ela não poderá ser configurada nesta caixa de diálogo Gerenciador de Grade. Em vez disso, você deve seguir estes passos:

- a. Reinicie o dispositivo: No Instalador do Dispositivo, selecione **Avançado > Reinicializar**.

A reinicialização pode levar vários minutos.

- b. Selecione **Configurar rede > Configuração de link** e habilite as redes apropriadas.
- c. Selecione **Configurar rede > Configuração de IP** e configure as redes habilitadas.
- d. Retorne à página inicial e clique em **Iniciar instalação**.
- e. No Grid Manager: se o nó estiver listado na tabela Nós aprovados, remova-o.
- f. Remova o nó da tabela Nós Pendentes.
- g. Aguarde até que o nó reapareça na lista de Nós Pendentes.
- h. Confirme se você pode configurar as redes apropriadas. Eles já devem estar preenchidos com as informações que você forneceu na página Configuração de IP do Instalador do Appliance.

Para obter informações adicionais, consulte o "[Início rápido para instalação de hardware](#)" para localizar instruções para seu aparelho.

8. Clique em **Salvar**.

A entrada do nó da grade é movida para a lista de nós aprovados.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
☐	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

9. Repita essas etapas para cada nó de grade pendente que você deseja aprovar.

Você deve aprovar todos os nós que deseja na grade. No entanto, você pode retornar a esta página a qualquer momento antes de clicar em **Instalar** na página Resumo. Você pode modificar as propriedades de um nó de grade aprovado selecionando seu botão de opção e clicando em **Editar**.

10. Quando terminar de aprovar os nós da grade, clique em **Avançar**.

Especificar informações do servidor Network Time Protocol

Você deve especificar as informações de configuração do Network Time Protocol (NTP) para o sistema StorageGRID, para que as operações executadas em servidores separados possam ser mantidas sincronizadas.

Sobre esta tarefa

Você deve especificar endereços IPv4 para os servidores NTP.

Você deve especificar servidores NTP externos. Os servidores NTP especificados devem usar o protocolo NTP.

Você deve especificar quatro referências de servidor NTP do Stratum 3 ou superior para evitar problemas com desvio de tempo.



Ao especificar a origem NTP externa para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft para uso em ambientes de alta precisão, como o StorageGRID.

"Limite de suporte para configurar o serviço Windows Time para ambientes de alta precisão"

Os servidores NTP externos são usados pelos nós aos quais você atribuiu anteriormente funções NTP primárias.



Certifique-se de que pelo menos dois nós em cada site possam acessar pelo menos quatro fontes NTP externas. Se apenas um nó em um site puder alcançar as fontes NTP, ocorrerão problemas de tempo se esse nó ficar inativo. Além disso, designar dois nós por site como fontes primárias de NTP garante um tempo preciso se um site estiver isolado do restante da rede.

Execute verificações adicionais para o VMware, como garantir que o hipervisor use a mesma fonte NTP que a máquina virtual e usar o VMTools para desabilitar a sincronização de tempo entre o hipervisor e as máquinas virtuais StorageGRID .

Passos

1. Especifique os endereços IPv4 para pelo menos quatro servidores NTP nas caixas de texto **Servidor 1** a **Servidor 4**.
2. Se necessário, selecione o sinal de mais ao lado da última entrada para adicionar entradas de servidor adicionais.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Network Time Protocol

Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.

Server 1

10.60.248.183

Server 2

10.227.204.142

Server 3

10.235.48.111

Server 4

0.0.0.0

+

3. Selecione **Avançar**.

Especificar informações do servidor DNS

Você deve especificar informações de DNS para seu sistema StorageGRID para poder acessar servidores externos usando nomes de host em vez de endereços IP.

Sobre esta tarefa

Especificando "[Informações do servidor DNS](#)" permite que você use nomes de host de nomes de domínio totalmente qualificados (FQDN) em vez de endereços IP para notificações por e-mail e AutoSupport.

Para garantir a operação correta, especifique dois ou três servidores DNS. Se você especificar mais de três, é possível que apenas três sejam usados devido a limitações conhecidas do sistema operacional em algumas plataformas. Se você tiver restrições de roteamento em seu ambiente, você pode "[personalizar a lista de servidores DNS](#)" para nós individuais (normalmente todos os nós em um site) usar um conjunto diferente de até três servidores DNS.

Se possível, use servidores DNS que cada site possa acessar localmente para garantir que um site isolado possa resolver os FQDNs para destinos externos.

Passos

1. Especifique o endereço IPv4 para pelo menos um servidor DNS na caixa de texto **Servidor 1**.
2. Se necessário, selecione o sinal de mais ao lado da última entrada para adicionar entradas de servidor adicionais.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" link. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (highlighted in blue), 7. Passwords, and 8. Summary. Below the progress bar, the "Domain Name Service" section is visible. It contains a text box for "Server 1" with the value "10.224.223.130" and a red 'x' icon. Below that is a text box for "Server 2" with the value "10.224.223.136" and a red '+' icon. The text below the text boxes reads: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport."

A melhor prática é especificar pelo menos dois servidores DNS. Você pode especificar até seis servidores DNS.

3. Selecione **Avançar**.

Especifique as senhas do sistema StorageGRID

Como parte da instalação do seu sistema StorageGRID, você precisa inserir as senhas que serão usadas para proteger seu sistema e executar tarefas de manutenção.

Sobre esta tarefa

Use a página Instalar senhas para especificar a senha de provisionamento e a senha do usuário root de gerenciamento da grade.

- A senha de provisionamento é usada como uma chave de criptografia e não é armazenada pelo sistema StorageGRID .
- Você deve ter a senha de provisionamento para os procedimentos de instalação, expansão e manutenção, incluindo o download do Pacote de Recuperação. Portanto, é importante que você armazene a senha de provisionamento em um local seguro.
- Você pode alterar a senha de provisionamento no Grid Manager se tiver a atual.
- A senha do usuário root de gerenciamento de grade pode ser alterada usando o Grid Manager.
- As senhas do console de linha de comando e SSH geradas aleatoriamente são armazenadas no `Passwords.txt` arquivo no Pacote de Recuperação.

Passos

1. Em **Provisioning Passphrase**, insira a senha de provisionamento que será necessária para fazer alterações na topologia de grade do seu sistema StorageGRID .

Armazene a senha de provisionamento em um local seguro.



Se, após a conclusão da instalação, você quiser alterar a senha de provisionamento posteriormente, poderá usar o Grid Manager. Selecione **CONFIGURAÇÃO > Controle de acesso > Senhas de grade**.

2. Em **Confirmar senha de provisionamento**, digite novamente a senha de provisionamento para confirmá-la.
3. Em **Senha do usuário raiz do Grid Management**, insira a senha a ser usada para acessar o Grid Manager como usuário "root".

Guarde a senha em um local seguro.

4. Em **Confirmar senha do usuário raiz**, digite novamente a senha do Grid Manager para confirmá-la.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning Passphrase

.....

Confirm Provisioning Passphrase

.....

Grid Management Root User Password

.....

Confirm Root User Password

.....

☒ Create random command line passwords.

- Se você estiver instalando uma grade para fins de prova de conceito ou demonstração, opcionalmente desmarque a caixa de seleção **Criar senhas aleatórias de linha de comando**.

Para implantações de produção, senhas aleatórias devem sempre ser usadas por motivos de segurança. Desmarque **Criar senhas aleatórias de linha de comando** apenas para grades de demonstração se quiser usar senhas padrão para acessar nós de grade a partir da linha de comando usando a conta "root" ou "admin".



Você será solicitado a baixar o arquivo do pacote de recuperação(sgws-recovery-package-id-revision.zip) depois de clicar em **Instalar** na página Resumo. Você deve ["baixar este arquivo"](#) para concluir a instalação. As senhas necessárias para acessar o sistema são armazenadas no Passwords.txt arquivo, contido no arquivo Recovery Package.

- Clique em **Avançar**.

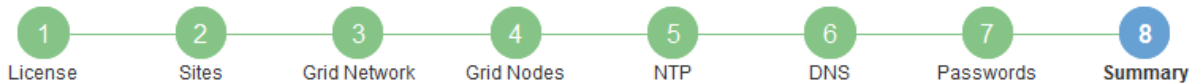
Revise sua configuração e conclua a instalação

Você deve revisar cuidadosamente as informações de configuração inseridas para garantir que a instalação seja concluída com sucesso.

Passos

- Veja a página **Resumo**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1	dc1-g1	dc1-s1
	dc1-s2	dc1-s3	NetApp-SGA

- Verifique se todas as informações de configuração da grade estão corretas. Use os links Modificar na página Resumo para voltar e corrigir quaisquer erros.
- Clique em **Instalar**.



Se um nó estiver configurado para usar a Rede do Cliente, o gateway padrão para esse nó muda da Rede de Grade para a Rede do Cliente quando você clica em **Instalar**. Se você perder a conectividade, certifique-se de estar acessando o nó de administração principal por meio de uma sub-rede acessível. Ver "[Diretrizes de rede](#)" para mais detalhes.

- Clique em **Baixar pacote de recuperação**.

Quando a instalação avança até o ponto em que a topologia da grade é definida, você é solicitado a baixar o arquivo do pacote de recuperação(.zip) e confirme se você consegue acessar com sucesso o conteúdo deste arquivo. Você deve baixar o arquivo do pacote de recuperação para poder recuperar o sistema StorageGRID se um ou mais nós da grade falharem. A instalação continua em segundo plano, mas você não poderá concluir a instalação e acessar o sistema StorageGRID até baixar e verificar este arquivo.

- Verifique se você pode extrair o conteúdo do .zip arquivo e salve-o em 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 .

6. Marque a caixa de seleção **Eu baixei e verifiquei com sucesso o arquivo do pacote de recuperação** e clique em **Avançar**.

Se a instalação ainda estiver em andamento, a página de status será exibida. Esta página indica o progresso da instalação de cada nó da grade.

Installation Status

If necessary, you may [Download the Recovery Package](#) file again.

Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage	IT
dc1-adm1		Site1		172.16.4.215/21			Starting services	
dc1-g1		Site1		172.16.4.216/21			Complete	
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers	
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed	
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed	

Quando o estágio Concluído for atingido para todos os nós da grade, a página de login do Gerenciador de Grade será exibida.

7. Sign in no Grid Manager usando o usuário "root" e a senha que você especificou durante a instalação.

Diretrizes pós-instalação

Após concluir a implantação e a configuração do nó de grade, siga estas diretrizes para endereçamento DHCP e alterações na configuração de rede.

- Se o DHCP foi usado para atribuir endereços IP, configure uma reserva DHCP para cada endereço IP nas redes que estão sendo usadas.

Você só pode configurar o DHCP durante a fase de implantação. Não é possível configurar o DHCP durante a configuração.



Os nós são reinicializados quando a configuração da rede de grade é alterada pelo DHCP, o que pode causar interrupções se uma alteração de DHCP afetar vários nós ao mesmo tempo.

- Você deve usar os procedimentos Alterar IP se quiser alterar endereços IP, máscaras de sub-rede e gateways padrão para um nó de grade. Ver "[Configurar endereços IP](#)".
- Se você fizer alterações na configuração de rede, incluindo alterações de roteamento e gateway, a conectividade do cliente com o nó de administração principal e outros nós da grade poderá ser perdida. Dependendo das alterações de rede aplicadas, pode ser necessário restabelecer essas conexões.

Instalação REST API

O StorageGRID fornece a API de instalação do StorageGRID para executar tarefas de instalação.

A API usa a plataforma de API de código aberto Swagger para fornecer a documentação da API. O Swagger permite que desenvolvedores e não desenvolvedores interajam com a API em uma interface de usuário que ilustra como a API responde a parâmetros e opções. Esta documentação pressupõe que você esteja familiarizado com tecnologias web padrão e o formato de dados JSON.



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.

Cada comando da API REST inclui a URL da API, uma ação HTTP, quaisquer parâmetros de URL obrigatórios ou opcionais e uma resposta de API esperada.

API de instalação do StorageGRID

A API de instalação do StorageGRID só estará disponível quando você estiver configurando inicialmente seu sistema StorageGRID e se precisar executar uma recuperação do nó de administração primário. A API de instalação pode ser acessada via HTTPS a partir do Grid Manager.

Para acessar a documentação da API, vá para a página de instalação no nó de administração principal e selecione **Ajuda > Documentação da API** na barra de menu.

A API de instalação do StorageGRID inclui as seguintes seções:

- **config** — Operações relacionadas ao lançamento do produto e versões da API. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **grid** — Operações de configuração em nível de grade. Você pode obter e atualizar as configurações da grade, incluindo detalhes da grade, sub-redes da rede da grade, senhas da grade e endereços IP dos servidores NTP e DNS.
- **nodes** — Operações de configuração em nível de nó. Você pode recuperar uma lista de nós de grade, excluir um nó de grade, configurar um nó de grade, visualizar um nó de grade e redefinir a configuração de um nó de grade.
- **provisão** — Operações de provisionamento. Você pode iniciar a operação de provisionamento e visualizar o status da operação de provisionamento.
- **recuperação** — Operações de recuperação do nó de administração principal. Você pode redefinir informações, carregar o Pacote de Recuperação, iniciar a recuperação e visualizar o status da operação de recuperação.
- **recovery-package** — Operações para baixar o pacote de recuperação.
- **sites** — Operações de configuração em nível de site. Você pode criar, visualizar, excluir e modificar um site.
- **temporary-password** — Operações na senha temporária para proteger a mgmt-api durante a instalação.

Para onde ir a seguir

Após concluir a instalação, execute as tarefas de integração e configuração necessárias. Você pode executar as tarefas opcionais conforme necessário.

Tarefas necessárias

- Configure o VMware vSphere Hypervisor para reinicialização automática.

Você deve configurar o hipervisor para reiniciar as máquinas virtuais quando o servidor for reiniciado. Sem uma reinicialização automática, as máquinas virtuais e os nós da grade permanecem desligados após a reinicialização do servidor. Para obter detalhes, consulte a documentação do VMware vSphere Hypervisor.

- "[Criar uma conta de inquilino](#)" para o protocolo do cliente S3 que será usado para armazenar objetos no

seu sistema StorageGRID .

- ["Acesso ao sistema de controle"](#) configurando grupos e contas de usuários. Opcionalmente, você pode ["configurar uma fonte de identidade federada"](#) (como Active Directory ou OpenLDAP), para que você possa importar grupos de administração e usuários. Ou você pode ["criar grupos e usuários locais"](#) .
- Integrar e testar o ["S3 API"](#) aplicativos cliente que você usará para carregar objetos no seu sistema StorageGRID .
- ["Configurar as regras de gerenciamento do ciclo de vida das informações \(ILM\) e a política de ILM"](#) que você deseja usar para proteger dados de objetos.
- Se sua instalação incluir nós de armazenamento de dispositivos, use o SANtricity OS para concluir as seguintes tarefas:
 - Conecte-se a cada dispositivo StorageGRID .
 - Verifique o recebimento dos dados do AutoSupport .

Ver ["Configurar hardware"](#) .

- Revise e siga o ["Diretrizes de reforço do sistema StorageGRID"](#) para eliminar riscos de segurança.
- ["Configurar notificações por e-mail para alertas do sistema"](#) .

Tarefas opcionais

- ["Atualizar endereços IP dos nós da grade"](#) se eles mudaram desde que você planejou sua implantação e gerou o Pacote de Recuperação.
- ["Configurar criptografia de armazenamento"](#), se necessário.
- ["Configurar compactação de armazenamento"](#) para reduzir o tamanho dos objetos armazenados, se necessário.
- ["Configurar interfaces VLAN"](#) para isolar e particionar o tráfego de rede, se necessário.
- ["Configurar grupos de alta disponibilidade"](#) para melhorar a disponibilidade de conexão para o Grid Manager, o Tenant Manager e os clientes S3, se necessário.
- ["Configurar pontos de extremidade do balanceador de carga"](#) para conectividade do cliente S3, se necessário.

Solucionar problemas de instalação

Caso ocorra algum problema durante a instalação do seu sistema StorageGRID , você pode acessar os arquivos de log da instalação.

A seguir estão os principais arquivos de log de instalação, que o suporte técnico pode precisar para resolver problemas.

- `/var/local/log/install.log` (encontrado em todos os nós da grade)
- `/var/local/log/gdu-server.log` (encontrado no nó de administração principal)

Informações relacionadas

Para saber como acessar os arquivos de log, consulte ["Referência de arquivos de log"](#) .

Se precisar de ajuda adicional, entre em contato ["Suporte NetApp"](#) .

A reserva de recursos da máquina virtual requer ajuste

Os arquivos OVF incluem uma reserva de recursos projetada para garantir que cada nó da grade tenha RAM e CPU suficientes para operar com eficiência. Se você criar máquinas virtuais implantando esses arquivos OVF no VMware e o número predefinido de recursos não estiver disponível, as máquinas virtuais não serão iniciadas.

Sobre esta tarefa

Se você tiver certeza de que o host da VM tem recursos suficientes para cada nó da grade, ajuste manualmente os recursos alocados para cada máquina virtual e tente iniciar as máquinas virtuais.

Passos

1. Na árvore do cliente do VMware vSphere Hypervisor, selecione a máquina virtual que não foi iniciada.
2. Clique com o botão direito do mouse na máquina virtual e selecione **Editar configurações**.
3. Na janela Propriedades de Máquinas Virtuais, selecione a guia **Recursos**.
4. Ajuste os recursos alocados à máquina virtual:
 - a. Selecione **CPU** e use o controle deslizante Reserva para ajustar os MHz reservados para esta máquina virtual.
 - b. Selecione **Memória** e use o controle deslizante Reserva para ajustar os MB reservados para esta máquina virtual.
5. Clique em **OK**.
6. Repita conforme necessário para outras máquinas virtuais hospedadas no mesmo host de VM.

A senha de instalação temporária foi desabilitada

Ao implantar um nó VMware, você pode, opcionalmente, especificar uma senha de instalação temporária. Você precisa ter essa senha para acessar o console da VM ou usar SSH antes que o novo nó entre na grade.

Se você optou por desabilitar a senha de instalação temporária, será necessário executar etapas adicionais para depurar problemas de instalação.

Você pode fazer qualquer um dos seguintes:

- Reimplante a VM, mas especifique uma senha de instalação temporária para que você possa acessar o console ou usar SSH para depurar problemas de instalação.
- Use o vCenter para definir a senha:
 - a. Desligue a VM.
 - b. Vá para **VM**, selecione a aba **Configurar** e selecione **Opções do vApp**.
 - c. Especifique o tipo de senha de instalação temporária a ser definida:
 - Selecione **CUSTOM_TEMPORARY_PASSWORD** para definir uma senha temporária personalizada.
 - Selecione **TEMPORARY_PASSWORD_TYPE** para usar o nome do nó como senha temporária.
 - d. Selecione **Definir valor**.
 - e. Defina a senha temporária:
 - Altere **CUSTOM_TEMPORARY_PASSWORD** para um valor de senha personalizado.
 - Atualize o **TEMPORARY_PASSWORD_TYPE** com o valor **Usar nome do nó**.

f. Reinicie a VM para aplicar a nova senha.

Atualizar o software StorageGRID

Atualizar o software StorageGRID

Use estas instruções para atualizar um sistema StorageGRID para uma nova versão.

Quando você executa a atualização, todos os nós no seu sistema StorageGRID são atualizados.

Antes de começar

Revise estes tópicos para saber mais sobre os novos recursos e aprimoramentos do StorageGRID 11.9, determinar se algum recurso foi descontinuado ou removido e descobrir mais sobre as alterações nas APIs do StorageGRID .

- ["Novidades no StorageGRID 11.9"](#)
- ["Recursos removidos ou obsoletos"](#)
- ["Alterações na API de gerenciamento de grade"](#)
- ["Alterações na API de gerenciamento de locatários"](#)

Novidades no StorageGRID 11.9

Esta versão do StorageGRID apresenta os seguintes recursos e alterações funcionais.

Escalabilidade

Nós de armazenamento somente de dados

Para permitir um dimensionamento mais granular, agora você pode instalar ["nós de armazenamento somente de dados"](#) . Quando o processamento de metadados não é crítico, você pode otimizar sua infraestrutura de forma econômica. Essa flexibilidade ajuda a acomodar diferentes cargas de trabalho e padrões de crescimento.

Melhorias no Cloud Storage Pool

Funções IAM em qualquer lugar

O StorageGRID agora oferece suporte a credenciais de curto prazo usando ["Funções do IAM em qualquer lugar no Amazon S3 para pools de armazenamento em nuvem"](#) .

Usar credenciais de longo prazo para acessar buckets do S3 representa riscos de segurança se essas credenciais forem comprometidas. Credenciais de curto prazo têm vida útil limitada, o que reduz o risco de acesso não autorizado.

Buckets de bloqueio de objeto S3

Agora você pode ["configurar um pool de armazenamento em nuvem usando um endpoint do Amazon S3"](#) . O S3 Object Lock ajuda a evitar a exclusão acidental ou maliciosa de objetos. Se você hierarquizar dados do StorageGRID para o Amazon S3, ter o bloqueio de objeto habilitado em ambos os sistemas aumentará a proteção de dados durante todo o ciclo de vida dos dados.

Multilocação

Limites de balde

Por "[definindo limites em buckets S3](#)", você pode evitar que os inquilinos monopolizem a capacidade. Além disso, o crescimento descontrolado pode resultar em custos inesperados. Ao definir limites, você pode estimar melhor as despesas de armazenamento dos inquilinos.

5.000 baldes por inquilino

Para aumentar a escalabilidade, o StorageGRID agora oferece suporte a até "[5.000 buckets S3 por locatário](#)". Cada grade pode ter no máximo 100.000 buckets.

Para dar suporte a 5.000 buckets, cada nó de armazenamento na grade deve ter no mínimo 64 GB de RAM.

Melhorias no bloqueio de objetos do S3

Os recursos de configuração por locatário fornecem o equilíbrio adequado entre flexibilidade e segurança de dados. Agora você pode configurar as definições de retenção por locatário para:

- Permitir ou não permitir modo de conformidade
- Defina um período máximo de retenção

Consulte:

- "[Gerenciar objetos com o S3 Object Lock](#)"
- "[Como os administradores de grade controlam a retenção de objetos](#)"
- "[Criar conta de inquilino](#)"

Compatibilidade S3

soma de verificação x-amz-checksum-sha256

- A API REST do S3 agora oferece suporte para `x-amz-checksum-sha256` [soma de verificação](#).
- O StorageGRID agora fornece suporte de soma de verificação SHA-256 para operações PUT, GET e HEAD. Essas somas de verificação melhoram a integridade dos dados.

Alterações no suporte ao protocolo S3

- Adicionado suporte para Mountpoint para Amazon S3, que permite que aplicativos se conectem diretamente aos buckets do S3 como se fossem sistemas de arquivos locais. Agora você pode usar o StorageGRID com mais aplicativos e mais casos de uso.
- Como parte da adição de suporte para Mountpoint, o StorageGRID 11.9 contém "[alterações adicionais no suporte ao protocolo S3](#)".

Manutenção e suporte

AutoSupport

"[AutoSupport](#)" agora cria automaticamente casos de falha de hardware para dispositivos legados.

Operações de clone de nó expandidas

A usabilidade do clone de nó foi expandida para oferecer suporte a nós de armazenamento maiores.

Tratamento aprimorado do ILM de marcadores de exclusão expirados

As regras de tempo de ingestão do ILM com um período de dias agora também removem marcadores de exclusão de objetos expirados. Os marcadores de exclusão só são removidos quando um período de dias tiver passado e o criador de exclusão atual tiver expirado (não há versões não atuais).

Consulte ["Como objetos versionados do S3 são excluídos"](#) e ["Exemplo de ciclo de vida de bucket tendo prioridade sobre política de ILM"](#).

Descomissionamento de nó aprimorado

Para proporcionar uma transição suave e eficiente para o hardware de próxima geração do StorageGRID, ["descomissionamento de nós"](#) foi melhorado.

Syslog para endpoints do balanceador de carga

Os logs de acesso ao ponto de extremidade do balanceador de carga contêm informações de solução de problemas, como códigos de status HTTP. StorageGRID agora suporta ["exportando esses logs para um servidor syslog externo"](#). Esse aprimoramento permite um gerenciamento de logs mais eficiente e integração com sistemas de monitoramento e alerta existentes.

Melhorias adicionais para manutenção e suporte

- Atualização da interface do usuário de métricas
- Novas qualificações do sistema operacional
- Suporte para novos componentes de terceiros

Segurança

Rotação de chaves de acesso SSH

Os administradores da rede agora podem ["atualizar e girar chaves SSH"](#). A capacidade de rotacionar chaves SSH é uma prática recomendada de segurança e um mecanismo de defesa proativo.

Alertas para logins root

Quando uma entidade desconhecida faz login no Grid Manager como root, ["um alerta é disparado"](#). Monitorar logins SSH root é uma medida proativa para proteger sua infraestrutura.

Melhorias no Grid Manager

Página de perfis de codificação de apagamento movida

A página de perfis de codificação de eliminação agora está localizada em **CONFIGURAÇÃO > Sistema > Codificação de eliminação**. Costumava estar no menu do ILM.

Melhorias na pesquisa

O ["campo de pesquisa no Grid Manager"](#) agora inclui melhor lógica de correspondência, permitindo que você encontre páginas pesquisando por abreviações comuns e pelos nomes de determinadas configurações dentro de uma página. Você também pode pesquisar mais tipos de itens, como nós, usuários e contas de locatários.

Recursos e funcionalidades removidos ou obsoletos

Alguns recursos e funcionalidades foram removidos ou descontinuados nesta versão. Revise estes itens para entender se você precisa atualizar os aplicativos cliente ou modificar sua configuração antes de atualizar.

Definições

Obsoleto

O recurso **não deve** ser usado em novos ambientes de produção. Ambientes de produção existentes podem continuar usando o recurso.

Fim da vida

Última versão enviada que suporta o recurso. Em alguns casos, a documentação do recurso pode ser removida nesta fase.

Removido

Primeira versão que **não** suporta o recurso.

Suporte ao fim do recurso StorageGRID

Recursos obsoletos serão removidos nas versões principais N+2. Por exemplo, se um recurso for obsoleto na versão N (por exemplo, 6.3), a última versão em que o recurso existirá será N+1 (por exemplo, 6.4). A versão N+2 (por exemplo, 6.5) é o primeiro lançamento quando o recurso não existe no produto.

Veja o ["Página de suporte da versão do software"](#) para obter informações adicionais.



Em determinadas situações, a NetApp pode encerrar o suporte para recursos específicos antes do indicado.

Recurso	Obsoleto	Fim da vida	Removido	Links para documentação anterior
Alarmes legados (<i>não alertas</i>)	11,7	11,8	11,9	"Referência de alarmes (StorageGRID 11.8)"

Recurso	Obsoleto	Fim da vida	Removido	Links para documentação anterior
Suporte ao nó de arquivo	11,7	11,8	11,9	"Considerações para descomissionamento de nós de arquivo (StorageGRID 11.8)" Observação: Antes de iniciar sua atualização, você deve: 1. Desativar todos os nós de arquivo. Ver "Descomissionamento de nós de grade (site de documentação do StorageGRID 11.8)" . 2. Remova todas as referências do nó de arquivo dos pools de armazenamento e políticas de ILM. Ver "Base de conhecimento da NetApp : Guia de resolução de atualização do software StorageGRID 11.9" .
Exportação de auditoria através de CIFS/Samba	11,1	11,6	11,7	
Serviço CLB	11,4	11,6	11,7	
Motor de contêiner Docker	11,8	11,9	A definir	O suporte ao Docker como mecanismo de contêiner para implantações somente de software está obsoleto. O Docker será substituído por outro mecanismo de contêiner em uma versão futura. Consulte o "lista de versões do Docker atualmente suportadas" .
Exportação de auditoria NFS	11,8	11,9	12,0	"Configurar acesso de cliente de auditoria para NFS (StorageGRID 11.8)"
Suporte à API Swift	11,7	11,9	12,0	"Use a API REST do Swift (StorageGRID 11.8)"
RHEL 8.8	11,9	11,9	12,0	
RHEL 9.0	11,9	11,9	12,0	
RHEL 9.2	11,9	11,9	12,0	
Ubuntu 18,04	11,9	11,9	12,0	

Recurso	Obsoleto	Fim da vida	Removido	Links para documentação anterior
Ubuntu 20,04	11,9	11,9	12,0	
Debian 11	11,9	11,9	12,0	

Consulte também:

- ["Alterações na API de gerenciamento de grade"](#)
- ["Alterações na API de gerenciamento de locatários"](#)

Alterações na API de gerenciamento de grade

O StorageGRID 11.9 usa a versão 4 da API de gerenciamento de grade. A versão 4 substitui a versão 3; no entanto, as versões 1, 2 e 3 ainda são suportadas.



Você pode continuar a usar versões obsoletas da API de gerenciamento com o StorageGRID 11.9; no entanto, o suporte para essas versões da API será removido em uma versão futura do StorageGRID. Após a atualização para o StorageGRID 11.9, você pode desativar as APIs obsoletas usando o PUT `/grid/config/management API`.

Para saber mais, acesse ["Use a API de gerenciamento de grade"](#).

Revise as configurações de conformidade após habilitar o bloqueio global de objetos do S3

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.

Solicitações mgmt-api legadas removidas

Essas solicitações legadas foram removidas:

`/grid/server-types`

`/grid/ntp-roles`

Mudanças em GET `/private/storage-usage API`

- Uma nova propriedade, `usageCacheDuration`, foi adicionado ao corpo da resposta. Esta propriedade especifica a duração (em segundos) pela qual o cache de consulta de uso permanece válido. Este valor se aplica ao verificar o uso em relação à cota de armazenamento do locatário e aos limites de capacidade do bucket.
- O GET `/api/v4/private/storage-usage` o comportamento foi corrigido para corresponder ao aninhamento do esquema.
- Essas alterações se aplicam somente à API privada.

Mudanças em GET `cross-grid-replication` API

A API GET `/org/containers/:name/cross-grid-replication` não requer mais acesso `Root(rootAccess)` permissão; no entanto, você deve pertencer a um grupo de usuários que tenha a permissão `Gerenciar todos os buckets(manageAllContainers)` ou `Ver todos os baldes(viewAllContainers)` permissão.

A API PUT `/org/containers/:name/cross-grid-replication` não foi alterada e ainda requer acesso `Root(rootAccess)` permissão.

Alterações na API de gerenciamento de locatários

O StorageGRID 11.9 usa a versão 4 da API de gerenciamento de locatários. A versão 4 substitui a versão 3; no entanto, as versões 1, 2 e 3 ainda são suportadas.



Você pode continuar a usar versões obsoletas da API de gerenciamento de locatários com o StorageGRID 11.9; no entanto, o suporte para essas versões da API será removido em uma versão futura do StorageGRID. Após a atualização para o StorageGRID 11.9, você pode desativar as APIs obsoletas usando o PUT `/grid/config/management` API.

Para saber mais, acesse "[Entenda a API de gerenciamento de locatários](#)".

Nova API para limite de capacidade de bucket

Você pode usar o `/org/containers/{bucketName}/quota-object-bytes` API com operações GET/PUT para obter e definir o limite de capacidade de armazenamento de um bucket.

Planeje e prepare-se para a atualização

Estimar o tempo para concluir uma atualização

Considere quando atualizar, com base em quanto tempo a atualização pode levar. Esteja ciente de quais operações você pode e não pode executar durante cada estágio da atualização.

Sobre esta tarefa

O tempo necessário para concluir uma atualização do StorageGRID depende de vários fatores, como carga do cliente e desempenho do hardware.

A tabela resume as principais tarefas de atualização e lista o tempo aproximado necessário para cada tarefa. As etapas após a tabela fornecem instruções que você pode usar para estimar o tempo de atualização do seu sistema.

Tarefa de atualização	Descrição	Tempo aproximado necessário	Durante esta tarefa
Execute pré-verificações e atualize o nó de administração primário	As pré-verificações de atualização são executadas e o nó de administração primário é interrompido, atualizado e reiniciado.	De 30 minutos a 1 hora, com os nós do dispositivo de serviços exigindo mais tempo. Erros de pré-verificação não resolvidos aumentarão esse tempo.	Você não consegue acessar o nó de administração principal. Podem ser relatados erros de conexão, os quais você pode ignorar. Executar as pré-verificações de atualização antes de iniciar a atualização permite resolver quaisquer erros antes da janela de manutenção de atualização agendada.
Iniciar serviço de atualização	O arquivo de software é distribuído e o serviço de atualização é iniciado.	3 minutos por nó de grade	
Atualizar outros nós da grade	O software em todos os outros nós da grade é atualizado na ordem em que você aprova os nós. Cada nó do seu sistema será desativado, um de cada vez.	De 15 minutos a 1 hora por nó, com os nós do dispositivo exigindo mais tempo Observação: Para nós de dispositivos, o instalador do dispositivo StorageGRID é atualizado automaticamente para a versão mais recente.	• Não altere a configuração da grade. • Não altere a configuração do nível de auditoria. • Não atualize a configuração do ILM. • Você está impedido de executar outros procedimentos de manutenção, como hotfix, descomissionamento ou expansão. Observação: se precisar realizar uma recuperação, entre em contato com o suporte técnico.
Habilitar recursos	Os novos recursos da nova versão estão habilitados.	Menos de 5 minutos	• Não altere a configuração da grade. • Não altere a configuração do nível de auditoria. • Não atualize a configuração do ILM. • Você não pode executar outro procedimento de manutenção.
Atualizar banco de dados	O processo de atualização verifica cada nó para verificar se o banco de dados Cassandra não precisa ser atualizado.	10 segundos por nó ou alguns minutos para toda a grade	A atualização do StorageGRID 11.8 para o 11.9 não requer uma atualização do banco de dados Cassandra; no entanto, o serviço Cassandra será interrompido e reiniciado em cada nó de armazenamento. Para futuras versões de recursos do StorageGRID, a etapa de atualização do banco de dados Cassandra pode levar vários dias para ser concluída.

Tarefa de atualização	Descrição	Tempo aproximado necessário	Durante esta tarefa
Etapas finais de atualização	Os arquivos temporários são removidos e a atualização para a nova versão é concluída.	5 minutos	Quando a tarefa Etapas finais de atualização for concluída, você poderá executar todos os procedimentos de manutenção.

Passos

1. Estime o tempo necessário para atualizar todos os nós da grade.
 - a. Multiplique o número de nós no seu sistema StorageGRID por 1 hora/nó.

Como regra geral, os nós de dispositivos demoram mais para serem atualizados do que os nós baseados em software.
 - b. Adicione 1 hora a esse tempo para contabilizar o tempo necessário para baixar o `.upgrade` arquivo, execute validações de pré-verificação e conclua as etapas finais de atualização.
2. Se você tiver nós Linux, adicione 15 minutos para cada nó para contabilizar o tempo necessário para baixar e instalar o pacote RPM ou DEB.
3. Calcule o tempo total estimado para a atualização somando os resultados das etapas 1 e 2.

Exemplo: Tempo estimado para atualização para o StorageGRID 11.9

Suponha que seu sistema tenha 14 nós de grade, dos quais 8 são nós Linux.

1. Multiplique 14 por 1 hora/nó.
2. Adicione 1 hora para contabilizar o download, a pré-verificação e as etapas finais.

O tempo estimado para atualizar todos os nós é de 15 horas.

3. Multiplique 8 por 15 minutos/nó para contabilizar o tempo de instalação do pacote RPM ou DEB nos nós Linux.

O tempo estimado para esta etapa é de 2 horas.

4. Some os valores.

Você deve aguardar até 17 horas para concluir a atualização do seu sistema para o StorageGRID 11.9.0.



Conforme necessário, você pode dividir a janela de manutenção em janelas menores, aprovando subconjuntos de nós de grade para atualização em várias sessões. Por exemplo, você pode preferir atualizar os nós no site A em uma sessão e depois atualizar os nós no site B em uma sessão posterior. Se você optar por executar a atualização em mais de uma sessão, esteja ciente de que não poderá começar a usar os novos recursos até que todos os nós tenham sido atualizados.

Como seu sistema é afetado durante a atualização

Saiba como seu sistema StorageGRID será afetado durante a atualização.

As atualizações do StorageGRID não causam interrupções

O sistema StorageGRID pode ingerir e recuperar dados de aplicativos clientes durante todo o processo de atualização. Se você aprovar a atualização de todos os nós do mesmo tipo (por exemplo, nós de armazenamento), os nós serão desativados um de cada vez, de modo que não haverá momento em que todos os nós da grade ou todos os nós da grade de um determinado tipo estarão indisponíveis.

Para permitir disponibilidade contínua, certifique-se de que sua política de ILM contenha regras que especifiquem o armazenamento de várias cópias de cada objeto. Você também deve garantir que todos os clientes S3 externos estejam configurados para enviar solicitações para um dos seguintes:

- Um endereço IP virtual de grupo de alta disponibilidade (HA)
- Um balanceador de carga de terceiros de alta disponibilidade
- Vários nós de gateway para cada cliente
- Vários nós de armazenamento para cada cliente

Os aplicativos do cliente podem sofrer interrupções de curto prazo

O sistema StorageGRID pode ingerir e recuperar dados de aplicativos clientes durante todo o processo de atualização; no entanto, as conexões do cliente com nós de gateway ou nós de armazenamento individuais podem ser interrompidas temporariamente se a atualização precisar reiniciar serviços nesses nós. A conectividade será restaurada após a conclusão do processo de atualização e os serviços serem retomados nos nós individuais.

Pode ser necessário agendar um tempo de inatividade para aplicar uma atualização se a perda de conectividade por um curto período não for aceitável. Você pode usar a aprovação seletiva para agendar quando determinados nós serão atualizados.



Você pode usar vários gateways e grupos de alta disponibilidade (HA) para fornecer failover automático durante o processo de atualização. Veja as instruções para ["configurando grupos de alta disponibilidade"](#).

O firmware do aparelho foi atualizado

Durante a atualização do StorageGRID 11.9:

- Todos os nós do dispositivo StorageGRID são atualizados automaticamente para a versão de firmware 3.9 do StorageGRID Appliance Installer.
- Os dispositivos SG6060 e SGF6024 são atualizados automaticamente para a versão de firmware do BIOS 3B08.EX e a versão de firmware do BMC 4.00.07.
- Os dispositivos SG100 e SG1000 são atualizados automaticamente para a versão de firmware do BIOS 3B13.EC e a versão de firmware do BMC 4.74.07.
- Os dispositivos SGF6112, SG6160, SG110 e SG1100 são atualizados automaticamente para a versão de firmware 3.16.07 do BMC.

As políticas de ILM são tratadas de forma diferente de acordo com seu status

- A política ativa permanecerá a mesma após a atualização.
- Somente as 10 políticas históricas mais recentes são preservadas na atualização.
- Se houver uma política proposta, ela será excluída durante a atualização.

Alertas podem ser acionados

Os alertas podem ser disparados quando os serviços iniciam e param e quando o sistema StorageGRID está operando como um ambiente de versão mista (alguns nós de grade executando uma versão anterior, enquanto outros foram atualizados para uma versão posterior). Outros alertas podem ser acionados após a conclusão da atualização.

Por exemplo, você pode ver o alerta **Não foi possível comunicar com o nó** quando os serviços são interrompidos, ou pode ver o alerta **Erro de comunicação do Cassandra** quando alguns nós foram atualizados para o StorageGRID 11.9, mas outros nós ainda estão executando o StorageGRID 11.8. Em geral, esses alertas serão apagados quando a atualização for concluída.

O alerta **Posicionamento do ILM inatingível** pode ser acionado quando os nós de armazenamento são interrompidos durante a atualização para o StorageGRID 11.9. Este alerta pode persistir por 1 dia após a conclusão da atualização.

Após a conclusão da atualização, você pode revisar quaisquer alertas relacionados à atualização selecionando **Alertas resolvidos recentemente** ou **Alertas atuais** no painel do Grid Manager.

Muitas notificações SNMP são geradas

Esteja ciente de que um grande número de notificações SNMP pode ser gerado quando os nós da grade são interrompidos e reiniciados durante a atualização. Para evitar notificações excessivas, desmarque a caixa de seleção **Habilitar notificações do agente SNMP (CONFIGURAÇÃO > Monitoramento > Agente SNMP)** para desabilitar as notificações SNMP antes de iniciar a atualização. Em seguida, reative as notificações após a conclusão da atualização.

As alterações de configuração são restritas



Esta lista se aplica especificamente a atualizações do StorageGRID 11.8 para o StorageGRID 11.9. Se você estiver atualizando para outra versão do StorageGRID, consulte a lista de alterações restritas nas instruções de atualização dessa versão.

Até que a tarefa **Habilitar novo recurso** seja concluída:

- Não faça nenhuma alteração na configuração da grade.
- Não habilite ou desabilite nenhum recurso novo.
- Não atualize a configuração do ILM. Caso contrário, você poderá experimentar um comportamento inconsistente e inesperado do ILM.
- Não aplique um hotfix nem recupere um nó de grade.



Entre em contato com o suporte técnico se precisar recuperar um nó durante a atualização.

- Você não deve gerenciar grupos de HA, interfaces de VLAN ou pontos de extremidade do balanceador de carga enquanto estiver atualizando para o StorageGRID 11.9.

- Não exclua nenhum grupo de HA até que a atualização para o StorageGRID 11.9 seja concluída. Endereços IP virtuais em outros grupos de HA podem se tornar inacessíveis.

Até que a tarefa **Etapas Finais de Atualização** seja concluída:

- Não realize um procedimento de expansão.
- Não execute um procedimento de descomissionamento.

Não é possível visualizar detalhes do bucket ou gerenciar buckets no Gerenciador de locatários

Durante a atualização para o StorageGRID 11.9 (ou seja, enquanto o sistema estiver operando como um ambiente de versão mista), não será possível visualizar detalhes do bucket ou gerenciar buckets usando o Gerenciador de Tenants. Um dos seguintes erros aparece na página Buckets no Gerenciador de Tenants:

- Você não pode usar esta API enquanto estiver atualizando para a versão 11.9.
- Não é possível visualizar detalhes de versão do bucket no Gerenciador de Tenants enquanto você estiver atualizando para a versão 11.9.

Este erro será resolvido após a conclusão da atualização para a versão 11.9.

Solução alternativa

Enquanto a atualização 11.9 estiver em andamento, use as seguintes ferramentas para visualizar detalhes do bucket ou gerenciar buckets, em vez de usar o Gerenciador de Tenants:

- Para executar operações S3 padrão em um bucket, use o ["API REST S3"](#) ou o ["API de gerenciamento de inquilinos"](#).
- Para executar operações personalizadas do StorageGRID em um bucket (por exemplo, visualizar e modificar a consistência do bucket, habilitar ou desabilitar atualizações de horário do último acesso ou configurar a integração de pesquisa), use a API de gerenciamento de locatários.

Verifique a versão instalada do StorageGRID

Antes de iniciar a atualização, verifique se a versão anterior do StorageGRID está instalada com o hotfix mais recente disponível aplicado.

Sobre esta tarefa

Antes de atualizar para o StorageGRID 11.9, sua grade deve ter o StorageGRID 11.8 instalado. Se você estiver usando uma versão anterior do StorageGRID, deverá instalar todos os arquivos de atualização anteriores junto com seus hotfixes mais recentes (altamente recomendado) até que a versão atual da sua grade seja StorageGRID 11.8.x.y.

Um possível caminho de atualização é mostrado no [exemplo](#).



A NetApp recomenda fortemente que você aplique o hotfix mais recente para cada versão do StorageGRID antes de atualizar para a próxima versão e que você também aplique o hotfix mais recente para cada nova versão instalada. Em alguns casos, você deve aplicar um hotfix para evitar o risco de perda de dados. Ver ["Downloads da NetApp : StorageGRID"](#) e as notas de versão de cada hotfix para saber mais.

Passos

1. Sign in no Grid Manager usando um ["navegador da web compatível"](#).

2. Na parte superior do Grid Manager, selecione **Ajuda > Sobre**.

3. Verifique se **Versão** é 11.8.x.y.

No número da versão StorageGRID 11.8.x.y:

- A **versão principal** tem um valor x de 0 (11.8.0).
- Um **hotfix**, se um foi aplicado, tem um valor y (por exemplo, 11.8.0.1).

4. Se **Versão** não for 11.8.x.y, vá para "[Downloads da NetApp : StorageGRID](#)" para baixar os arquivos de cada versão anterior, incluindo o hotfix mais recente para cada versão.

5. Obtenha as instruções de atualização para cada versão que você baixou. Em seguida, execute o procedimento de atualização de software para essa versão e aplique o hotfix mais recente para essa versão (altamente recomendado).

Veja o "[Procedimento de correção do StorageGRID](#)".

Exemplo: Atualizar para o StorageGRID 11.9 da versão 11.6

O exemplo a seguir mostra as etapas para atualizar do StorageGRID versão 11.6 para a versão 11.8 em preparação para uma atualização do StorageGRID 11.9.

Baixe e instale o software na seguinte sequência para preparar seu sistema para atualização:

1. Atualize para a versão principal do StorageGRID 11.6.0.
2. Aplique o mais recente hotfix StorageGRID 11.6.0.y.
3. Atualize para a versão principal do StorageGRID 11.7.0.
4. Aplique o mais recente hotfix StorageGRID 11.7.0.y.
5. Atualize para a versão principal do StorageGRID 11.8.0.
6. Aplique o mais recente hotfix StorageGRID 11.8.0.y.

Obtenha os materiais necessários para uma atualização de software

Antes de iniciar a atualização do software, obtenha todos os materiais necessários.

Item	Notas
Laptop de serviço	O laptop de serviço deve ter: • Porta de rede • Cliente SSH (por exemplo, PuTTY)
"Navegador da Web compatível"	O suporte ao navegador normalmente muda para cada versão do StorageGRID . Certifique-se de que seu navegador seja compatível com a nova versão do StorageGRID .
Senha de provisionamento	A senha é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está listada no <code>Passwords.txt</code> arquivo.

Item	Notas
Arquivo Linux RPM ou DEB	Se algum nó for implantado em hosts Linux, você deve "baixe e instale o pacote RPM ou DEB em todos os hosts" antes de iniciar a atualização. Certifique-se de que seu sistema operacional atenda aos requisitos mínimos de versão do kernel do StorageGRID: • "Instalar o StorageGRID em hosts Red Hat Enterprise Linux" • "Instalar o StorageGRID em hosts Ubuntu ou Debian"
Documentação do StorageGRID	• "Notas de lançamento" para StorageGRID 11.9 (é necessário fazer login). Leia-as atentamente antes de iniciar a atualização. • "Guia de resolução de atualização de software StorageGRID" para a versão principal para a qual você está atualizando (é necessário fazer login) • Outro "Documentação do StorageGRID", conforme necessário.

Verifique a condição do sistema

Antes de atualizar um sistema StorageGRID, verifique se o sistema está pronto para acomodar a atualização. Certifique-se de que o sistema esteja funcionando normalmente e que todos os nós da rede estejam operacionais.

Passos

1. Sign in no Grid Manager usando um ["navegador da web compatível"](#).
2. Verifique e resolva quaisquer alertas ativos.
3. Confirme se não há tarefas de grade conflitantes ativas ou pendentes.
 - a. Selecione **SUORTE > Ferramentas > Topologia de grade**.
 - b. Selecione **site > Nó de administração primário > CMN > Tarefas de grade > Configuração**.

As tarefas de avaliação do gerenciamento do ciclo de vida da informação (ILME) são as únicas tarefas de grade que podem ser executadas simultaneamente com a atualização do software.

- c. Se houver outras tarefas de grade ativas ou pendentes, aguarde até que elas terminem ou liberem o bloqueio.



Entre em contato com o suporte técnico se uma tarefa não for concluída ou não liberar seu bloqueio.

4. Consulte ["Comunicações internas do nó da rede"](#) e ["Comunicações externas"](#) para garantir que todas as portas necessárias para o StorageGRID 11.9 sejam abertas antes da atualização.



Nenhuma porta adicional é necessária ao atualizar para o StorageGRID 11.9.

A seguinte porta necessária foi adicionada no StorageGRID 11.7. Certifique-se de que ele esteja disponível antes de atualizar para o StorageGRID 11.9.

Porta	Descrição
18086	Porta TCP usada para solicitações S3 do balanceador de carga StorageGRID para LDR e o novo serviço LDR. Antes de atualizar, confirme se esta porta está aberta de todos os nós da grade para todos os nós de armazenamento. O bloqueio desta porta causará interrupções no serviço S3 após a atualização para o StorageGRID 11.9.



Se você tiver aberto alguma porta de firewall personalizada, você será notificado durante a pré-verificação da atualização. Você deve entrar em contato com o suporte técnico antes de prosseguir com a atualização.

Atualizar software

Início rápido de atualização

Antes de iniciar a atualização, revise o fluxo de trabalho geral. A página de atualização do StorageGRID orienta você em cada etapa da atualização.

1

Preparar hosts Linux

Se algum nó StorageGRID for implantado em hosts Linux, ["instale o pacote RPM ou DEB em cada host"](#) antes de iniciar a atualização.

2

Carregar arquivos de atualização e hotfix

No nó de administração principal, acesse a página de atualização do StorageGRID e carregue o arquivo de atualização e o arquivo de hotfix, se necessário.

3

Baixar pacote de recuperação

Baixe o Pacote de Recuperação atual antes de iniciar a atualização.

4

Executar pré-verificações de atualização

As pré-verificações de atualização ajudam a detectar problemas para que você possa resolvê-los antes de iniciar a atualização propriamente dita.

5

Iniciar atualização

Quando você inicia a atualização, as pré-verificações são executadas novamente e o nó de administração principal é atualizado automaticamente. Você não pode acessar o Grid Manager enquanto o nó de administração principal estiver sendo atualizado. Os registros de auditoria também não estarão disponíveis. Esta atualização pode levar até 30 minutos.

6

Baixar pacote de recuperação

Após a atualização do nó de administração principal, baixe um novo pacote de recuperação.

7

Aprovar nós

Você pode aprovar nós de grade individuais, grupos de nós de grade ou todos os nós de grade.



Não aprove a atualização de um nó de grade a menos que tenha certeza de que o nó está pronto para ser interrompido e reinicializado.

8

Retomar as operações

Quando todos os nós da grade forem atualizados, novos recursos serão habilitados e você poderá retomar as operações. Você deve esperar para executar um procedimento de descomissionamento ou expansão até que a tarefa em segundo plano **Atualizar banco de dados** e a tarefa **Etapas finais de atualização** sejam concluídas.

Informações relacionadas

["Estimar o tempo para concluir uma atualização"](#)

Linux: Baixe e instale o pacote RPM ou DEB em todos os hosts

Se algum nó StorageGRID estiver implantado em hosts Linux, baixe e instale um pacote RPM ou DEB adicional em cada um desses hosts antes de iniciar a atualização.

Baixar arquivos de atualização, Linux e hotfix

Ao executar uma atualização do StorageGRID no Grid Manager, você será solicitado a baixar o arquivo de atualização e qualquer hotfix necessário como primeira etapa. No entanto, se você precisar baixar arquivos para atualizar hosts Linux, poderá economizar tempo baixando todos os arquivos necessários com antecedência.

Passos

1. Vá para ["Downloads da NetApp : StorageGRID"](#) .
2. Selecione o botão para baixar a versão mais recente ou selecione outra versão no menu suspenso e selecione **Ir**.

As versões do software StorageGRID têm este formato: 11.x.y. Os hotfixes do StorageGRID têm este formato: 11.x.y.z.

3. Sign in com o nome de usuário e a senha da sua conta NetApp .
4. Se um aviso de Cuidado/Leitura Obrigatória aparecer, anote o número do hotfix e marque a caixa de seleção.
5. Leia o Contrato de Licença do Usuário Final (CLUF), marque a caixa de seleção e selecione **Aceitar e Continuar**.

A página de downloads da versão selecionada será exibida. A página contém três colunas.

6. Na segunda coluna (**Upgrade StorageGRID**), baixe dois arquivos:

- O arquivo de atualização para a versão mais recente (este é o arquivo na seção denominada **VMware, SG1000 ou SG100 Primary Admin Node**). Embora esse arquivo não seja necessário até que você execute a atualização, baixá-lo agora economizará tempo.
- Um arquivo RPM ou DEB em qualquer um .tgz ou .zip formatar. Selecione o .zip arquivo se você estiver executando o Windows no laptop de serviço.

- Red Hat Enterprise Linux

`StorageGRID-Webscale-version-RPM-uniqueID.zip`

`StorageGRID-Webscale-version-RPM-uniqueID.tgz`

- Ubuntu ou Debian

`StorageGRID-Webscale-version-DEB-uniqueID.zip`

`StorageGRID-Webscale-version-DEB-uniqueID.tgz`

7. Se você precisou concordar com um aviso de Cuidado/Leitura Obrigatória devido a um hotfix necessário, baixe o hotfix:

- a. Voltar para ["Downloads da NetApp : StorageGRID"](#) .
- b. Selecione o número do hotfix no menu suspenso.
- c. Concorde novamente com o aviso de Cuidado e o CLUF.
- d. Baixe e salve o hotfix e seu README.

Você será solicitado a carregar o arquivo de hotfix na página de atualização do StorageGRID quando iniciar a atualização.

Instalar arquivo em todos os hosts Linux

Execute estas etapas antes de atualizar o software StorageGRID .

Passos

1. Extraia os pacotes RPM ou DEB do arquivo de instalação.
2. Instale os pacotes RPM ou DEB em todos os hosts Linux.

Veja as etapas para instalar os serviços do host StorageGRID nas instruções de instalação:

- ["Red Hat Enterprise Linux: Instalar serviços de host StorageGRID"](#)
- ["Ubuntu ou Debian: instalar serviços de host StorageGRID"](#)

Os novos pacotes são instalados como pacotes adicionais.

Remover arquivos de instalação de versões anteriores

Para liberar espaço em hosts Linux, você pode remover os arquivos de instalação de versões anteriores do StorageGRID que não são mais necessárias.

Passos

1. Remova os arquivos de instalação antigos do StorageGRID .

Chapéu Vermelho

1. Capture a lista de pacotes StorageGRID instalados: `dnf list | grep -i storagegrid`.

Exemplo:

```
[root@rhel-example ~]# dnf list | grep -i storagegrid
StorageGRID-Webscale-Images-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Images-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Images-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Images-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
StorageGRID-Webscale-Service-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Service-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Service-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Service-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
[root@rhel-example ~]#
```

2. Remover pacotes StorageGRID anteriores: `dnf remove images-package service-package`



Não remova os arquivos de instalação da versão do StorageGRID que você está executando no momento ou das versões do StorageGRID para as quais você planeja atualizar.

Você pode ignorar com segurança os avisos que aparecem. Eles se referem a arquivos que foram substituídos quando você instala pacotes StorageGRID mais recentes.

Exemplo:

```
[root@rhel-example ~]# dnf remove StorageGRID-Webscale-Images-11-6-
0.x86_64 StorageGRID-Webscale-Service-11-6-0.x86_64
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can
use subscription-manager to register.

Dependencies resolved.
=====
```

```

=====
Package                Architecture      Version      Repository
Size
=====
=====
Removing:
StorageGRID-Webscale-Images-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 2.7 G
StorageGRID-Webscale-Service-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 7.5 M

Transaction Summary
=====
=====
Remove 2 Packages

Freed space: 2.8 G
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing: 1/1
  Running scriptlet: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 1/2
  Erasing: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 1/2
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv6.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv4.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui64.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui48.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/__init__.
pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/sets.pyc:
remove failed: No such file or directory

```

```
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/ip/rfc1924.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/ip/nmap.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/ip/iana.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/ip/glob.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/ip/__init__.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/fbsocket.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/eui/ieee.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/eui/__init__.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/core.pyc: remove  
failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/subnet_spl  
itter.pyc: remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/__init__.p  
yc: remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/compat.pyc: remove  
failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/__init__.pyc:  
remove failed: No such file or directory
```

```
Erasing: StorageGRID-Webscale-Images-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64 2/2
```

```
Verifying: StorageGRID-Webscale-Images-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64 1/2
```

```
Verifying: StorageGRID-Webscale-Service-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64 2/2
```

```
Installed products updated.
```

```
Removed:
```

```
StorageGRID-Webscale-Images-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64  
StorageGRID-Webscale-Service-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64
```

```
Complete!
```

```
[root@rhel-example ~]#
```

Ubuntu e Debian

1. Capture a lista de pacotes StorageGRID instalados: `dpkg -l | grep storagegrid`

Exemplo:

```
root@debian-example:~# dpkg -l | grep storagegrid  
ii storagegrid-webscale-images-11-6-0 11.6.0-20220210.0232.8d56cfe  
amd64 StorageGRID Webscale docker images for 11.6.0  
ii storagegrid-webscale-images-11-7-0 11.7.0-  
20230424.2238.1a2cf8c.dev-signed amd64 StorageGRID Webscale docker  
images for 11.7.0  
ii storagegrid-webscale-images-11-8-0 11.8.0-20240131.0139.e3e0c87  
amd64 StorageGRID Webscale docker images for 11.8.0  
ii storagegrid-webscale-images-11-9-0 11.9.0-20240826.1753.4aeeb70  
amd64 StorageGRID Webscale docker images for 11.9.0  
ii storagegrid-webscale-service-11-6-0 11.6.0-20220210.0232.8d56cfe  
amd64 StorageGRID Webscale host services for 11.6.0  
ii storagegrid-webscale-service-11-7-0 11.7.0-20230424.2238.1a2cf8c  
amd64 StorageGRID Webscale host services for 11.7.0  
ii storagegrid-webscale-service-11-8-0 11.8.0-20240131.0139.e3e0c87  
amd64 StorageGRID Webscale host services for 11.8.0  
ii storagegrid-webscale-service-11-9-0 11.9.0-20240826.1753.4aeeb70  
amd64 StorageGRID Webscale host services for 11.9.0  
root@debian-example:~#
```

2. Remover pacotes StorageGRID anteriores: `dpkg -r images-package service-package`



Não remova os arquivos de instalação da versão do StorageGRID que você está executando no momento ou das versões do StorageGRID para as quais você planeja atualizar.

Exemplo:

```
root@debian-example:~# dpkg -r storagegrid-webscale-service-11-6-0
storagegrid-webscale-images-11-6-0
(Reading database ... 38190 files and directories currently
installed.)
Removing storagegrid-webscale-service-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
locale: Cannot set LC_CTYPE to default locale: No such file or
directory
locale: Cannot set LC_MESSAGES to default locale: No such file or
directory
locale: Cannot set LC_ALL to default locale: No such file or
directory
dpkg: warning: while removing storagegrid-webscale-service-11-6-0,
directory '/usr/lib/python2.7/dist-
packages/netapp/storagegrid/vendor/latest' not empty so not removed
Removing storagegrid-webscale-images-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
root@debian-example:~#
```

1. Remover imagens de contêiner StorageGRID .

Docker

1. Capture a lista de imagens de contêiner instaladas: `docker images`

Exemplo:

```
[root@docker-example ~]# docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED
storagegrid-11.9.0	Admin_Node	610f2595bcb4	2 days ago
2.77GB			
storagegrid-11.9.0	Storage_Node	7f73d33eb880	2 days ago
2.65GB			
storagegrid-11.9.0	API_Gateway	2f0bb79526e9	2 days ago
1.82GB			
storagegrid-11.8.0	Storage_Node	7125480de71b	7 months ago
2.54GB			
storagegrid-11.8.0	Admin_Node	404e9f1bd173	7 months ago
2.63GB			
storagegrid-11.8.0	Archive_Node	c3294a29697c	7 months ago
2.39GB			
storagegrid-11.8.0	API_Gateway	1f88f24b9098	7 months ago
1.74GB			
storagegrid-11.7.0	Storage_Node	1655350eff6f	16 months ago
2.51GB			
storagegrid-11.7.0	Admin_Node	872258dd0dc8	16 months ago
2.48GB			
storagegrid-11.7.0	Archive_Node	121e7c8b6d3b	16 months ago
2.41GB			
storagegrid-11.7.0	API_Gateway	5b7a26e382de	16 months ago
1.77GB			
storagegrid-11.6.0	Admin_Node	ee39f71a73e1	2 years ago
2.38GB			
storagegrid-11.6.0	Storage_Node	f5ef895dcad0	2 years ago
2.08GB			
storagegrid-11.6.0	Archive_Node	5782de552db0	2 years ago
1.95GB			
storagegrid-11.6.0	API_Gateway	cb480ed37eea	2 years ago
1.35GB			

```
[root@docker-example ~]#
```

2. Remova as imagens de contêiner das versões anteriores do StorageGRID : `docker rmi image id`



Não remova as imagens de contêiner da versão do StorageGRID que você está executando no momento ou das versões do StorageGRID para as quais você planeja atualizar.

Exemplo:

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051ddf02
Deleted:
sha256:5f269aabf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8cccafa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66bde
[root@docker-example ~]#
```

Podman

1. Capture a lista de imagens de contêiner instaladas: `podman images`

Exemplo:


```
[root@podman-example ~]# podman images
```

REPOSITORY SIZE	TAG	IMAGE ID	CREATED
localhost/storagegrid-11.8.0 ago 2.57 GB	Storage_Node	7125480de71b	7 months
localhost/storagegrid-11.8.0 ago 2.67 GB	Admin_Node	404e9f1bd173	7 months
localhost/storagegrid-11.8.0 ago 2.42 GB	Archive_Node	c3294a29697c	7 months
localhost/storagegrid-11.8.0 ago 1.77 GB	API_Gateway	1f88f24b9098	7 months
localhost/storagegrid-11.7.0 ago 2.54 GB	Storage_Node	1655350eff6f	16 months
localhost/storagegrid-11.7.0 ago 2.51 GB	Admin_Node	872258dd0dc8	16 months
localhost/storagegrid-11.7.0 ago 2.44 GB	Archive_Node	121e7c8b6d3b	16 months
localhost/storagegrid-11.7.0 ago 1.8 GB	API_Gateway	5b7a26e382de	16 months
localhost/storagegrid-11.6.0 ago 2.42 GB	Admin_Node	ee39f71a73e1	2 years
localhost/storagegrid-11.6.0 ago 2.11 GB	Storage_Node	f5ef895dcad0	2 years
localhost/storagegrid-11.6.0 ago 1.98 GB	Archive_Node	5782de552db0	2 years
localhost/storagegrid-11.6.0 ago 1.38 GB	API_Gateway	cb480ed37eea	2 years

```
[root@podman-example ~]#
```

2. Remova as imagens de contêiner das versões anteriores do StorageGRID : `podman rmi image id`



Não remova as imagens de contêiner da versão do StorageGRID que você está executando no momento ou das versões do StorageGRID para as quais você planeja atualizar.

Exemplo:

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

Executar a atualização

Você pode atualizar para o StorageGRID 11.9 e aplicar o hotfix mais recente para essa versão ao mesmo tempo. A página de atualização do StorageGRID fornece o caminho de atualização recomendado e links diretamente para as páginas de download corretas.

Antes de começar

Você revisou todas as considerações e concluiu todas as etapas de planejamento e preparação.

Acesse a página de atualização do StorageGRID

Como primeiro passo, acesse a página de atualização do StorageGRID no Grid Manager.

Passos

1. Sign in no Grid Manager usando um ["navegador da web compatível"](#).
2. Selecione **MANUTENÇÃO > Sistema > Atualização de software**.
3. No bloco de atualização do StorageGRID, selecione **Atualizar**.

Selecionar arquivos

O caminho de atualização na página de atualização do StorageGRID indica quais versões principais (por exemplo, 11.9.0) e hotfixes (por exemplo, 11.9.0.1) você deve instalar para obter a versão mais recente do StorageGRID. Você deve instalar as versões e os hotfixes recomendados na ordem mostrada.



Se nenhum caminho de atualização for mostrado, seu navegador pode não conseguir acessar o site de suporte da NetApp, ou a caixa de seleção **Verificar atualizações de software** na página AutoSupport (**SUPPORT > Tools > * AutoSupport* > Settings**) pode estar desabilitada.

Passos

1. Para a etapa **Selecionar arquivos**, revise o caminho de atualização.
2. Na seção Baixar arquivos, selecione cada link **Download** para baixar os arquivos necessários do site de suporte da NetApp.

Se nenhum caminho de atualização for mostrado, vá para ["Downloads da NetApp : StorageGRID"](#) para determinar se uma nova versão ou hotfix está disponível e para baixar os arquivos necessários.



Se você precisar baixar e instalar um pacote RPM ou DEB em todos os hosts Linux, talvez já tenha os arquivos de atualização e hotfix do StorageGRID listados no caminho de atualização.

3. Selecione **Navegar** para carregar o arquivo de atualização de versão para o StorageGRID:
`NetApp_StorageGRID_11.9.0_Software_uniqueID.upgrade`

Quando o processo de upload e validação estiver concluído, uma marca de seleção verde aparecerá ao lado do nome do arquivo.

4. Se você baixou um arquivo de hotfix, selecione **Procurar** para enviar esse arquivo. O hotfix será aplicado automaticamente como parte da atualização da versão.
5. Selecione **Continuar**.

Executar pré-verificações

Executar pré-verificações permite que você detecte e resolva quaisquer problemas de atualização antes de começar a atualizar sua rede.

Passos

1. Para a etapa **Executar pré-verificações**, comece inserindo a senha de provisionamento da sua grade.
2. Selecione **Baixar pacote de recuperação**.

Você deve baixar a cópia atual do arquivo do Pacote de Recuperação antes de atualizar o Nó de Administração principal. O arquivo Recovery Package permite restaurar o sistema caso ocorra uma falha.

3. Quando o arquivo for baixado, confirme se você pode acessar o conteúdo, incluindo o `Passwords.txt` arquivo.
4. Copie o arquivo baixado(`.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 .

5. Selecione **Executar pré-verificações** e aguarde a conclusão das pré-verificações.
6. Revise os detalhes de cada pré-verificação relatada e resolva quaisquer erros relatados. Veja o "[Guia de resolução de atualização de software StorageGRID](#)" para a versão StorageGRID 11.9.

Você deve resolver todos os *erros* de pré-verificação antes de poder atualizar seu sistema. No entanto, você não precisa abordar os *avisos* de pré-verificação antes de atualizar.



Se você tiver aberto alguma porta de firewall personalizada, você será notificado durante a validação da pré-verificação. Você deve entrar em contato com o suporte técnico antes de prosseguir com a atualização.

7. Se você fez alguma alteração de configuração para resolver os problemas relatados, selecione **Executar pré-verificações** novamente para obter resultados atualizados.

Se todos os erros tiverem sido resolvidos, você será solicitado a iniciar a atualização.

Iniciar atualização e atualizar o nó de administração principal

Quando você inicia a atualização, as pré-verificações de atualização são executadas novamente e o nó de administração principal é atualizado automaticamente. Esta parte da atualização pode levar até 30 minutos.



Você não poderá acessar nenhuma outra página do Grid Manager enquanto o nó de administração principal estiver sendo atualizado. Os registros de auditoria também não estarão disponíveis.

Passos

1. Selecione **Iniciar atualização**.

Um aviso aparecerá para lembrá-lo de que você perderá temporariamente o acesso ao Grid Manager.

2. Selecione **OK** para confirmar o aviso e iniciar a atualização.
3. Aguarde até que as pré-verificações de atualização sejam realizadas e o nó de administração principal

seja atualizado.



Se algum erro de pré-verificação for relatado, resolva-o e selecione **Iniciar atualização** novamente.

Se a grade tiver outro nó de administração on-line e pronto, você poderá usá-lo para monitorar o status do nó de administração principal. Assim que o nó de administração principal for atualizado, você poderá aprovar os outros nós da grade.

4. Conforme necessário, selecione **Continuar** para acessar a etapa **Atualizar outros nós**.

Atualizar outros nós

Você deve atualizar todos os nós da grade, mas pode executar várias sessões de atualização e personalizar a sequência de atualização. Por exemplo, você pode preferir atualizar os nós no site A em uma sessão e depois atualizar os nós no site B em uma sessão posterior. Se você optar por executar a atualização em mais de uma sessão, esteja ciente de que não poderá começar a usar os novos recursos até que todos os nós tenham sido atualizados.

Se a ordem em que os nós são atualizados for importante, aprove os nós ou grupos de nós um de cada vez e aguarde até que a atualização seja concluída em cada nó antes de aprovar o próximo nó ou grupo de nós.



Quando a atualização começa em um nó da grade, os serviços nesse nó são interrompidos. Mais tarde, o nó da grade é reinicializado. Para evitar interrupções de serviço para aplicativos clientes que estão se comunicando com o nó, não aprove a atualização para um nó a menos que tenha certeza de que o nó está pronto para ser interrompido e reinicializado. Conforme necessário, agende uma janela de manutenção ou notifique os clientes.

Passos

1. Para a etapa **Atualizar outros nós**, revise o Resumo, que fornece a hora de início da atualização como um todo e o status de cada tarefa de atualização principal.
 - **Iniciar serviço de atualização** é a primeira tarefa de atualização. Durante esta tarefa, o arquivo de software é distribuído aos nós da grade e o serviço de atualização é iniciado em cada nó.
 - Quando a tarefa **Iniciar serviço de atualização** estiver concluída, a tarefa **Atualizar outros nós de grade** será iniciada e você será solicitado a baixar uma nova cópia do Pacote de Recuperação.
2. Quando solicitado, digite sua senha de provisionamento e baixe uma nova cópia do Pacote de Recuperação.



Você deve baixar uma nova cópia do arquivo do pacote de recuperação após a atualização do nó de administração principal. O arquivo Recovery Package permite restaurar o sistema caso ocorra uma falha.

3. Revise as tabelas de status para cada tipo de nó. Há tabelas para nós de administração não primários, nós de gateway e nós de armazenamento.

Um nó de grade pode estar em um destes estágios quando as tabelas aparecem pela primeira vez:

- Descompactando a atualização
- Baixando
- Aguardando aprovação

4. Quando estiver pronto para selecionar nós de grade para atualização (ou se precisar desaprovar nós selecionados), use estas instruções:

Tarefa	Instrução
Pesquisar nós específicos para aprovar, como todos os nós em um site específico	Digite a sequência de pesquisa no campo Pesquisar
Selecione todos os nós para atualização	Selecione Aprovar todos os nós
Selecione todos os nós do mesmo tipo para atualização (por exemplo, todos os nós de armazenamento)	Selecione o botão Aprovar tudo para o tipo de nó Se você aprovar mais de um nó do mesmo tipo, os nós serão atualizados um de cada vez.
Selecione um nó individual para atualização	Selecione o botão Aprovar para o nó
Adiar a atualização em todos os nós selecionados	Selecione Desaprovar todos os nós
Adiar a atualização em todos os nós selecionados do mesmo tipo	Selecione o botão Desaprovar tudo para o tipo de nó
Adiar a atualização em um nó individual	Selecione o botão Desaprovar para o nó

5. Aguarde até que os nós aprovados passem por estas etapas de atualização:

- Aprovado e aguardando atualização
- Parando serviços



Não é possível remover um nó quando seu estágio atinge **Parando serviços**. O botão **Desaprovar** está desabilitado.

- Parando o recipiente
- Limpando imagens do Docker
- Atualizando pacotes básicos do sistema operacional



Quando um nó do dispositivo atinge esse estágio, o software StorageGRID Appliance Installer no dispositivo é atualizado. Este processo automatizado garante que a versão do StorageGRID Appliance Installer permaneça sincronizada com a versão do software StorageGRID .

- Reiniciando



Alguns modelos de aparelhos podem ser reiniciados várias vezes para atualizar o firmware e o BIOS.

- Executando etapas após a reinicialização
- Iniciando serviços

- Feito

6. Repita o [etapa de aprovação](#) quantas vezes forem necessárias até que todos os nós da grade tenham sido atualizados.

Atualização completa

Quando todos os nós da grade tiverem concluído os estágios de atualização, a tarefa **Atualizar outros nós da grade** será mostrada como Concluída. As tarefas de atualização restantes são executadas automaticamente em segundo plano.

Passos

1. Assim que a tarefa **Habilitar recursos** for concluída (o que ocorre rapidamente), você pode começar a usar o ["novos recursos"](#) na versão atualizada do StorageGRID .
2. Durante a tarefa **Atualizar banco de dados**, o processo de atualização verifica cada nó para verificar se o banco de dados Cassandra não precisa ser atualizado.



A atualização do StorageGRID 11.8 para o 11.9 não requer uma atualização do banco de dados Cassandra; no entanto, o serviço Cassandra será interrompido e reiniciado em cada nó de armazenamento. Para futuras versões de recursos do StorageGRID , a etapa de atualização do banco de dados Cassandra pode levar vários dias para ser concluída.

3. Quando a tarefa **Atualizar banco de dados** for concluída, aguarde alguns minutos para que as **Etapas finais de atualização** sejam concluídas.
4. Quando as **Etapas finais de atualização** forem concluídas, a atualização estará concluída. O primeiro passo, **Selecionar arquivos**, é exibido novamente com um banner verde de sucesso.
5. Verifique se as operações da rede retornaram ao normal:
 - a. Verifique se os serviços estão operando normalmente e se não há alertas inesperados.
 - b. Confirme se as conexões do cliente com o sistema StorageGRID estão operando conforme o esperado.

Solucionar problemas de atualização

Se algo der errado ao realizar uma atualização, você poderá resolver o problema sozinho. Se você não conseguir resolver um problema, reúna o máximo de informações possível e entre em contato com o suporte técnico.

A atualização não foi concluída

As seções a seguir descrevem como se recuperar de situações em que a atualização falhou parcialmente.

Erros de pré-verificação de atualização

Para detectar e resolver problemas, você pode executar manualmente as pré-verificações de atualização antes de iniciar a atualização real. A maioria dos erros de pré-verificação fornece informações sobre como resolver o problema.

Falhas de provisionamento

Se o processo de provisionamento automático falhar, entre em contato com o suporte técnico.

O nó da grade trava ou não inicia

Se um nó da grade travar durante o processo de atualização ou não iniciar com sucesso após a conclusão da atualização, entre em contato com o suporte técnico para investigar e corrigir quaisquer problemas subjacentes.

A ingestão ou recuperação de dados é interrompida

Se a ingestão ou recuperação de dados for interrompida inesperadamente quando você não estiver atualizando um nó de grade, entre em contato com o suporte técnico.

Erros de atualização do banco de dados

Se a atualização do banco de dados falhar com um erro, tente atualizar novamente. Se falhar novamente, entre em contato com o suporte técnico.

Informações relacionadas

["Verificando a condição do sistema antes de atualizar o software"](#)

Problemas de interface do usuário

Você pode ter problemas com o Grid Manager ou o Tenant Manager durante ou após a atualização.

O Grid Manager exibe várias mensagens de erro durante a atualização

Se você atualizar seu navegador ou navegar para outra página do Grid Manager enquanto o nó de administração principal estiver sendo atualizado, poderá ver várias mensagens "503: Serviço indisponível" e "Problema ao conectar ao servidor". Você pode ignorar essas mensagens com segurança — elas deixarão de aparecer assim que o nó for atualizado.

Se essas mensagens aparecerem por mais de uma hora após o início da atualização, algo pode ter ocorrido que impediu a atualização do nó de administração principal. Se você não conseguir resolver o problema sozinho, entre em contato com o suporte técnico.

A interface da Web não responde conforme o esperado

O Grid Manager ou o Tenant Manager podem não responder conforme o esperado após a atualização do software StorageGRID .

Se você tiver problemas com a interface da web:

- Certifique-se de que você está usando um ["navegador da web compatível"](#) .



O suporte ao navegador normalmente muda para cada versão do StorageGRID .

- Limpe o cache do seu navegador.

Limpar o cache remove recursos desatualizados usados pela versão anterior do software StorageGRID e permite que a interface do usuário opere corretamente novamente. Para obter instruções, consulte a documentação do seu navegador.

Mensagens de erro "Verificação de disponibilidade de imagem do Docker"

Ao tentar iniciar o processo de atualização, você pode receber uma mensagem de erro que diz "Os seguintes

problemas foram identificados pelo conjunto de validação de verificação de disponibilidade de imagem do Docker". Todos os problemas devem ser resolvidos antes que você possa concluir a atualização.

Entre em contato com o suporte técnico se não tiver certeza das alterações necessárias para resolver os problemas identificados.

Mensagem	Causa	Solução
Não foi possível determinar a versão de atualização. Arquivo de informações da versão de atualização {file_path} não correspondeu ao formato esperado.	O pacote de atualização está corrompido.	Faça upload novamente do pacote de atualização e tente novamente. Se o problema persistir, entre em contato com o suporte técnico.
Arquivo de informações da versão de atualização {file_path} não foi encontrado. Não foi possível determinar a versão de atualização.	O pacote de atualização está corrompido.	Faça upload novamente do pacote de atualização e tente novamente. Se o problema persistir, entre em contato com o suporte técnico.
Não é possível determinar a versão de lançamento atualmente instalada em {node_name} .	Um arquivo crítico no nó está corrompido.	Entre em contato com o suporte técnico.
Erro de conexão ao tentar listar versões em {node_name}	O nó está offline ou a conexão foi interrompida.	Verifique se todos os nós estão online e acessíveis a partir do nó de administração principal e tente novamente.
O host para o nó {node_name} não tem StorageGRID {upgrade_version} imagem carregada. Imagens e serviços devem ser instalados no host antes que a atualização possa prosseguir.	Os pacotes RPM ou DEB para a atualização não foram instalados no host onde o nó está sendo executado ou as imagens ainda estão em processo de importação. Observação: Este erro se aplica somente a nós que estão sendo executados como contêineres no Linux.	Verifique se os pacotes RPM ou DEB foram instalados em todos os hosts Linux onde os nós estão em execução. Certifique-se de que a versão esteja correta tanto para o serviço quanto para o arquivo de imagens. Aguarde alguns minutos e tente novamente. Ver "Linux: Instale o pacote RPM ou DEB em todos os hosts" .
Erro ao verificar o nó {node_name}	Ocorreu um erro inesperado.	Aguarde alguns minutos e tente novamente.
Erro não detectado ao executar pré-verificações. {error_string}	Ocorreu um erro inesperado.	Aguarde alguns minutos e tente novamente.

Aplicar hotfix do StorageGRID

Procedimento de correção do StorageGRID

Pode ser necessário aplicar um hotfix ao seu sistema StorageGRID se problemas com o software forem detectados e resolvidos entre os lançamentos de recursos.

Os hotfixes do StorageGRID contêm alterações de software que são disponibilizadas fora de um recurso ou lançamento de patch. As mesmas alterações estão incluídas em uma versão futura. Além disso, cada versão de hotfix contém um resumo de todos os hotfixes anteriores dentro da versão do recurso ou patch.

Considerações para aplicar um hotfix

Não é possível aplicar um hotfix do StorageGRID quando outro procedimento de manutenção estiver em execução. Por exemplo, você não pode aplicar um hotfix enquanto um procedimento de desativação, expansão ou recuperação estiver em execução.



Se um procedimento de desativação de nó ou site for pausado, você poderá aplicar um hotfix com segurança. Além disso, você pode aplicar um hotfix durante os estágios finais de um procedimento de atualização do StorageGRID. Consulte as instruções para atualizar o software StorageGRID para obter detalhes.

Depois de carregar o hotfix no Grid Manager, ele será aplicado automaticamente ao nó de administração principal. Em seguida, você pode aprovar a aplicação do hotfix ao restante dos nós no seu sistema StorageGRID.

Se um hotfix não for aplicado a um ou mais nós, o motivo da falha aparecerá na coluna Detalhes da tabela de progresso do hotfix. Você deve resolver quaisquer problemas que causaram as falhas e depois tentar todo o processo novamente. Os nós com uma aplicação bem-sucedida anterior do hotfix serão ignorados em aplicações subsequentes. Você pode tentar novamente o processo de hotfix com segurança quantas vezes forem necessárias até que todos os nós tenham sido atualizados. O hotfix deve ser instalado com sucesso em todos os nós da grade para que o aplicativo seja concluído.

Embora os nós da grade sejam atualizados com a nova versão do hotfix, as alterações reais em um hotfix podem afetar apenas serviços específicos em tipos específicos de nós. Por exemplo, um hotfix pode afetar apenas o serviço LDR em nós de armazenamento.

Como os hotfixes são aplicados para recuperação e expansão

Depois que um hotfix é aplicado à sua grade, o nó de administração principal instala automaticamente a mesma versão do hotfix em todos os nós restaurados por operações de recuperação ou adicionados em uma expansão.

No entanto, se você precisar recuperar o nó de administração principal, deverá instalar manualmente a versão correta do StorageGRID e, em seguida, aplicar o hotfix. A versão final do StorageGRID do nó administrativo primário deve corresponder à versão dos outros nós na grade.

O exemplo a seguir ilustra como aplicar um hotfix ao recuperar o nó de administração primário:

1. Suponha que a grade esteja executando uma versão StorageGRID 11.A.B com o hotfix mais recente. A "versão em grade" é 11.A.B.y.
2. O nó de administração primário falha.

3. Você reimplanta o nó de administração primário usando o StorageGRID 11.A.B e executa o procedimento de recuperação.



Conforme necessário para corresponder à versão da grade, você pode usar uma versão secundária ao implantar o nó; não é necessário implantar a versão principal primeiro.

4. Em seguida, aplique o hotfix 11.A.B.y ao nó de administração primário.

Para obter mais informações, consulte ["Configurar nó de administração primário de substituição"](#).

Como seu sistema é afetado quando você aplica um hotfix

Você deve entender como seu sistema StorageGRID será afetado quando você aplicar um hotfix.

Os hotfixes do StorageGRID não causam interrupções

O sistema StorageGRID pode ingerir e recuperar dados de aplicativos clientes durante todo o processo de hotfix. Se você aprovar todos os nós do mesmo tipo para hotfix (por exemplo, nós de armazenamento), os nós serão desativados um de cada vez, de modo que não haverá momento em que todos os nós da grade ou todos os nós da grade de um determinado tipo estarão indisponíveis.

Para permitir disponibilidade contínua, certifique-se de que sua política de ILM contenha regras que especifiquem o armazenamento de várias cópias de cada objeto. Você também deve garantir que todos os clientes S3 externos estejam configurados para enviar solicitações para um dos seguintes:

- Um endereço IP virtual de grupo de alta disponibilidade (HA)
- Um balanceador de carga de terceiros de alta disponibilidade
- Vários nós de gateway para cada cliente
- Vários nós de armazenamento para cada cliente

Os aplicativos do cliente podem sofrer interrupções de curto prazo

O sistema StorageGRID pode ingerir e recuperar dados de aplicativos clientes durante todo o processo de hotfix; no entanto, as conexões do cliente com nós de gateway ou nós de armazenamento individuais podem ser interrompidas temporariamente se o hotfix precisar reiniciar serviços nesses nós. A conectividade será restaurada após a conclusão do processo de hotfix e os serviços serem retomados nos nós individuais.

Pode ser necessário agendar um tempo de inatividade para aplicar um hotfix se a perda de conectividade por um curto período não for aceitável. Você pode usar a aprovação seletiva para agendar quando determinados nós serão atualizados.



Você pode usar vários gateways e grupos de alta disponibilidade (HA) para fornecer failover automático durante o processo de hotfix. Veja as instruções para ["configurando grupos de alta disponibilidade"](#).

Alertas e notificações SNMP podem ser acionados

Alertas e notificações SNMP podem ser acionados quando os serviços são reiniciados e quando o sistema StorageGRID está operando como um ambiente de versão mista (alguns nós de grade executando uma versão anterior, enquanto outros foram atualizados para uma versão posterior). Em geral, esses alertas e

notificações serão apagados quando o hotfix for concluído.

As alterações de configuração são restritas

Ao aplicar um hotfix ao StorageGRID:

- Não faça nenhuma alteração na configuração da grade (por exemplo, especificando sub-redes da rede da grade ou aprovando nós de grade pendentes) até que o hotfix tenha sido aplicado a todos os nós.
- Não atualize a configuração do ILM até que o hotfix tenha sido aplicado a todos os nós.

Obtenha os materiais necessários para o hotfix

Antes de aplicar um hotfix, você deve obter todos os materiais necessários.

Item	Notas
Arquivo de correção do StorageGRID	Você deve baixar o arquivo de hotfix do StorageGRID .
• Porta de rede • "Navegador da Web compatível" • Cliente SSH (por exemplo, PuTTY)	
Pacote de Recuperação(.zip) arquivo	Antes de aplicar um hotfix," baixe o arquivo do pacote de recuperação mais recente " caso ocorra algum problema durante o hotfix. Depois que o hotfix for aplicado, baixe uma nova cópia do arquivo do Pacote de Recuperação e salve-o em um local seguro. O arquivo do Pacote de Recuperação atualizado permite restaurar o sistema caso ocorra uma falha.
Arquivo Passwords.txt	Opcional e usado somente se você estiver aplicando um hotfix manualmente usando o cliente SSH. O Passwords.txt o arquivo faz parte do Pacote de Recuperação .zip arquivo.
Senha de provisionamento	A senha é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está listada no Passwords.txt arquivo.
Documentação relacionada	readme.txt`arquivo para o hotfix. Este arquivo está incluído na página de download do hotfix. Não deixe de revisar o `readme archive com cuidado antes de aplicar o hotfix.

Baixar arquivo de hotfix

Você deve baixar o arquivo de hotfix antes de poder aplicá-lo.

Passos

1. Vá para "[Downloads da NetApp : StorageGRID](#)".
2. Selecione a seta para baixo em **Software disponível** para ver uma lista de hotfixes disponíveis para download.



As versões do arquivo de hotfix têm o formato: 11.4.x.y.

3. Revise as alterações incluídas na atualização.



Se você acabou de "[recuperou o nó de administração primário](#)" e você precisa aplicar um hotfix, selecione a mesma versão do hotfix que está instalada nos outros nós da grade.

- a. Selecione a versão do hotfix que deseja baixar e selecione **Ir**.
- b. Sign in usando o nome de usuário e a senha da sua conta NetApp.
- c. Leia e aceite o Contrato de Licença do Usuário Final.

A página de download da versão selecionada será exibida.

- d. Baixe o hotfix `readme.txt` arquivo para ver um resumo das alterações incluídas no hotfix.

4. Selecione o botão de download do hotfix e salve o arquivo.



Não altere o nome deste arquivo.



Se você estiver usando um dispositivo macOS, o arquivo de hotfix pode ser salvo automaticamente como um `.txt` arquivo. Se for, você deve renomear o arquivo sem o `.txt` extensão.

5. Selecione um local para o download e selecione **Salvar**.

Verifique a condição do sistema antes de aplicar o hotfix

Você deve verificar se o sistema está pronto para acomodar o hotfix.

1. Sign in no Grid Manager usando um "[navegador da web compatível](#)".
2. Se possível, certifique-se de que o sistema esteja funcionando normalmente e que todos os nós da rede estejam conectados à rede.

Os nós conectados têm marcas de verificação verdes  na página Nós.

3. Verifique e resolva quaisquer alertas atuais, se possível.
4. Certifique-se de que não haja outros procedimentos de manutenção em andamento, como um procedimento de atualização, recuperação, expansão ou desativação.

Você deve esperar a conclusão de quaisquer procedimentos de manutenção ativos antes de aplicar um hotfix.

Não é possível aplicar um hotfix do StorageGRID quando outro procedimento de manutenção estiver em execução. Por exemplo, você não pode aplicar um hotfix enquanto um procedimento de desativação, expansão ou recuperação estiver em execução.



Se um nó ou site "[procedimento de descomissionamento está pausado](#)", você pode aplicar um hotfix com segurança. Além disso, você pode aplicar um hotfix durante os estágios finais de um procedimento de atualização do StorageGRID. Veja as instruções para "[atualizando o software StorageGRID](#)".

Aplicar hotfix

O hotfix é aplicado primeiro automaticamente ao nó de administração principal. Em seguida, você deve aprovar a aplicação do hotfix em outros nós da grade até que todos os nós estejam executando a mesma versão do software. Você pode personalizar a sequência de aprovação selecionando aprovar nós de grade individuais, grupos de nós de grade ou todos os nós de grade.

Antes de começar

- Você revisou o "[considerações para aplicar um hotfix](#)".
- Você tem a senha de provisionamento.
- Você tem acesso Root ou permissão de Manutenção.

Sobre esta tarefa

- Você pode atrasar a aplicação de um hotfix em um nó, mas o processo de hotfix não estará concluído até que você aplique o hotfix em todos os nós.
- Você não pode executar uma atualização de software do StorageGRID ou uma atualização do sistema operacional SANtricity até concluir o processo de hotfix.

Passos

1. Sign in no Grid Manager usando um "[navegador da web compatível](#)".
2. Selecione **MANUTENÇÃO > Sistema > Atualização de software**.

A página Atualização de software é exibida.

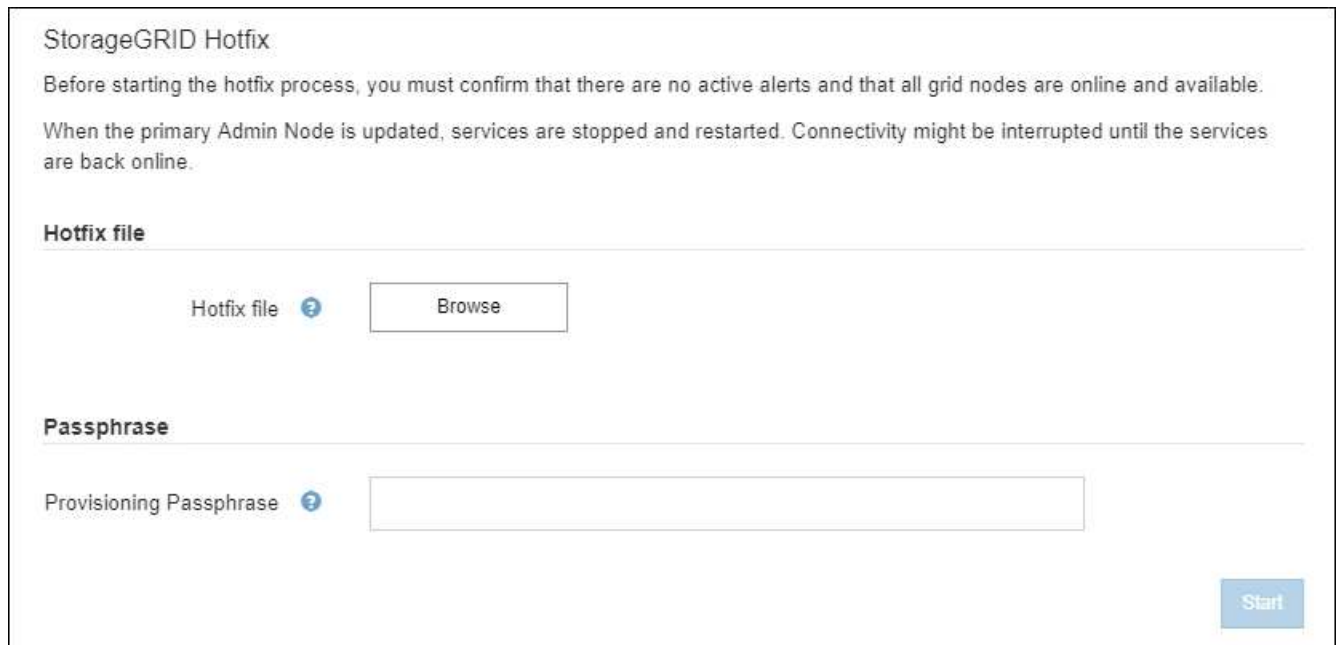
Software update

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances. NetApp recommends you apply the latest hotfix before and after each software upgrade. Some hotfixes are required to prevent data loss.

StorageGRID upgrade Upgrade to the next StorageGRID version and apply the latest hotfix for that version. Upgrade →	StorageGRID hotfix Apply a hotfix to your current StorageGRID software version. Apply hotfix →	SANtricity OS update Update the SANtricity OS software on your StorageGRID storage appliances. Update →

3. Selecione **Aplicar hotfix**.

A página StorageGRID Hotfix é exibida.



StorageGRID Hotfix

Before starting the hotfix process, you must confirm that there are no active alerts and that all grid nodes are online and available.

When the primary Admin Node is updated, services are stopped and restarted. Connectivity might be interrupted until the services are back online.

Hotfix file

Hotfix file ? Browse

Passphrase

Provisioning Passphrase ?

Start

4. Selecione o arquivo de hotfix que você baixou do site de suporte da NetApp .

- a. Selecione **Navegar**.
- b. Localize e selecione o arquivo.

`hotfix-install-version`

- c. Selecione **Abrir**.

O arquivo foi carregado. Quando o upload estiver concluído, o nome do arquivo será exibido no campo Detalhes.



Não altere o nome do arquivo, pois isso faz parte do processo de verificação.

5. Digite a senha de provisionamento na caixa de texto.

O botão **Iniciar** fica habilitado.

6. Selecione **Iniciar**.

Um aviso aparece informando que a conexão do seu navegador pode ser perdida temporariamente, pois os serviços no nó de administração principal são reiniciados.

7. Selecione **OK** para começar a aplicar o hotfix ao nó de administração principal.

Quando o hotfix começa:

- a. As validações de hotfix são executadas.



Se algum erro for relatado, resolva-o, carregue novamente o arquivo de hotfix e selecione **Iniciar** novamente.

- b. A tabela de progresso da instalação do hotfix é exibida.

Esta tabela mostra todos os nós na sua grade e o estágio atual da instalação do hotfix para cada nó. Os nós na tabela são agrupados por tipo (nós de administração, nós de gateway e nós de armazenamento).

- c. A barra de progresso chega à conclusão e, em seguida, o nó de administração principal é exibido como "Concluído".

Hotfix Installation Progress

Approve All
Remove All

Admin Nodes - 1 out of 1 completed

Site	Name	Progress	Stage	Details	Action
Vancouver	VTC-ADM1-101-191		Complete		

8. Opcionalmente, classifique as listas de nós em cada agrupamento em ordem crescente ou decrescente por **Site**, **Nome**, **Progresso**, **Estágio** ou **Detalhes**. Ou insira um termo na caixa **Pesquisar** para pesquisar nós específicos.
9. Aprovar os nós da grade que estão prontos para serem atualizados. Os nós aprovados do mesmo tipo são atualizados um de cada vez.



Não aprove o hotfix para um nó a menos que tenha certeza de que o nó está pronto para ser atualizado. Quando o hotfix é aplicado a um nó de grade, alguns serviços nesse nó podem ser reiniciados. Essas operações podem causar interrupções de serviço para clientes que estão se comunicando com o nó.

- Selecione um ou mais botões **Aprovar** para adicionar um ou mais nós individuais à fila de hotfixes.
- Selecione o botão **Aprovar tudo** dentro de cada agrupamento para adicionar todos os nós do mesmo tipo à fila de hotfixes. Se você inseriu critérios de pesquisa na caixa **Pesquisar**, o botão **Aprovar tudo** será aplicado a todos os nós selecionados pelos critérios de pesquisa.



O botão **Aprovar tudo** no topo da página aprova todos os nós listados na página, enquanto o botão **Aprovar tudo** no topo de um agrupamento de tabelas aprova apenas todos os nós naquele grupo. Se a ordem em que os nós são atualizados for importante, aprove os nós ou grupos de nós um de cada vez e aguarde até que a atualização seja concluída em cada nó antes de aprovar o(s) próximo(s) nó(s).

- Selecione o botão de nível superior **Aprovar tudo** na parte superior da página para adicionar todos os nós na grade à fila de hotfixes.



Você deve concluir o hotfix do StorageGRID antes de iniciar uma atualização de software diferente. Se você não conseguir concluir o hotfix, entre em contato com o suporte técnico.

- Selecione **Remover** ou **Remover tudo** para remover um nó ou todos os nós da fila de hotfixes.

Quando o estágio avança além de "Na fila", o botão **Remover** fica oculto e você não pode mais remover o nó do processo de hotfix.

Storage Nodes - 1 out of 9 completed						Approve All	Remove All
Search							
Site	Name	Progress	Stage	Details	Action		
Raleigh	RAL-S1-101-196		Queued		Remove		
Raleigh	RAL-S2-101-197		Complete				
Raleigh	RAL-S3-101-198		Queued		Remove		
Sunnyvale	SVL-S1-101-199		Queued		Remove		
Sunnyvale	SVL-S2-101-93		Waiting for you to approve		Approve		
Sunnyvale	SVL-S3-101-94		Waiting for you to approve		Approve		
Vancouver	VTC-S1-101-193		Waiting for you to approve		Approve		
Vancouver	VTC-S2-101-194		Waiting for you to approve		Approve		
Vancouver	VTC-S3-101-195		Waiting for you to approve		Approve		

10. Aguarde enquanto o hotfix é aplicado a cada nó de grade aprovado.

Quando o hotfix for instalado com sucesso em todos os nós, a tabela Progresso da instalação do hotfix será fechada. Um banner verde mostra a data e a hora em que o hotfix foi concluído.

11. Se o hotfix não puder ser aplicado a nenhum nó, revise o erro de cada nó, resolva o problema e repita essas etapas.

O procedimento não estará concluído até que o hotfix seja aplicado com sucesso a todos os nós. Você pode tentar novamente o processo de hotfix quantas vezes forem necessárias até que ele seja concluído.

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 logo "NetApp StorageGRID®" is displayed. Below it, the title "Grid Manager" is centered. The form includes a "Username" label followed by a text input field containing a single vertical bar "|". Below the username field is a "Password" label followed by an empty password input field. A blue "Sign in" button is positioned below the password field. At the bottom of the form, there are three links: "Tenant sign in", "NetApp support", and "NetApp.com", all in blue text.

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

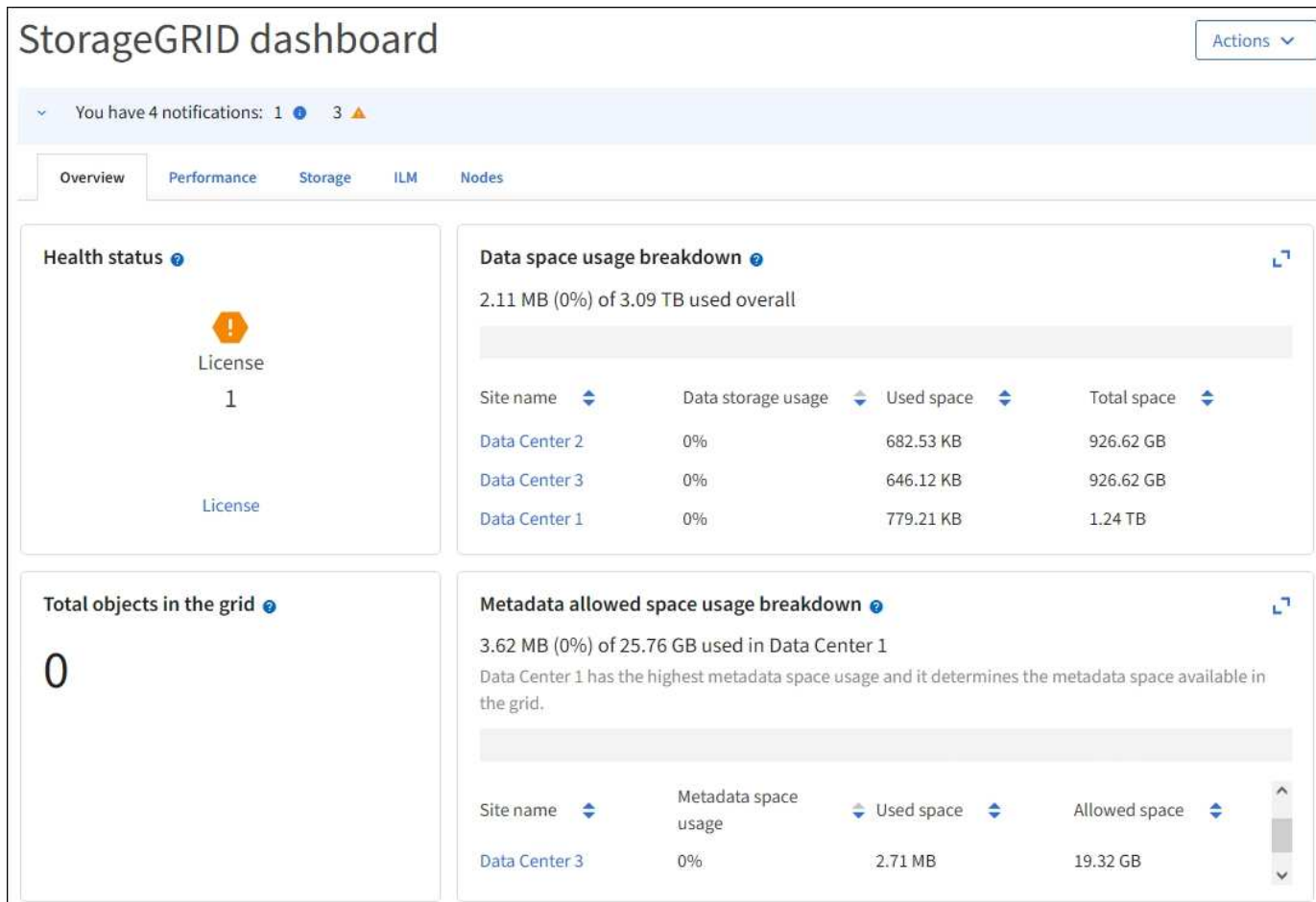
Sign in

- 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, there is a logo consisting of a square icon with a stylized 'N' followed by the text 'NetApp StorageGRID®'. Below the logo, the text 'Sign in' is displayed in a large, bold font. Underneath, there is a section titled 'Recent' with a dropdown menu showing 'Grid Manager'. Below that is a section titled 'Account' with a text input field containing the number '0'. A blue button labeled 'Sign in' is positioned below the input field. At the bottom of the form, there is a link for 'NetApp support' followed by a vertical bar and the text '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

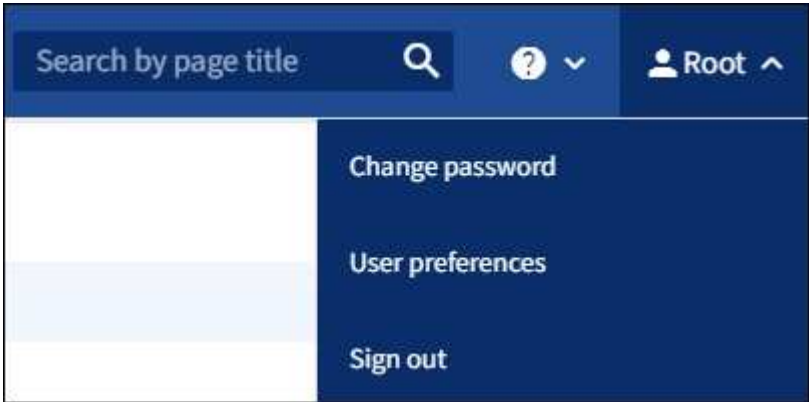
1. Digite o nome de domínio totalmente qualificado ou o endereço IP do outro nó de administração na barra de endereços do navegador.
2. Se sua sessão SSO expirou, insira suas credenciais novamente.

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

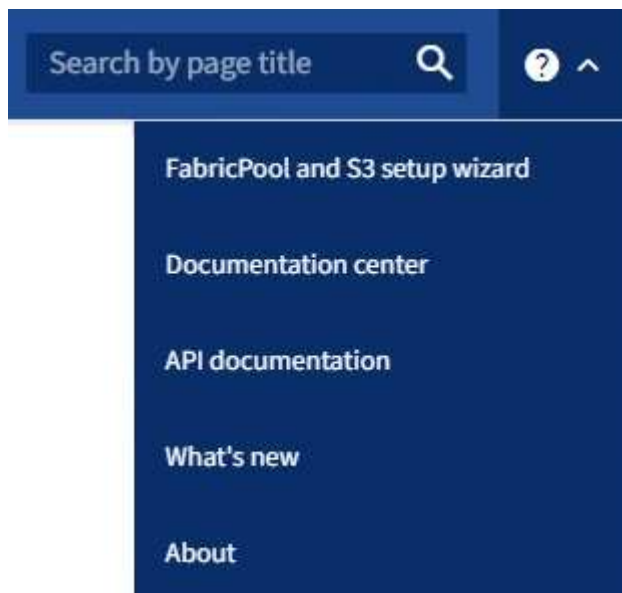
- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem ["permissões de acesso específicas"](#).



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=fZHRT0MwFIZfhh...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=fZHRT0MwFIZfhh...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=MjAxOC0xMS0wNzoxNjoxMjoxMjoxOVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

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

- i. Salve o SAMLResponse do campo oculto:

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

- j. Usando o 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: MSISignoutProtocol=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:**
- **SUPORTE > 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](#)



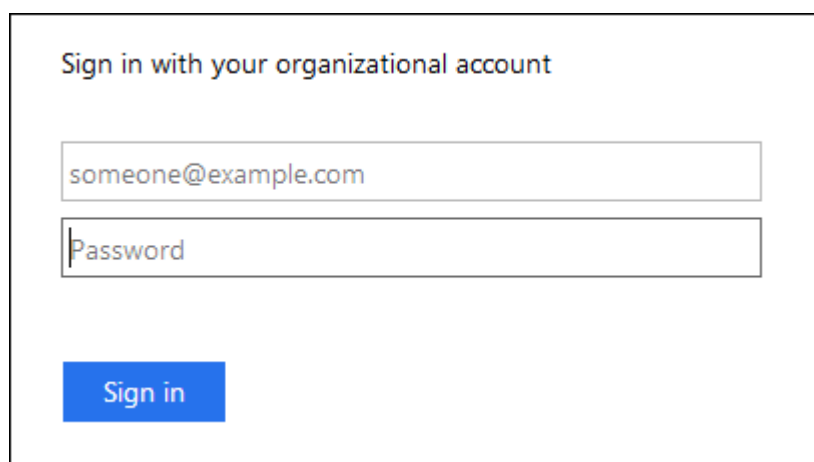
A página de Sign in do StorageGRID não é exibida quando você insere o URL completo de uma conta de locatário (ou seja, um nome de domínio totalmente qualificado ou endereço IP seguido por `/?accountId=20-digit-account-id`). Em vez disso, você será imediatamente redirecionado para a página de login SSO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



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

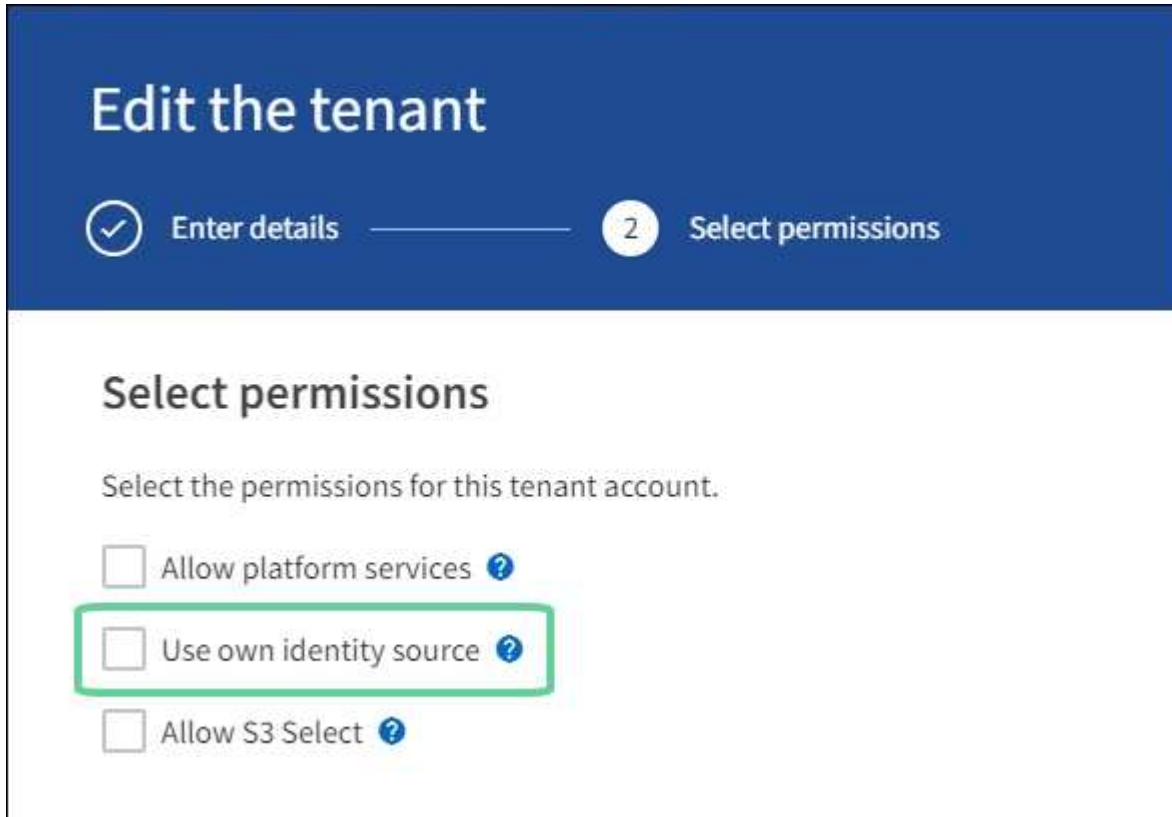
1. Se houver contas de locatários existentes, confirme se nenhum deles está usando sua própria fonte de identidade.



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.

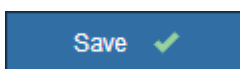
- Por exemplo, se sua grade tiver apenas um nó de administração e você não pretende adicionar mais nós de administração no futuro, insira `SG` ou `StorageGRID` .
- Se sua grade incluir mais de um nó de administração, inclua a string `[HOSTNAME]` no identificador. Por exemplo, `SG-[HOSTNAME]` . Isso gera 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 confianças 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**.

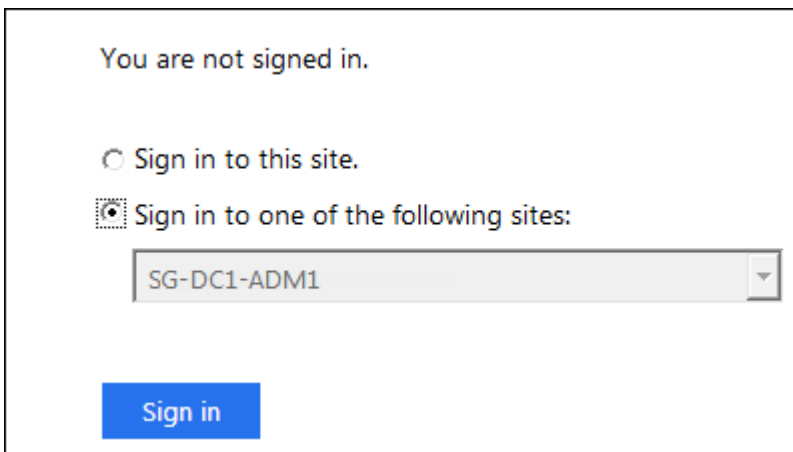
Sandbox mode

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*.



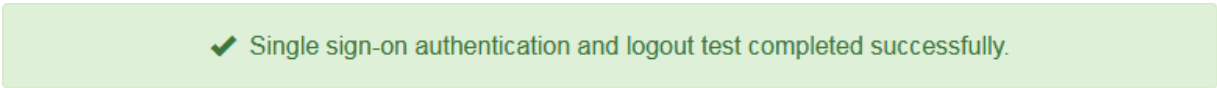
You are not signed in.

☐ 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.
- 
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.

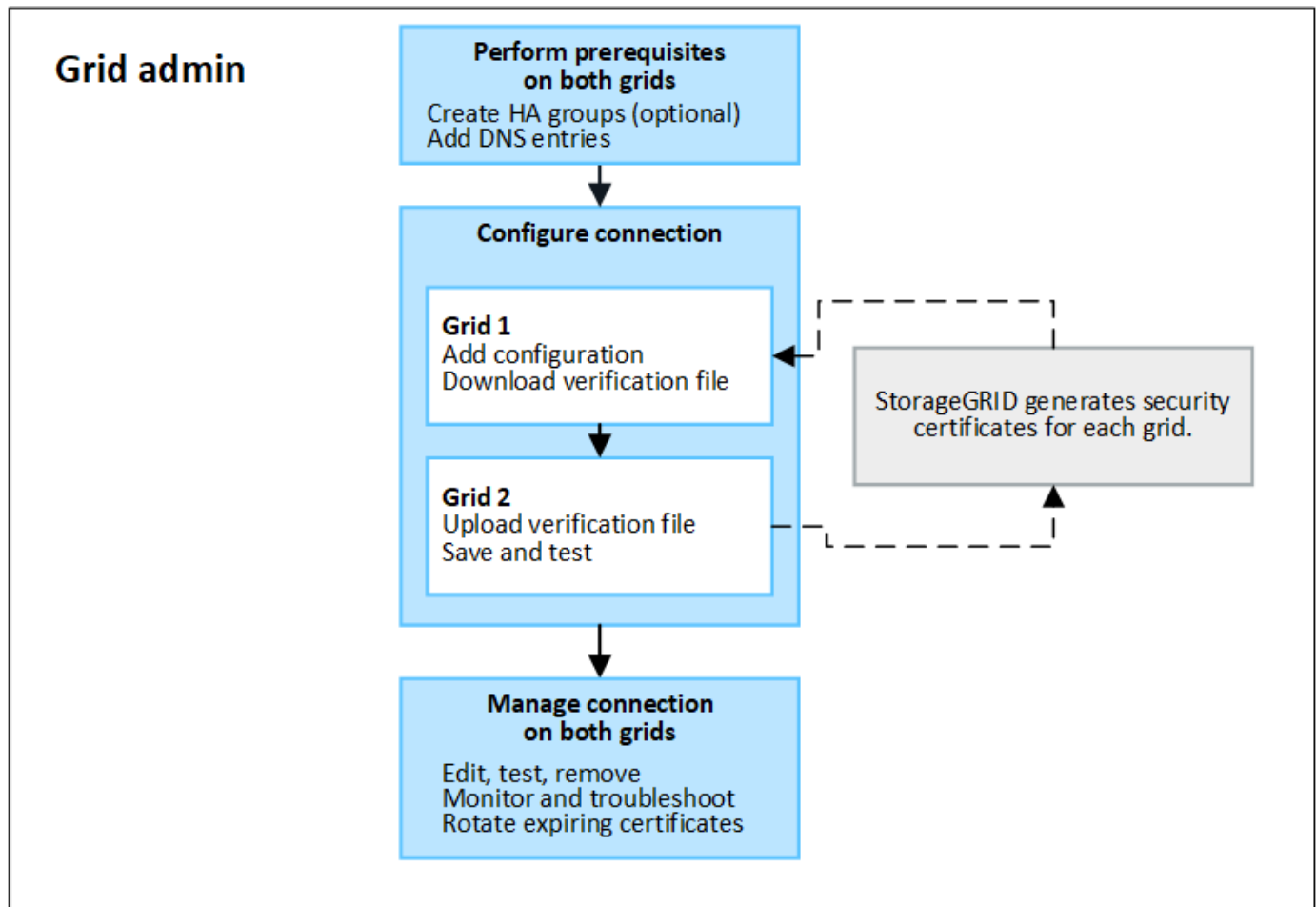
O que é uma conexão de federação de rede?

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.

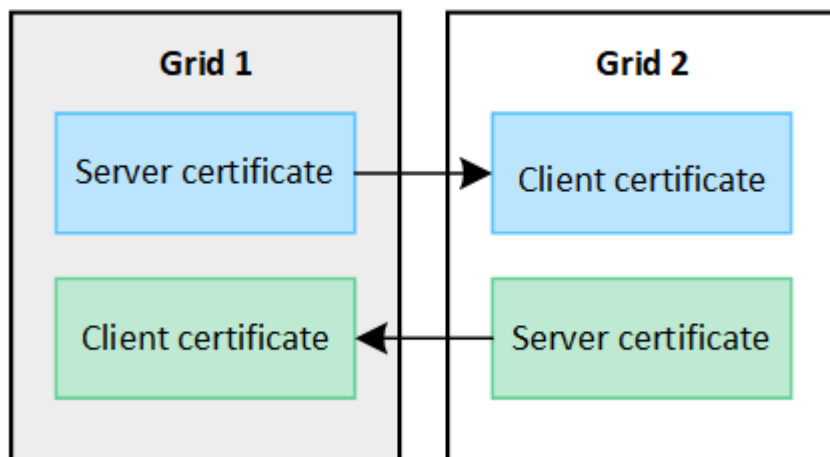
Você deve garantir que nenhum nó em nenhuma das grades use esta porta para outras conexões.

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"](#)

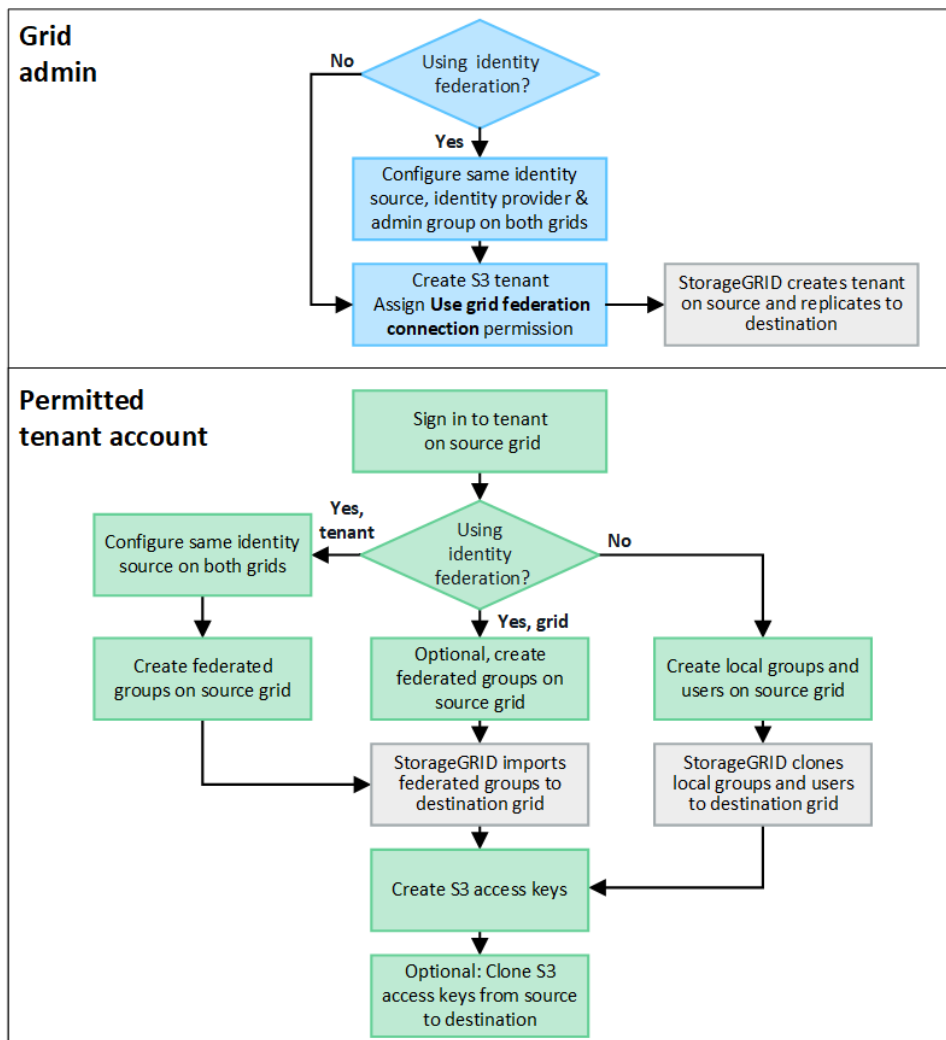
O que é clone de conta?

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.

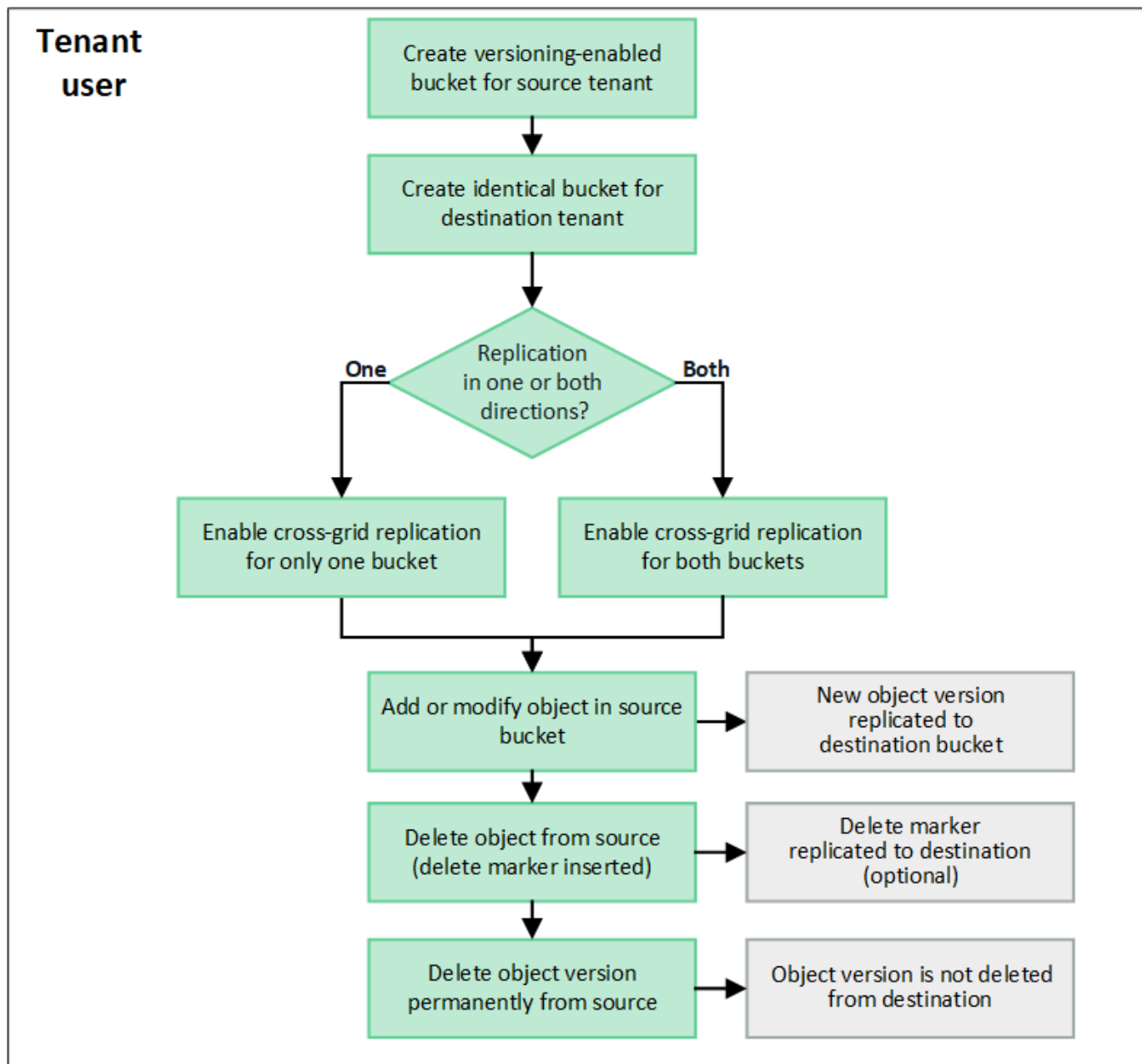
Para obter detalhes sobre o fluxo de trabalho da conta de locatário permitida e saber como grupos, usuários e chaves de acesso S3 são clonados, consulte ["Clonar grupos de locatários e usuários"](#) e ["Clonar chaves de acesso S3 usando a API"](#) .

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

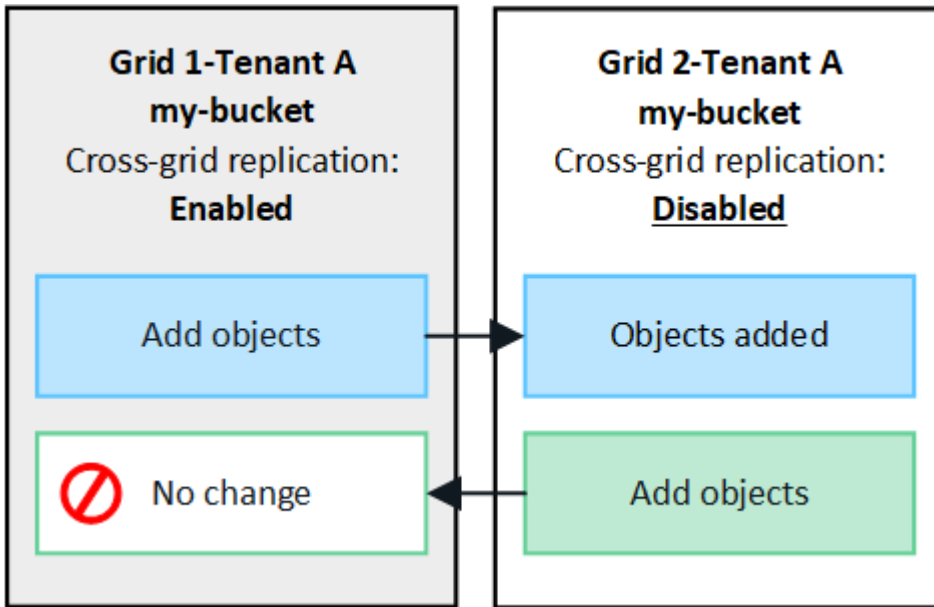
"Gerenciar replicação entre redes"

Como funciona a replicação entre redes

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

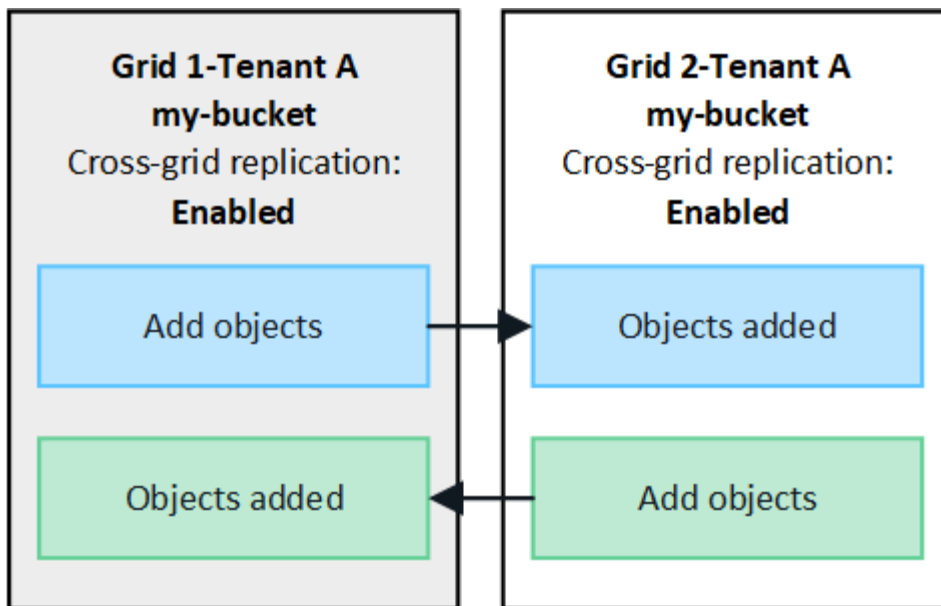
Replicação em uma direção

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.

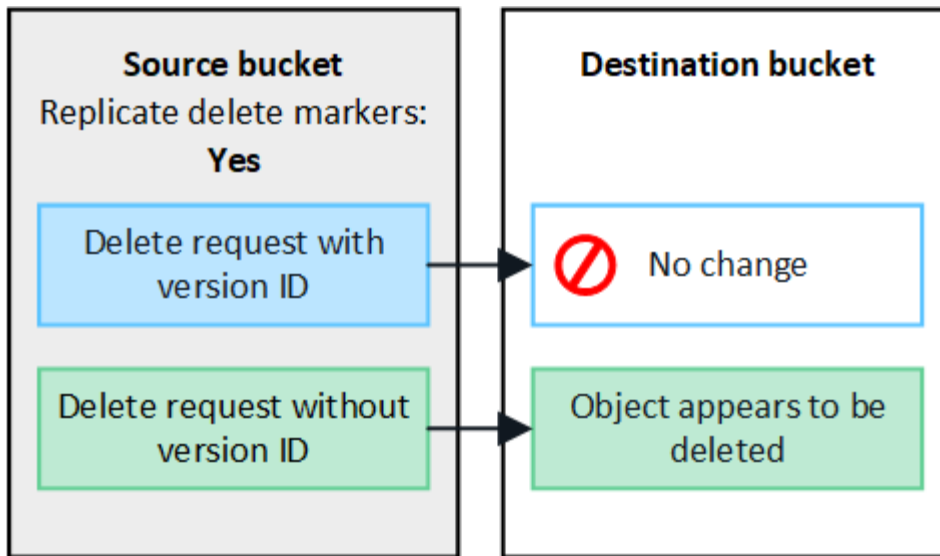
Para entender o que acontece quando um cliente S3 exclui objetos de um bucket que tem a replicação entre grades habilitada, revise como os clientes S3 excluem objetos de buckets que têm o controle de versão habilitado, da seguinte maneira:

- 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.

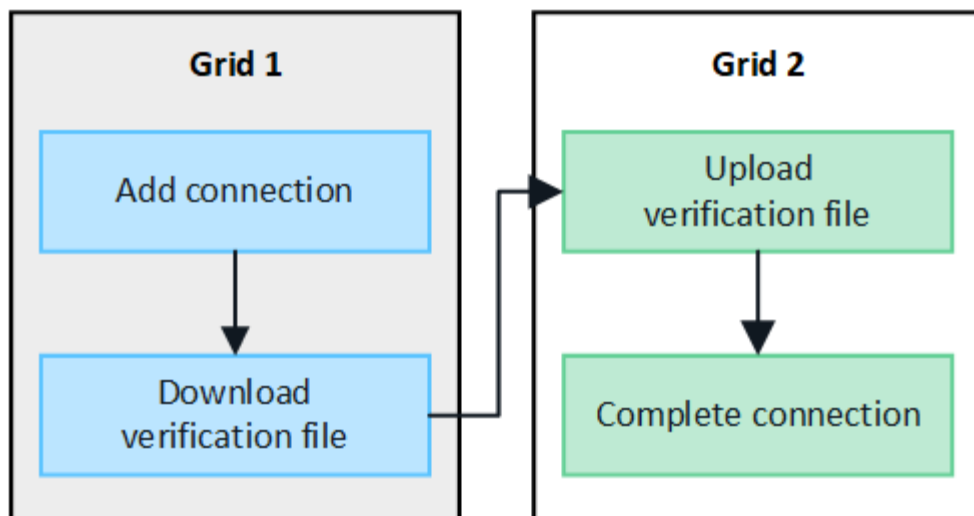
	Replicação entre grades	Serviço de replicação CloudMirror
Como é configurado?	1. Configure uma conexão de federação de grade entre duas grades. 2. Adicione novas contas de locatários, que são clonadas automaticamente para a outra grade. 3. Adicione novos grupos de locatários e usuários, que também são 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

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

Página de detalhes

- Selecione um nome de conexão para exibir seus detalhes.
- 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.

- 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

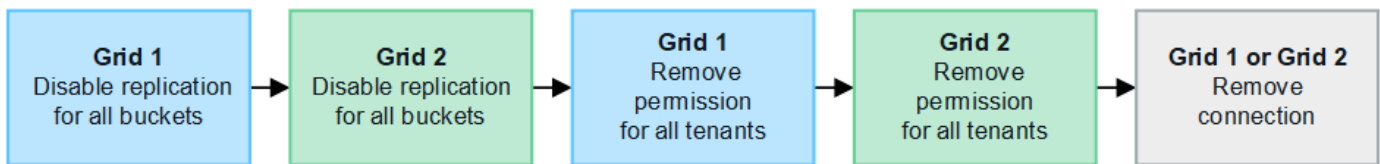
- Sign in no Grid Manager a partir do nó de administração principal em qualquer uma das grades.
- Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.
- Em qualquer uma das guias da página Federação da grade, selecione o nome da conexão para exibir seus detalhes.
- Selecione a aba **Certificados**.

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

Search...

Displaying one result

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

3. Opcionalmente, selecione a 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

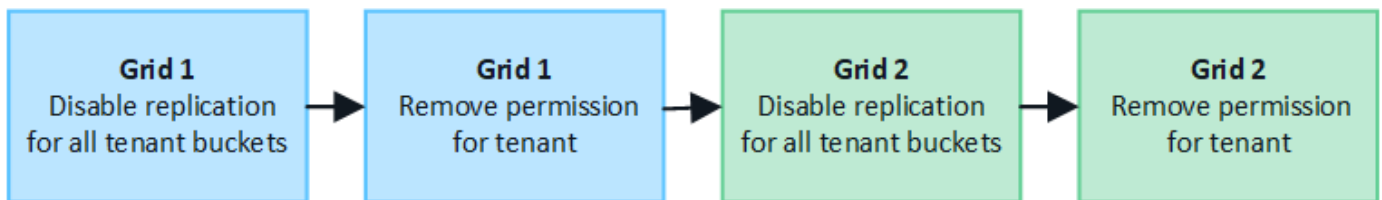
Se você precisar remover um locatário que tenha a permissão **Usar conexão de federação de grade**, siga as instruções gerais para [excluindo uma conta de inquilino](#) e observe o seguinte:

- 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](#)

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.

6. 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.

7. 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

1. Sign in na grade onde o alerta foi acionado.
2. Vá para **CONFIGURAÇÃO > Sistema > Federação de grade** e localize o nome da conexão listado no alerta.
3. Na guia Inquilinos permitidos, observe a coluna **Último erro** para determinar quais contas de inquilinos apresentam erros.
4. Para saber mais sobre a falha, consulte as instruções em "[Monitorar conexões de federação de rede](#)" para revisar as métricas de replicação entre grades.
5. Para cada conta de locatário afetada:
 - a. 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.
 - b. Conforme necessário, aumente a cota do locatário na grade de destino para permitir que novos objetos sejam salvos.
6. Para cada locatário afetado, faça login no Gerenciador de Locatários em ambas as grades para poder comparar a lista de buckets.
7. 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**.
8. 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 x-amz-server-side-encryption 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. - x-amz-server-side-encryption-customer-algorithm - x-amz-server-side-encryption-customer-key - x-amz-server-side-encryption-customer-key-MD5	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 globalCertificado 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:

- a. Acesse o Grid Manager.
- b. Selecione **CONFIGURAÇÃO > Segurança > Certificados**
- c. Na guia **Global**, selecione **Certificado de interface de gerenciamento**.

7. Configure seu cliente de gerenciamento para usar o certificado público que você copiou. Inclua as tags 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

1. Selecione **CONFIGURAÇÃO > Segurança > Certificados**.
2. Na guia **Global**, selecione **Certificado de interface de gerenciamento**.
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`

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

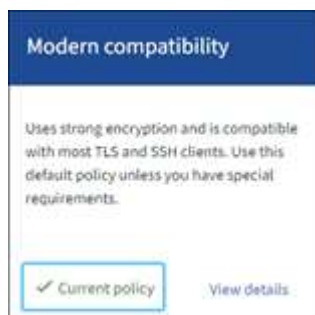
- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você tem o "[Permissão de acesso root](#)".

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?

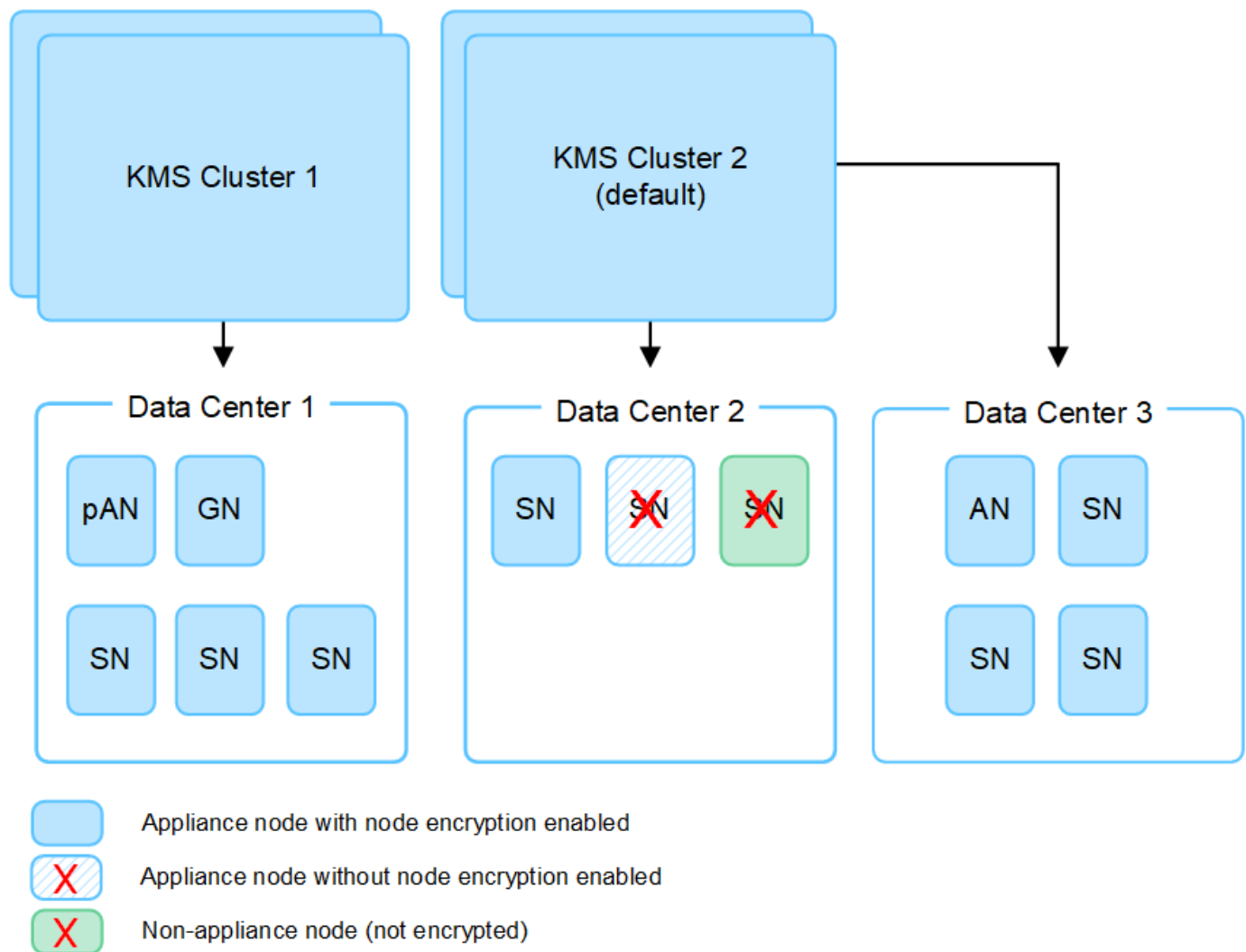
Você pode configurar um ou mais servidores externos de gerenciamento de chaves para fornecer chaves de

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.

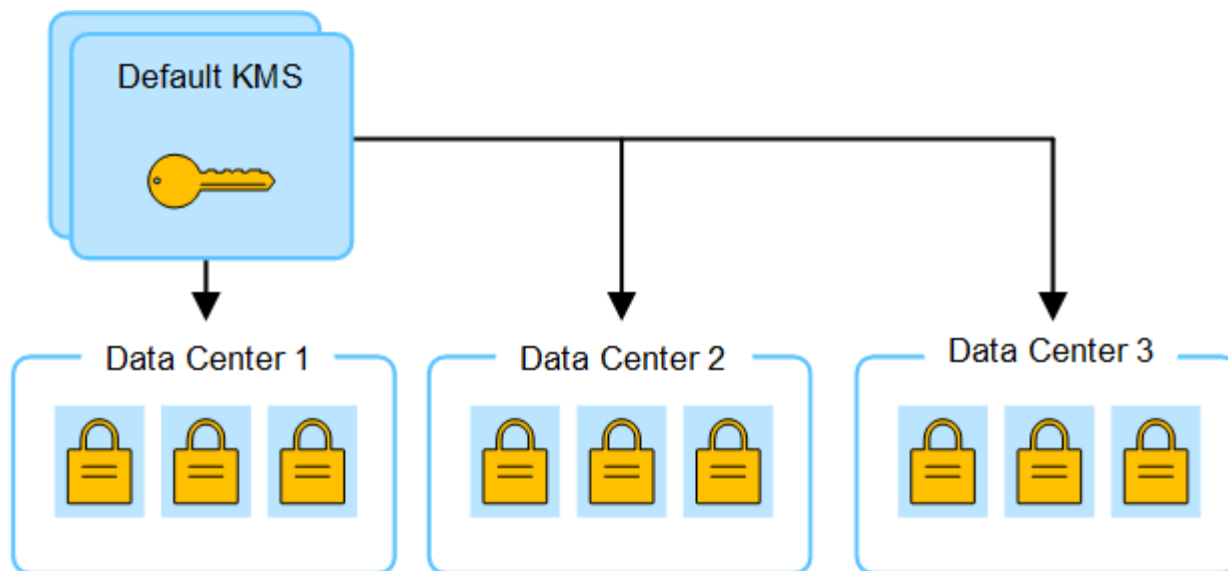
Considerações para alterar o KMS de um site

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.

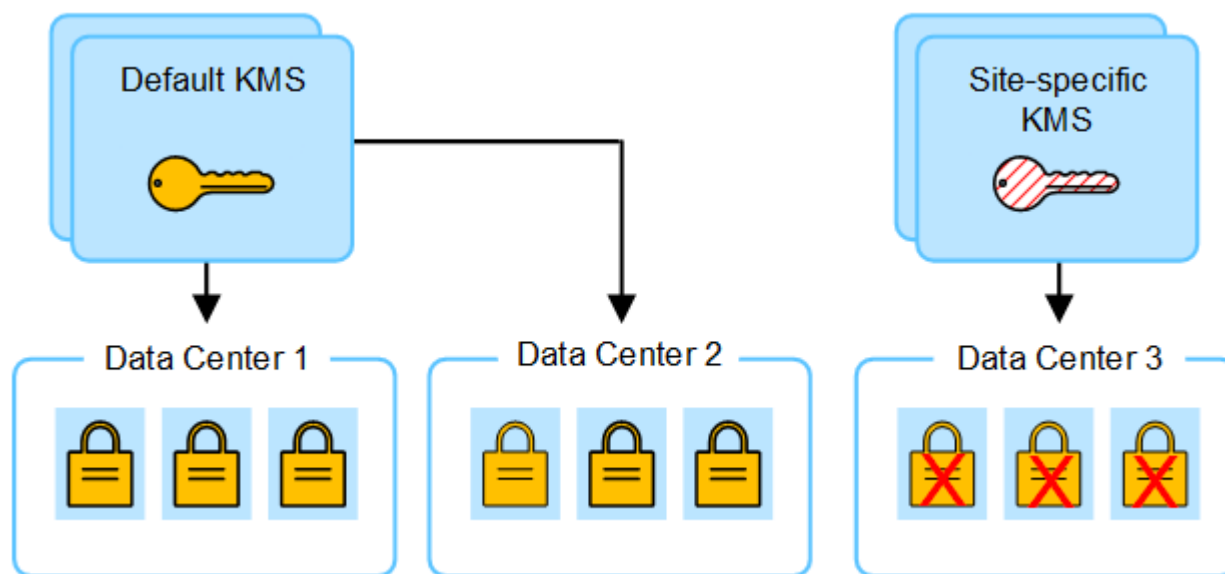
Se você alterar o KMS usado para um site, deverá garantir que os nós do dispositivo criptografados anteriormente naquele site possam ser descriptografados usando a chave armazenada no novo KMS. Em alguns casos, pode ser necessário copiar a versão atual da chave de criptografia do KMS original para o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

Por exemplo:

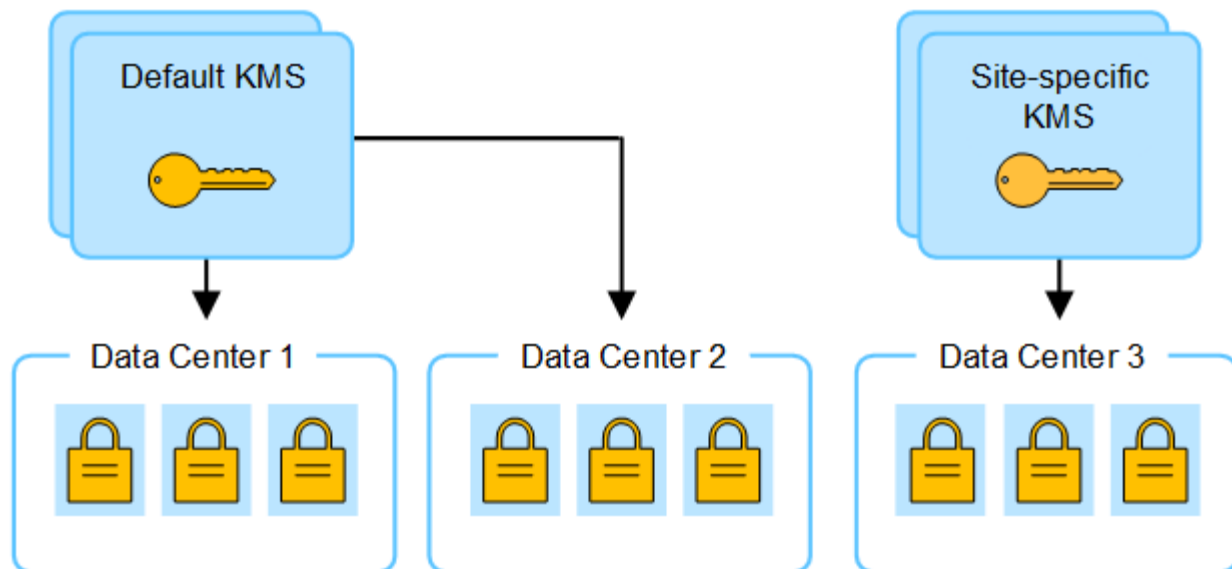
1. Inicialmente, você configura um KMS padrão que se aplica a todos os sites que não têm um KMS dedicado.
2. Quando o KMS é salvo, todos os nós do dispositivo que têm a configuração **Criptografia de nó** ativada se conectam ao KMS e solicitam a chave de criptografia. Esta chave é usada para criptografar 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.

- 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

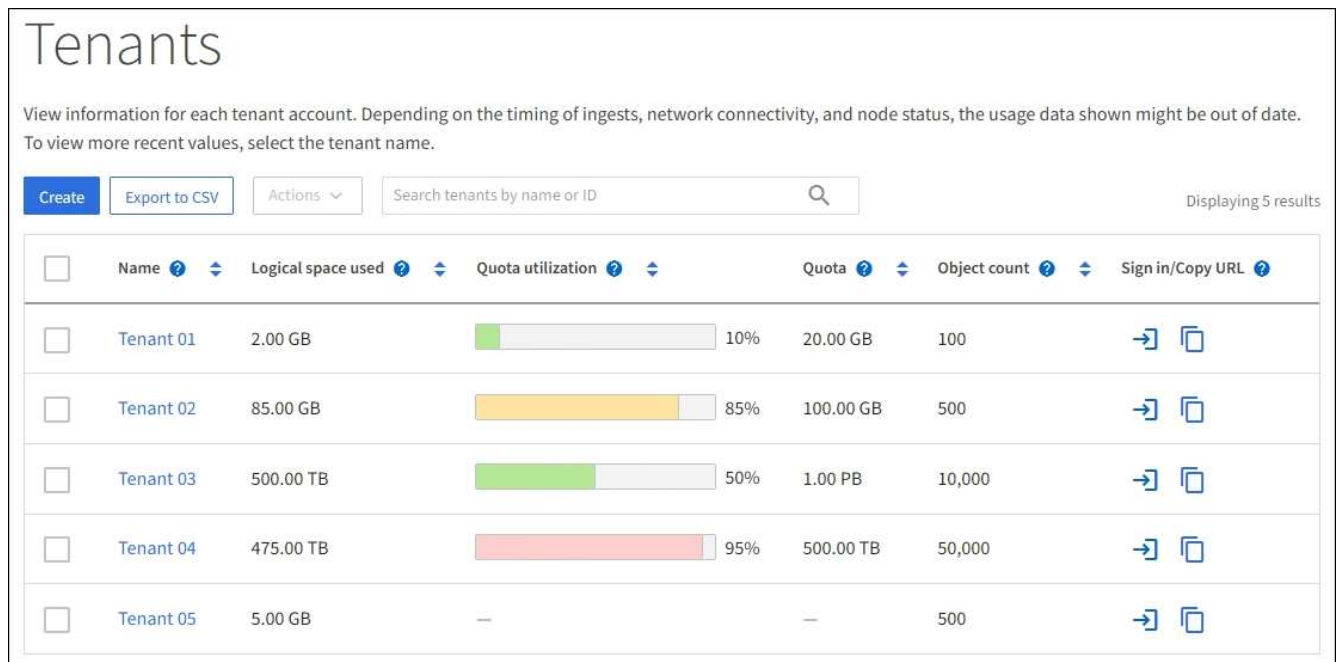
- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem ["permissões de acesso específicas"](#) .

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.

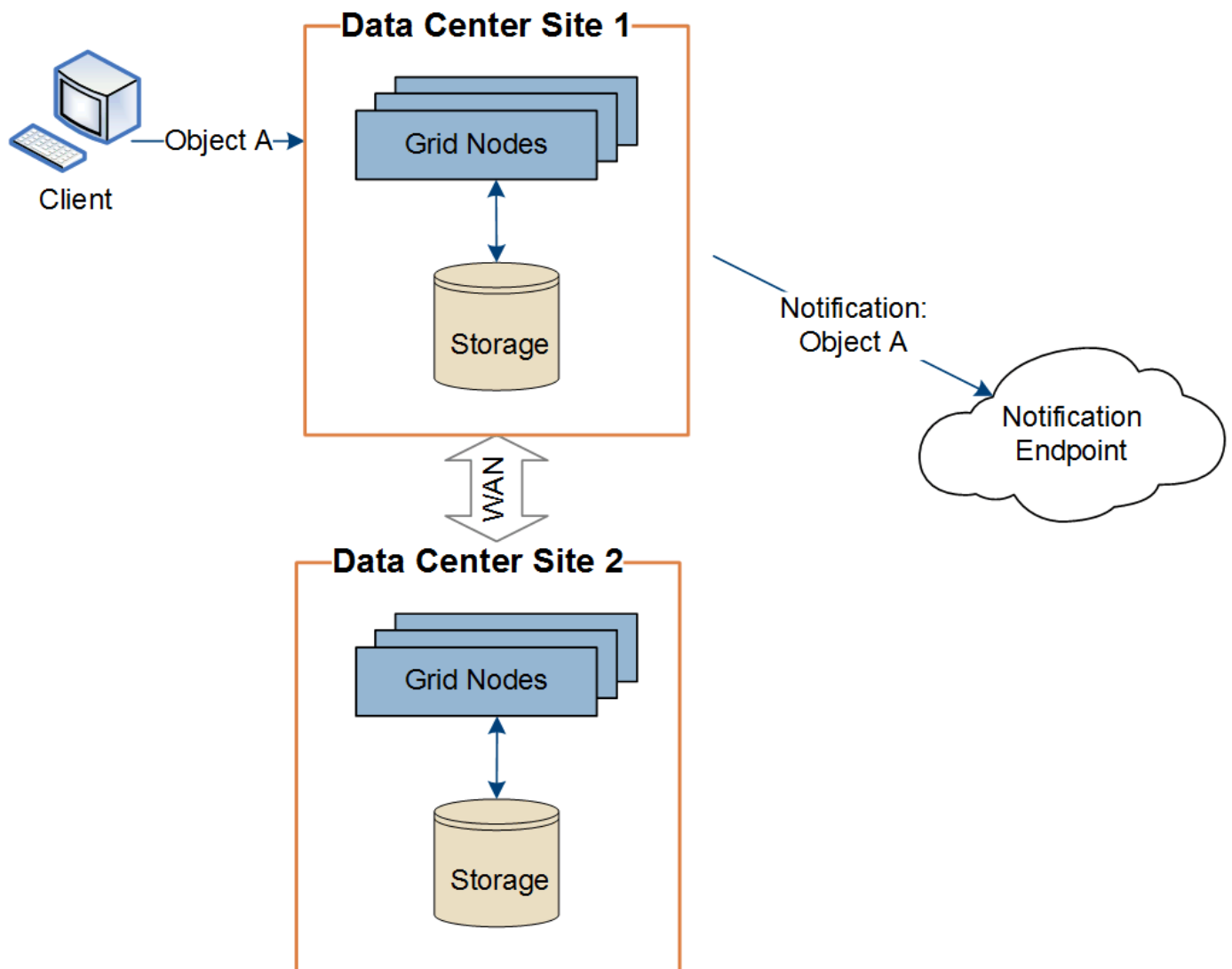
Informações relacionadas

["Use uma conta de inquilino"](#)

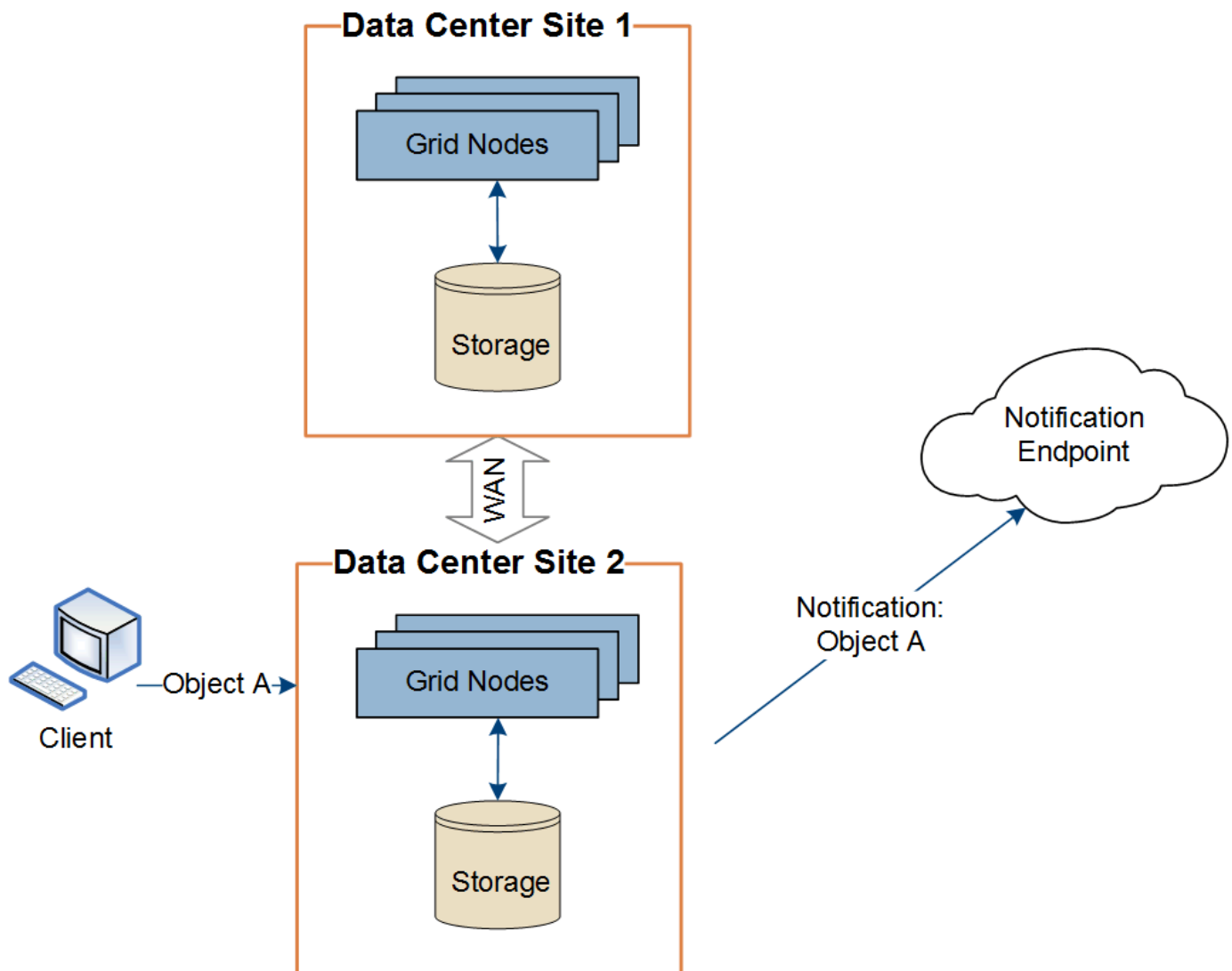
Entrega de mensagens de serviços de plataforma por site

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.

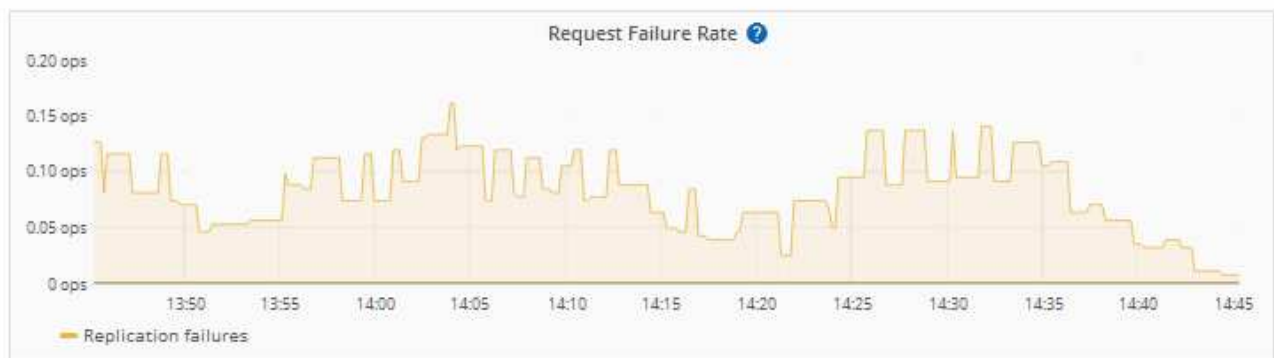
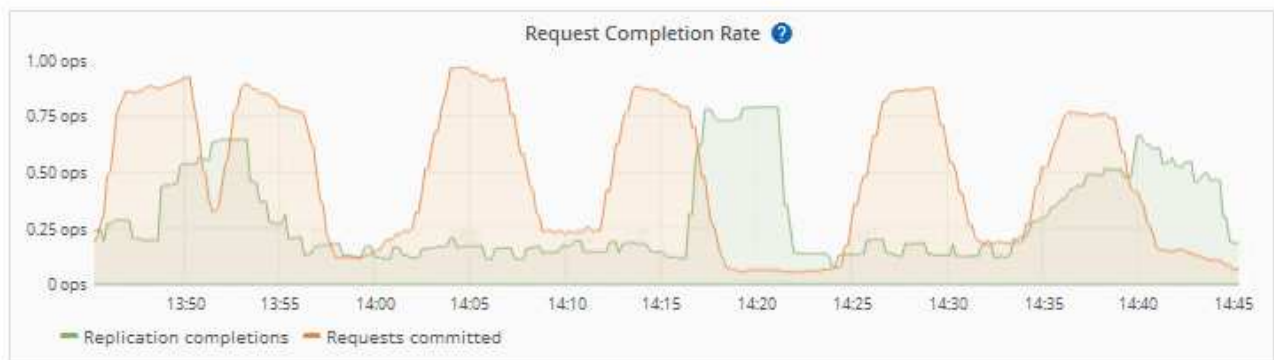
O único efeito visível é que as solicitações S3 recebidas levarão mais tempo para serem executadas. Se você começar a detectar um desempenho significativamente mais lento, reduza a taxa de ingestão ou use um ponto de extremidade com maior capacidade. Se o acúmulo de solicitações continuar a crescer, 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.

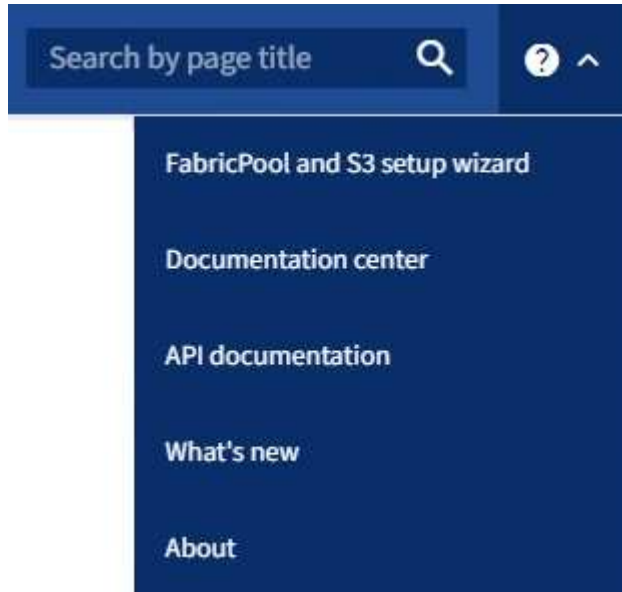
Antes de começar

- 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

- a. Para criar um novo grupo HA, selecione **Criar grupo HA**.
- b. 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.

- c. 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.

- d. 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.

- e. 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

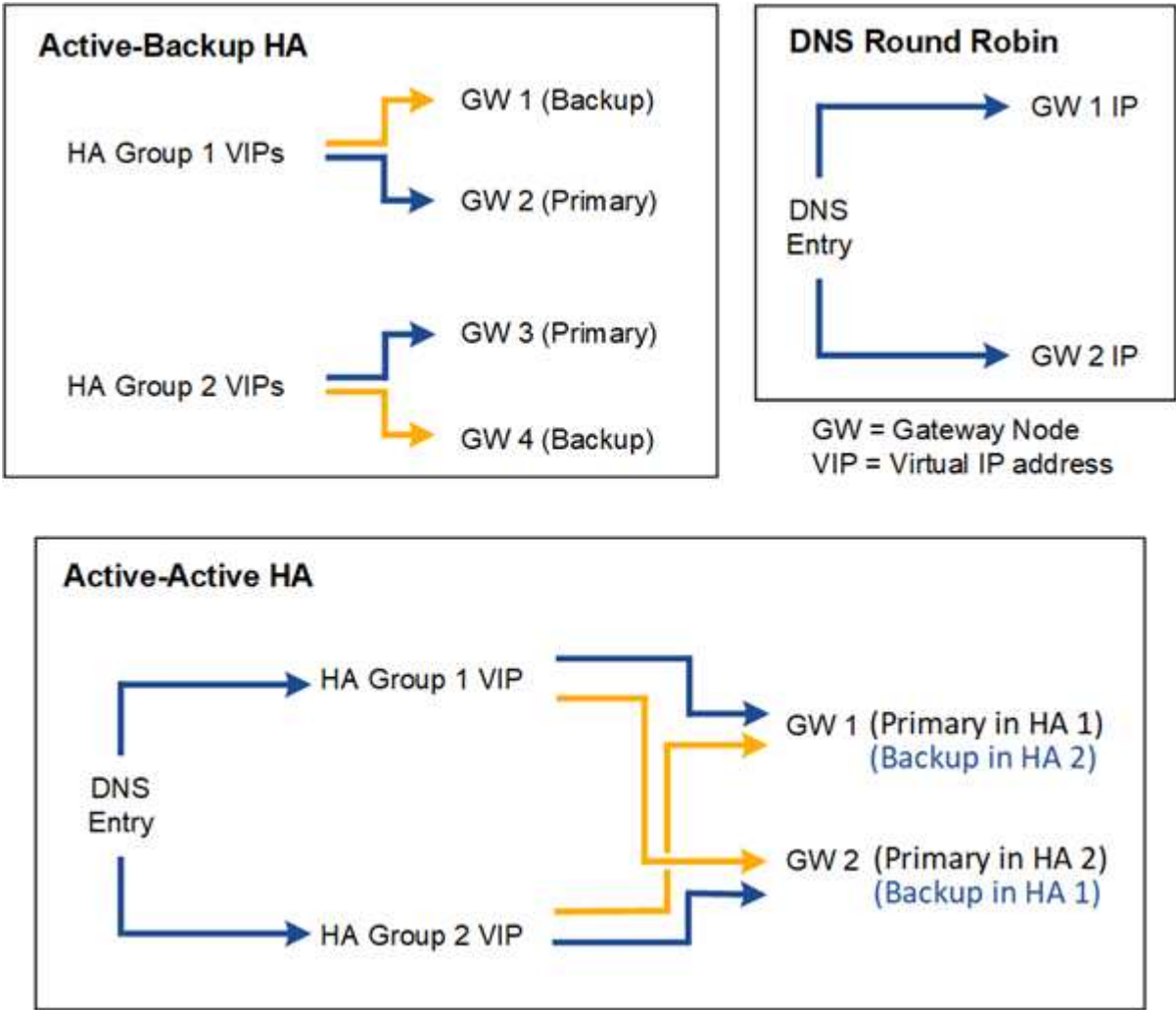
desconectado e deverá fazer login novamente para retomar sua tarefa.

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



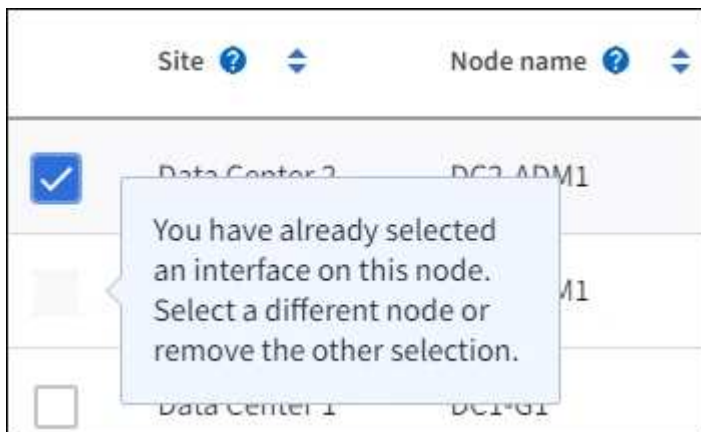
Após criar uma interface VLAN, aguarde até 5 minutos para que a nova interface apareça na tabela.

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.

5. 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.

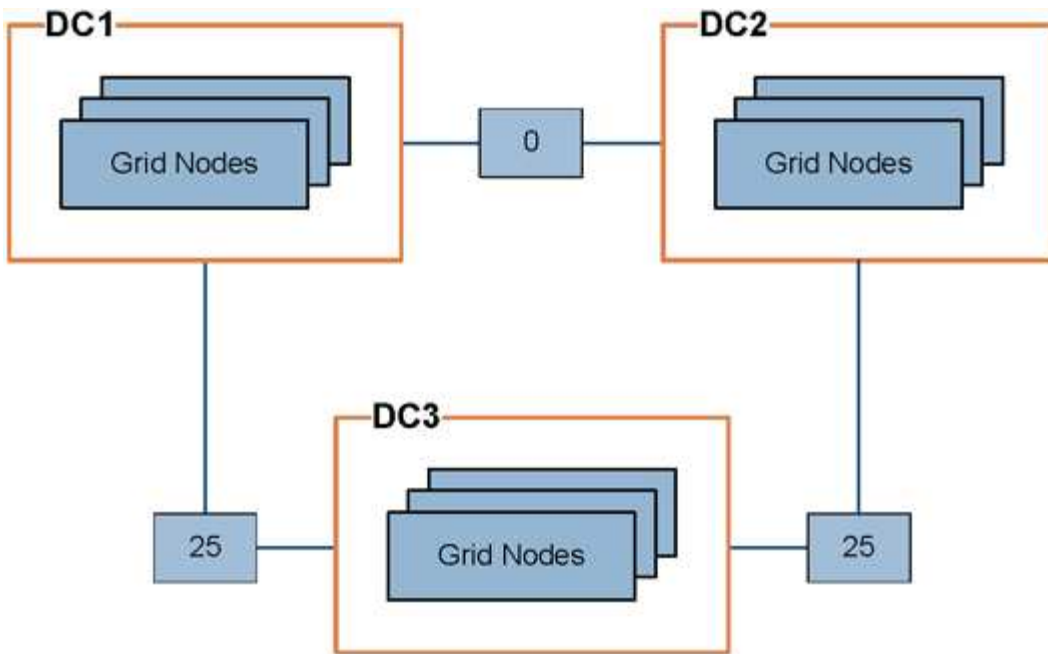
Gerenciar custos de link

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

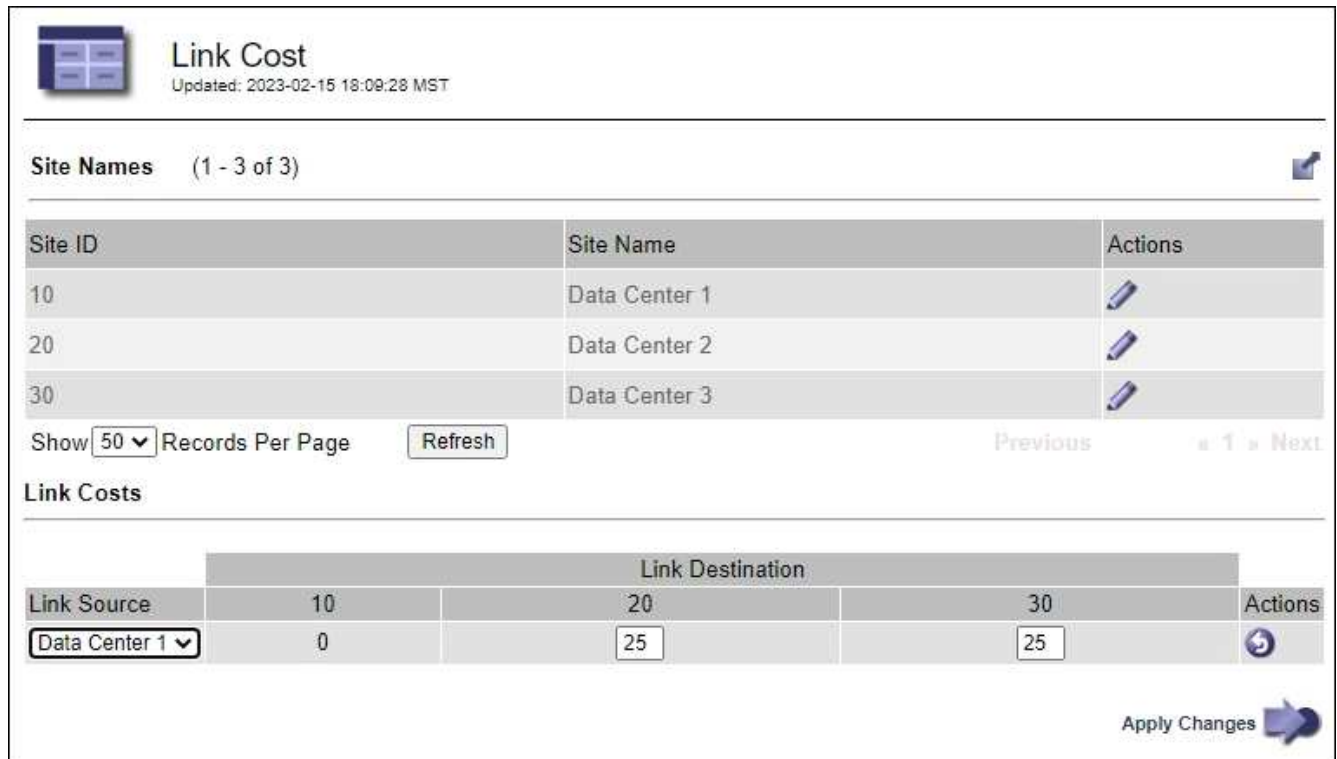
Você pode atualizar os custos de link entre sites de data center para refletir a latência entre sites.

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 **SUORTE > 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 **SUORTE > 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 intercepções 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.

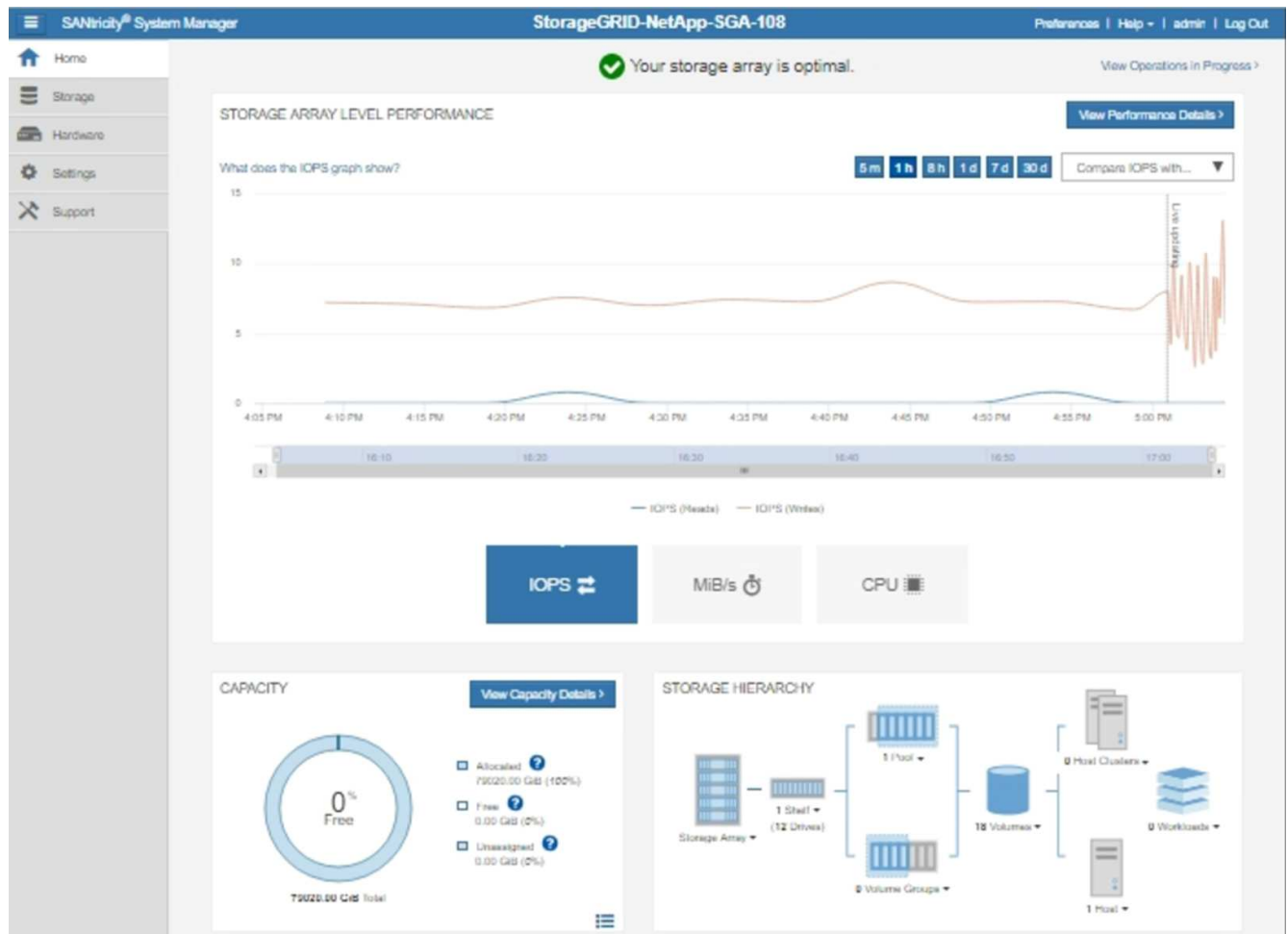


Este procedimento serve apenas para configurar um servidor proxy StorageGRID para pacotes E-Series AutoSupport . Para obter detalhes adicionais sobre a configuração do E-Series AutoSupport , consulte o ["Documentação do NetApp E-Series e SANtricity"](#) .

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.

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:

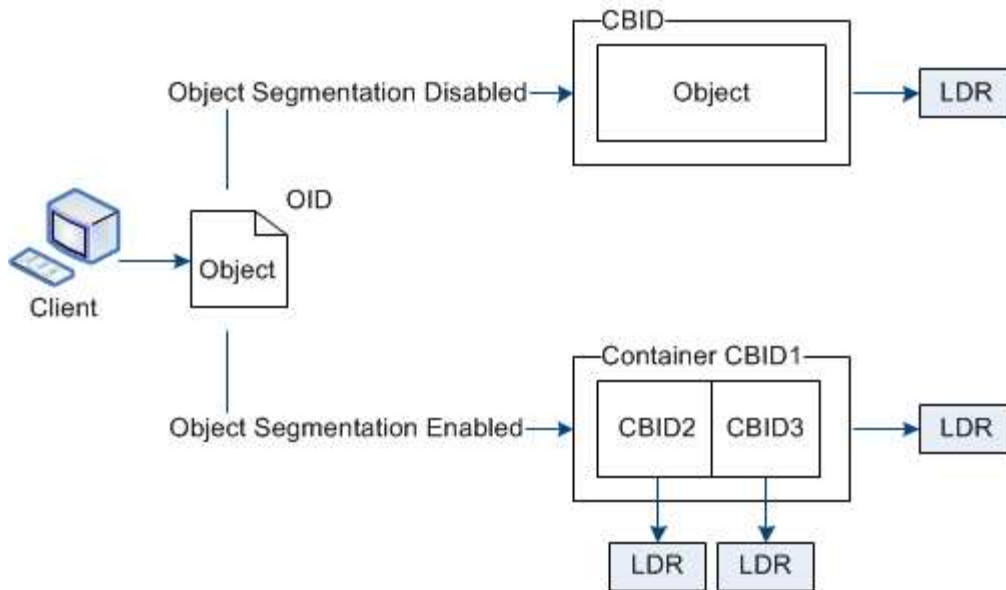
- Gerenciando opções de armazenamento
- Entendendo o que são marcas d'água de volume de armazenamento e como você pode usar substituições de marca d'água para controlar quando os nós de armazenamento se tornam somente leitura
- Monitoramento e gerenciamento do espaço usado para metadados de objetos
- 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 multiparte 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.

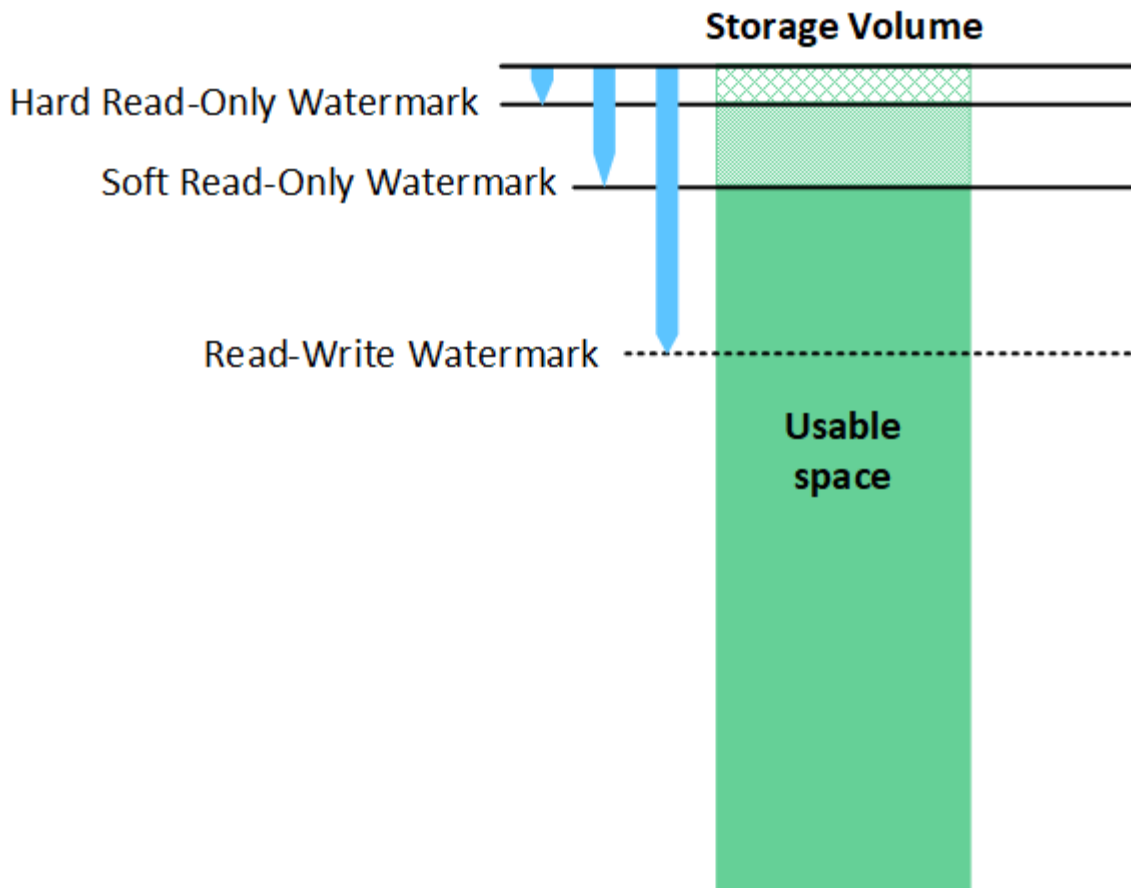
O contêiner e os segmentos não são necessariamente armazenados no mesmo nó de armazenamento. O contêiner e os segmentos podem ser armazenados em qualquer nó de armazenamento dentro do pool de armazenamento especificado na regra ILM.

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 **SUPORTE > 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:

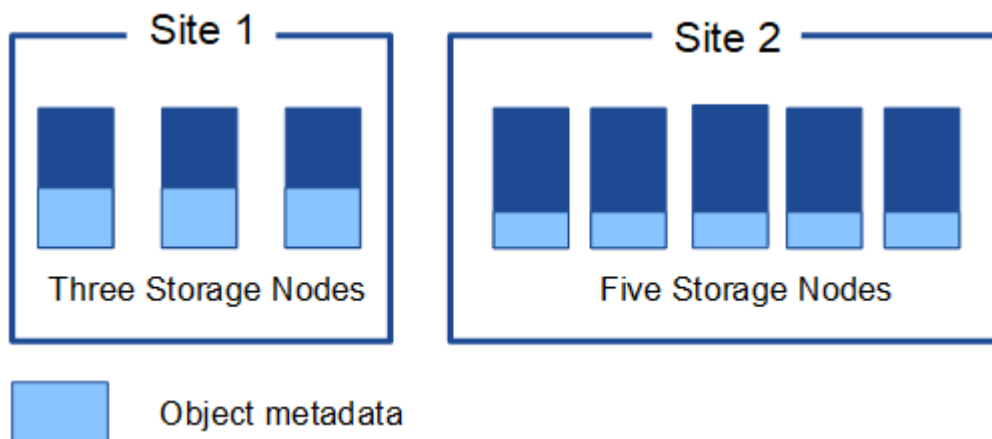
- Metadados do sistema, incluindo um ID exclusivo para cada objeto (UUID), o nome do objeto, o nome do bucket do S3, o nome ou ID da conta do locatário, o tamanho lógico do objeto, a data e a hora em que o objeto foi criado pela primeira vez e a data e a hora em que o objeto foi modificado pela última 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?

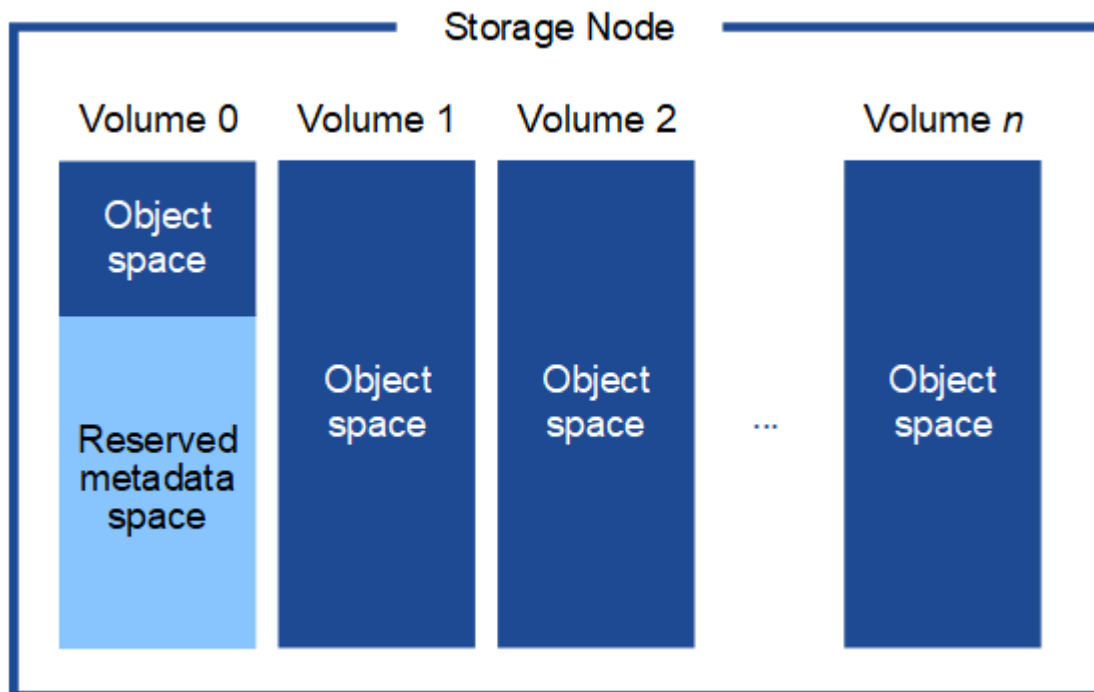
O StorageGRID mantém metadados de objetos em um banco de dados Cassandra, que é armazenado independentemente dos dados do objeto. Para fornecer redundância e proteger os metadados do objeto contra perdas, o StorageGRID armazena três cópias dos metadados para todos os objetos no sistema em cada site.

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.

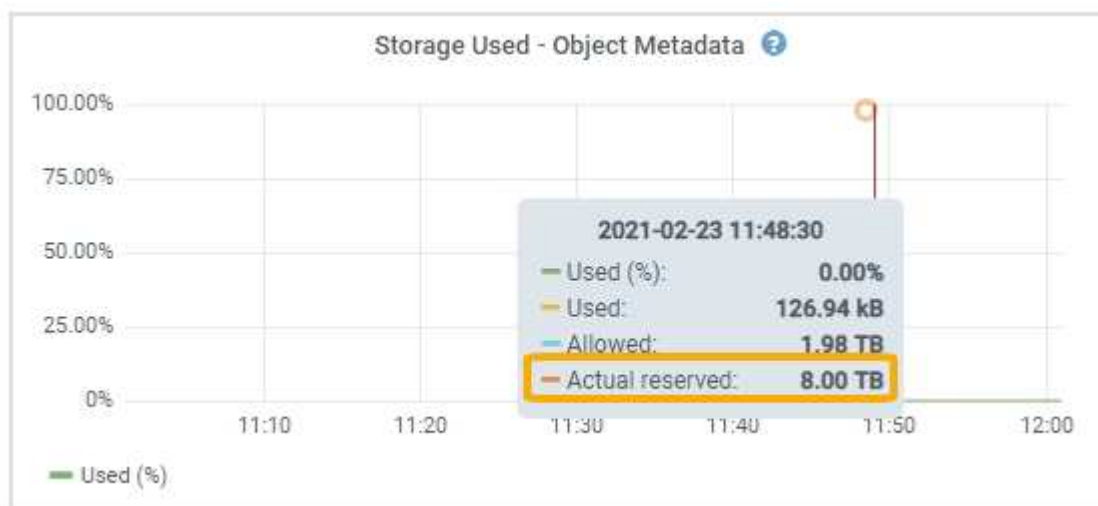
Tamanho do volume 0 para o nó	Espaço real reservado para metadados
Menos de 500 GB (uso não produtivo)	10% do volume 0
500 GB ou mais + ou + Nós de armazenamento somente de metadados	O menor desses valores: • Volume 0 • Configuração de espaço reservado de metadados Observação: somente um rangedb é necessário 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.

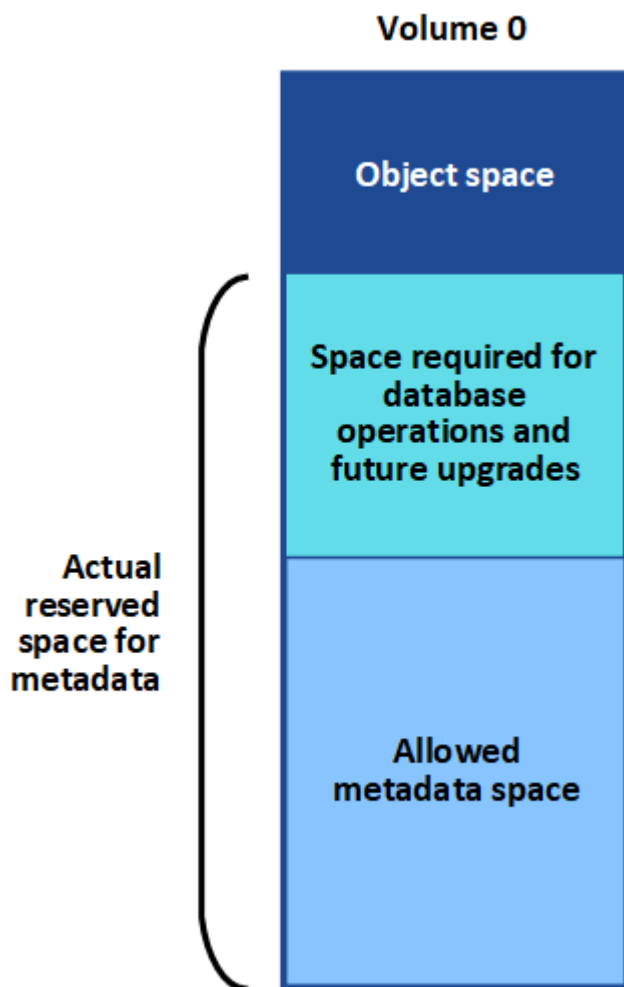
Exemplo de espaço de metadados reservado real

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.

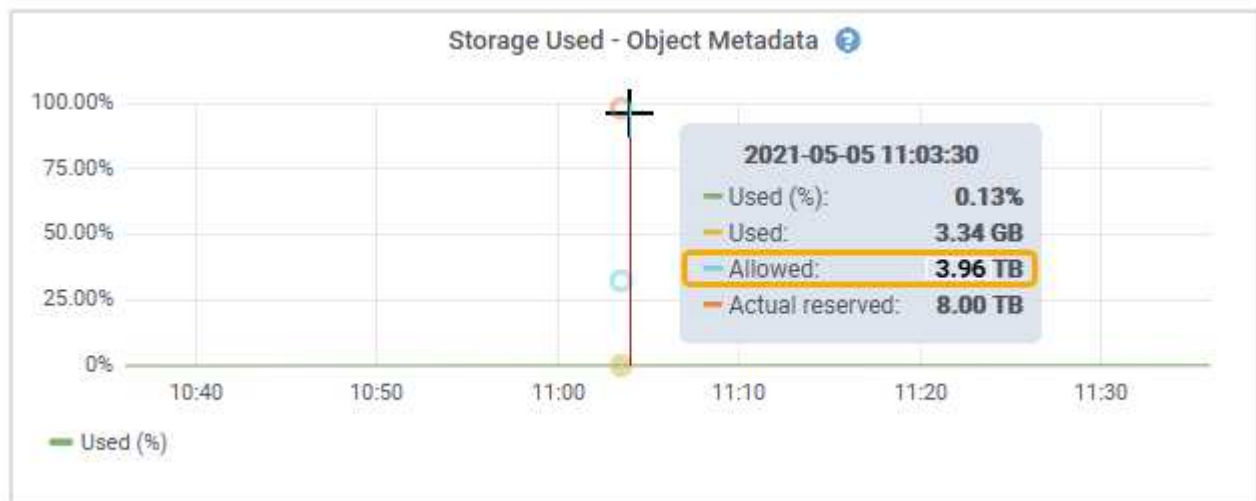
		Quantidade de memória no nó de armazenamento	
	< 128 GB	>= 128 GB	Espaço reservado real para metadados
≤ 4 TB	60% do espaço real reservado para metadados, até um máximo de 1,32 TB	60% do espaço real reservado para metadados, até um máximo de 1,98 TB	4 TB

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

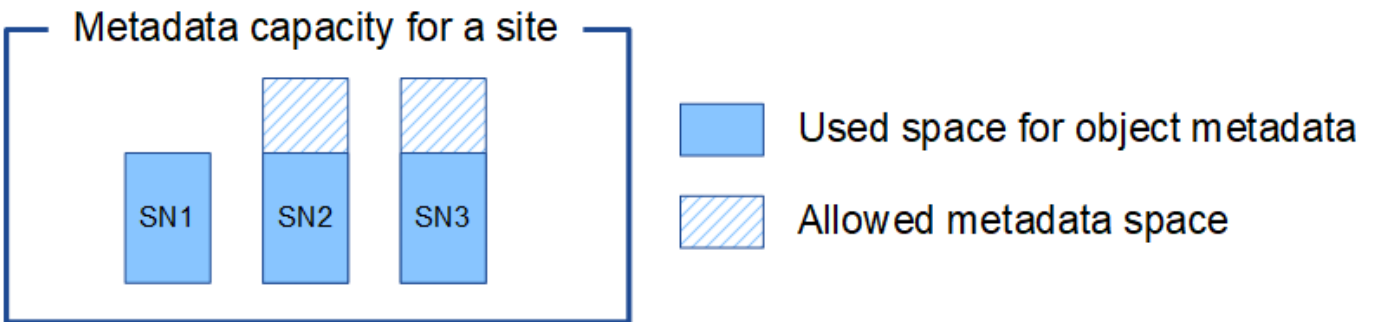
Conforme descrito acima, o StorageGRID distribui uniformemente os metadados dos objetos entre os nós de armazenamento em cada site. Por esse motivo, se um site contiver nós de armazenamento de tamanhos diferentes, o menor nó no site determinará a capacidade de metadados do site.

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.
- Selecione **NODES**.
 - Selecione o primeiro nó de armazenamento na grade.
 - Selecione a aba Armazenamento.
 - Na seção Volumes, localize a entrada **/var/local/rangedb/0**.
 - 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.
- 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.
- Selecione **NODES**.
 - Selecione o primeiro nó de armazenamento na grade.
 - Selecione a aba **Hardware**.
 - Passe o cursor sobre o gráfico de uso de memória. Certifique-se de que a **Memória Total** seja de pelo menos 128 GB.
 - 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.
- Selecione **CONFIGURAÇÃO > Sistema > Opções de armazenamento**.
 - Selecione a aba Configuração.
 - Na seção Marcas d'água de armazenamento, selecione **Espaço reservado para metadados**.
 - 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"](#).

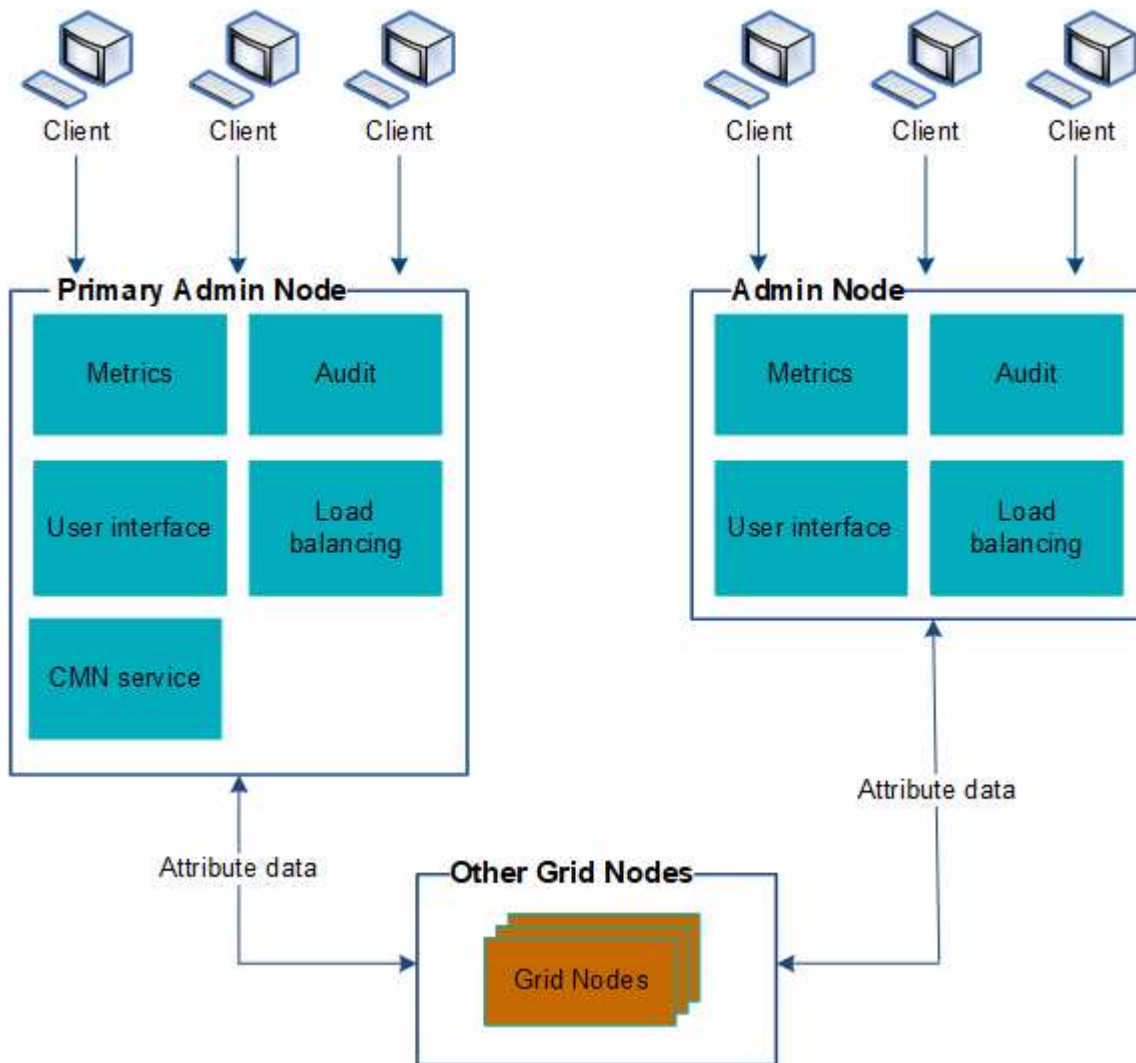
Gerenciar nós de administração

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.

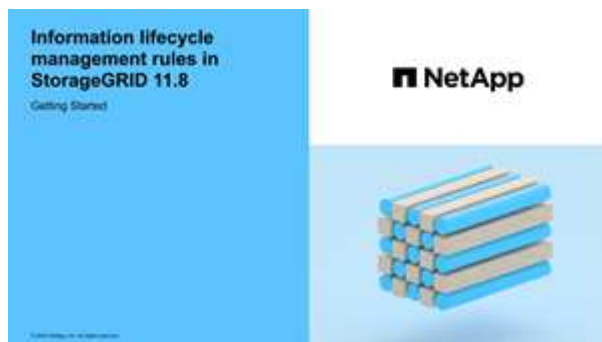
Use estas instruções para:

- 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.

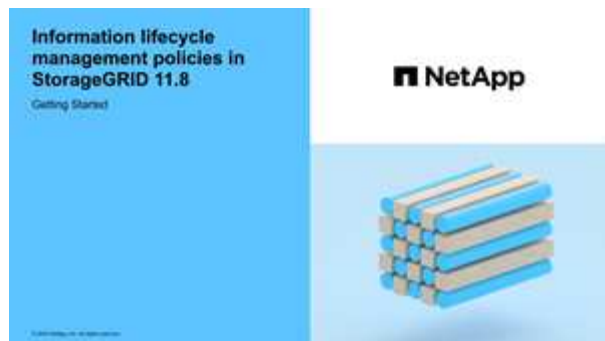
Saber mais

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

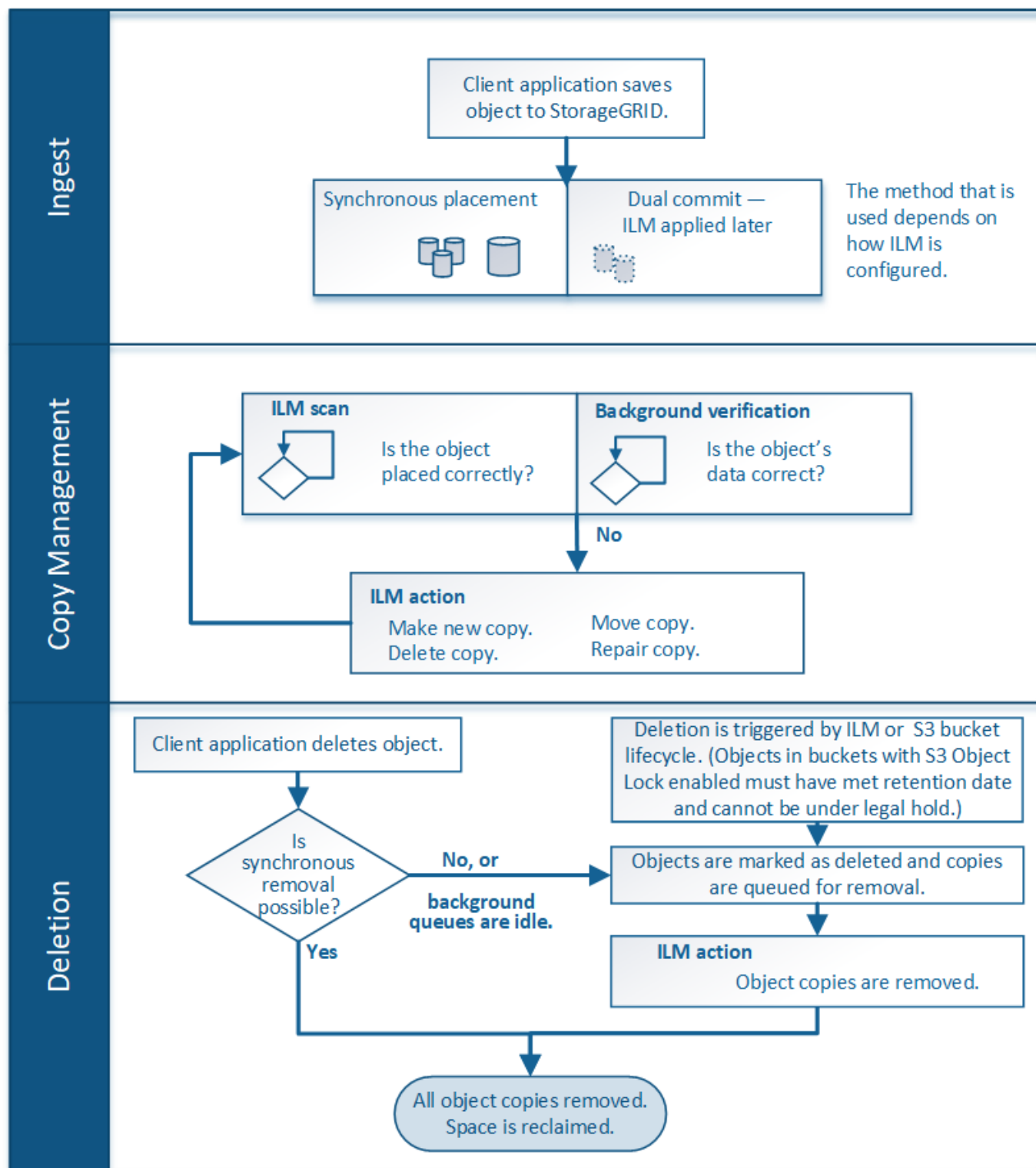
Entender como o StorageGRID usa o ILM para gerenciar objetos durante cada estágio de sua vida útil pode ajudar você a criar uma política mais eficaz.

- **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

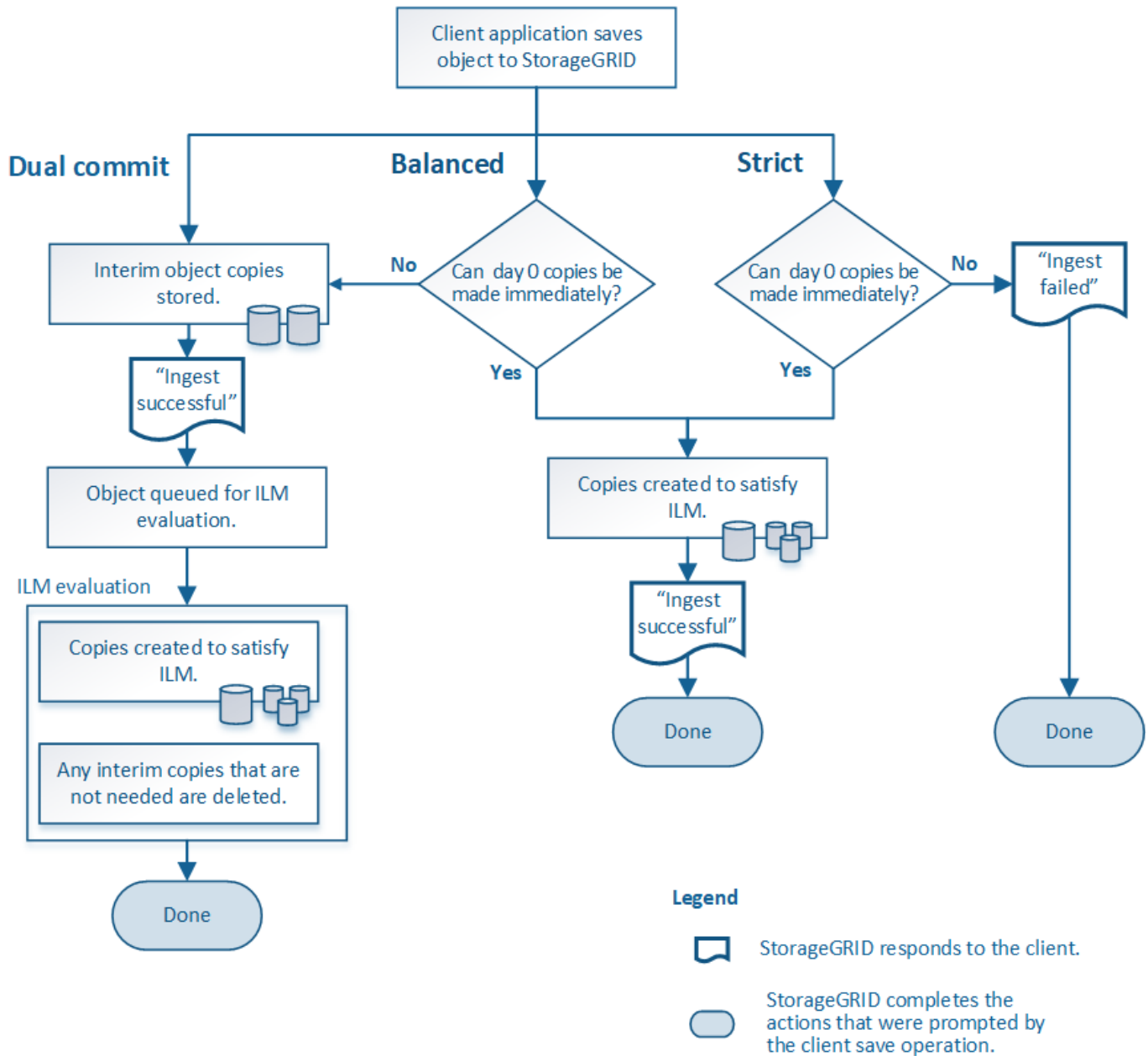
Ao criar uma regra de ILM, você especifica uma das três opções para proteger objetos na ingestão: Confirmação dupla, Estrita ou Balanceada.

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"](#)

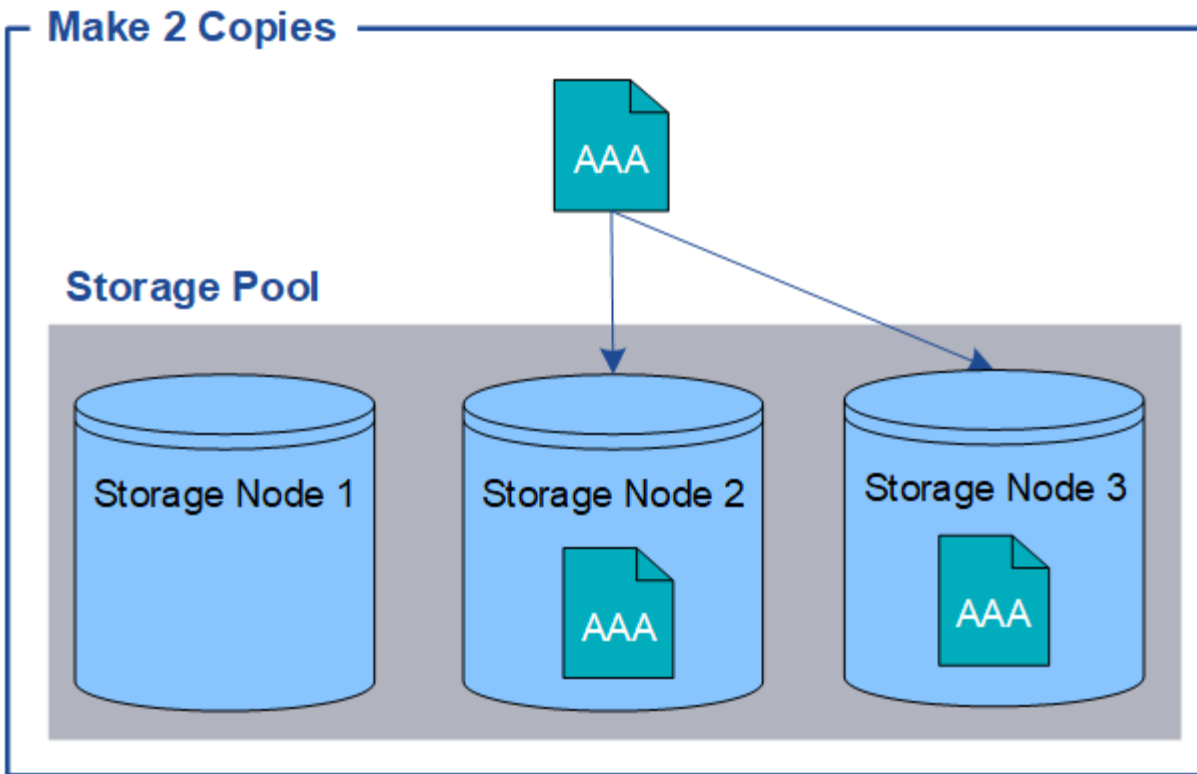
Como os objetos são armazenados (replicação ou codificação de eliminação)

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.



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"](#)

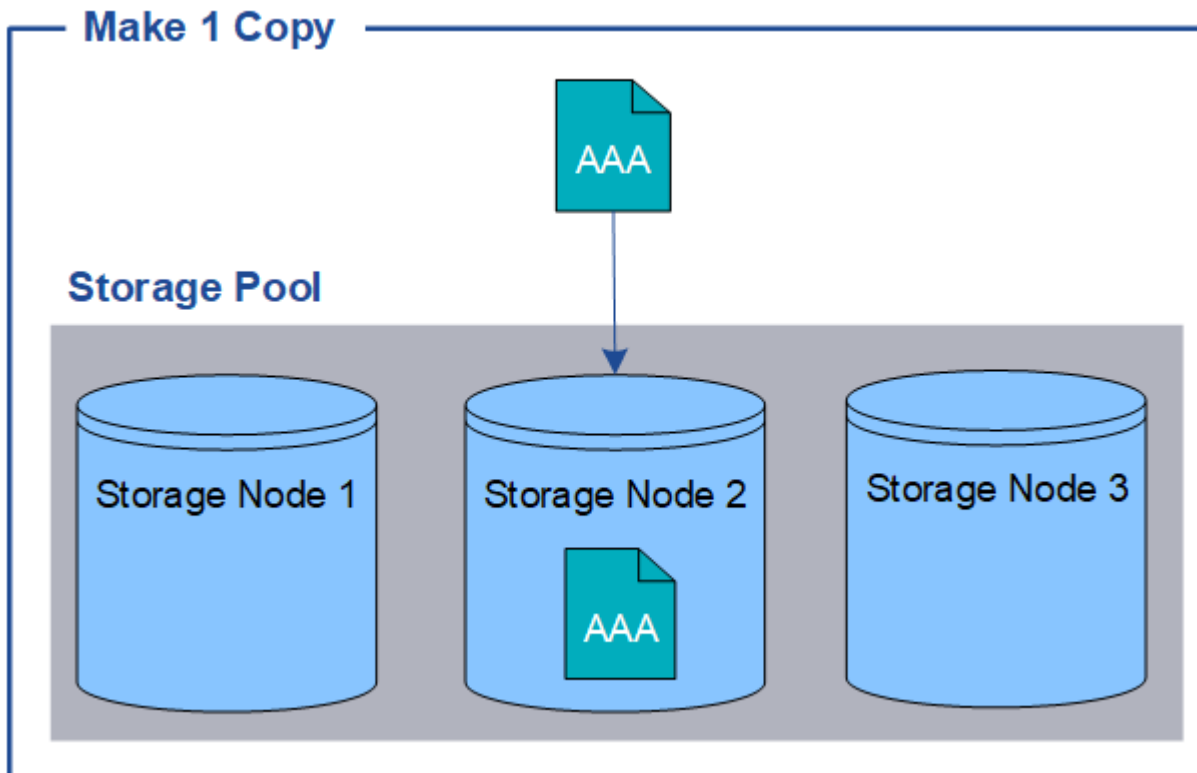
Por que você não deve usar replicação de cópia única

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.

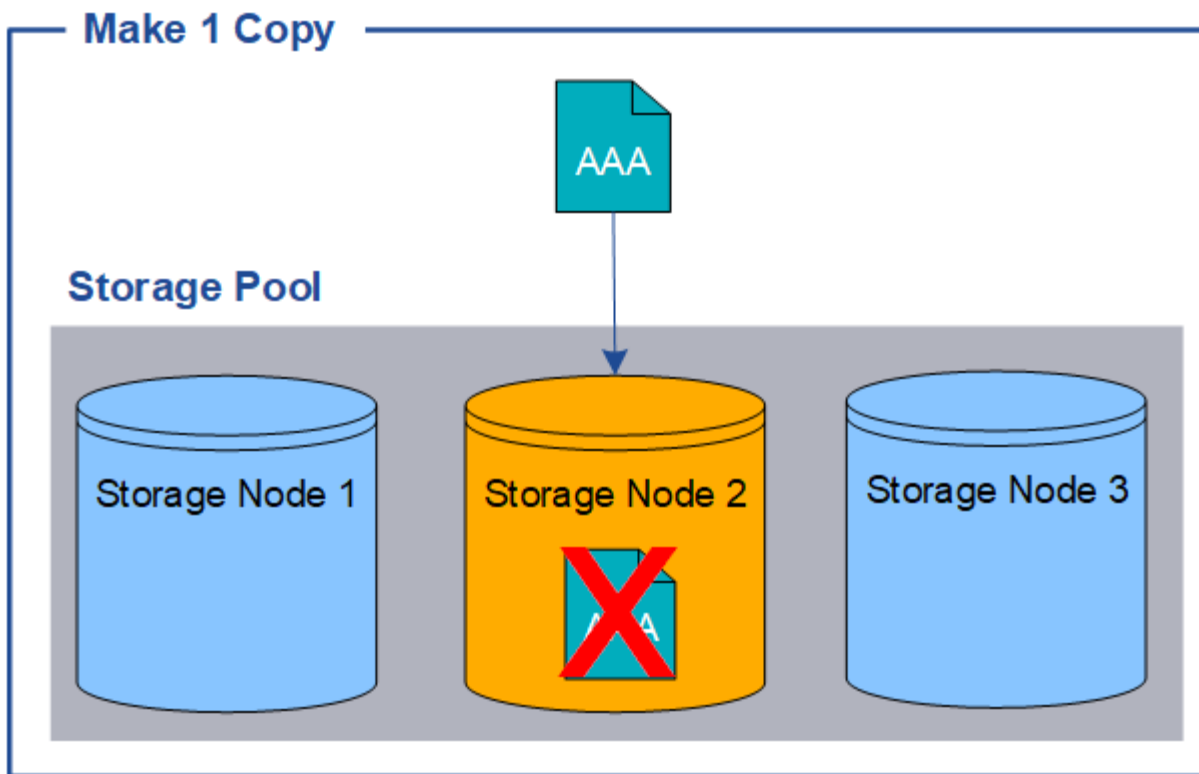


Não use uma regra de ILM que crie apenas uma cópia replicada para qualquer período de tempo. Se existir apenas uma cópia replicada de um objeto, esse objeto será perdido se um nó de armazenamento falhar ou tiver um erro significativo. Você também perde temporariamente o acesso ao objeto durante procedimentos de manutenção, como atualizações.

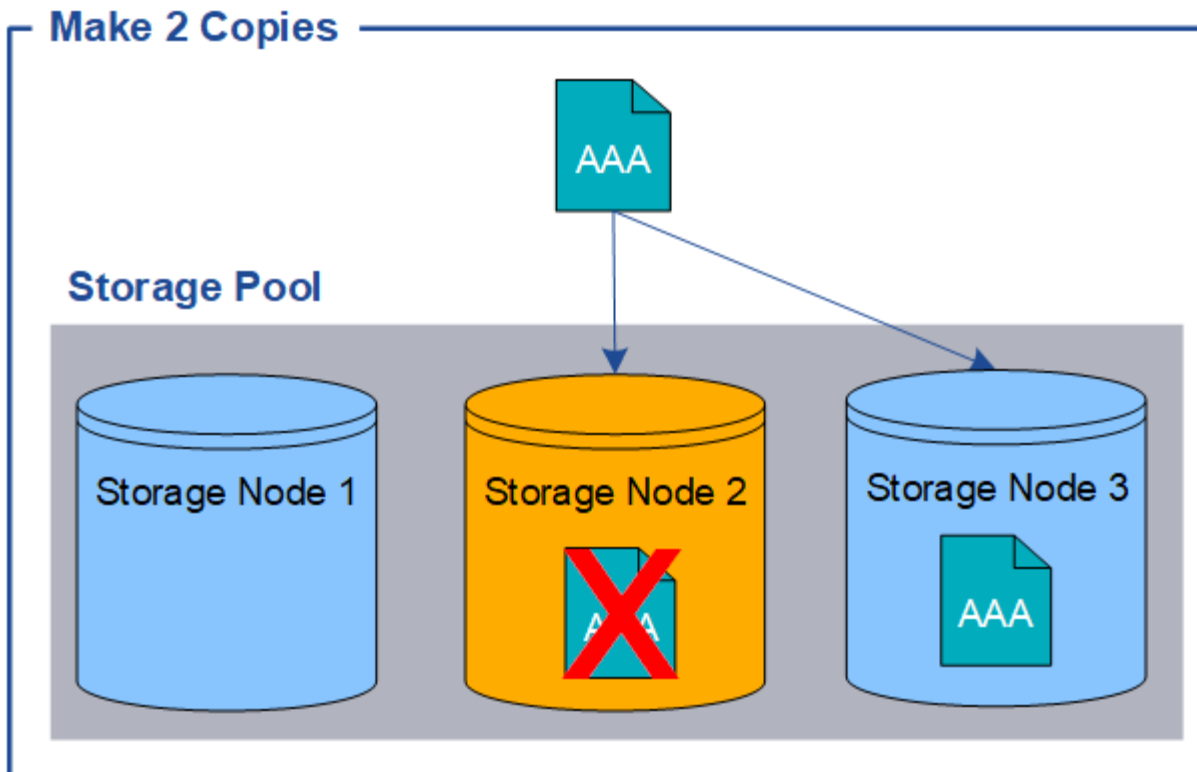
No exemplo a seguir, a regra Make 1 Copy ILM especifica que uma cópia replicada de um objeto seja colocada em um pool de armazenamento que contém três nós de armazenamento. Quando um objeto que corresponde a essa regra é ingerido, o StorageGRID coloca uma única cópia em apenas um nó de armazenamento.



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.



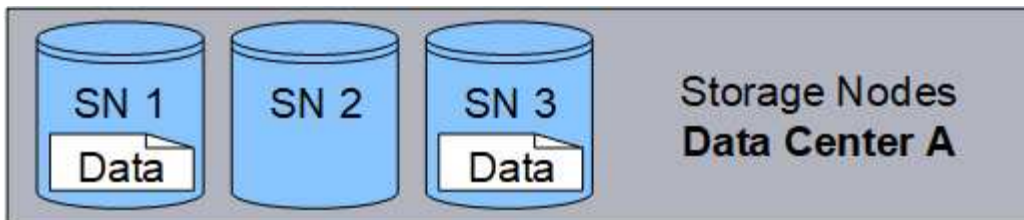
O que é codificação de eliminação?

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.

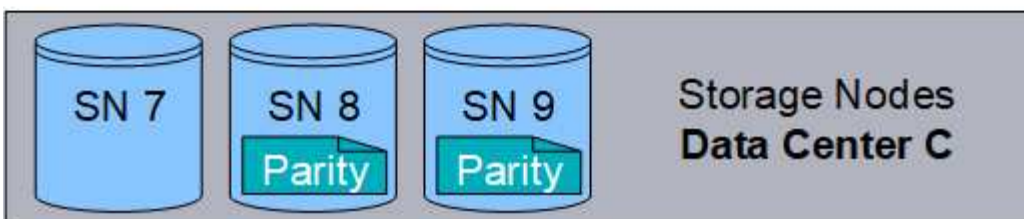
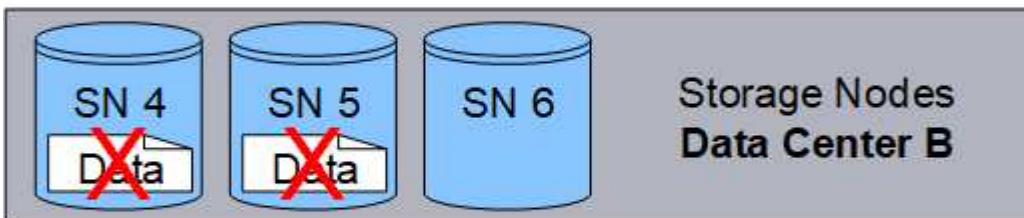
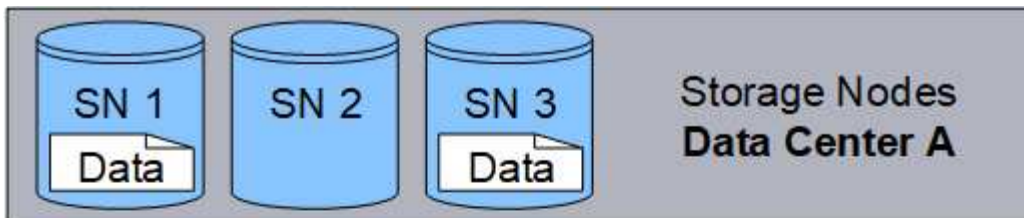
Quando um objeto é acessado, ele é remontado usando os fragmentos armazenados. Se um dado ou um fragmento de paridade for corrompido ou perdido, o algoritmo de codificação de eliminação pode recriar esse fragmento usando um subconjunto dos dados e fragmentos de paridade restantes.

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"](#).

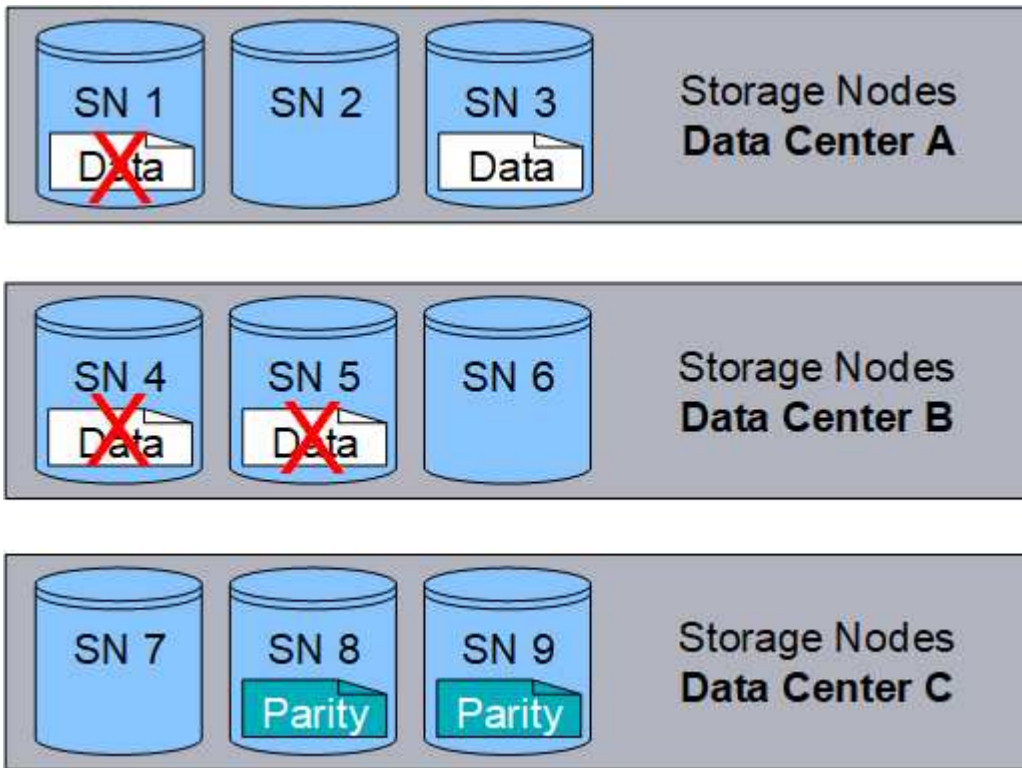
O exemplo a seguir ilustra o uso de um algoritmo de codificação de eliminação nos dados de um objeto. Neste exemplo, a regra ILM usa um esquema de codificação de eliminação 4+2. Cada objeto é dividido em quatro fragmentos de dados iguais, e dois fragmentos de paridade são computados a partir dos dados 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 cálculos 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](#)".

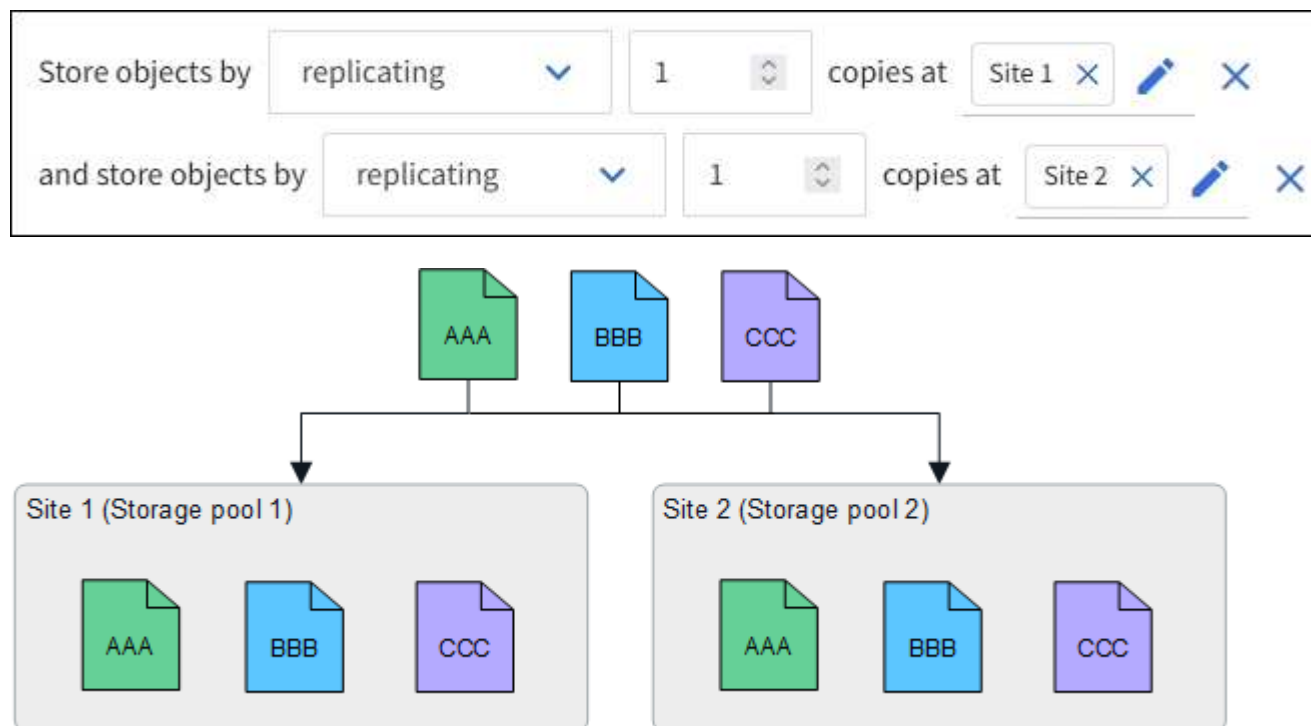
Exemplo de replicação

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:



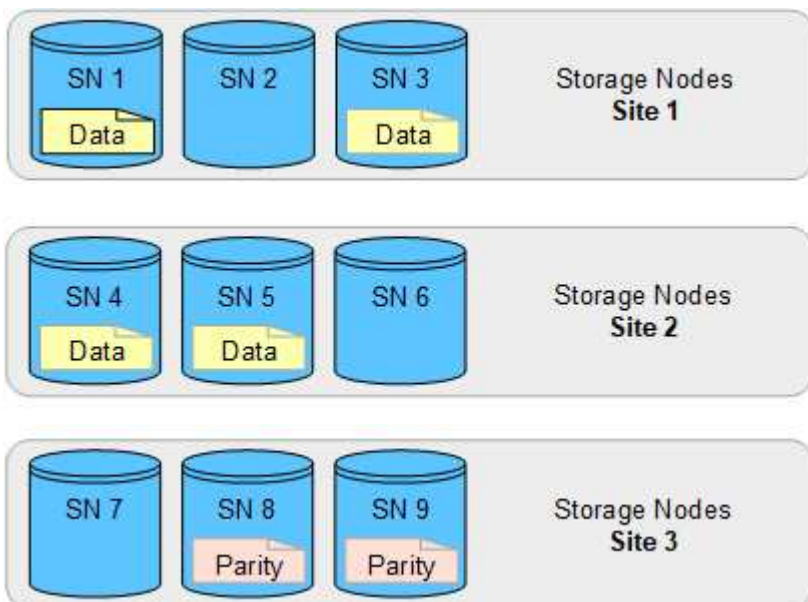
Neste exemplo:

- 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.

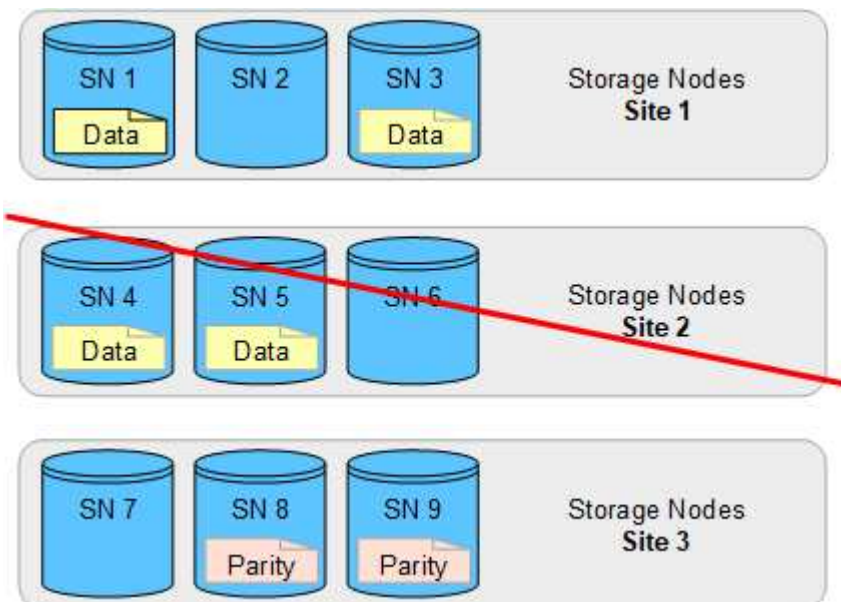


A codificação de eliminação é permitida em pools de armazenamento que contêm qualquer número de sites *exceto* dois sites.

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

- Nome da conta:** Insira o nome da conta de armazenamento que possui o contêiner externo
- 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.

4. 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.

5. 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.
- **Rigoroso:** 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.

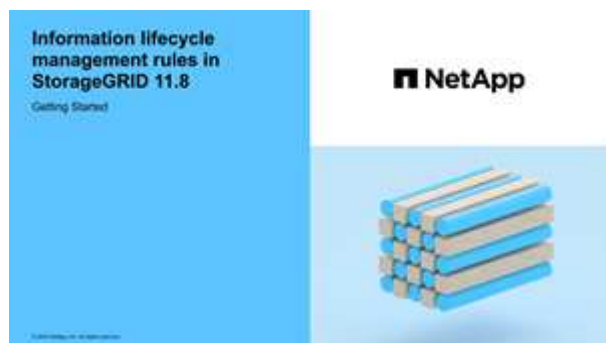


Se você quiser criar a regra ILM padrão para uma política, siga o ["instruções para criar uma regra ILM padrão"](#) em vez de.

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.

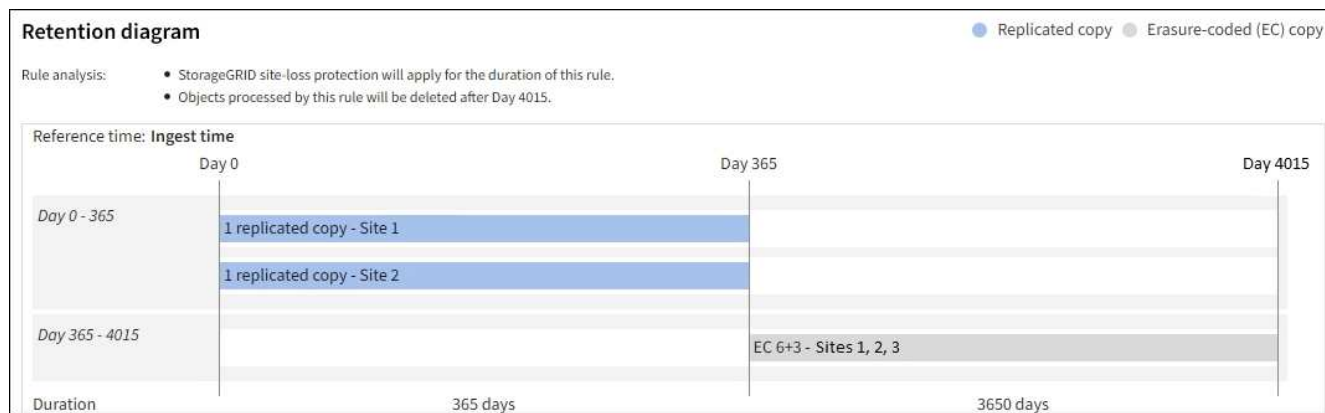
7. No diagrama de retenção, confirme suas instruções de posicionamento.

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

Example ILM policy

Reason for change

Example

Manage rules

1. Select the rules you want to add to the policy.

2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	↕ EC for test-tenant-1	Tenant is test-tenant-1
Default	Default rule	—

Ao criar a regra padrão, tenha em mente 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 irrecoverável 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"](#).

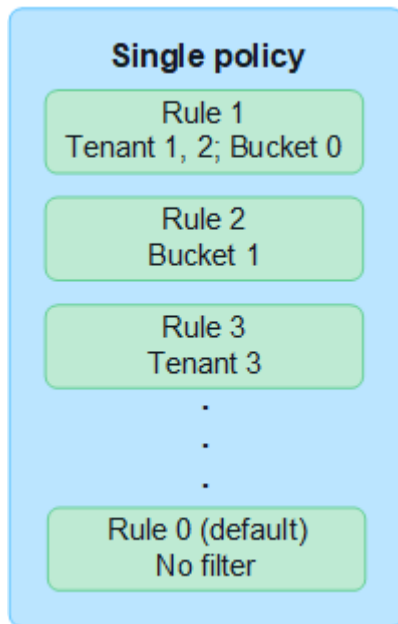
Uma ou muitas políticas de ILM ativas?

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.

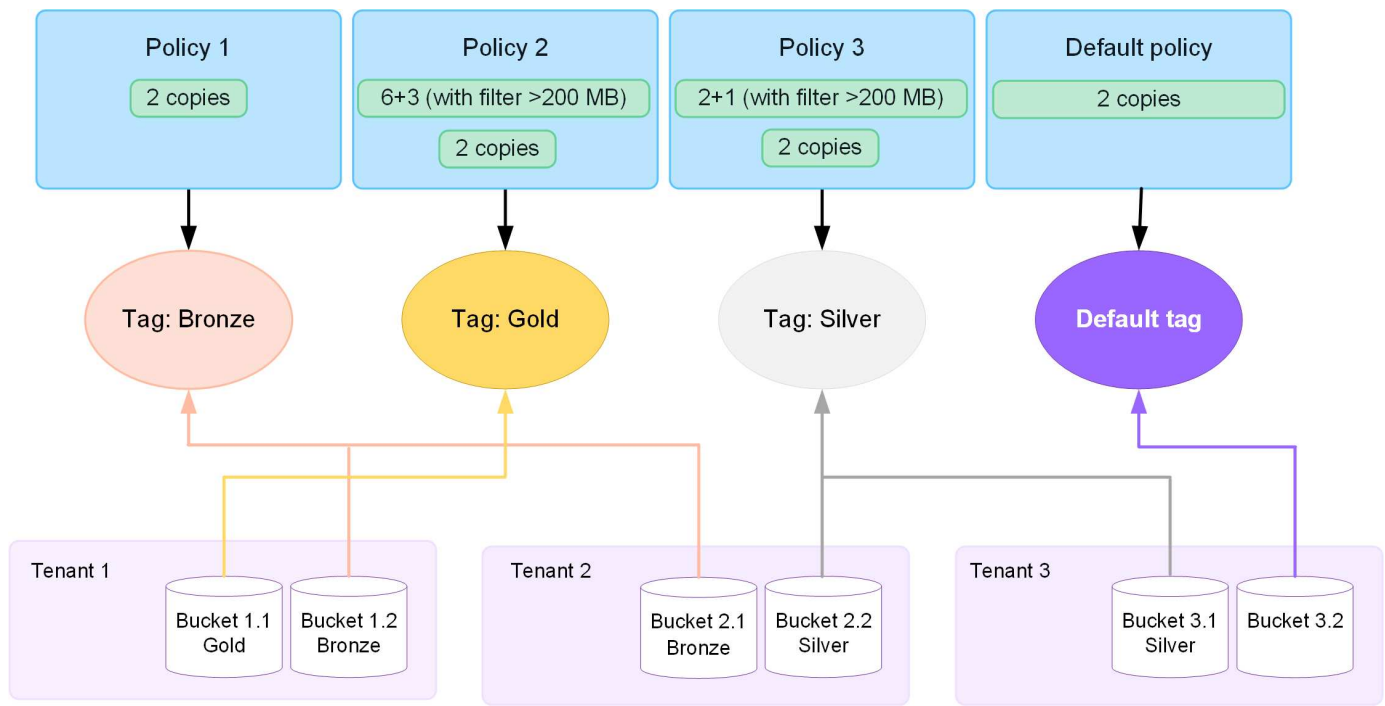
Tags de política do ILM

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

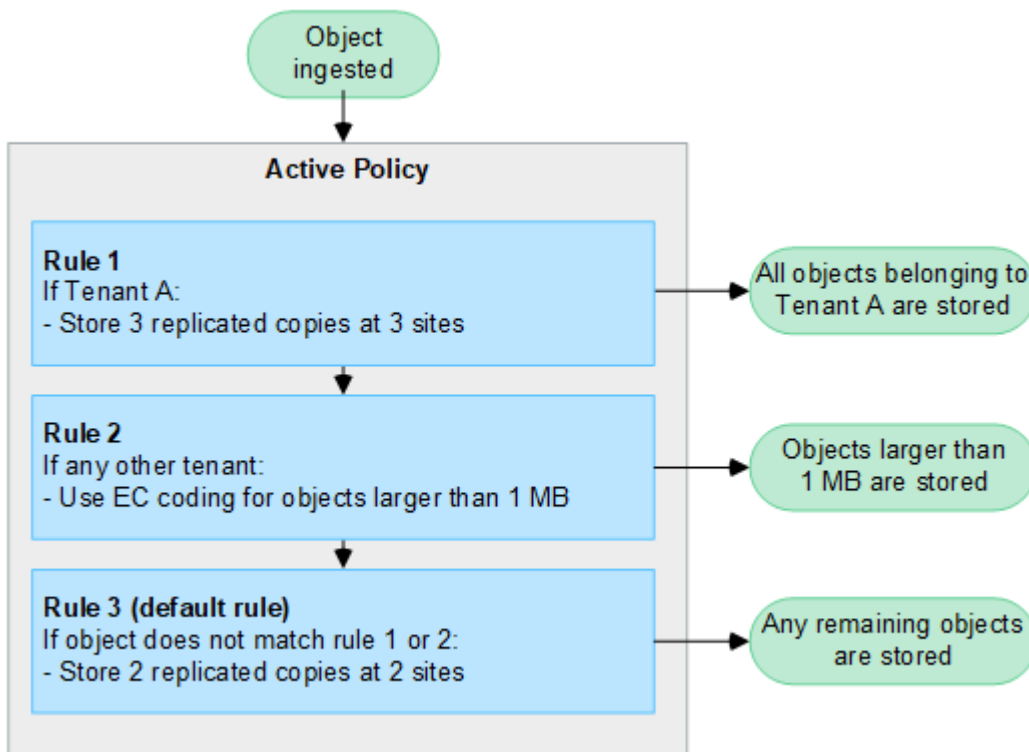
Por exemplo, uma política de ILM pode conter três regras de ILM que especificam o seguinte:

- **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.

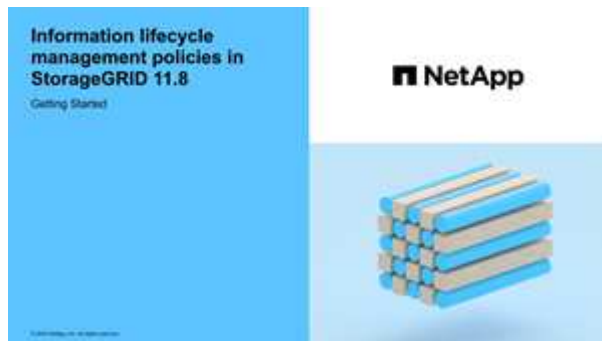
Bloqueio de objeto S3 não habilitado

- 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": "CTNT",
  "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

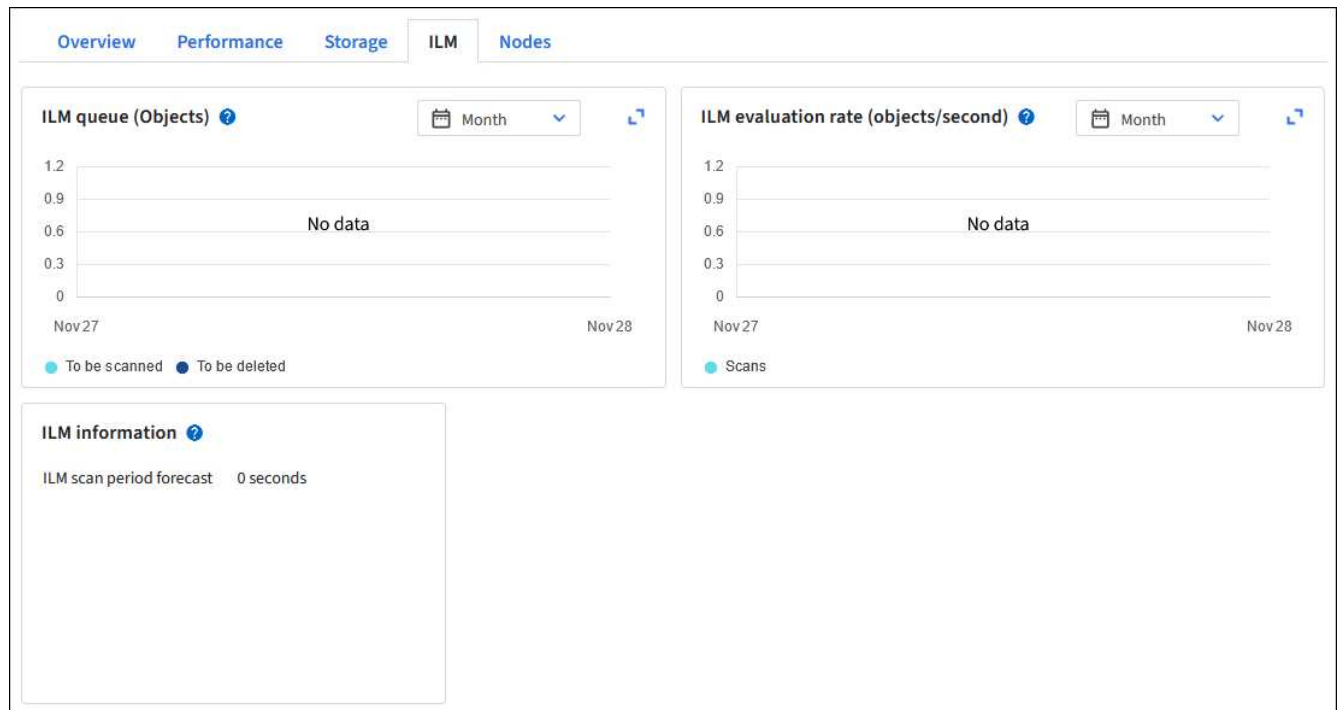
1. Selecione **Painel > ILM**.



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-ingridos 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

720

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, localtário 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 localtário 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 localtário. 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 localtário e um bucket diferentes para cada nível local

Para usar mais de um localtário 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 localtário, 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"](#) .

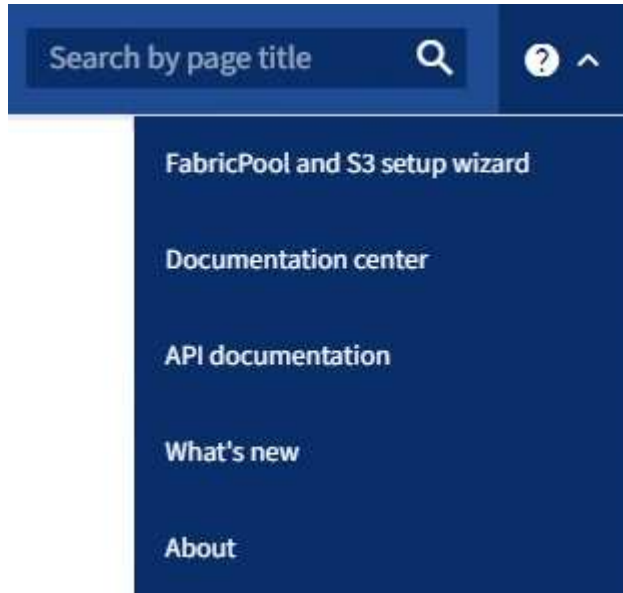
- Você tem o ["Permissão de acesso root"](#) .

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 [Etapas 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

- a. Para criar um novo grupo HA, selecione **Criar grupo HA**.
- b. 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.

- c. 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.

- d. 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.

- e. 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 localitário 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	Dois 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.
 - a. Anexe um ou mais agregados à camada de nuvem.
 - b. 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.

Use locatários e clientes do StorageGRID

Use uma conta de inquilino

Use uma conta de inquilino

Uma conta de locatário permite que você use a API REST do Simple Storage Service (S3) ou a API REST do Swift para armazenar e recuperar objetos em um sistema StorageGRID .

O que é uma conta de inquilino?

Cada conta de locatário tem seus próprios grupos federados ou locais, usuários, buckets S3 ou contêineres Swift 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 o sistema StorageGRID estiver sendo usado dentro de uma empresa, o armazenamento de objetos da grade pode ser segregado pelos diferentes departamentos da organização. Por exemplo, pode haver contas de inquilinos 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, também poderá usar buckets e políticas de bucket do S3 para segregar objetos entre os departamentos de uma empresa. Você não precisa criar contas de inquilino separadas. Veja as instruções para implementação "[Buckets S3 e políticas de bucket](#)" para mais informações.

- **Caso de uso do provedor de serviços:** Se o sistema StorageGRID estiver sendo usado por um provedor de serviços, o armazenamento de objetos da grade poderá ser segregado pelas diferentes entidades que alugam o armazenamento. Por exemplo, pode haver contas de inquilinos para a Empresa A, Empresa B, Empresa C e assim por diante.

Como criar uma conta de inquilino

As contas de inquilino são criadas por um "[Administrador de grade StorageGRID usando o Grid Manager](#)". Ao criar uma conta de locatário, o administrador da grade especifica o seguinte:

- 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, os administradores de grade podem 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.

Configurar locatários do S3

Depois de um ["A conta do locatário S3 foi criada"](#), você pode acessar o Gerenciador de Inquilinos 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 você possa criar e gerenciar buckets S3 com o Tenant Manager, você deve usar um ["Cliente S3"](#) ou ["Console S3"](#) para ingerir e gerenciar objetos.

Como entrar e sair

Sign in no Gerenciador de Inquilinos

Você acessa o Tenant Manager inserindo a URL do inquilino na barra de endereço de um ["navegador da web compatível"](#).

Antes de começar

- Você tem suas credenciais de login.
- Você tem uma URL para acessar o Gerenciador de Tenants, fornecida pelo administrador da sua grade. O URL será semelhante a um destes exemplos:

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

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

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

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

A URL sempre inclui um nome de domínio totalmente qualificado (FQDN), o endereço IP de um nó administrativo ou o endereço IP virtual de um grupo HA de nós administrativos. Também pode incluir um número de porta, o ID da conta do locatário de 20 dígitos ou ambos.

- Se a URL não incluir o ID da conta de 20 dígitos do locatário, você terá esse ID de conta.
- Você está usando um ["navegador da web compatível"](#).
- Os cookies estão habilitados no seu navegador.
- Você pertence a um grupo de usuários que tem ["permissões de acesso específicas"](#).

Passos

1. Lançar um ["navegador da web compatível"](#).

2. Na barra de endereço do navegador, digite o URL para acessar o Tenant Manager.
3. Se você receber um alerta de segurança, instale o certificado usando o assistente de instalação do navegador.
4. Sign in no Gerenciador de Inquilinos.

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

Não usar SSO

Se o StorageGRID não estiver usando SSO, uma das seguintes telas será exibida:

- Página de login do Grid Manager. Selecione o link **Login do locatário**.



NetApp StorageGRID®

Grid Manager

Username

Password

Sign in

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

- Página de login do Gerenciador de inquilinos. O campo **Conta** pode já estar preenchido, conforme mostrado abaixo.

The screenshot shows the NetApp StorageGRID Tenant Manager login interface. At the top is the NetApp StorageGRID logo. Below it is the title 'Tenant Manager'. The form includes a 'Recent' section with a dropdown menu currently showing '-- Optional --'. Below that is an 'Account' field containing the 20-digit ID '64600207336181242061'. This is followed by 'Username' and 'Password' input fields. A blue 'Sign in' button is positioned below the password field. At the bottom of the form, there are links for 'NetApp support' and 'NetApp.com'.

- i. Se o ID da conta de 20 dígitos do locatário não for exibido, selecione o nome da conta do locatário se ele aparecer na lista de contas recentes ou insira o ID da conta.
- ii. Digite seu nome de usuário e senha.
- iii. Selecione * Sign in*.

O painel do Gerenciador de inquilinos é exibido.

- iv. Se você recebeu uma senha inicial de outra pessoa, selecione **nome de usuário > Alterar senha** para proteger sua conta.

Usando SSO

Se o StorageGRID estiver usando SSO, uma das seguintes telas será exibida:

- Página SSO da sua organização. Por exemplo:

Sign in with your organizational account

someone@example.com

Password

Sign in

Insira suas credenciais SSO padrão e selecione * Sign in*.

- Página de login do Tenant Manager SSO.



- Se o ID da conta de 20 dígitos do locatário não for exibido, selecione o nome da conta do locatário se ele aparecer na lista de contas recentes ou insira o ID da conta.
- Selecione * Sign in*.
- Sign in com suas credenciais SSO padrão na página de login SSO da sua organização.

O painel do Gerenciador de inquilinos é exibido.

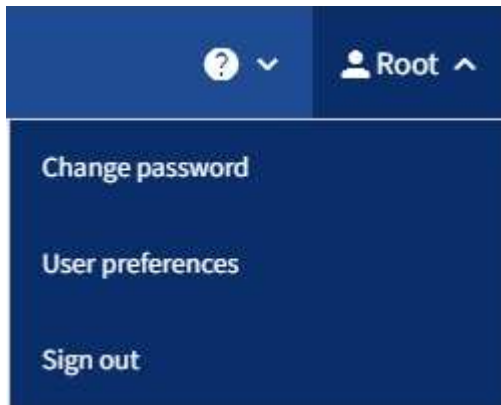
Sair do Gerenciador de Inquilinos

Quando terminar de trabalhar com o Tenant Manager, você deverá 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. Localize o menu suspenso de nome de usuário no canto superior direito da interface do usuário.



2. Selecione o nome de usuário e depois selecione **Sair**.

- Se o SSO não estiver em uso:

Você está desconectado do nó de administração. A página de login do Gerenciador de inquilinos é exibida.



Se você tiver entrado em mais de um nó de administração, será necessário sair de cada nó.

- Se o SSO estiver habilitado:

Você está desconectado de todos os nós de administração que estava acessando. A página de Sign in do StorageGRID é exibida. O nome da conta do locatário que você acabou de acessar é listado como padrão no menu suspenso **Contas recentes**, e o **ID da conta** do locatário é exibido.



Se o SSO estiver habilitado e você também estiver conectado ao Grid Manager, você também deverá sair do Grid Manager para sair do SSO.

Entenda o painel do Tenant Manager

O painel do Tenant Manager fornece uma visão geral da configuração de uma conta de locatário e da quantidade de espaço usado por objetos nos buckets (S3) ou contêineres (Swift) do locatário. Se o locatário tiver uma cota, o painel mostrará quanto da cota foi usado e quanto resta. Se houver algum erro relacionado à conta do locatário, os erros serão exibidos no painel.



Os valores do Espaço utilizado são estimativas. Essas estimativas são afetadas pelo tempo de ingestão, pela conectividade de rede e pelo status do nó.

Quando os objetos são carregados, o painel fica como no exemplo a seguir:

Dashboard

16 Buckets
[View buckets](#)

2 Platform services
endpoints
[View endpoints](#)

0 Groups
[View groups](#)

1 User
[View users](#)

Storage usage ?

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage ?

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details ?

Name: Tenant02
ID: 3341 1240 0546 8283 2208
✓ Platform services enabled
✓ Can use own identity source
✓ S3 Select enabled

Informações da conta do inquilino

A parte superior do painel exibe o número de buckets ou contêineres, grupos e usuários configurados. Ele também exibe o número de pontos de extremidade de serviços de plataforma, se algum tiver sido configurado. Selecione os links para ver os detalhes.

Dependendo do "[permissões de gerenciamento de inquilinos](#)" você tem e as opções que você configurou, o restante do painel exibe várias combinações de diretrizes, uso de armazenamento, informações de objeto e detalhes do locatário.

Armazenamento e uso de cota

O painel de uso de armazenamento contém as seguintes informações:

- A quantidade de dados de objeto para o locatário.

Este valor indica a quantidade total de dados de objetos carregados e não representa o espaço usado para armazenar cópias desses objetos e seus metadados.

- Se uma cota for definida, a quantidade total de espaço disponível para dados de objeto e a quantidade e a porcentagem de espaço restante. A cota limita a quantidade de dados de objetos que podem ser ingeridos.



O uso da cota é baseado em estimativas internas e pode ser excedido em alguns casos. Por exemplo, o StorageGRID verifica a cota quando um locatário começa a carregar objetos e rejeita novas ingestões se o locatário tiver excedido a cota. No entanto, o StorageGRID não leva em consideração o tamanho do upload atual ao determinar se a cota foi excedida. Se os objetos forem excluídos, um locatário poderá ser temporariamente impedido de carregar novos objetos até que o uso da cota seja recalculado. Os cálculos de uso de cota podem levar 10 minutos ou mais.

- Um gráfico de barras que representa os tamanhos relativos dos maiores baldes ou recipientes.

Você pode colocar o cursor sobre qualquer um dos segmentos do gráfico para visualizar o espaço total consumido por aquele bucket ou contêiner.



- Para corresponder ao gráfico de barras, uma lista dos maiores buckets ou contêineres, incluindo a quantidade total de dados do objeto e o número de objetos para cada bucket ou contêiner.

Bucket name	Space used	Number of objects
 Bucket-02	944.7 GB	7,575
 Bucket-09	899.6 GB	589,677
 Bucket-15	889.6 GB	623,542
 Bucket-06	846.4 GB	648,619
 Bucket-07	730.8 GB	808,655
 Bucket-04	700.8 GB	420,493
 Bucket-11	663.5 GB	993,729
 Bucket-03	656.9 GB	379,329
 9 other buckets	2.3 TB	5,171,588

Se o inquilino tiver mais de nove baldes ou contêineres, todos os outros baldes ou contêineres serão combinados em uma única entrada na parte inferior da lista.



Para alterar as unidades dos valores de armazenamento exibidos no Gerenciador de Tenants, selecione o menu suspenso do usuário no canto superior direito do Gerenciador de Tenants e selecione **Preferências do usuário**.

Alertas de uso de cota

Se os alertas de uso de cota tiverem sido habilitados no Grid Manager, esses alertas aparecerão no Tenant Manager quando a cota estiver baixa ou for excedida, da seguinte forma:

- Se 90% ou mais da cota de um locatário tiver sido usada, o alerta **Uso alto da cota do locatário** será acionado.

Considere pedir ao administrador da sua rede para aumentar a cota.

- Se você exceder sua cota, uma notificação informará que você não poderá carregar novos objetos.

Uso do limite de capacidade

Se você definiu um limite de capacidade para seus buckets, o painel do Gerenciador de Tenants exibirá uma lista dos principais buckets por uso de limite de capacidade.

Se nenhum limite for definido para um bucket, sua capacidade será ilimitada. No entanto, se sua conta de locatário tiver uma cota total de armazenamento e essa cota for atingida, você não poderá ingerir mais objetos, independentemente do limite de capacidade restante em um bucket.

Erros de endpoint

Se você usou o Grid Manager para configurar um ou mais endpoints para uso com serviços de plataforma, o painel do Tenant Manager exibirá um alerta se algum erro de endpoint tiver ocorrido nos últimos sete dias.



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.

Para ver detalhes sobre "erros de ponto de extremidade de serviços de plataforma", selecione **Endpoints** para exibir a página Endpoints.

API de gerenciamento de inquilinos

Entenda a API de gerenciamento de locatários

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

API de gerenciamento de inquilinos:

- Utiliza a plataforma de API de código aberto Swagger. O Swagger fornece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores interajam com a API. A interface de usuário do Swagger fornece detalhes completos e documentação para cada operação de API.
- Usos "controle de versão para oferecer suporte a atualizações não disruptivas".

Para acessar a documentação do Swagger para a API de gerenciamento de locatários:

1. Sign in no Gerenciador de Inquilinos.
2. Na parte superior do Gerenciador de Tenants, selecione o ícone de ajuda e selecione **Documentação da API**.

Operações de API

A API de gerenciamento de locatários organiza as operações de API disponíveis nas seguintes seções:

- **conta:** Operações na conta do locatário atual, incluindo obtenção de informações de uso de armazenamento.
- **auth:** Operações para realizar autenticação de sessão do usuário.

A API de gerenciamento de locatários oferece suporte ao esquema de autenticação de token de portador. Para um login de locatário, você fornece um nome de usuário, senha e accountId 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").

Para obter informações sobre como melhorar a segurança da autenticação, consulte ["Proteja-se contra falsificação de solicitação entre sites"](#).



Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Veja o ["instruções para usar a API de gerenciamento de grade"](#).

- **config:** Operações relacionadas ao lançamento do produto e versões da API de gerenciamento de locatários. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **contêineres:** Operações em buckets S3 ou contêineres Swift.
- **deactivated-features:** Operações para visualizar recursos que podem ter sido desativados.
- **endpoints:** Operações para gerenciar um endpoint. Os endpoints permitem que um bucket S3 use um serviço externo para replicação, notificações ou integração de pesquisa do StorageGRID CloudMirror.
- **grid-federation-connections:** Operações em conexões de federação de rede e replicação entre redes.
- **grupos:** Operações para gerenciar grupos de inquilinos locais e recuperar grupos de inquilinos federados de uma fonte de identidade externa.
- **identity-source:** Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupos federados e usuários.
- **ilm:** Operações em configurações de gerenciamento do ciclo de vida da informação (ILM).
- **regiões:** Operações para determinar quais regiões foram configuradas para o sistema StorageGRID.
- **s3:** Operações para gerenciar chaves de acesso S3 para usuários locatários.
- **s3-object-lock:** Operações nas configurações globais de bloqueio de objeto S3, usadas para dar suporte à conformidade regulatória.
- **usuários:** Operações para visualizar e gerenciar usuários locatários.

Detalhes da operação

Ao expandir cada operação de API, você pode ver sua ação HTTP, 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

/org/groups

Lists Tenant User Groups

Parameters

Try it out

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

Responses

Response content type

application/json

Code	Description
200	Example Value Model <pre>{ "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.1" }</pre>

Emitir solicitações de API



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. Selecione a ação HTTP para ver os detalhes da solicitação.
2. 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.
3. Determine se você precisa modificar o corpo da solicitação de exemplo. Se sim, você pode selecionar **Modelo** para saber os requisitos de cada campo.

4. Selecione **Experimentar**.
5. Forneça quaisquer parâmetros necessários ou modifique o corpo da solicitação conforme necessário.
6. Selecione **Executar**.
7. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

Controle de versão da API de gerenciamento de locatários

A API de gerenciamento de locatários 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.

Para configurar a proteção CSRF, use o ["API de gerenciamento de grade"](#) ou ["API de gerenciamento de inquilinos"](#).



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.

Usar conexões de federação de grade

Clonar grupos de locatários e usuários

Se um locatário foi criado ou editado para usar uma conexão de federação de grade, esse locatário é replicado de um sistema StorageGRID (o locatário de origem) para outro sistema StorageGRID (o locatário de réplica). Após o locatário ser replicado, todos os grupos e usuários adicionados ao locatário de origem são clonados no locatário de réplica.

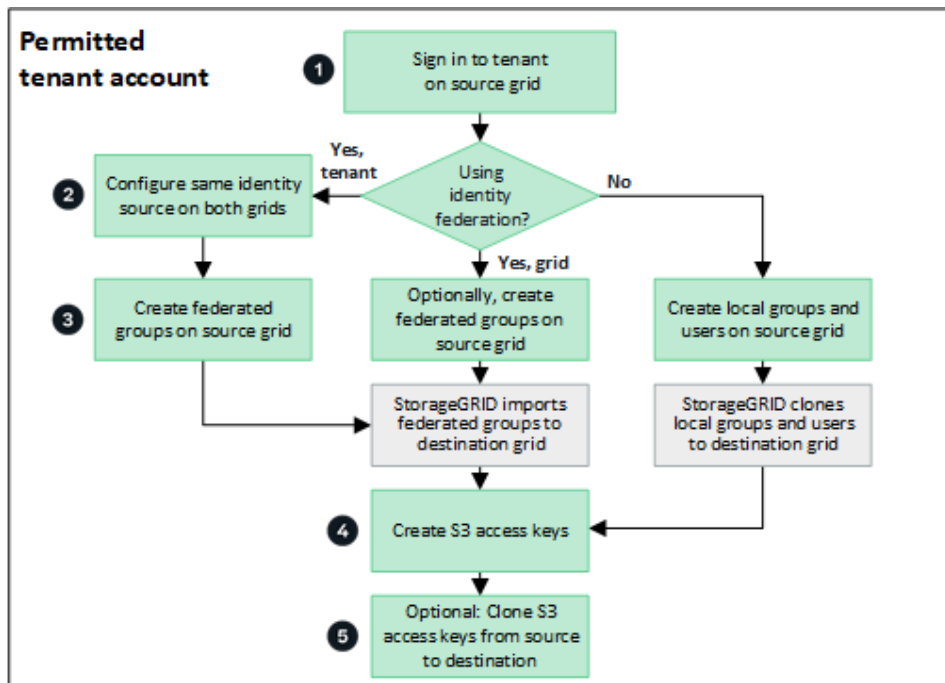
O sistema StorageGRID onde o locatário é criado originalmente é a *grade de origem* do locatário. O sistema StorageGRID onde o locatário é replicado é a *grade de destino* do locatário. Ambas as contas de locatário têm o mesmo ID de conta, nome, descrição, cota de armazenamento e permissões atribuídas, mas o locatário de destino não tem inicialmente uma senha de usuário raiz. Para mais detalhes, veja ["O que é clone de conta"](#) e ["Gerenciar inquilinos permitidos"](#).

A clonagem das informações da conta do locatário é necessária para ["replicação entre grades"](#) de objetos de balde. Ter os mesmos grupos de locatários e usuários em ambas as grades garante que você possa acessar os buckets e objetos correspondentes em qualquer uma das grades.

Fluxo de trabalho do locatário para clonagem de conta

Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, revise o diagrama de fluxo de trabalho para ver as etapas que você executará para clonar grupos, usuários e chaves de acesso do

S3.



Estas são as principais etapas do fluxo de trabalho:

1

Sign in como inquilino

Sign in na conta do locatário na grade de origem (a grade onde o locatário foi criado inicialmente).

2

Opcionalmente, configure a federação de identidade

Se sua conta de locatário tiver a permissão **Usar fonte de identidade própria** para usar grupos e usuários federados, configure a mesma fonte de identidade (com as mesmas configurações) para as contas de locatário de origem e de destino. Grupos e usuários federados não podem ser clonados, a menos que ambas as grades estejam usando a mesma fonte de identidade. Para obter instruções, consulte ["Usar federação de identidade"](#).

3

Criar grupos e usuários

Ao criar grupos e usuários, sempre comece pela grade de origem do locatário. Quando você adiciona um novo grupo, o StorageGRID o clona automaticamente na grade de destino.

- Se a federação de identidade estiver configurada para todo o sistema StorageGRID ou para sua conta de locatário, ["criar novos grupos de inquilinos"](#) importando grupos federados da fonte de identidade.
- Se você não estiver usando federação de identidade, ["criar novos grupos locais"](#) e então ["criar usuários locais"](#).

4

Criar chaves de acesso S3

Você pode ["crie suas próprias chaves de acesso"](#) ou para ["criar chaves de acesso de outro usuário"](#) na grade

de origem ou na grade de destino para acessar os buckets nessa grade.

5

Opcionalmente, clone as chaves de acesso S3

Se você precisar acessar buckets com as mesmas chaves de acesso em ambas as grades, crie as chaves de acesso na grade de origem e use a API do Tenant Manager para cloná-las manualmente na grade de destino. Para obter instruções, consulte ["Clonar chaves de acesso S3 usando a API"](#) .

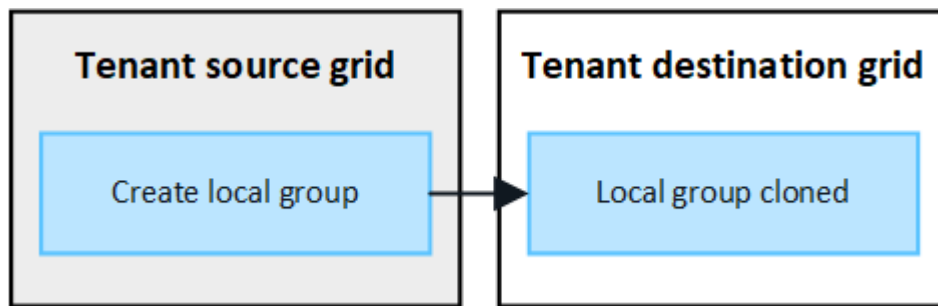
Como grupos, usuários e chaves de acesso do S3 são clonados?

Revise esta seção para entender como grupos, usuários e chaves de acesso do S3 são clonados entre a grade de origem do locatário e a grade de destino do locatário.

Grupos locais criados na grade de origem são clonados

Depois que uma conta de locatário é criada e replicada para a grade de destino, o StorageGRID clona automaticamente todos os grupos locais que você adiciona à grade de origem do locatário para a grade de destino do locatário.

Tanto o grupo original quanto seu clone têm o mesmo modo de acesso, permissões de grupo e política de grupo do S3. Para obter instruções, consulte ["Criar grupos para locatário S3"](#) .

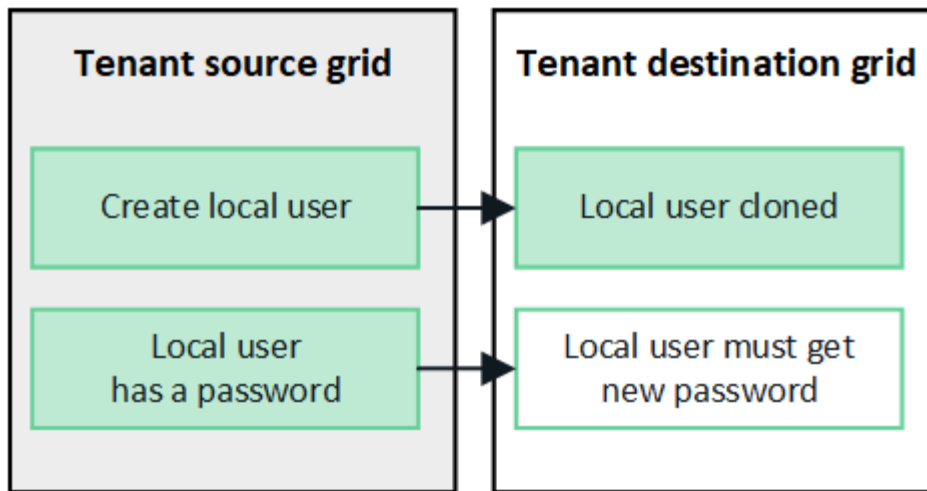


Qualquer usuário selecionado ao criar um grupo local na grade de origem não será incluído quando o grupo for clonado na grade de destino. Por esse motivo, não selecione usuários ao criar o grupo. Em vez disso, selecione o grupo ao criar os usuários.

Usuários locais criados na grade de origem são clonados

Quando você cria um novo usuário local na grade de origem, o StorageGRID clona automaticamente esse usuário na grade de destino. Tanto o usuário original quanto seu clone têm o mesmo nome completo, nome de usuário e configuração **Negar acesso**. Ambos os usuários também pertencem aos mesmos grupos. Para obter instruções, consulte ["Gerenciar usuários locais"](#) .

Por motivos de segurança, as senhas dos usuários locais não são clonadas para a grade de destino. Se um usuário local precisar acessar o Tenant Manager na grade de destino, o usuário raiz da conta do locatário deverá adicionar uma senha para esse usuário na grade de destino. Para obter instruções, consulte ["Gerenciar usuários locais"](#) .

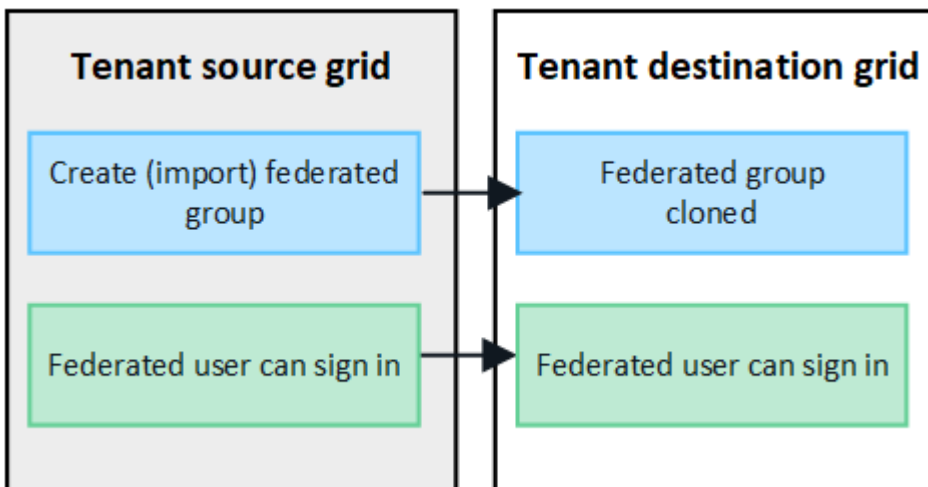


Os grupos federados criados na grade de origem são clonados

Assumindo os requisitos para usar o clone de conta com ["login único"](#) e ["federação de identidade"](#) foram atendidos, os grupos federados que você cria (importa) para o locatário na grade de origem são clonados automaticamente para o locatário na grade de destino.

Ambos os grupos têm o mesmo modo de acesso, permissões de grupo e política de grupo S3.

Depois que os grupos federados são criados para o locatário de origem e clonados para o locatário de destino, os usuários federados podem fazer login no locatário em qualquer grade.

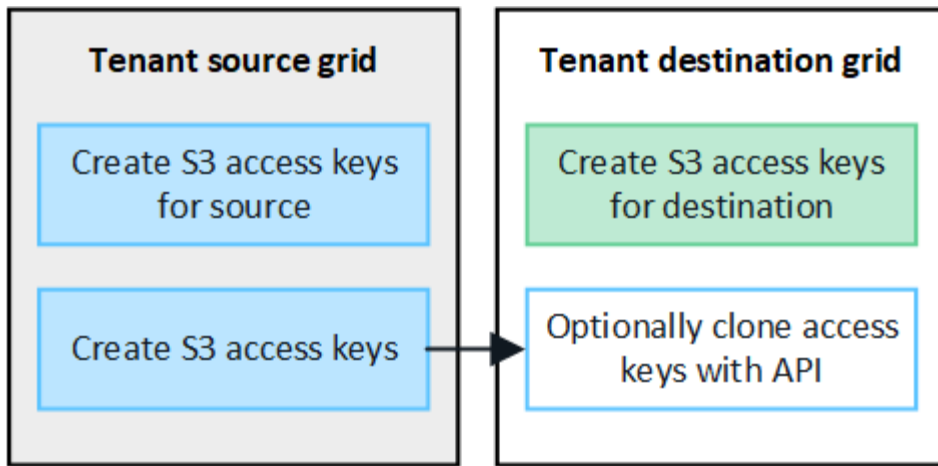


As chaves de acesso S3 podem ser clonadas manualmente

O StorageGRID não clona automaticamente as chaves de acesso do S3 porque a segurança é melhorada ao ter chaves diferentes em cada grade.

Para gerenciar chaves de acesso nas duas grades, você pode fazer o seguinte:

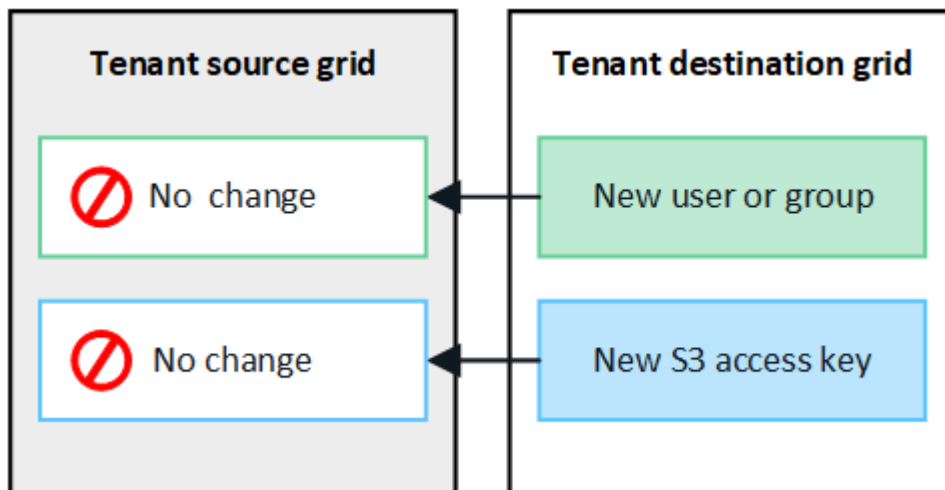
- Se você não precisa usar as mesmas chaves para cada grade, você pode ["crie suas próprias chaves de acesso"](#) ou ["criar chaves de acesso de outro usuário"](#) em cada grade.
- Se você precisar usar as mesmas chaves em ambas as grades, você pode criar chaves na grade de origem e então usar a API do Tenant Manager para manualmente ["clonar as chaves"](#) para a grade de destino.



Quando você clona chaves de acesso S3 para um usuário federado, tanto o usuário quanto as chaves de acesso S3 são clonadas para o locatário de destino.

Grupos e usuários adicionados à grade de destino não são clonados

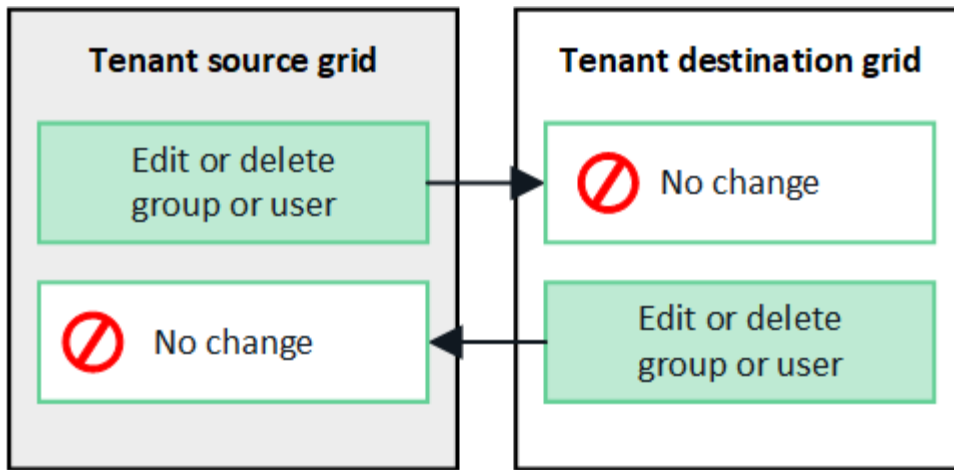
A clonagem ocorre somente da grade de origem do locatário para a grade de destino do locatário. Se você criar ou importar grupos e usuários na grade de destino do locatário, o StorageGRID não clonará esses itens de volta para a grade de origem do locatário.



Grupos, usuários e chaves de acesso editados ou excluídos não são clonados

A clonagem ocorre somente quando você cria novos grupos e usuários.

Se você editar ou excluir grupos, usuários ou chaves de acesso em qualquer grade, suas alterações não serão clonadas na outra grade.



Clonar chaves de acesso S3 usando a API

Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, você poderá usar a API de gerenciamento de locatários para clonar manualmente as chaves de acesso do S3 do locatário na grade de origem para o locatário na grade de destino.

Antes de começar

- A conta do locatário tem a permissão **Usar conexão de federação de grade**.
- A conexão da federação de rede tem um **Status de conexão** de **Conectado**.
- Você está conectado ao Tenant Manager na grade de origem do inquilino usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Gerencie suas próprias credenciais S3 ou permissão de acesso Root"](#).
- Se você estiver clonando chaves de acesso para um usuário local, o usuário já existe em ambas as grades.



Quando você clona chaves de acesso S3 para um usuário federado, tanto o usuário quanto as chaves de acesso S3 são adicionadas ao locatário de destino.

Clone suas próprias chaves de acesso

Você pode clonar suas próprias chaves de acesso se precisar acessar os mesmos buckets em ambas as grades.

Passos

1. Usando o Tenant Manager na grade de origem, ["crie suas próprias chaves de acesso"](#) e baixe o `.csv` arquivo.
2. Na parte superior do Gerenciador de Tenants, selecione o ícone de ajuda e selecione **Documentação da API**.
3. Na seção **s3**, selecione o seguinte ponto de extremidade:

`POST /org/users/current-user/replicate-s3-access-key`

POST

`/org/users/current-user/replicate-s3-access-key` Clone the current user's S3 key to the other grids.



4. Selecione **Experimentar**.
5. Na caixa de texto **body**, substitua as entradas de exemplo para **accessKey** e **secretAccessKey** pelos valores do arquivo **.csv** que você baixou.

Certifique-se de manter as aspas duplas em torno de cada string.



The screenshot shows a REST client interface with a light green header. The header contains the label **body** with a red asterisk and the word "required" in red. Below the header, there are two tabs: "Edit Value" and "Model". The "Model" tab is selected, and it displays a JSON object with the following content:

```
{
  "accessKey": "AKIAIOSFODNN7EXAMPLE",
  "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
  "expires": "2028-09-04T00:00:00.000Z"
}
```

6. Se a chave expirar, substitua a entrada de exemplo para **expires** pela data e hora de expiração como uma sequência de caracteres no formato de data e hora ISO 8601 (por exemplo, 2024-02-28T22:46:33-08:00). Se a chave não expirar, insira **null** como valor para a entrada **expires** (ou remova a linha **Expires** e a vírgula anterior).
7. Selecione **Executar**.
8. Confirme se o código de resposta do servidor é **204**, indicando que a chave foi clonada com sucesso para a grade de destino.

Clonar as chaves de acesso de outro usuário

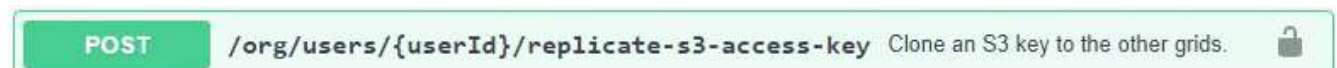
Você pode clonar as chaves de acesso de outro usuário se ele precisar acessar os mesmos buckets em ambas as grades.

Passos

1. Usando o Tenant Manager na grade de origem, "[crie as chaves de acesso S3 do outro usuário](#)" e baixe o **.csv** arquivo.
2. Na parte superior do Gerenciador de Tenants, selecione o ícone de ajuda e selecione **Documentação da API**.
3. Obtenha o ID do usuário. Você precisará desse valor para clonar as chaves de acesso do outro usuário.
 - a. Na seção **usuários**, selecione o seguinte endpoint:

```
GET /org/users
```
 - b. Selecione **Experimentar**.
 - c. Especifique quaisquer parâmetros que você deseja usar ao pesquisar usuários.
 - d. Selecione **Executar**.
 - e. Encontre o usuário cujas chaves você deseja clonar e copie o número no campo **id**.
4. Na seção **s3**, selecione o seguinte ponto de extremidade:

```
POST /org/users/{userId}/replicate-s3-access-key
```



The screenshot shows a REST client interface with a light green header. The header contains the label **POST** in white text on a green background. Below the header, there is a text input field containing the URL `/org/users/{userId}/replicate-s3-access-key`. To the right of the input field, there is a button labeled "Clone an S3 key to the other grids." and a lock icon.

5. Selecione **Experimentar**.
6. Na caixa de texto **userid**, cole o ID do usuário que você copiou.
7. Na caixa de texto **corpo**, substitua as entradas de exemplo para **chave de acesso de exemplo e chave de acesso secreta** pelos valores do arquivo **.csv** desse usuário.

Certifique-se de manter as aspas duplas ao redor da string.

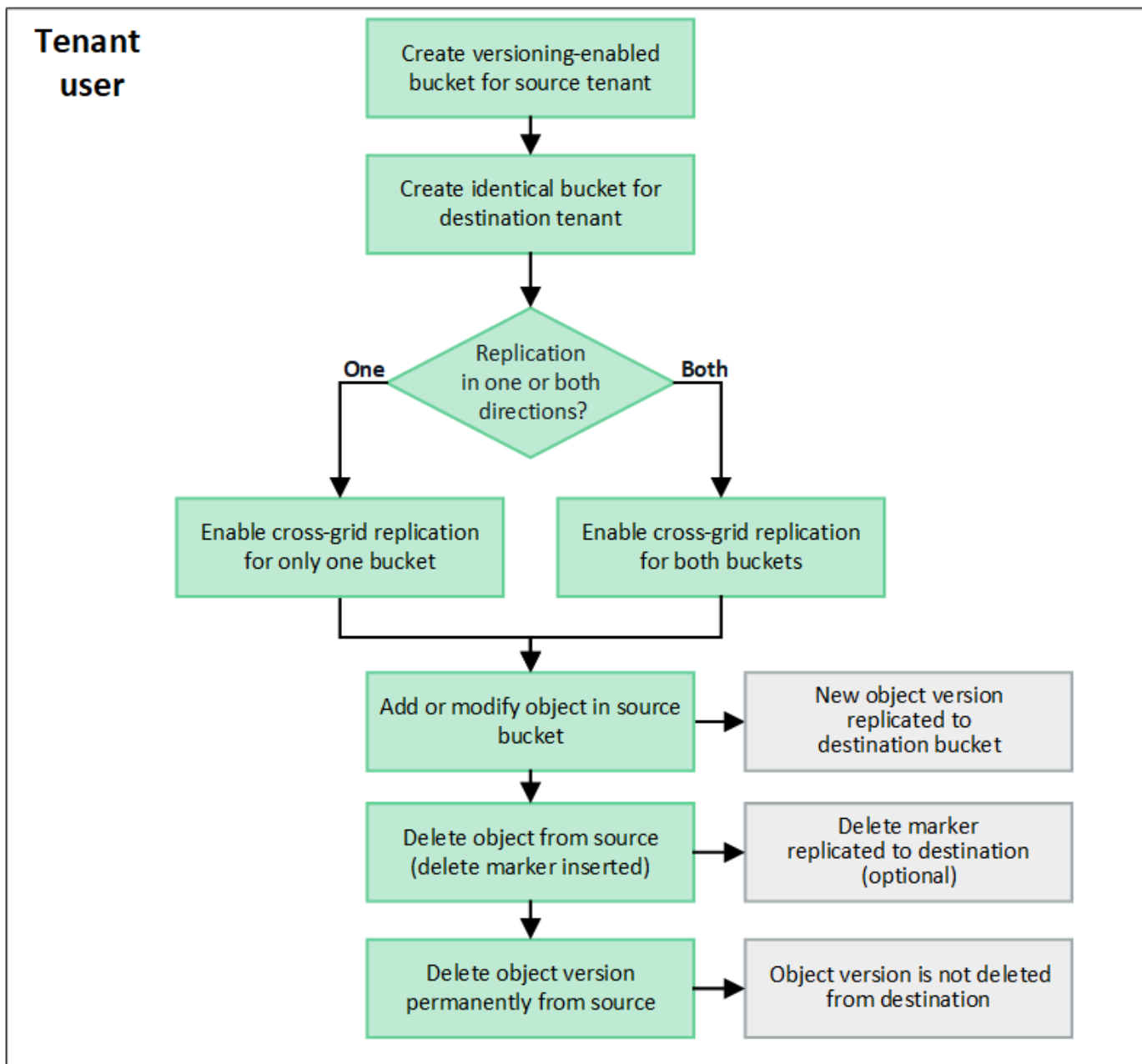
8. Se a chave expirar, substitua a entrada de exemplo para **expires** pela data e hora de expiração como uma sequência de caracteres no formato de data e hora ISO 8601 (por exemplo, `2023-02-28T22:46:33-08:00`). Se a chave não expirar, insira **null** como valor para a entrada **expires** (ou remova a linha **Expires** e a vírgula anterior).
9. Selecione **Executar**.
10. Confirme se o código de resposta do servidor é **204**, indicando que a chave foi clonada com sucesso para a grade de destino.

Gerenciar replicação entre redes

Se sua conta de locatário recebeu a permissão **Usar conexão de federação de grade** quando foi criada, você pode usar a replicação entre grades para replicar objetos automaticamente entre buckets na grade de origem do locatário e buckets na grade de destino do locatário. A replicação entre grades pode ocorrer em uma ou ambas as direções.

Fluxo de trabalho para replicação entre grades

O diagrama de fluxo de trabalho resume as etapas que você executará para configurar a replicação entre grades entre buckets em duas grades. Essas etapas são descritas com mais detalhes abaixo.



Configurar replicação entre grades

Antes de poder usar a replicação entre grades, você deve fazer login nas contas de locatário correspondentes em cada grade e criar buckets idênticos. Em seguida, você pode habilitar a replicação entre grades em um ou ambos os buckets.

Antes de começar

- Você revisou os requisitos para replicação entre redes. Ver ["O que é replicação entre grades"](#) .
- Você está usando um ["navegador da web compatível"](#) .
- A conta do locatário tem a permissão **Usar conexão de federação de grade** e contas de locatário idênticas existem em ambas as grades. Ver ["Gerenciar os inquilinos permitidos para conexão de federação de rede"](#) .
- O usuário locatário com o qual você fará login já existe em ambas as grades e pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#) .

- Se você for efetuar login na grade de destino do locatário como um usuário local, o usuário raiz da conta do locatário definiu uma senha para sua conta de usuário nessa grade.

Crie dois buckets idênticos

Como primeiro passo, faça login nas contas de locatários correspondentes em cada grade e crie buckets idênticos.

Passos

1. A partir de qualquer grade na conexão de federação de grade, crie um novo bucket:
 - a. Sign in na conta do locatário usando as credenciais de um usuário locatário que exista em ambas as grades.



Se você não conseguir fazer login na grade de destino do locatário como um usuário local, confirme se o usuário raiz da conta do locatário definiu uma senha para sua conta de usuário.

- b. Siga as instruções para "[criar um bucket S3](#)".
 - c. Na guia **Gerenciar configurações de objeto**, selecione **Ativar controle de versão de objeto**.
 - d. Se o S3 Object Lock estiver habilitado para seu sistema StorageGRID, não habilite o S3 Object Lock para o bucket.
 - e. Selecione **Criar bucket**.
 - f. Selecione **Concluir**.
2. Repita essas etapas para criar um bucket idêntico para a mesma conta de locatário na outra grade na conexão de federação da grade.



Conforme necessário, cada bucket pode usar uma região diferente.

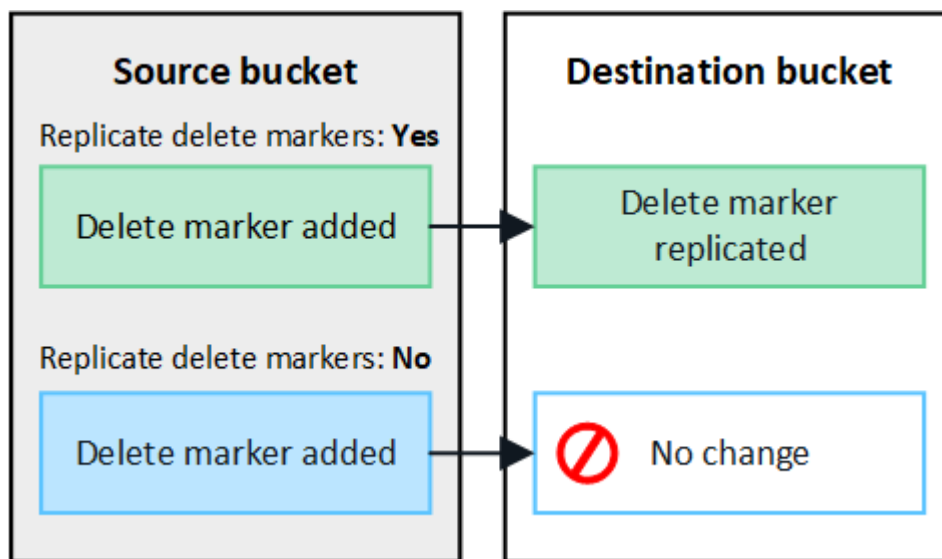
Habilitar replicação entre redes

Você deve executar estas etapas antes de adicionar qualquer objeto a qualquer um dos buckets.

Passos

1. A partir de uma grade cujos objetos você deseja replicar, habilite "[replicação entre grades em uma direção](#)":
 - a. Sign in na conta do locatário do bucket.
 - b. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
 - c. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
 - d. Selecione a aba **Replicação entre grades**.
 - e. Selecione **Ativar** e revise a lista de requisitos.
 - f. Se todos os requisitos forem atendidos, selecione a conexão de federação de rede que você deseja usar.
 - g. Opcionalmente, altere a configuração de **Replicar marcadores de exclusão** para determinar o que acontece na grade de destino se um cliente S3 emitir uma solicitação de exclusão para a grade de origem que não inclua um ID de versão:

- **Sim** (padrão): Um marcador de exclusão é adicionado ao bucket de origem e replicado no bucket de destino.
- **Não**: Um marcador de exclusão é adicionado ao bucket de origem, mas não é replicado no bucket de destino.



Se a solicitação de exclusão incluir um ID de versão, essa versão do objeto será removida permanentemente do bucket de origem. O StorageGRID não replica solicitações de exclusão que incluem um ID de versão, portanto, a mesma versão do objeto não é excluída do destino.

Ver ["O que é replicação entre grades"](#) para mais detalhes.

- Opcionalmente, altere a configuração da categoria de auditoria **Replicação entre grades** para gerenciar o volume de mensagens de auditoria:
 - **Erro** (padrão): Somente solicitações de replicação entre grades com falha são incluídas na saída de auditoria.
 - **Normal**: Todas as solicitações de replicação entre grades são incluídas, o que aumenta significativamente o volume da saída de auditoria.
- Revise suas seleções. Você não poderá alterar essas configurações a menos que ambos os buckets estejam vazios.
- Selecione **Ativar e testar**.

Após alguns instantes, uma mensagem de sucesso é exibida. Os objetos adicionados a este bucket agora serão replicados automaticamente para a outra grade. **A replicação entre grades** é mostrada como um recurso habilitado na página de detalhes do bucket.

- Opcionalmente, vá para o balde correspondente na outra grade e ["permitir a replicação entre redes em ambas as direções"](#).

Replicação de teste entre grades

Se a replicação entre grades estiver habilitada para um bucket, talvez seja necessário verificar se a conexão e a replicação entre grades estão funcionando corretamente e se os buckets de origem e destino ainda atendem a todos os requisitos (por exemplo, o controle de versão ainda está habilitado).

Antes de começar

- Você está usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#) .

Passos

1. Sign in na conta do locatário do bucket.
2. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
3. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
4. Selecione a aba **Replicação entre grades**.
5. Selecione **Testar conexão**.

Se a conexão estiver saudável, um banner de sucesso será exibido. Caso contrário, uma mensagem de erro será exibida, que você e o administrador da grade podem usar para resolver o problema. Para obter detalhes, consulte ["Solucionar erros de federação de grade"](#) .

6. Se a replicação entre grades estiver configurada para ocorrer em ambas as direções, vá para o bucket correspondente na outra grade e selecione **Testar conexão** para verificar se a replicação entre grades está funcionando na outra direção.

Desabilitar replicação entre grades

Você pode interromper permanentemente a replicação entre grades se não quiser mais copiar objetos para a outra grade.

Antes de desabilitar a replicação entre grades, observe o seguinte:

- Desabilitar a replicação entre grades não remove nenhum objeto que já tenha sido copiado entre grades. Por exemplo, objetos em `my-bucket` na Grade 1 que foram copiados para `my-bucket` na Grade 2 não serão removidos se você desabilitar a replicação entre grades para esse bucket. Se você quiser excluir esses objetos, deverá removê-los manualmente.
- Se a replicação entre grades estiver habilitada para cada um dos buckets (ou seja, se a replicação ocorrer em ambas as direções), você poderá desabilitar a replicação entre grades para um ou ambos os buckets. Por exemplo, você pode querer desabilitar a replicação de objetos de `my-bucket` na Grade 1 para `my-bucket` na Grade 2, enquanto continua a replicar objetos de `my-bucket` na Grade 2 para `my-bucket` na Grade 1.
- Você deve desabilitar a replicação entre redes antes de poder remover a permissão de um locatário para usar a conexão de federação de rede. Ver ["Gerenciar inquilinos permitidos"](#) .
- Se você desabilitar a replicação entre grades para um bucket que contém objetos, não será possível habilitá-la novamente, a menos que você exclua todos os objetos dos buckets de origem e de destino.



Não é possível reativar a replicação a menos que ambos os buckets estejam vazios.

Antes de começar

- Você está usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#) .

Passos

1. A partir da grade cujos objetos você não deseja mais replicar, interrompa a replicação entre grades para o bucket:

- a. Sign in na conta do locatário do bucket.
- b. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
- c. Selecione o nome do bucket na tabela para acessar a página de detalhes do bucket.
- d. Selecione a aba **Replicação entre grades**.
- e. Selecione **Desativar replicação**.
- f. Se você tiver certeza de que deseja desabilitar a replicação entre grades para este bucket, digite **Sim** na caixa de texto e selecione **Desabilitar**.

Após alguns instantes, uma mensagem de sucesso é exibida. Novos objetos adicionados a este bucket não podem mais ser replicados automaticamente para a outra grade. **A replicação entre grades** não é mais exibida como um recurso Habilitado na página Buckets.

2. Se a replicação entre grades foi configurada para ocorrer em ambas as direções, vá para o bucket correspondente na outra grade e pare a replicação entre grades na outra direção.

Ver conexões de federação de grade

Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, você poderá visualizar as conexões permitidas.

Antes de começar

- A conta do locatário tem a permissão **Usar conexão de federação de grade**.
- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#).

Passos

1. Selecione **ARMAZENAMENTO (S3) > Conexões de federação de rede**.

A página de conexão da federação Grid é exibida e inclui uma tabela que resume as seguintes informações:

Coluna	Descrição
Nome da conexão	As conexões da federação de grade que este locatário tem permissão para usar.
Buckets com replicação entre grades	Para cada conexão de federação de grade, os buckets de locatários que têm replicação entre grades habilitada. Os objetos adicionados a esses buckets serão replicados para a outra grade na conexão.
Último erro	Para cada conexão de federação de grade, o erro mais recente ocorrido, se houver, quando os dados estavam sendo replicados para a outra grade. Ver Limpe o último erro .

2. Opcionalmente, selecione um nome de bucket para ["ver detalhes do bucket"](#).

Limpar o último erro

Um erro pode aparecer na coluna **Último erro** 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.



Esta coluna mostra apenas o último erro de replicação entre grades que ocorreu; erros anteriores que possam ter ocorrido não serão mostrados.

Passos

1. Se uma mensagem aparecer na coluna **Último erro**, visualize o texto da mensagem.

Por exemplo, esse erro indica que o bucket de destino para replicação entre grades estava em um estado inválido, possivelmente porque o controle de versão foi suspenso ou o bloqueio de objeto do S3 estava habilitado.

Grid federation connections

Clear error

Search...

🔍

Displaying one result

Connection name	Buckets with cross-grid replication	Last error
☐ Grid 1-Grid 2	my-cgr-bucket	2022-12-07 16:02:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)

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 conexão na tabela.
4. Selecione **Limpar erro**.
5. Selecione **Sim** para limpar a mensagem e atualizar o status do sistema.
6. 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.

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

Gerenciar grupos e usuários

Usar federação de identidade

O uso da federação de identidades agiliza a configuração de grupos de locatários e usuários e permite que usuários locatários efetuem login na conta do locatário usando credenciais conhecidas.

Configurar federação de identidade para o Tenant Manager

Você pode configurar a federação de identidade para o Gerenciador de Locatários se quiser que grupos de locatários 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 Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#) .
- 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 o servidor OpenLDAP](#) .
- Se você planeja usar o Transport Layer Security (TLS) para comunicações com o servidor LDAP, o provedor de identidade deve usar o TLS 1.2 ou 1.3. Ver ["Cifras suportadas para conexões TLS de saída"](#) .

Sobre esta tarefa

A possibilidade de configurar um serviço de federação de identidade para seu locatário depende de como sua conta de locatário foi configurada. Seu locatário pode compartilhar o serviço de federação de identidade que foi configurado para o Grid Manager. Se você vir esta mensagem ao acessar a página Federação de Identidade, não será possível configurar uma fonte de identidade federada separada para este locatário.



This tenant account uses the LDAP server that is configured for the Grid Manager.
Contact the grid administrator for information or to change this setting.

Insira a configuração

Ao configurar a federação de identidade, você fornece os valores que o StorageGRID precisa para se conectar a um serviço LDAP.

Passos

1. Selecione **GERENCIAMENTO 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 o 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 inquilinos

Criar grupos para um locatário S3

Você pode gerenciar permissões para grupos de usuários do S3 importando grupos federados ou criando grupos locais.

Antes de começar

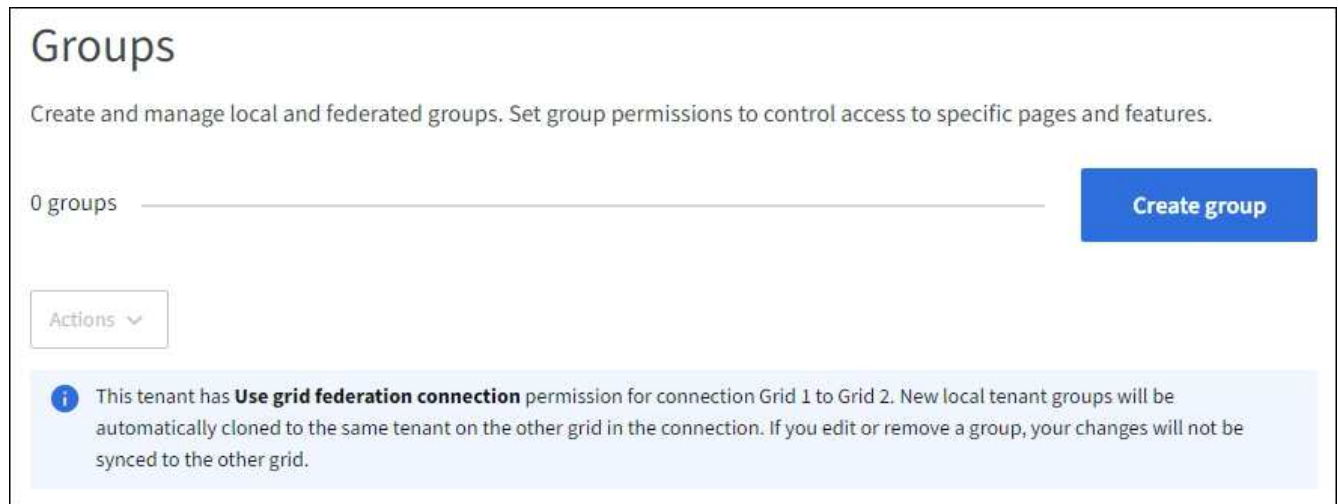
- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#) .
- Se você planeja importar um grupo federado, você tem ["federação de identidade configurada"](#) , e o grupo federado já existe na fonte de identidade configurada.
- Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, você revisou o fluxo de trabalho e as considerações para ["clonagem de grupos de inquilinos e usuários"](#) , e você está conectado à grade de origem do locatário.

Acesse o assistente Criar grupo

Como primeiro passo, acesse o assistente Criar grupo.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO > Grupos**.
2. Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, confirme se um banner azul aparece, indicando que novos grupos criados nesta grade serão clonados para o mesmo locatário na outra grade na conexão. Se este banner não aparecer, você pode estar conectado à grade de destino do locatário.



3. Selecione **Criar grupo**.

Escolha um tipo de grupo

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

Passos

1. Selecione a guia **Grupo local** para criar um grupo local ou selecione a guia **Grupo federado** para importar um grupo da fonte de identidade configurada anteriormente.

Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID , os usuários pertencentes a grupos locais não poderão fazer logon no Gerenciador de locatários, embora possam usar aplicativos cliente para gerenciar os recursos do locatário, com base nas permissões do grupo.

2. Digite o nome do grupo.

- **Grupo local:** insira um nome de exibição e um nome exclusivo. Você pode editar o nome de exibição mais tarde.



Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, ocorrerá um erro de clonagem se o mesmo **Nome exclusivo** já existir para o locatário na grade de destino.

- **Grupo federado:** Insira o nome exclusivo. Para o Active Directory, o nome exclusivo é o nome associado ao sAMAccountName atributo. Para OpenLDAP, o nome exclusivo é o nome associado ao uid atributo.

3. Selecione **Continuar**.

Gerenciar permissões de grupo

As permissões de grupo controlam quais tarefas os usuários podem executar no Tenant Manager e na Tenant Management API.

Passos

1. Para **Modo de acesso**, selecione uma das seguintes opções:
 - **Leitura e gravação** (padrão): os usuários podem fazer login no Tenant Manager e gerenciar a configuração do locatário.
 - **Somente leitura**: os usuários podem apenas visualizar configurações e recursos. Eles não podem fazer nenhuma alteração ou executar nenhuma operação no Tenant Manager ou na Tenant 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 uma ou mais permissões para este grupo.

Ver "[Permissões de gerenciamento de inquilinos](#)".

3. Selecione **Continuar**.

Definir política de grupo S3

A política de grupo determina quais permissões de acesso ao S3 os usuários terão.

Passos

1. Selecione a política que você deseja usar para este grupo.

Política de grupo	Descrição
Sem acesso S3	Padrão. Os usuários neste grupo não têm acesso aos recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar esta opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
Acesso somente leitura	Os usuários neste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários neste grupo podem listar objetos e ler dados de objetos, metadados e tags. Quando você seleciona esta opção, a string JSON para uma política de grupo somente leitura aparece na caixa de texto. Você não pode editar esta sequência.
Acesso total	Os usuários neste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona esta opção, a string JSON para uma política de grupo de acesso total aparece na caixa de texto. Você não pode editar esta sequência.

Política de grupo	Descrição
Mitigação de Ransomware	Esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários neste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que tenham o controle de versão de objetos habilitado. Usuários do Tenant Manager que têm a permissão Gerenciar todos os buckets podem substituir esta política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação Multifator (MFA) quando disponível.
Personalizado	Os usuários do grupo recebem as permissões que você especifica na caixa de texto.

- Se você selecionou **Personalizado**, insira a política de grupo. Cada política de grupo tem um limite de tamanho de 5.120 bytes. Você deve inserir uma string válida no formato JSON.

Para obter informações detalhadas sobre políticas de grupo, incluindo sintaxe de linguagem e exemplos, consulte ["Exemplo de políticas de grupo"](#).

- 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)

Você pode salvar o grupo sem adicionar usuários ou, opcionalmente, adicionar quaisquer usuários locais que já existam.



Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, todos os usuários selecionados ao criar um grupo local na grade de origem não serão incluídos quando o grupo for clonado na grade de destino. Por esse motivo, não selecione usuários ao criar o grupo. Em vez disso, selecione o grupo ao criar os usuários.

Passos

- Opcionalmente, selecione um ou mais usuários locais para este grupo.
- Selecione **Criar grupo** e **Concluir**.

O grupo que você criou aparece na lista de grupos.

Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade** e você estiver na grade de origem do locatário, o novo grupo será clonado na grade de destino do locatário. **Sucesso** aparece como **Status de clonagem** na seção Visão geral da página de detalhes do grupo.

Criar grupos para um locatário Swift

Você pode gerenciar permissões de acesso para uma conta de locatário do Swift importando grupos federados ou criando grupos locais. Pelo menos um grupo deve ter a permissão de Administrador do Swift, necessária para gerenciar os contêineres e objetos de uma conta de locatário do Swift.



O suporte para aplicativos cliente Swift foi descontinuado e será removido em uma versão futura.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#) .
- Se você planeja importar um grupo federado, você tem ["federação de identidade configurada"](#) , e o grupo federado já existe na fonte de identidade configurada.

Acesse o assistente Criar grupo

Passos

Como primeiro passo, acesse o assistente Criar grupo.

1. Selecione **GERENCIAMENTO DE ACESSO > Grupos**.
2. Selecione **Criar grupo**.

Escolha um tipo de grupo

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

Passos

1. Selecione a guia **Grupo local** para criar um grupo local ou selecione a guia **Grupo federado** para importar um grupo da fonte de identidade configurada anteriormente.

Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID , os usuários pertencentes a grupos locais não poderão fazer logon no Gerenciador de locatários, embora possam usar aplicativos cliente para gerenciar os recursos do locatário, com base nas permissões do grupo.

2. Digite o nome do grupo.
 - **Grupo local:** insira um nome de exibição e um nome exclusivo. Você pode editar o nome de exibição mais tarde.
 - **Grupo federado:** Insira o nome exclusivo. Para o Active Directory, o nome exclusivo é o nome associado ao `sAMAccountName` atributo. Para OpenLDAP, o nome exclusivo é o nome associado ao `uid` atributo.
3. Selecione **Continuar**.

Gerenciar permissões de grupo

As permissões de grupo controlam quais tarefas os usuários podem executar no Tenant Manager e na Tenant Management API.

Passos

1. Para **Modo de acesso**, selecione uma das seguintes opções:
 - **Leitura e gravação** (padrão): os usuários podem fazer login no Tenant Manager e gerenciar a configuração do locatário.
 - **Somente leitura:** os usuários podem apenas visualizar configurações e recursos. Eles não podem fazer nenhuma alteração ou executar nenhuma operação no Tenant Manager ou na Tenant 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 a caixa de seleção **Acesso root** se os usuários do grupo precisarem fazer login no Gerenciador de Tenants ou na API de Gerenciamento de Tenants.
3. Selecione **Continuar**.

Definir política de grupo Swift

Os usuários do Swift precisam de permissão de administrador para autenticar na API REST do Swift para criar contêineres e ingerir objetos.

1. Selecione a caixa de seleção **Administrador Swift** se os usuários do grupo precisarem usar a API REST do Swift para gerenciar contêineres e objetos.
2. 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)

Você pode salvar o grupo sem adicionar usuários ou, opcionalmente, adicionar quaisquer usuários locais que já existam.

Passos

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

Se você ainda não criou usuários locais, pode adicionar este grupo ao usuário na página Usuários. Ver ["Gerenciar usuários locais"](#).

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

O grupo que você criou aparece na lista de grupos.

Permissões de gerenciamento de inquilinos

Antes de criar um grupo de locatários, considere quais permissões você deseja atribuir a esse grupo. As permissões de gerenciamento de locatários determinam quais tarefas os usuários podem executar usando o Gerenciador de Locatários ou a API de Gerenciamento de Locatários. Um usuário pode pertencer a um ou mais grupos. As permissões são cumulativas se um usuário pertencer a vários grupos.

Para fazer login no Tenant Manager ou usar a API de gerenciamento de locatários, os usuários devem pertencer a um grupo que tenha pelo menos uma permissão. Todos os usuários que podem fazer login podem executar as seguintes tarefas:

- Ver o painel
- Alterar sua própria senha (para usuários locais)

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.

Você pode atribuir as seguintes permissões a um grupo. Observe que os locatários do S3 e do Swift têm permissões de grupo diferentes.

Permissão	Descrição	Detalhes
Acesso root	Fornecer acesso total ao Gerenciador de Inquilinos e à API de Gerenciamento de Inquilinos.	Os usuários do Swift devem ter permissão de acesso Root para fazer login na conta do locatário.
Administrador	Somente inquilinos do Swift. Fornece acesso total aos contêineres e objetos Swift para esta conta de locatário	Os usuários do Swift devem ter permissão de administrador do Swift para executar qualquer operação com a API REST do Swift.
Gerencie suas próprias credenciais S3	Permite que os usuários criem e removam suas próprias chaves de acesso S3.	Usuários que não têm essa permissão não veem a opção de menu ARMAZENAMENTO (S3) > Minhas chaves de acesso S3 .
Ver todos os baldes	Locatários S3: Permite que os usuários visualizem todos os buckets e configurações de buckets. Inquilinos Swift: Permite que usuários Swift visualizem todos os contêineres e configurações de contêineres usando a API de gerenciamento de inquilinos.	Usuários que não têm a permissão Exibir todos os buckets ou Gerenciar todos os buckets não veem a opção de menu Buckets. Esta permissão é substituída pela permissão Gerenciar todos os buckets. Não afeta as políticas de grupo ou bucket do S3 usadas pelos clientes do S3 ou pelo Console do S3. Você só pode atribuir essa permissão a grupos Swift da API de gerenciamento de locatários. Você não pode atribuir essa permissão a grupos Swift usando o Gerenciador de Tenants.

Permissão	Descrição	Detalhes
Gerenciar todos os buckets	Locatários S3: permite que os usuários usem o Gerenciador de Locatários e a API de Gerenciamento de Locatários para criar e excluir buckets S3 e gerenciar as configurações de todos os buckets S3 na conta do locatário, independentemente das políticas de grupo ou bucket S3. Inquilinos Swift: Permite que usuários Swift controlem a consistência dos contêineres Swift usando a API de gerenciamento de inquilinos.	Usuários que não têm a permissão Exibir todos os buckets ou Gerenciar todos os buckets não veem a opção de menu Buckets. Esta permissão substitui a permissão Exibir todos os buckets. Não afeta as políticas de grupo ou bucket do S3 usadas pelos clientes do S3 ou pelo Console do S3. Você só pode atribuir essa permissão a grupos Swift da API de gerenciamento de locatários. Você não pode atribuir essa permissão a grupos Swift usando o Gerenciador de Tenants.
Gerenciar endpoints	Permite que os usuários usem o Tenant Manager ou a Tenant Management API para criar ou editar pontos de extremidade de serviço da plataforma, que são usados como destino para os serviços da plataforma StorageGRID .	Usuários que não têm essa permissão não veem a opção de menu Pontos de extremidade de serviços da plataforma .
Usar a guia Console do S3	Quando combinado com a permissão Exibir todos os buckets ou Gerenciar todos os buckets, permite que os usuários visualizem e gerenciem objetos na guia Console do S3 na página de detalhes de um bucket.	

Gerenciar grupos

Gerencie seus grupos de inquilinos conforme necessário para visualizar, editar ou duplicar um grupo e muito mais.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#) .

Ver ou editar grupo

Você pode visualizar e editar as informações básicas e detalhes de cada grupo.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO > Grupos**.
2. Revise as informações fornecidas na página Grupos, que lista informações básicas para todos os grupos locais e federados para esta conta de locatário.

Se a conta do locatário tiver a permissão **Usar conexão de federação de grade** e você estiver visualizando grupos na grade de origem do locatário:

- Uma mensagem de banner indica que se você editar ou remover um grupo, suas alterações não serão sincronizadas com a outra grade.
 - Conforme necessário, uma mensagem de banner indica se os grupos não foram clonados para o locatário na grade de destino. Você pode [tentar novamente um clone de grupo](#) que falhou.
3. Se você quiser alterar o nome do grupo:
 - a. Marque a caixa de seleção do grupo.
 - b. Selecione **Ações > Editar nome do grupo**.
 - c. Digite o novo nome.
 - d. Selecione **Salvar alterações**.
 4. Se quiser ver mais detalhes ou fazer edições adicionais, faça um dos seguintes:
 - Selecione o nome do grupo.
 - Marque a caixa de seleção do grupo e selecione **Ações > Exibir detalhes do grupo**.
 5. Revise a seção Visão geral, que mostra as seguintes informações para cada grupo:
 - Nome de exibição
 - Nome único
 - Tipo
 - Modo de acesso
 - Permissões
 - Política S3
 - Número de usuários neste grupo
 - Campos adicionais se a conta do locatário tiver a permissão **Usar conexão de federação de grade** e você estiver visualizando o grupo na grade de origem do locatário:
 - Status de clonagem, **Sucesso** ou **Falha**
 - Um banner azul indicando que se você editar ou excluir este grupo, suas alterações não serão sincronizadas com a outra grade.
 6. Edite as configurações do grupo conforme necessário. Ver ["Criar grupos para um locatário S3"](#) e ["Criar grupos para um locatário Swift"](#) para obter detalhes sobre o que inserir.
 - a. Na seção Visão geral, altere o nome de exibição selecionando o nome ou o ícone de edição .
 - b. Na aba **Permissões do grupo**, atualize as permissões e selecione **Salvar alterações**.
 - c. Na aba **Política de grupo**, faça as alterações e selecione **Salvar alterações**.
 - Se você estiver editando um grupo S3, opcionalmente selecione uma política de grupo S3 diferente ou insira a string JSON para uma política personalizada, conforme necessário.
 - Se você estiver editando um grupo Swift, opcionalmente, selecione ou desmarque a caixa de seleção **Administrador Swift**.
 7. Para adicionar um ou mais usuários locais existentes ao grupo:
 - a. Selecione a aba Usuários.

Manage users

You can add users to this group or remove users from this group.

Add users
Remove Users

Displaying 1 results

Username	Full Name	Denied
User_02	User_02_Managers	

b. Selecione **Adicionar usuários**.

c. Selecione os usuários existentes que você deseja adicionar e selecione **Adicionar usuários**.

Uma mensagem de sucesso aparece no canto superior direito.

8. Para remover usuários locais do grupo:

a. Selecione a aba Usuários.

b. Selecione **Remover usuários**.

c. Selecione os usuários que deseja remover e selecione **Remover usuários**.

Uma mensagem de sucesso aparece no canto superior direito.

9. Confirme se você selecionou **Salvar alterações** para cada seção alterada.

Grupo duplicado

Você pode duplicar um grupo existente para criar novos grupos mais rapidamente.



Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade** e você duplicar um grupo da grade de origem do locatário, o grupo duplicado será clonado na grade de destino do locatário.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO > Grupos**.
2. Marque a caixa de seleção do grupo que você deseja duplicar.
3. Selecione **Ações > Duplicar grupo**.
4. Ver ["Criar grupos para um locatário S3"](#) ou ["Criar grupos para um locatário Swift"](#) para obter detalhes sobre o que inserir.
5. Selecione **Criar grupo**.

Clone do grupo de repetição

Para tentar novamente um clone que falhou:

1. Selecione cada grupo que indica *(Falha na clonagem)* abaixo do nome do grupo.
2. Selecione **Ações > Clonar grupos**.

3. Veja o status da operação de clonagem na página de detalhes de cada grupo que você está clonando.

Para obter informações adicionais, consulte ["Clonar grupos de locatários e usuários"](#) .

Excluir um ou mais grupos

Você pode excluir um ou mais grupos. Qualquer usuário que pertença apenas a um grupo excluído não poderá mais fazer login no Gerenciador de Locatários nem usar a conta do locatário.



Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade** e você excluir um grupo, o StorageGRID não excluirá o grupo correspondente na outra grade. Se você precisar manter essas informações sincronizadas, exclua o mesmo grupo de ambas as grades.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO > Grupos**.
2. Marque a caixa de seleção de cada grupo que você deseja excluir.
3. Selecione **Ações > Excluir grupo** ou **Ações > Excluir grupos**.

Uma caixa de diálogo de confirmação é exibida.

4. Selecione **Excluir grupo** ou **Excluir grupos**.

Gerenciar usuários locais

Você pode criar usuários locais e atribuí-los a grupos locais para determinar quais recursos esses usuários podem acessar. O Tenant Manager inclui um usuário local predefinido, chamado "root". Embora você possa adicionar e remover usuários locais, não é possível remover o usuário root.



Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID , os usuários locais não poderão fazer logon no Tenant Manager ou na Tenant Management API, embora possam usar aplicativos cliente para acessar os recursos do locatário, com base nas permissões do grupo.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#) .
- Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, você revisou o fluxo de trabalho e as considerações para ["clonagem de grupos de inquilinos e usuários"](#) , e você está conectado à grade de origem do locatário.

Criar um usuário local

Você pode criar um usuário local e atribuí-lo a um ou mais grupos locais para controlar suas permissões de acesso.

Usuários do S3 que não pertencem a nenhum grupo não têm permissões de gerenciamento ou políticas de grupo do S3 aplicadas a eles. Esses usuários podem ter acesso ao bucket do S3 concedido por meio de uma política de bucket.

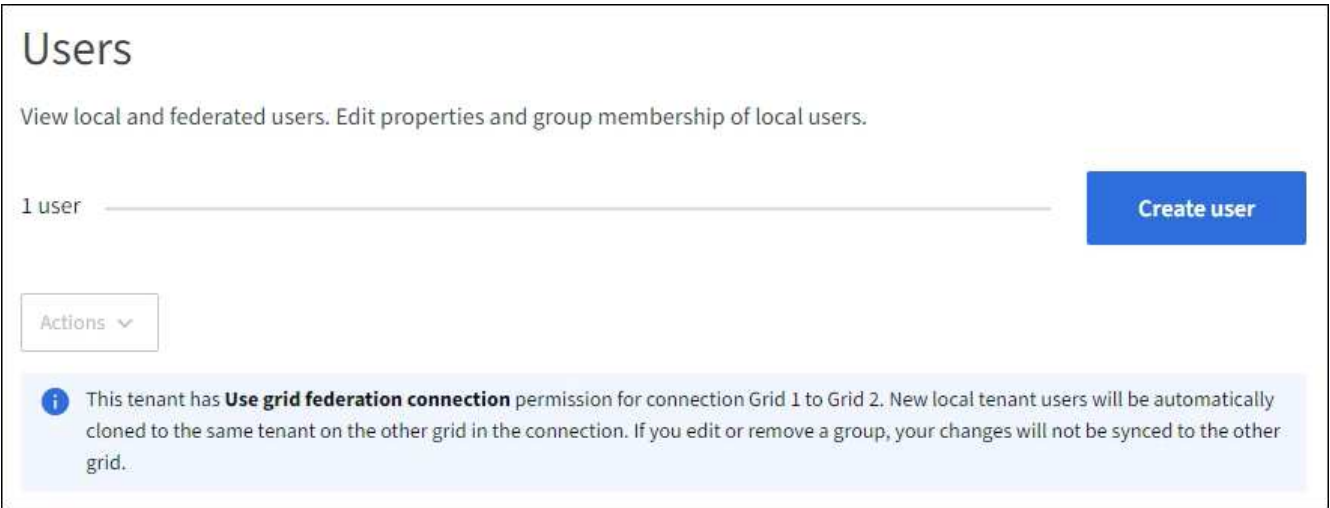
Usuários do Swift que não pertencem a nenhum grupo não têm permissões de gerenciamento ou acesso ao contêiner do Swift.

Acesse o assistente Criar usuário

Passos

- 1. Selecione **GERENCIAMENTO DE ACESSO > Usuários**.

Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, um banner azul indicará que esta é a grade de origem do locatário. Todos os usuários locais que você criar nesta grade serão clonados para a outra grade na conexão.



- 2. Selecione **Criar usuário**.

Insira as credenciais

Passos

- 1. Para a etapa **Inserir credenciais do usuário**, preencha os seguintes campos.

Campo	Descrição
Nome completo	O nome completo deste usuário, por exemplo, o nome e o sobrenome de uma pessoa ou o nome de um aplicativo.
Nome de usuário	O nome que este usuário usará para fazer login. Os nomes de usuário devem ser exclusivos e não podem ser alterados. Observação: se sua conta de locatário tiver a permissão Usar conexão de federação de grade , ocorrerá um erro de clonagem se o mesmo Nome de usuário já existir para o locatário na grade de destino.
Senha e Confirmar senha	A senha que o usuário usará inicialmente ao fazer login.

Campo	Descrição
Negar acesso	Selecione Sim para impedir que este usuário faça login na conta do locatário, mesmo que ele ainda pertença a um ou mais grupos. Por exemplo, selecione Sim para suspender temporariamente a capacidade de um usuário fazer login.

2. Selecione **Continuar**.

Atribuir a grupos

Passos

1. Atribua o usuário a um ou mais grupos locais para determinar quais tarefas ele pode executar.

Atribuir um usuário a grupos é opcional. Se preferir, você pode selecionar usuários ao criar ou editar grupos.

Usuários que não pertencem a nenhum grupo não terão permissões de gerenciamento. As permissões são cumulativas. Os usuários terão todas as permissões para todos os grupos aos quais pertencem. Ver ["Permissões de gerenciamento de inquilinos"](#).

2. Selecione **Criar usuário**.

Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade** e você estiver na grade de origem do locatário, o novo usuário local será clonado na grade de destino do locatário.

Sucesso aparece como **Status de clonagem** na seção Visão geral da página de detalhes do usuário.

3. Selecione **Concluir** para retornar à página Usuários.

Ver ou editar usuário local

Passos

1. Selecione **GERENCIAMENTO DE ACESSO > Usuários**.
2. Revise as informações fornecidas na página Usuários, que lista informações básicas para todos os usuários locais e federados desta conta de locatário.

Se a conta do locatário tiver a permissão **Usar conexão de federação de grade** e você estiver visualizando o usuário na grade de origem do locatário:

- Uma mensagem de banner indica que se você editar ou remover um usuário, suas alterações não serão sincronizadas com a outra grade.
- Conforme necessário, uma mensagem de banner indica se os usuários não foram clonados para o locatário na grade de destino. Você pode [tente novamente um clone de usuário que falhou](#).

3. Se você quiser alterar o nome completo do usuário:
 - a. Marque a caixa de seleção para o usuário.
 - b. Selecione **Ações > Editar nome completo**.
 - c. Digite o novo nome.
 - d. Selecione **Salvar alterações**.
4. Se quiser ver mais detalhes ou fazer edições adicionais, faça um dos seguintes:

- Selecione o nome de usuário.
 - Marque a caixa de seleção do usuário e selecione **Ações > Exibir detalhes do usuário**.
5. Revise a seção Visão geral, que mostra as seguintes informações para cada usuário:
- Nome completo
 - Nome de usuário
 - Tipo de usuário
 - Acesso negado
 - Modo de acesso
 - Associação ao grupo
 - Campos adicionais se a conta do locatário tiver a permissão **Usar conexão de federação de grade** e você estiver visualizando o usuário na grade de origem do locatário:
 - Status de clonagem, **Sucesso** ou **Falha**
 - Um banner azul indicando que se você editar este usuário, suas alterações não serão sincronizadas com a outra grade.
6. Edite as configurações do usuário conforme necessário. Ver [Criar usuário local](#) para obter detalhes sobre o que inserir.
- a. Na seção Visão geral, altere o nome completo selecionando o nome ou o ícone de edição  .

Você não pode alterar o nome de usuário.
 - b. Na aba **Senha**, altere a senha do usuário e selecione **Salvar alterações**.
 - c. Na aba **Acesso**, selecione **Não** para permitir que o usuário faça login ou selecione **Sim** para impedir que o usuário faça login. Em seguida, selecione **Salvar alterações**.
 - d. Na aba **Chaves de acesso**, selecione **Criar chave** e siga as instruções para "[criando chaves de acesso S3 de outro usuário](#)".
 - e. Na guia **Grupos**, selecione **Editar grupos** para adicionar o usuário aos grupos ou removê-lo dos grupos. Em seguida, selecione **Salvar alterações**.
7. Confirme se você selecionou **Salvar alterações** para cada seção alterada.

Usuário local duplicado

Você pode duplicar um usuário local para criar um novo usuário mais rapidamente.



Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade** e você duplicar um usuário da grade de origem do locatário, o usuário duplicado será clonado para a grade de destino do locatário.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO > Usuários**.
2. Marque a caixa de seleção do usuário que você deseja duplicar.
3. Selecione **Ações > Duplicar usuário**.
4. Ver [Criar usuário local](#) para obter detalhes sobre o que inserir.
5. Selecione **Criar usuário**.

Repetir clonagem do usuário

Para tentar novamente um clone que falhou:

1. Selecione cada usuário que indica (*Falha na clonagem*) abaixo do nome do usuário.
2. Selecione **Ações > Clonar usuários**.
3. Veja o status da operação de clonagem na página de detalhes de cada usuário que você está clonando.

Para obter informações adicionais, consulte "[Clonar grupos de locatários e usuários](#)".

Excluir um ou mais usuários locais

Você pode excluir permanentemente um ou mais usuários locais que não precisam mais acessar a conta de locatário do StorageGRID .



Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade** e você excluir um usuário local, o StorageGRID não excluirá o usuário correspondente na outra grade. Se você precisar manter essas informações sincronizadas, deverá excluir o mesmo usuário de ambas as grades.



Você deve usar a fonte de identidade federada para excluir usuários federados.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO > Usuários**.
2. Marque a caixa de seleção para cada usuário que você deseja excluir.
3. Selecione **Ações > Excluir usuário** ou **Ações > Excluir usuários**.

Uma caixa de diálogo de confirmação é exibida.

4. Selecione **Excluir usuário** ou **Excluir usuários**.

Gerenciar chaves de acesso S3

Gerenciar chaves de acesso S3

Cada usuário de uma conta de locatário do S3 deve ter uma chave de acesso para armazenar e recuperar objetos no sistema StorageGRID . Uma chave de acesso consiste em um ID de chave de acesso e uma chave de acesso secreta.

As chaves de acesso S3 podem ser gerenciadas da seguinte forma:

- Usuários que têm a permissão **Gerenciar suas próprias credenciais S3** podem criar ou remover suas próprias chaves de acesso S3.
- Usuários que têm a permissão **Acesso root** podem gerenciar as chaves de acesso para a conta root do S3 e todos os outros usuários. As chaves de acesso root fornecem acesso total a todos os buckets e objetos para o locatário, a menos que sejam explicitamente desabilitadas por uma política de bucket.

O StorageGRID suporta autenticação Signature versão 2 e Signature versão 4. O acesso entre contas não é permitido, a menos que seja explicitamente habilitado por uma política de bucket.

Crie suas próprias chaves de acesso S3

Se você estiver usando um locatário S3 e tiver a permissão apropriada, poderá criar suas próprias chaves de acesso S3. Você precisa ter uma chave de acesso para acessar seus buckets e objetos.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Gerencie suas próprias credenciais S3 ou permissão de acesso Root"](#) .

Sobre esta tarefa

Você pode criar uma ou mais chaves de acesso S3 que permitem criar e gerenciar buckets para sua conta de locatário. Depois de criar uma nova chave de acesso, atualize o aplicativo com seu novo ID de chave de acesso e chave de acesso secreta. Por segurança, não crie mais chaves do que o necessário e exclua as chaves que não estiver usando. Se você tiver apenas uma chave e ela estiver prestes a expirar, crie uma nova chave antes que a antiga expire e, em seguida, exclua-a.

Cada chave pode ter um tempo de expiração específico ou não ter expiração. Siga estas diretrizes para o tempo de expiração:

- Defina um tempo de expiração para suas chaves para limitar seu acesso a um determinado período de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco caso seu ID de chave de acesso e sua chave de acesso secreta sejam acidentalmente expostos. Chaves expiradas são removidas automaticamente.
- Se o risco de segurança no seu ambiente for baixo e você não precisar criar novas chaves periodicamente, não será necessário definir um tempo de expiração para suas chaves. Se você decidir criar novas chaves posteriormente, exclua as chaves antigas manualmente.



Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidas para sua conta no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

Passos

1. Selecione **ARMAZENAMENTO (S3) > Minhas chaves de acesso**.

A página Minhas chaves de acesso é exibida e lista todas as chaves de acesso existentes.

2. Selecione **Criar chave**.

3. Faça um dos seguintes:

- Selecione **Não definir um tempo de expiração** para criar uma chave que não irá expirar. (Padrão)
- Selecione **Definir um tempo de expiração** e defina a data e a hora de expiração.



A data de validade pode ser de no máximo cinco anos a partir da data atual. O tempo de expiração pode ser de no mínimo um minuto a partir da hora atual.

4. Selecione **Criar chave de acesso**.

A caixa de diálogo Baixar chave de acesso é exibida, listando seu ID de chave de acesso e sua chave de acesso secreta.

5. 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.



Não feche esta caixa de diálogo até ter copiado ou baixado estas informações. Não é possível copiar ou baixar chaves depois que a caixa de diálogo for fechada.

6. Selecione **Concluir**.

A nova chave está listada na página Minhas chaves de acesso.

7. Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, opcionalmente, use a API de gerenciamento de locatários para clonar manualmente as chaves de acesso do S3 do locatário na grade de origem para o locatário na grade de destino. Ver "[Clonar chaves de acesso S3 usando a API](#)".

Visualize suas chaves de acesso S3

Se você estiver usando um locatário S3 e tiver o "[permissão apropriada](#)", você pode visualizar uma lista de suas chaves de acesso S3. Você pode classificar a lista por tempo de expiração para determinar quais chaves expirarão em breve. Conforme necessário, você pode "[criar novas chaves](#)" ou "[teclas de exclusão](#)" que você não está mais usando.



Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidas para sua conta no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um "[navegador da web compatível](#)".
- Você pertence a um grupo de usuários que possui o recurso Gerenciar suas próprias credenciais do S3 "[permissão](#)".

Passos

1. Selecione **ARMAZENAMENTO (S3) > Minhas chaves de acesso**.
2. Na página Minhas chaves de acesso, classifique todas as chaves de acesso existentes por **Tempo de expiração** ou **ID da chave de acesso**.
3. Conforme necessário, crie novas chaves ou exclua aquelas que você não estiver mais usando.

Se você criar novas chaves antes que as chaves existentes expirem, poderá começar a usá-las sem perder temporariamente o acesso aos objetos na conta.

Chaves expiradas são removidas automaticamente.

Exclua suas próprias chaves de acesso S3

Se você estiver usando um locatário S3 e tiver a permissão apropriada, poderá excluir suas próprias chaves de acesso S3. Depois que uma chave de acesso é excluída, ela

não pode mais ser usada para acessar os objetos e buckets na conta do locatário.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você tem o ["Permissão para gerenciar suas próprias credenciais do S3"](#).



Os buckets e objetos do S3 pertencentes à sua conta podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidas para sua conta no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da sua conta e nunca as compartilhe com outros usuários.

Passos

1. Selecione **ARMAZENAMENTO (S3) > Minhas chaves de acesso**.
2. Na página Minhas chaves de acesso, marque a caixa de seleção de cada chave de acesso que deseja remover.
3. Selecione **tecla Delete**.
4. Na caixa de diálogo de confirmação, selecione **Tecla Delete**.

Uma mensagem de confirmação aparece no canto superior direito da página.

Crie chaves de acesso S3 de outro usuário

Se você estiver usando um locatário do S3 e tiver a permissão apropriada, poderá criar chaves de acesso do S3 para outros usuários, como aplicativos que precisam de acesso a buckets e objetos.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#).

Sobre esta tarefa

Você pode criar uma ou mais chaves de acesso S3 para outros usuários para que eles possam criar e gerenciar buckets para suas contas de locatário. Depois de criar uma nova chave de acesso, atualize o aplicativo com o novo ID da chave de acesso e a nova chave de acesso secreta. Por segurança, não crie mais chaves do que o usuário precisa e exclua as chaves que não estão sendo usadas. Se você tiver apenas uma chave e ela estiver prestes a expirar, crie uma nova chave antes que a antiga expire e, em seguida, exclua-a.

Cada chave pode ter um tempo de expiração específico ou não ter expiração. Siga estas diretrizes para o tempo de expiração:

- Defina um tempo de expiração para as chaves para limitar o acesso do usuário a um determinado período de tempo. Definir um tempo de expiração curto pode ajudar a reduzir o risco se o ID da chave de acesso e a chave de acesso secreta forem expostos acidentalmente. Chaves expiradas são removidas automaticamente.
- Se o risco de segurança no seu ambiente for baixo e você não precisar criar novas chaves periodicamente, não será necessário definir um tempo de expiração para as chaves. Se você decidir criar novas chaves posteriormente, exclua as chaves antigas manualmente.



Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidas para esse usuário no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da conta e nunca as compartilhe com outros usuários.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO > Usuários**.
2. Selecione o usuário cujas chaves de acesso S3 você deseja gerenciar.

A página de detalhes do usuário é exibida.

3. Selecione **Teclas de acesso** e depois selecione **Criar chave**.
4. Faça um dos seguintes:
 - Selecione **Não definir um tempo de expiração** para criar uma chave que não expira. (Padrão)
 - Selecione **Definir um tempo de expiração** e defina a data e a hora de expiração.



A data de validade pode ser de no máximo cinco anos a partir da data atual. O tempo de expiração pode ser de no mínimo um minuto a partir da hora atual.

5. Selecione **Criar chave de acesso**.

A caixa de diálogo Baixar chave de acesso é exibida, listando o ID da chave de acesso e a chave de acesso secreta.

6. 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.



Não feche esta caixa de diálogo até ter copiado ou baixado estas informações. Não é possível copiar ou baixar chaves depois que a caixa de diálogo for fechada.

7. Selecione **Concluir**.

A nova chave é listada na guia Chaves de acesso da página de detalhes do usuário.

8. Se sua conta de locatário tiver a permissão **Usar conexão de federação de grade**, opcionalmente, use a API de gerenciamento de locatários para clonar manualmente as chaves de acesso do S3 do locatário na grade de origem para o locatário na grade de destino. Ver "[Clonar chaves de acesso S3 usando a API](#)".

Ver as chaves de acesso S3 de outro usuário

Se você estiver usando um locatário S3 e tiver permissões apropriadas, poderá visualizar as chaves de acesso S3 de outro usuário. Você pode classificar a lista por tempo de expiração para determinar quais chaves expirarão em breve. Conforme necessário, você pode criar novas chaves e excluir chaves que não estão mais em uso.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um "[navegador da web compatível](#)".
- Você tem o "[Permissão de acesso root](#)".



Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidas para esse usuário no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da conta e nunca as compartilhe com outros usuários.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO > Usuários**.
2. Na página Usuários, selecione o usuário cujas chaves de acesso S3 você deseja visualizar.
3. Na página Detalhes do usuário, selecione **Chaves de acesso**.
4. Classifique as chaves por **Tempo de expiração** ou **ID da chave de acesso**.
5. Conforme necessário, crie novas chaves e exclua manualmente as chaves que não estão mais em uso.

Se você criar novas chaves antes que as chaves existentes expirem, o usuário poderá começar a usar as novas chaves sem perder temporariamente o acesso aos objetos na conta.

Chaves expiradas são removidas automaticamente.

Informações relacionadas

- ["Crie chaves de acesso S3 de outro usuário"](#)
- ["Excluir chaves de acesso S3 de outro usuário"](#)

Excluir chaves de acesso S3 de outro usuário

Se você estiver usando um locatário S3 e tiver permissões apropriadas, poderá excluir as chaves de acesso S3 de outro usuário. Depois que uma chave de acesso é excluída, ela não pode mais ser usada para acessar os objetos e buckets na conta do locatário.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).



Os buckets e objetos do S3 pertencentes a um usuário podem ser acessados usando o ID da chave de acesso e a chave de acesso secreta exibidas para esse usuário no Gerenciador de Tenants. Por esse motivo, proteja as chaves de acesso como faria com uma senha. Alterne as chaves de acesso regularmente, remova quaisquer chaves não utilizadas da conta e nunca as compartilhe com outros usuários.

Passos

1. Selecione **GERENCIAMENTO DE ACESSO > Usuários**.
2. Na página Usuários, selecione o usuário cujas chaves de acesso S3 você deseja gerenciar.
3. Na página Detalhes do usuário, selecione **Chaves de acesso** e marque a caixa de seleção de cada chave de acesso que deseja excluir.
4. Selecione **Ações > Excluir chave selecionada**.
5. Na caixa de diálogo de confirmação, selecione **Tecla Delete**.

Uma mensagem de confirmação aparece no canto superior direito da página.

Gerenciar buckets S3

Criar um bucket S3

Você pode usar o Tenant Manager para criar buckets do S3 para dados de objetos.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem acesso Root ou Gerenciar todos os buckets ["permissão"](#) . Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.



Permissões para definir ou modificar propriedades de bloqueio de objeto S3 de buckets ou objetos podem ser concedidas por ["política de bucket ou política de grupo"](#) .

- Se você planeja habilitar o S3 Object Lock para um bucket, um administrador de grade habilitou a configuração global S3 Object Lock para o sistema StorageGRID , e você revisou os requisitos para buckets e objetos do S3 Object Lock.
- Se cada locatário tiver 5.000 buckets, cada nó de armazenamento na grade terá no mínimo 64 GB de RAM.



Cada grade pode ter no máximo 100.000 buckets.

Acesse o assistente

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
2. Selecione **Criar bucket**.

Insira os detalhes

Passos

1. Insira detalhes do bucket.

Campo	Descrição
Nome do balde	Um nome para o bucket que esteja em conformidade com estas regras: • Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário). • Deve ser compatível com DNS. • Deve conter no mínimo 3 e no máximo 63 caracteres. • Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hifens. • Não deve conter pontos em solicitações de estilo de hospedagem virtual. Os períodos causarão problemas com a verificação do certificado curinga do servidor. Para mais informações, consulte o "Documentação da Amazon Web Services (AWS) sobre regras de nomenclatura de buckets" . Observação: você não pode alterar o nome do bucket depois de criá-lo.
Região	A região do balde. O administrador do StorageGRID gerencia as regiões disponíveis. A região de um bucket pode afetar a política de proteção de dados aplicada aos objetos. Por padrão, todos os buckets são criados no <code>us-east-1</code> região. Observação: você não pode alterar a região depois de criar o bucket.

2. Selecione **Continuar**.

Gerenciar configurações

Passos

1. Opcionalmente, habilite o controle de versão de objeto para o bucket.

Habilite o controle de versão de objetos se quiser armazenar todas as versões de cada objeto neste bucket. Você pode então recuperar versões anteriores de um objeto conforme necessário. Você deve habilitar o controle de versão de objetos se o bucket for usado para replicação entre grades.

2. Se a configuração global do S3 Object Lock estiver habilitada, opcionalmente habilite o S3 Object Lock para que o bucket armazene objetos usando um modelo WORM (gravar uma vez e ler várias vezes).

Habilite o Bloqueio de Objetos S3 para um bucket somente se você precisar manter objetos por um período fixo de tempo, por exemplo, para atender a determinados requisitos regulatórios. O Bloqueio de Objetos do S3 é uma configuração permanente que ajuda a evitar que objetos sejam excluídos ou substituídos por um período fixo de tempo ou indefinidamente.



Depois que a configuração de bloqueio de objeto do S3 é habilitada para um bucket, ela não pode ser desabilitada. Qualquer pessoa com as permissões corretas pode adicionar objetos a este bucket que não podem ser alterados. Talvez você não consiga excluir esses objetos ou o próprio bucket.

Se você habilitar o S3 Object Lock para um bucket, o controle de versão do bucket será habilitado automaticamente.

3. Se você selecionou **Ativar bloqueio de objeto S3**, opcionalmente ative **Retenção padrão** para este bucket.



O administrador da sua rede deve dar-lhe permissão para ["usar recursos específicos do S3 Object Lock"](#).

Quando a **Retenção padrão** estiver habilitada, novos objetos adicionados ao bucket serão automaticamente protegidos contra exclusão ou substituição. A configuração **Retenção padrão** não se aplica a objetos que têm seus próprios períodos de retenção.

- a. Se **Retenção padrão** estiver habilitado, especifique um **Modo de retenção padrão** para o bucket.

Modo de retenção padrão	Descrição
Governança	• Usuários com o <code>s3:BypassGovernanceRetention</code> permissão pode usar o <code>x-amz-bypass-governance-retention: true</code> cabeçalho de solicitação para ignorar as 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.
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. Observação: o administrador da sua rede deve permitir que você use o modo de conformidade.

- b. Se **Retenção padrão** estiver habilitado, especifique o **Período de retenção padrão** para o bucket.

O **Período de retenção padrão** indica por quanto tempo novos objetos adicionados a este bucket devem ser retidos, a partir do momento em que são ingeridos. Especifique um valor menor ou igual ao período máximo de retenção do locatário, conforme definido pelo administrador da grade.

Um período de retenção *máximo*, que pode ser um valor de 1 dia a 100 anos, é definido quando o administrador da grade cria o locatário. Quando você define um período de retenção *padrão*, ele não pode exceder o valor definido para o período máximo de retenção. Se necessário, peça ao administrador da sua rede para aumentar ou diminuir o período máximo de retenção.

4. Opcionalmente, selecione **Ativar limite de capacidade**.

O limite de capacidade é a capacidade máxima disponível para os objetos deste bucket. Este valor representa uma quantidade lógica (tamanho do objeto), não uma quantidade física (tamanho no disco).

Se nenhum limite for definido, a capacidade deste bucket será ilimitada. Consulte ["Limite de utilização da capacidade"](#) para maiores informações.

5. Selecione **Criar bucket**.

O bucket é criado e adicionado à tabela na página Buckets.

6. Opcionalmente, selecione **Ir para a página de detalhes do bucket** para ["ver detalhes do bucket"](#) e executar configurações adicionais.

Ver detalhes do bucket

Você pode visualizar os buckets na sua conta de locatário.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root, gerenciar todos os buckets ou visualizar todos os buckets"](#). Essas permissões substituem as configurações de permissão em políticas de grupo ou bucket.

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.

A página Buckets é exibida.

2. Revise a tabela de resumo para cada bucket.

Conforme necessário, você pode classificar as informações por qualquer coluna ou pode avançar e voltar na lista.



Os valores de Contagem de Objetos, Espaço Usado e Uso exibidos são estimativas. Essas estimativas são afetadas pelo tempo de ingestão, pela conectividade de rede e pelo status do nó. Se os buckets tiverem o controle de versão habilitado, as versões de objetos excluídas serão incluídas na contagem de objetos.

Nome

Nome exclusivo do bucket, que não pode ser alterado.

Recursos habilitados

A lista de recursos habilitados para o bucket.

Bloqueio de Objeto S3

Se o bloqueio de objeto S3 está habilitado para o bucket.

Esta coluna aparece somente se o Bloqueio de Objeto S3 estiver habilitado para a grade. Esta coluna também mostra informações para quaisquer buckets compatíveis legados.

Região

A região do bucket, que não pode ser alterada. Esta coluna está oculta por padrão.

Contagem de objetos

O número de objetos neste bucket. Se os buckets tiverem o controle de versão habilitado, versões de

objetos não atuais serão incluídas neste valor.

Quando objetos são adicionados ou excluídos, esse valor pode não ser atualizado imediatamente.

Espaço utilizado

O tamanho lógico de todos os objetos no bucket. O tamanho lógico não inclui o espaço real necessário para cópias replicadas ou codificadas para eliminação ou para metadados de objetos.

Este valor pode levar até 10 minutos para ser atualizado.

Uso

A porcentagem utilizada do limite de capacidade do bucket, se um tiver sido definido.

O valor de uso é baseado em estimativas internas e pode ser excedido em alguns casos. Por exemplo, o StorageGRID verifica o limite de capacidade (se definido) quando um locatário começa a carregar objetos e rejeita novas ingestões para esse bucket se o locatário tiver excedido o limite de capacidade. No entanto, o StorageGRID não leva em consideração o tamanho do upload atual ao determinar se o limite de capacidade foi excedido. Se os objetos forem excluídos, um locatário poderá ser temporariamente impedido de carregar novos objetos neste bucket até que o uso do limite de capacidade seja recalculado. Os cálculos podem levar 10 minutos ou mais.

Este valor indica o tamanho lógico, não o tamanho físico necessário para armazenar os objetos e seus metadados.

Capacidade

Se definido, o limite de capacidade do bucket.

Data de criação

Data e hora em que o bucket foi criado. Esta coluna está oculta por padrão.

3. Para visualizar detalhes de um bucket específico, selecione o nome do bucket na tabela.
 - a. Veja as informações resumidas na parte superior da página da web para confirmar os detalhes do bucket, como região e contagem de objetos.
 - b. Veja a barra de uso do limite de capacidade. Se o uso for de 100% ou próximo de 100%, considere aumentar o limite ou excluir alguns objetos.
 - c. Conforme necessário, selecione **Excluir objetos no bucket** e **Excluir bucket**.



Preste muita atenção aos avisos que aparecem quando você seleciona cada uma dessas opções. Para mais informações, consulte:

- ["Excluir todos os objetos em um bucket"](#)
- ["Excluir um bucket"](#)(o balde deve estar vazio)

- d. Visualize ou altere as configurações do bucket em cada uma das guias, conforme necessário.
 - **Console S3:** visualize os objetos do bucket. Para mais informações, consulte ["Usar o console S3"](#).
 - **Opções de bucket:** visualize ou altere as configurações de opções. Algumas configurações, como o S3 Object Lock, não podem ser alteradas após a criação do bucket.
 - ["Gerenciar consistência de bucket"](#)
 - ["Últimas atualizações de tempo de acesso"](#)

- "Limite de capacidade"
- "Controle de versão de objetos"
- "Bloqueio de Objeto S3"
- "Retenção de bucket padrão"
- "Gerenciar replicação entre redes"(se permitido para o inquilino)
- **Serviços de plataforma:**"Gerenciar serviços de plataforma" (se permitido para o inquilino)
- **Acesso ao bucket:** visualize ou altere as configurações de opções. Você deve ter permissões de acesso específicas.
 - Configurar"Compartilhamento de Recursos de Origem Cruzada (CORS)" para que o bucket e os objetos no bucket sejam acessíveis a aplicativos web em outros domínios.
 - "Controlar o acesso do usuário"para um bucket S3 e objetos nesse bucket.

Aplicar uma tag de política ILM a um bucket

Escolha uma tag de política de ILM para aplicar a um bucket com base nos seus requisitos de armazenamento de objetos.

A política ILM controla onde os dados do objeto são armazenados e se eles são excluídos após um determinado período de tempo. O administrador da grade cria políticas de ILM e as atribui a tags de política de ILM ao usar várias políticas ativas.



Evite reatribuir frequentemente a tag de política de um bucket. Caso contrário, poderão ocorrer problemas de desempenho.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um"navegador da web compatível" .
- Você pertence a um grupo de usuários que tem o"Permissão de acesso root, gerenciar todos os buckets ou visualizar todos os buckets" . Essas permissões substituem as configurações de permissão em políticas de grupo ou bucket.

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.

A página Buckets é exibida. Conforme necessário, você pode classificar as informações por qualquer coluna ou pode avançar e voltar na lista.

2. Selecione o nome do bucket ao qual você deseja atribuir uma tag de política do ILM.

Você também pode alterar a atribuição de tags da política ILM para um bucket que já tenha uma tag atribuída.



Os valores de Contagem de Objetos e Espaço Usado exibidos são estimativas. Essas estimativas são afetadas pelo tempo de ingestão, pela conectividade de rede e pelo status do nó. Se os buckets tiverem o controle de versão habilitado, as versões de objetos excluídas serão incluídas na contagem de objetos.

3. Na guia Opções de bucket, expanda o acordeão de tags de política do ILM. Este acordeão só aparece se o administrador da grade tiver habilitado o uso de tags de política personalizadas.

4. Leia a descrição de cada tag de política para determinar qual tag deve ser aplicada ao bucket.



Alterar a tag de política do ILM para um bucket acionará a reavaliação do ILM de todos os objetos no bucket. Se a nova política reter objetos por um tempo limitado, os objetos mais antigos serão excluídos.

5. Selecione o botão de opção para a tag que você deseja atribuir ao bucket.

6. Selecione **Salvar alterações**. Uma nova tag de bucket S3 será definida no bucket com a chave `NTAP-SG-ILM-BUCKET-TAG` e o valor do nome da tag de política do ILM.



Certifique-se de que seus aplicativos S3 não substituam ou excluam acidentalmente a nova tag de bucket. Se esta tag for omitida ao aplicar um novo TagSet ao bucket, os objetos no bucket voltarão a ser avaliados em relação à política ILM padrão.



Defina e modifique tags de política do ILM usando somente o Tenant Manager ou a API do Tenant Manager onde a tag de política do ILM é validada. Não modifique o `NTAP-SG-ILM-BUCKET-TAG` Marcação de política do ILM usando a API `PutBucketTagging` do S3 ou a API `DeleteBucketTagging` do S3.



Alterar a tag de política atribuída a um bucket tem um impacto temporário no desempenho enquanto os objetos estão sendo reavaliados usando a nova política do ILM.

Gerenciar política de bucket

Você pode controlar o acesso do usuário a um bucket do S3 e aos objetos nesse bucket.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#). As permissões Exibir todos os buckets e Gerenciar todos os buckets permitem apenas a visualização.
- Você verificou se o número necessário de nós de armazenamento e sites está disponível. Se dois ou mais nós de armazenamento não estiverem disponíveis em nenhum site, ou se um site não estiver disponível, as alterações nessas configurações poderão não estar disponíveis.

Passos

1. Selecione **Buckets** e, em seguida, selecione o bucket que você deseja gerenciar.
2. Na página de detalhes do bucket, selecione **Acesso ao bucket > Política do bucket**.
3. Faça um dos seguintes:
 - Insira uma política de bucket marcando a caixa de seleção **Ativar política**. Em seguida, insira uma string válida no formato JSON.

Cada política de bucket tem um limite de tamanho de 20.480 bytes.
 - Modifique uma política existente editando a sequência de caracteres.
 - Desabilite uma política desmarcando **Habilitar política**.

Para obter informações detalhadas sobre políticas de bucket, incluindo sintaxe de linguagem e exemplos, consulte ["Exemplos de políticas de bucket"](#).

Gerenciar consistência de bucket

Os valores de consistência podem ser usados para especificar a disponibilidade de alterações nas configurações do bucket, bem como para fornecer um equilíbrio entre a disponibilidade dos objetos dentro de um bucket e a consistência desses objetos em diferentes nós de armazenamento e sites. Você pode alterar os valores de consistência para que sejam diferentes dos valores padrão para que os aplicativos clientes possam atender às suas necessidades operacionais.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Gerenciar todos os buckets ou permissão de acesso root"](#). Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

Diretrizes de consistência de bucket

A consistência do bucket é usada para determinar a consistência dos aplicativos cliente que afetam objetos dentro desse bucket do S3. Em geral, você deve usar a consistência **Read-after-new-write** para seus buckets.

Alterar consistência do bucket

Se a consistência **Leitura após nova gravação** não atender aos requisitos do aplicativo cliente, você poderá alterar a consistência definindo a consistência do bucket ou usando o `Consistency-Control` cabeçalho. O `Consistency-Control` O cabeçalho substitui a consistência do bucket.



Quando você altera a consistência de um bucket, somente os objetos ingeridos após a alteração têm a garantia de atender à configuração revisada.

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
2. Selecione o nome do bucket na tabela.

A página de detalhes do bucket é exibida.

3. Na aba **Opções do bucket**, selecione o ****** acordeão.
4. Selecione uma consistência para operações executadas nos objetos neste bucket.
 - **Todos**: Oferece o mais alto nível de consistência. Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
 - **Strong-global**: Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
 - **Strong-site**: Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.
 - **Leitura após nova gravação** (padrão): 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 .

5. Selecione **Salvar alterações**.

O que acontece quando você altera as configurações do bucket

Os buckets têm várias configurações que afetam o comportamento dos buckets e dos objetos dentro deles.

As seguintes configurações de bucket usam consistência **forte** por padrão. Se dois ou mais nós de armazenamento não estiverem disponíveis em nenhum site, ou se um site não estiver disponível, quaisquer alterações nessas configurações poderão não estar disponíveis.

- ["Exclusão de bucket vazio em segundo plano"](#)
- ["Último horário de acesso"](#)
- ["Ciclo de vida do bucket"](#)
- ["Política de balde"](#)
- ["Etiquetagem de balde"](#)
- ["Controle de versão de bucket"](#)
- ["Bloqueio de Objeto S3"](#)
- ["Criptografia de bucket"](#)



O valor de consistência para controle de versão de bucket, bloqueio de objeto S3 e criptografia de bucket não pode ser definido como um valor que não seja fortemente consistente.

As seguintes configurações de bucket não usam consistência forte e têm maior disponibilidade para alterações. Alterações nessas configurações podem levar algum tempo até surtirem efeito.

- ["Configuração de serviços de plataforma: integração de notificação, replicação ou pesquisa"](#)
- ["Configuração CORS"](#)
- [Alterar consistência do bucket](#)



Se a consistência padrão usada ao alterar as configurações do bucket não atender aos requisitos do aplicativo cliente, você poderá alterar a consistência usando o `Consistency-Control` cabeçalho para o ["API REST S3"](#) ou usando o `reducedConsistency` ou `force` opções no ["API de gerenciamento de inquilinos"](#) .

Habilitar ou desabilitar atualizações do último horário de acesso

Quando os administradores de grade criam as regras de gerenciamento do ciclo de vida das informações (ILM) para um sistema StorageGRID , eles podem, opcionalmente, especificar que o último horário de acesso de um objeto seja usado para determinar se esse objeto deve ser movido para um local de armazenamento diferente. Se estiver usando um locatário do S3, você poderá aproveitar essas regras habilitando atualizações de horário do último acesso para os objetos em um bucket do S3.

Estas instruções se aplicam somente a sistemas StorageGRID que incluem pelo menos uma regra ILM que usa a opção **Último horário de acesso** como um filtro avançado ou como um horário de referência. Você pode ignorar essas instruções se o seu sistema StorageGRID não incluir essa regra. Ver ["Usar a hora do último acesso nas regras do ILM"](#) para mais detalhes.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Gerenciar todos os buckets ou permissão de acesso root"](#) . Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.

Sobre esta tarefa

Último horário de acesso é uma das opções disponíveis para a instrução de posicionamento **Horário de referência** para uma regra ILM. Definir o Tempo de referência para uma regra como Hora do último acesso permite que os administradores da grade especifiquem que os objetos sejam colocados em determinados locais de armazenamento com base em quando esses objetos foram recuperados (lidos ou visualizados) pela última vez.

Por exemplo, para garantir que objetos visualizados recentemente permaneçam em um armazenamento mais rápido, um administrador de grade pode criar uma regra ILM especificando o seguinte:

- Objetos recuperados no mês passado devem permanecer nos nós de armazenamento locais.
- Objetos que não foram recuperados no último mês devem ser movidos para um local externo.

Por padrão, as atualizações do último horário de acesso são desabilitadas. Se o seu sistema StorageGRID incluir uma regra ILM que usa a opção **Último horário de acesso** e você quiser que essa opção se aplique a objetos neste bucket, você deverá habilitar atualizações para o último horário de acesso para os buckets do S3 especificados nessa regra.



Atualizar o último horário de acesso quando um objeto é recuperado pode reduzir o desempenho do StorageGRID , especialmente para objetos pequenos.

Um impacto no desempenho ocorre com as atualizações do último horário de acesso porque o StorageGRID deve executar estas etapas adicionais sempre que os objetos são recuperados:

- Atualizar os objetos com novos registros de data e hora
- Adicione os objetos à fila do ILM para que eles possam ser reavaliados em relação às regras e políticas atuais do ILM

A tabela resume o comportamento aplicado a todos os objetos no bucket quando o último horário de acesso é desabilitado ou habilitado.

Tipo de solicitação	Comportamento se o último horário de acesso estiver desabilitado (padrão)		Comportamento se o último horário de acesso estiver habilitado	
	Último horário de acesso atualizado?	Objeto adicionado à fila de avaliação do ILM?	Último horário de acesso atualizado?	Objeto adicionado à fila de avaliação do ILM?
Solicitação para recuperar um objeto, sua lista de controle de acesso ou seus metadados	Não	Não	Sim	Sim

Solicitação para atualizar os metadados de um objeto	Sim	Sim	Sim	Sim
Solicitação para listar objetos ou versões de objetos	Não	Não	Não	Não
Solicitação para copiar um objeto de um bucket para outro	• Não, para a cópia de origem • Sim, para a cópia de destino	• Não, para a cópia de origem • Sim, para a cópia de destino	• Sim, 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	Sim, para o objeto montado	Sim, para o objeto montado

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
2. Selecione o nome do bucket na tabela.

A página de detalhes do bucket é exibida.

3. Na aba **Opções do bucket**, selecione o acordeão **Atualizações de hora do último acesso**.
4. Habilitar ou desabilitar atualizações de horário do último acesso.
5. Selecione **Salvar alterações**.

Alterar o controle de versão do objeto para um bucket

Se estiver usando um locatário do S3, você poderá alterar o estado de controle de versão dos buckets do S3.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Gerenciar todos os buckets ou permissão de acesso root"](#). Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Você verificou se o número necessário de nós de armazenamento e sites está disponível. Se dois ou mais nós de armazenamento não estiverem disponíveis em nenhum site, ou se um site não estiver disponível, as alterações nessas configurações poderão não estar disponíveis.

Sobre esta tarefa

Você pode habilitar ou suspender o controle de versão de objetos para um bucket. Depois de habilitar o controle de versão para um bucket, ele não poderá retornar a um estado sem versão. No entanto, você pode suspender o controle de versão do bucket.

- Desativado: o controle de versão nunca foi habilitado

- **Habilitado:** o controle de versão está habilitado
- **Suspenso:** o controle de versão foi habilitado anteriormente e está suspenso

Para mais informações, consulte o seguinte:

- ["Controle de versão de objetos"](#)
- ["Regras e políticas do ILM para objetos versionados do S3 \(Exemplo 4\)"](#)
- ["Como os objetos são excluídos"](#)

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
2. Selecione o nome do bucket na tabela.

A página de detalhes do bucket é exibida.

3. Na aba **Opções do bucket**, selecione o acordeão **Controle de versão do objeto**.
4. Selecione um estado de controle de versão para os objetos neste bucket.

O controle de versão de objetos deve permanecer habilitado para um bucket usado para replicação entre grades. Se o bloqueio de objeto S3 ou a conformidade com o legado estiver habilitado, as opções de **Controle de versão do objeto** serão desabilitadas.

Opção	Descrição
Habilitar controle de versão	Habilite o controle de versão de objetos se quiser armazenar todas as versões de cada objeto neste bucket. Você pode então recuperar versões anteriores de um objeto conforme necessário. Objetos que já estavam no bucket serão versionados quando forem modificados por um usuário.
Suspender o controle de versão	Suspenda o controle de versão do objeto se não quiser mais que novas versões do objeto sejam criadas. Você ainda pode recuperar qualquer versão de objeto existente.

5. Selecione **Salvar alterações**.

Use o S3 Object Lock para reter objetos

Você pode usar o S3 Object Lock se os buckets e objetos precisarem estar em conformidade com os requisitos regulatórios de retenção.



O administrador da grade deve lhe dar permissão para usar recursos específicos do S3 Object Lock.

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](#)

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](#)".

Tarefas de bloqueio de objeto S3

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 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.

Ainda posso gerenciar buckets compatíveis legados?

O recurso S3 Object Lock substitui o recurso Compliance que estava disponível em versões anteriores do StorageGRID . Se você criou buckets compatíveis usando uma versão anterior do StorageGRID, poderá continuar a gerenciar as configurações desses buckets; no entanto, não poderá mais criar novos buckets compatíveis. Para obter instruções, consulte https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5 ["Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"] .

Atualizar retenção padrão do bloqueio de objeto S3

Se você habilitou o Bloqueio de Objeto S3 ao criar o bucket, poderá editá-lo para alterar as configurações de retenção padrão. Você pode habilitar (ou desabilitar) a retenção padrão e definir um modo e um período de retenção padrão.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Gerenciar todos os buckets ou permissão de acesso root"](#) . Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- O S3 Object Lock está habilitado globalmente para seu sistema StorageGRID , e você habilitou o S3 Object Lock quando criou o bucket. Ver ["Use o S3 Object Lock para reter objetos"](#) .

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
2. Selecione o nome do bucket na tabela.

A página de detalhes do bucket é exibida.

3. Na aba **Opções do Bucket**, selecione o acordeão **S3 Object Lock**.
4. Opcionalmente, habilite ou desabilite a **Retenção padrão** para este bucket.

As alterações nessa configuração não se aplicam a objetos que já estão no bucket ou a quaisquer objetos que possam ter seus próprios períodos de retenção.

5. Se **Retenção padrão** estiver habilitado, especifique um **Modo de retenção padrão** para o bucket.

Modo de retenção padrão	Descrição
Governança	• Usuários com o <code>s3:BypassGovernanceRetention</code> permissão pode usar o <code>x-amz-bypass-governance-retention: true</code> cabeçalho de solicitação para ignorar as 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.

Modo de retenção padrão	Descrição
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. Observação: o administrador da sua rede deve permitir que você use o modo de conformidade.

6. Se **Retenção padrão** estiver habilitado, especifique o **Período de retenção padrão** para o bucket.

O **Período de retenção padrão** indica por quanto tempo novos objetos adicionados a este bucket devem ser retidos, a partir do momento em que são ingeridos. Especifique um valor menor ou igual ao período máximo de retenção do locatário, conforme definido pelo administrador da grade.

Um período de retenção *máximo*, que pode ser um valor de 1 dia a 100 anos, é definido quando o administrador da grade cria o locatário. Quando você define um período de retenção *padrão*, ele não pode exceder o valor definido para o período máximo de retenção. Se necessário, peça ao administrador da sua rede para aumentar ou diminuir o período máximo de retenção.

7. Selecione **Salvar alterações**.

Configurar 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.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Para solicitações de configuração GET CORS, você pertence a um grupo de usuários que tem o ["Permissão para gerenciar todos os buckets ou visualizar todos os buckets"](#). Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Para solicitações de configuração PUT CORS, você pertence a um grupo de usuários que tem o ["Permissão para gerenciar todos os buckets"](#). Esta permissão substitui as configurações de permissões em políticas de grupo ou bucket.
- O ["Permissão de acesso root"](#) fornece acesso a todas as solicitações de configuração do CORS.

Sobre esta tarefa

O compartilhamento de recursos entre origens (CORS) é um mecanismo de segurança que permite que aplicativos web clientes em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket S3 chamado `Images` para armazenar gráficos. Ao configurar o CORS para o `Images` bucket, você pode permitir que as imagens nesse bucket sejam exibidas no site `http://www.example.com`.

Habilitar CORS para um bucket

Passos

1. Use um editor de texto para criar o XML necessário. Este exemplo mostra o XML usado para habilitar o CORS para um bucket S3. Especificamente:
 - Permite que qualquer domínio envie solicitações GET para o bucket
 - Permite apenas o `http://www.example.com` domínio para enviar solicitações GET, POST e DELETE
 - Todos os cabeçalhos de solicitação são permitidos

```
<CORSConfiguration
  xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
  <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
  <CORSRule>
    <AllowedOrigin>http://www.example.com</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
</CORSConfiguration>
```

Para obter mais informações sobre o XML de configuração do CORS, consulte ["Documentação da Amazon Web Services \(AWS\): Guia do usuário do Amazon Simple Storage Service"](#).

2. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
3. Selecione o nome do bucket na tabela.

A página de detalhes do bucket é exibida.

4. Na aba **Acesso ao bucket**, selecione o acordeão **Compartilhamento de recursos entre origens (CORS)**.
5. Marque a caixa de seleção **Ativar CORS**.
6. Cole o XML de configuração do CORS na caixa de texto.
7. Selecione **Salvar alterações**.

Modificar configuração CORS

Passos

1. Atualize o XML de configuração do CORS na caixa de texto ou selecione **Limpar** para recomençar.
2. Selecione **Salvar alterações**.

Desabilitar configuração CORS

Passos

1. Desmarque a caixa de seleção **Ativar CORS**.
2. Selecione **Salvar alterações**.

Excluir objetos no bucket

Você pode usar o Gerenciador de Tenants para excluir os objetos em um ou mais buckets.

Considerações e requisitos

Antes de executar essas etapas, observe o seguinte:

- Quando você exclui os objetos em um bucket, o StorageGRID remove permanentemente todos os objetos e todas as versões de objetos em cada bucket selecionado de todos os nós e sites no seu sistema StorageGRID . O StorageGRID também remove quaisquer metadados de objetos relacionados. Você não poderá recuperar essas informações.
- A exclusão de todos os objetos em um bucket pode levar minutos, dias ou até semanas, dependendo do número de objetos, cópias de objetos e operações simultâneas.
- Se um balde tiver "[Bloqueio de objeto S3 habilitado](#)" , ele pode permanecer no estado **Excluindo objetos: somente leitura** por *anos*.



Um bucket que usa o S3 Object Lock permanecerá no estado **Excluindo objetos: somente leitura** até que a data de retenção seja atingida para todos os objetos e quaisquer retenções legais sejam removidas.

- Enquanto os objetos estão sendo excluídos, o estado do bucket é **Excluindo objetos: somente leitura**. Nesse estado, você não pode adicionar novos objetos ao bucket.
- Quando todos os objetos forem excluídos, o bucket permanecerá no estado somente leitura. Você pode fazer um dos seguintes:
 - Retorne o bucket ao modo de gravação e reutilize-o para novos objetos
 - Excluir o balde
 - Mantenha o bucket no modo somente leitura para reservar seu nome para uso futuro
- Se um bucket tiver o controle de versão de objeto habilitado, os marcadores de exclusão que foram criados no StorageGRID 11.8 ou posterior poderão ser removidos usando Excluir objetos nas operações do bucket.
- Se um bucket tiver o controle de versão de objeto habilitado, a operação de exclusão de objetos não removerá os marcadores de exclusão que foram criados no StorageGRID 11.7 ou anterior. Veja informações sobre como excluir objetos em um bucket em "[Como objetos versionados do S3 são excluídos](#)" .
- Se você usar "[replicação entre grades](#)" , observe o seguinte:
 - Usar esta opção não exclui nenhum objeto do bucket na outra grade.
 - Se você selecionar esta opção para o bucket de origem, o alerta **Falha de replicação entre grades** será acionado se você adicionar objetos ao bucket de destino na outra grade. Se você não puder garantir que ninguém adicionará objetos ao bucket na outra grade, "[desabilitar replicação entre redes](#)" para esse bucket antes de excluir todos os objetos do bucket.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Permissão de acesso root"](#) . Esta permissão substitui as configurações de permissões em políticas de grupo ou bucket.

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.

A página Buckets é exibida e mostra todos os buckets do S3 existentes.

2. Use o menu **Ações** ou a página de detalhes de um bucket específico.

Menu de ações

- a. Marque a caixa de seleção de cada bucket do qual você deseja excluir objetos.
- b. Selecione **Ações > Excluir objetos no bucket**.

Página de detalhes

- a. Selecione um nome de bucket para exibir seus detalhes.
- b. Selecione **Excluir objetos no bucket**.

3. Quando a caixa de diálogo de confirmação aparecer, revise os detalhes, digite **Sim** e selecione **OK**.
4. Aguarde o início da operação de exclusão.

Depois de alguns minutos:

- Um banner de status amarelo aparece na página de detalhes do bucket. A barra de progresso representa a porcentagem de objetos que foram excluídos.
- **(somente leitura)** aparece após o nome do bucket na página de detalhes do bucket.
- **(Excluindo objetos: somente leitura)** aparece ao lado do nome do bucket na página Buckets.

Buckets > my-bucket

my-bucket (read-only)

Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 3

[View bucket contents in Experimental S3 Console](#)

Delete bucket

 **All bucket objects are being deleted**

StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select **Stop deleting objects**. You cannot restore objects that have already been deleted.

0% (0 of 3 objects deleted)

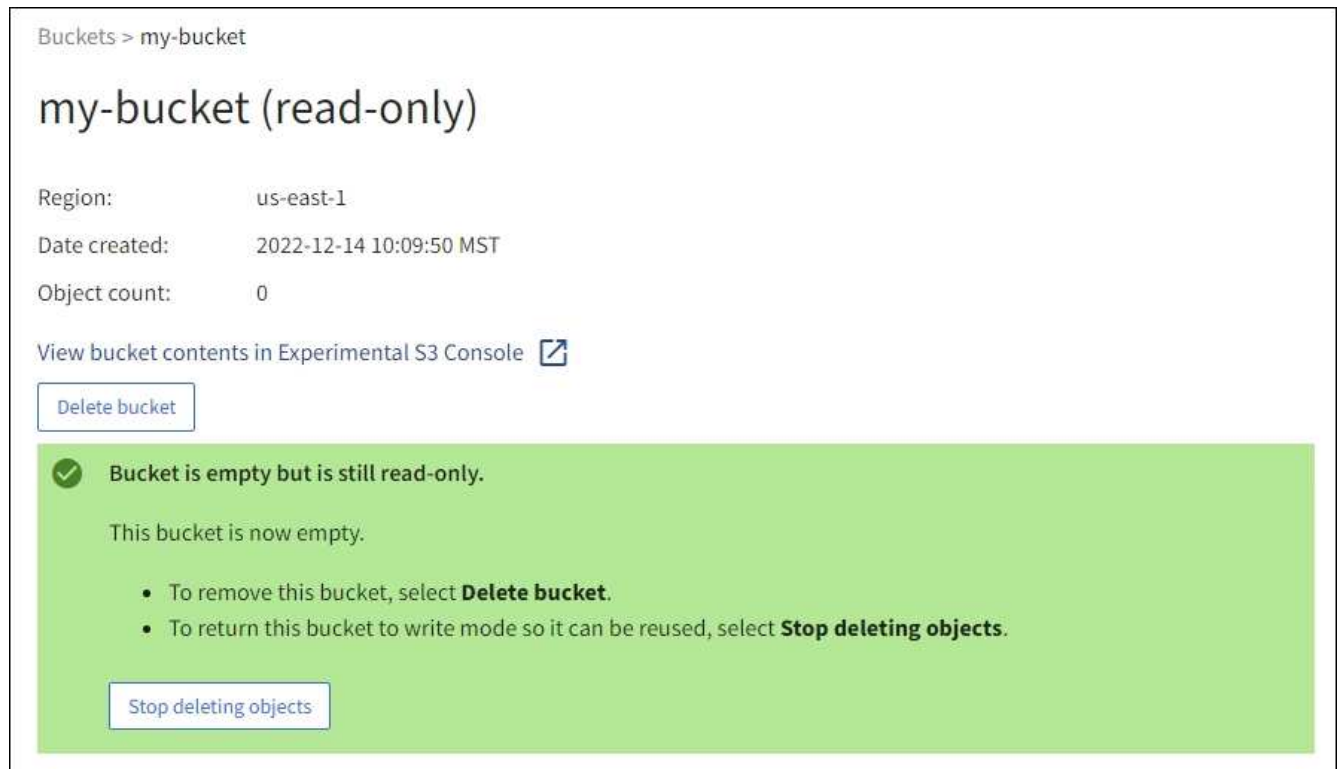
Stop deleting objects

5. Conforme necessário enquanto a operação estiver em execução, selecione **Parar de excluir objetos** para interromper o processo. Em seguida, opcionalmente, selecione **Excluir objetos no bucket** para retomar o processo.

Quando você seleciona **Parar de excluir objetos**, o bucket retorna ao modo de gravação; no entanto, você não pode acessar ou restaurar nenhum objeto que tenha sido excluído.

6. Aguarde a conclusão da operação.

Quando o bucket está vazio, o banner de status é atualizado, mas o bucket permanece somente leitura.



7. Faça um dos seguintes:

- Saia da página para manter o bucket no modo somente leitura. Por exemplo, você pode manter um bucket vazio no modo somente leitura para reservar o nome do bucket para uso futuro.
- Exclua o bucket. Você pode selecionar **Excluir bucket** para excluir um único bucket ou retornar à página Buckets e selecionar **Ações > Excluir** buckets para remover mais de um bucket.



Se você não conseguir excluir um bucket versionado depois que todos os objetos forem excluídos, os marcadores de exclusão poderão permanecer. Para excluir o bucket, você deve remover todos os marcadores de exclusão restantes.

- Retorne o bucket ao modo de gravação e, opcionalmente, reutilize-o para novos objetos. Você pode selecionar **Parar de excluir objetos** para um único bucket ou retornar à página Buckets e selecionar **Ação > Parar de excluir objetos** para mais de um bucket.

Excluir bucket S3

Você pode usar o Gerenciador de Tenants para excluir um ou mais buckets do S3 que estão vazios.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Gerenciar todos os buckets ou permissão de acesso root"](#). Essas permissões substituem as configurações de permissões em políticas de grupo ou bucket.
- Os buckets que você deseja excluir estão vazios. Se os buckets que você deseja excluir *não* estiverem vazios, ["excluir objetos do bucket"](#).

Sobre esta tarefa

Estas instruções descrevem como excluir um bucket S3 usando o Gerenciador de Tenants. Você também

pode excluir buckets S3 usando o ["API de gerenciamento de inquilinos"](#) ou o ["API REST S3"](#) .

Não é possível excluir um bucket do S3 se ele contiver objetos, versões de objetos não atuais ou marcadores de exclusão. Para obter informações sobre como os objetos versionados do S3 são excluídos, consulte ["Como os objetos são excluídos"](#) .

Passos

1. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.

A página Buckets é exibida e mostra todos os buckets do S3 existentes.

2. Use o menu **Ações** ou a página de detalhes de um bucket específico.

Menu de ações

- a. Marque a caixa de seleção de cada bucket que você deseja excluir.
- b. Selecione **Ações > Excluir buckets**.

Página de detalhes

- a. Selecione um nome de bucket para exibir seus detalhes.
- b. Selecione **Excluir bucket**.

3. Quando a caixa de diálogo de confirmação aparecer, selecione **Sim**.

O StorageGRID confirma que cada bucket está vazio e então exclui cada bucket. Esta operação pode levar alguns minutos.

Se um bucket não estiver vazio, uma mensagem de erro será exibida. Você deve ["exclua todos os objetos e quaisquer marcadores de exclusão no bucket"](#) antes de poder excluir o bucket.

Usar o console S3

Você pode usar o Console S3 para visualizar e gerenciar os objetos em um bucket S3.

O console S3 permite que você:

- Carregar, baixar, renomear, copiar, mover e excluir objetos
- Visualizar, reverter, baixar e excluir versões de objetos
- Pesquisar objetos por prefixo
- Gerenciar tags de objetos
- Exibir metadados do objeto
- Visualizar, criar, renomear, copiar, mover e excluir pastas

O S3 Console oferece uma experiência de usuário aprimorada para os casos mais comuns. Ele não foi projetado para substituir operações de CLI ou API em todas as situações.



Se o uso do Console S3 fizer com que as operações demorem muito (por exemplo, minutos ou horas), considere:

- Reduzindo o número de objetos selecionados
- Usando métodos não gráficos (API ou CLI) para acessar seus dados

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Se você quiser gerenciar objetos, pertença a um grupo de usuários que tenha permissão de acesso Root. Como alternativa, você pertence a um grupo de usuários que tem a permissão Usar a guia Console do S3 e a permissão Exibir todos os buckets ou Gerenciar todos os buckets. Ver ["Permissões de gerenciamento de inquilinos"](#).
- Uma política de grupo ou bucket S3 foi configurada para o usuário. Ver ["Use políticas de acesso a buckets e grupos"](#).
- Você sabe o ID da chave de acesso e a chave de acesso secreta do usuário. Opcionalmente, você tem um `.csv` arquivo contendo essas informações. Veja o ["instruções para criar chaves de acesso"](#).

Passos

1. Selecione **ARMAZENAMENTO > Buckets > nome do bucket**.
2. Selecione a aba Console S3.
3. Cole o ID da chave de acesso e a chave de acesso secreta nos campos. Caso contrário, selecione **Carregar chaves de acesso** e selecione seu `.csv` arquivo.
4. Selecione * Sign in*.
5. A tabela de objetos de bucket é exibida. Você pode gerenciar objetos conforme necessário.

Informações adicionais

- **Pesquisar por prefixo:** O recurso de pesquisa por prefixo pesquisa apenas objetos que começam com uma palavra específica relativa à pasta atual. A pesquisa não inclui objetos que contenham a palavra em outro lugar. Esta regra também se aplica a objetos dentro de pastas. Por exemplo, uma busca por `folder1/folder2/somefile-` retornaria objetos que estão dentro do `folder1/folder2/` pasta e comece com a palavra `somefile-`.
- **Arrastar e soltar:** Você pode arrastar e soltar arquivos do gerenciador de arquivos do seu computador para o Console S3. Entretanto, você não pode carregar pastas.
- **Operações em pastas:** Quando você move, copia ou renomeia uma pasta, todos os objetos na pasta são atualizados um de cada vez, o que pode levar algum tempo.
- **Exclusão permanente quando o controle de versão do bucket está desabilitado:** quando você substitui ou exclui um objeto em um bucket com o controle de versão desabilitado, a operação é permanente. Ver ["Alterar o controle de versão do objeto para um bucket"](#).

Gerenciar serviços da plataforma S3

Serviços da plataforma S3

Visão geral e considerações sobre serviços de plataforma

Antes de implementar serviços de plataforma, revise a visão geral e as considerações para usar esses serviços.

Para obter informações sobre o S3, consulte ["Usar API REST do S3"](#).

Visão geral dos serviços da plataforma

Os serviços da plataforma StorageGRID podem ajudar você a implementar uma estratégia de nuvem híbrida, permitindo que você envie notificações de eventos e cópias de objetos S3 e metadados de objetos para destinos externos.

Como o local de destino dos serviços de plataforma geralmente é externo à sua implantação do StorageGRID, os serviços de plataforma oferecem o poder e a flexibilidade que vêm do uso de recursos de armazenamento externo, serviços de notificação e serviços de pesquisa ou análise para seus dados.

Qualquer combinação de serviços de plataforma pode ser configurada para um único bucket S3. Por exemplo, você pode configurar ambos ["Serviço CloudMirror"](#) e ["notificações"](#) em um bucket StorageGRID S3 para que você possa espelhar objetos específicos no Amazon Simple Storage Service (S3), enquanto envia uma notificação sobre cada objeto para um aplicativo de monitoramento de terceiros para ajudar você a rastrear suas despesas com a AWS.



O uso dos serviços da plataforma deve ser habilitado para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a API de gerenciamento de grade.

Como os serviços da plataforma são configurados

Os serviços de plataforma se comunicam com endpoints externos que você configura usando o ["Gerente de inquilinos"](#) ou o ["API de gerenciamento de inquilinos"](#). Cada ponto de extremidade representa um destino externo, como um bucket do StorageGRID S3, um bucket do Amazon Web Services, um tópico do Amazon SNS ou um cluster do Elasticsearch hospedado localmente, na AWS ou em outro lugar.

Depois de criar um ponto de extremidade externo, você pode habilitar um serviço de plataforma para um bucket adicionando configuração XML ao bucket. A configuração XML identifica os objetos nos quais o bucket deve atuar, a ação que o bucket deve executar e o ponto de extremidade que o bucket deve usar para o serviço.

Você deve adicionar configurações XML separadas para cada serviço de plataforma que deseja configurar. Por exemplo:

- Se você quiser todos os objetos cujas chaves começam com `/images` para ser replicado em um bucket do Amazon S3, você deve adicionar uma configuração de replicação ao bucket de origem.
- Se você também quiser enviar notificações quando esses objetos forem armazenados no bucket, adicione uma configuração de notificações.
- Se quiser indexar os metadados desses objetos, você deve adicionar a configuração de notificação de metadados usada para implementar a integração de pesquisa.

O formato do XML de configuração é regido pelas APIs REST do S3 usadas para implementar os serviços da plataforma StorageGRID :

Serviço de plataforma	API REST S3	Consulte
Replicação do CloudMirror	• Obter replicação do Bucket • PutBucketReplicação	• "Replicação do CloudMirror" • "Operações em baldes"
Notificações	• Obter configuração de notificação de bucket • Configuração de notificação PutBucket	• "Notificações" • "Operações em baldes"
Integração de pesquisa	• Configuração de notificação de metadados do GET Bucket • Configuração de notificação de metadados do PUT Bucket	• "Integração de pesquisa" • "Operações personalizadas do StorageGRID"

Considerações sobre o uso de serviços de plataforma

Consideração	Detalhes
Monitoramento de endpoint de destino	Você deve monitorar a disponibilidade de cada ponto de extremidade de destino. Se a conectividade com o ponto de extremidade de destino for perdida por um longo período de tempo e houver um grande acúmulo de solicitações, solicitações adicionais de clientes (como solicitações PUT) para o StorageGRID falharão. Você deve tentar novamente essas solicitações com falha quando o ponto de extremidade estiver acessível.
Limitação do ponto de extremidade de destino	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.

Consideração	Detalhes
Garantias de encomenda	O StorageGRID garante a ordenação das operações em um objeto dentro de um site. Desde que todas as operações em um objeto estejam no mesmo site, o estado final do objeto (para replicação) sempre será igual ao estado em StorageGRID. O StorageGRID faz o melhor esforço possível para ordenar solicitações quando operações são feitas em sites do StorageGRID . Por exemplo, se você gravar um objeto inicialmente no site A e depois substituir o mesmo objeto no site B, não há garantia de que o objeto final replicado pelo CloudMirror para o bucket de destino seja o objeto mais recente.
Exclusões de objetos controladas por ILM	Para corresponder ao comportamento de exclusão do AWS CRR e do Amazon Simple Notification Service, as solicitações de notificação de eventos e do CloudMirror não são enviadas quando um objeto no bucket de origem é excluído devido às regras do StorageGRID ILM. Por exemplo, nenhuma solicitação de notificação de eventos ou do CloudMirror será enviada se uma regra do ILM excluir um objeto após 14 dias. Em contraste, solicitações de integração de pesquisa são enviadas quando objetos são excluídos devido ao ILM.
Usando endpoints do Kafka	Para endpoints do Kafka, o TLS mútuo não é suportado. Como resultado, se você tiver <code>ssl.client.auth</code> definido para <code>required</code> na configuração do seu broker Kafka, isso pode causar problemas de configuração do endpoint Kafka. A autenticação de endpoints do Kafka usa os seguintes tipos de autenticação. Esses tipos são diferentes daqueles usados para autenticação de outros endpoints, como o Amazon SNS, e exigem credenciais de nome de usuário e senha. • SASL/SIM • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 Observação: As configurações de proxy de armazenamento configuradas não se aplicam aos pontos de extremidade dos serviços da plataforma Kafka.

Considerações sobre o uso do serviço de replicação CloudMirror

Consideração	Detalhes
Status de replicação	O StorageGRID não oferece suporte a <code>x-amz-replication-status</code> cabeçalho.

Consideração	Detalhes
Tamanho do objeto	O tamanho máximo para objetos que podem ser replicados para um bucket de destino pelo serviço de replicação do CloudMirror é 5 TiB, que é o mesmo que o tamanho máximo de objeto <i>compatível</i>. Observação: O tamanho máximo <i>recomendado</i> para uma única operação PutObject é 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multiparte.
Controle de versão de bucket e IDs de versão	Se o bucket S3 de origem no StorageGRID tiver o versionamento habilitado, você também deverá habilitar o versionamento para o bucket de destino. Ao usar o controle de versão, observe que a ordenação das versões de objetos no bucket de destino é de melhor esforço e não é garantida pelo serviço CloudMirror, devido a limitações no protocolo S3. Observação: Os IDs de versão do bucket de origem no StorageGRID não estão relacionados aos IDs de versão do bucket de destino.
Marcação para versões de objetos	O serviço CloudMirror não replica nenhuma solicitação PutObjectTagging ou DeleteObjectTagging que forneça um ID de versão, devido a limitações no protocolo S3. Como os IDs de versão para a origem e o destino não estão relacionados, não há como garantir que uma atualização de tag para um ID de versão específico será replicada. Em contraste, o serviço CloudMirror replica solicitações PutObjectTagging ou DeleteObjectTagging que não especificam um ID de versão. Essas solicitações atualizam as tags para a chave mais recente (ou a versão mais recente, se o bucket tiver versão). Ingestões normais com tags (não atualizações de marcação) também são replicadas.
Uploads multipartes e ETag valores	Ao espelhar objetos que foram carregados usando um upload multiparte, o serviço CloudMirror não preserva as partes. Como resultado, o ETag o valor para o objeto espelhado será diferente do ETag valor do objeto original.
Objetos criptografados com SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente)	O serviço CloudMirror não oferece suporte a objetos criptografados com SSE-C. Se você tentar ingerir um objeto no bucket de origem para replicação do CloudMirror e a solicitação incluir os cabeçalhos de solicitação SSE-C, a operação falhará.
Bucket com bloqueio de objeto S3 habilitado	A replicação não é suportada para buckets de origem ou destino com o S3 Object Lock habilitado.

Entenda o serviço de replicação do CloudMirror

Você pode habilitar a replicação do CloudMirror para um bucket do S3 se quiser que o StorageGRID replique objetos especificados adicionados ao bucket para um ou mais buckets de destino externos.

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 não será suportada se o bucket de origem tiver o S3 Object Lock habilitado.

CloudMirror e ILM

A replicação do CloudMirror opera independentemente das políticas de ILM ativas da grade. O serviço CloudMirror replica objetos conforme eles são armazenados no bucket de origem e os entrega ao bucket de destino o mais rápido possível. A entrega de objetos replicados é acionada quando a ingestão do objeto é bem-sucedida.

CloudMirror e replicação entre grades

A replicação do CloudMirror tem semelhanças e diferenças importantes com o recurso de replicação entre grades. Consulte ["Comparar a replicação entre grades e a replicação do CloudMirror"](#).

CloudMirror e buckets S3

A replicação do CloudMirror normalmente é configurada para usar um bucket S3 externo como destino. No entanto, você também pode configurar a replicação para usar outra implantação do StorageGRID ou qualquer serviço compatível com S3.

Baldes existentes

Quando você habilita a replicação do CloudMirror para um bucket existente, somente os novos objetos adicionados a esse bucket são replicados. Nenhum objeto existente no bucket é replicado. Para forçar a replicação de objetos existentes, você pode atualizar os metadados do objeto existente executando uma cópia do objeto.



Se você estiver usando a replicação do CloudMirror para copiar objetos para um destino do Amazon S3, esteja ciente de que o Amazon S3 limita o tamanho dos metadados definidos pelo usuário em cada cabeçalho de solicitação PUT a 2 KB. Se um objeto tiver metadados definidos pelo usuário maiores que 2 KB, esse objeto não será replicado.

Vários baldes de destino

Para replicar objetos em um único bucket para vários buckets de destino, especifique o destino de cada regra no XML de configuração de replicação. Não é possível replicar um objeto em mais de um bucket ao mesmo tempo.

Buckets versionados ou não versionados

Você pode configurar a replicação do CloudMirror em buckets versionados ou não versionados. Os buckets de destino podem ser versionados ou não versionados. Você pode usar qualquer combinação de buckets versionados e não versionados. Por exemplo, você pode especificar um bucket versionado como destino para um bucket de origem não versionado, ou vice-versa. Você também pode replicar entre buckets não versionados.

Exclusão, loops de replicação e eventos

Comportamento de exclusão

É o mesmo que o comportamento de exclusão do serviço Amazon S3, Cross-Region Replication (CRR). Excluir um objeto em um bucket de origem nunca exclui um objeto replicado no destino. Se os buckets de origem e destino forem versionados, o marcador de exclusão será replicado. Se o bucket de destino não

tiver versão, a exclusão de um objeto no bucket de origem não replicará o marcador de exclusão para o bucket de destino nem excluirá o objeto de destino.

Proteção contra loops de replicação

À medida que os objetos são replicados para o bucket de destino, o StorageGRID os marca como "réplicas". Um bucket StorageGRID de destino não replicará objetos marcados como réplicas novamente, protegendo você de loops de replicação acidentais. Essa marcação de réplica é interna ao StorageGRID e não impede que você aproveite o AWS CRR ao usar um bucket do Amazon S3 como destino.



O cabeçalho personalizado usado para marcar uma réplica é `x-ntap-sg-replica`. Essa marcação evita um espelho em cascata. O StorageGRID suporta um CloudMirror bidirecional entre duas grades.

Eventos no bucket de destino

A exclusividade e a ordem dos eventos no bucket de destino não são garantidas. Mais de uma cópia idêntica de um objeto de origem pode ser entregue ao destino como resultado de operações realizadas para garantir o sucesso da entrega. Em casos raros, quando o mesmo objeto é atualizado simultaneamente de dois ou mais sites StorageGRID diferentes, a ordem das operações no bucket de destino pode não corresponder à ordem dos eventos no bucket de origem.

Entenda as notificações para buckets

Você pode habilitar a notificação de eventos para um bucket do S3 se quiser que o StorageGRID envie notificações sobre eventos especificados para um cluster Kafka de destino ou para o 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.

As notificações de eventos são criadas no bucket de origem, conforme especificado na configuração de notificação, e são entregues ao destino. Se um evento associado a um objeto for bem-sucedido, uma notificação sobre esse evento será criada e enfileirada para entrega.

A exclusividade e a ordem das notificações não são garantidas. Mais de uma notificação de um evento pode ser entregue ao destino como resultado de operações realizadas para garantir o sucesso da entrega. E como a entrega é assíncrona, não há garantia de que a ordem temporal das notificações no destino corresponda à ordem dos eventos no bucket de origem, principalmente para operações originadas de diferentes sites do StorageGRID. Você pode usar o `sequencer` digite a mensagem do evento para determinar a ordem dos eventos para um objeto específico, conforme descrito na documentação do Amazon S3.

As notificações de eventos do StorageGRID seguem a API do Amazon S3 com algumas limitações.

- Os seguintes tipos de eventos são suportados:
 - `s3:ObjetoCriado`:
 - `s3:ObjectCreated:Colocar`
 - `s3:ObjetoCriado:Post`
 - `s3:ObjetoCriado:Copiar`
 - `s3:ObjetoCriado:CompleteMultipartUpload`
 - `s3:ObjetoRemovido`:

- s3:ObjetoRemovido:Excluir
- s3:ObjetoRemovido:ExcluirMarcadorCriado
- s3:Restauração de Objeto:Postagem
- As notificações de eventos enviadas do StorageGRID usam o formato JSON padrão, mas não incluem algumas chaves e usam valores específicos para outras, conforme mostrado na tabela:

Nome da chave	Valor StorageGRID
fonte do evento	sgws:s3
Região aws	<i>não incluído</i>
x-amz-id-2	<i>não incluído</i>
arn	urn:sgws:s3:::bucket_name

Entenda o serviço de integração de pesquisa

Você pode habilitar a integração de pesquisa para um bucket do S3 se quiser usar um serviço externo de pesquisa e análise de dados para seus metadados de objeto.

O serviço de integração de pesquisa é um serviço StorageGRID personalizado que envia automaticamente e de forma assíncrona metadados de objetos do S3 para um ponto de extremidade de destino sempre que um objeto é criado ou excluído, ou seus metadados ou tags são atualizados. Você pode então usar ferramentas sofisticadas de pesquisa, análise de dados, visualização ou aprendizado de máquina fornecidas pelo serviço de destino para pesquisar, analisar e obter insights dos dados do seu objeto.

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 a data de retenção e o status de retenção legal) dos objetos não serão incluídos nos metadados enviados ao Elasticsearch.



Como o serviço de integração de pesquisa faz com que metadados de objetos sejam enviados a um destino, seu XML de configuração é chamado de "XML de configuração de notificação *metadata*". Este XML de configuração é diferente do "XML de configuração de notificação" usado para habilitar notificações de *eventos*.

Integração de pesquisa e buckets S3

Você pode habilitar o serviço de integração de pesquisa para qualquer bucket versionado ou não versionado. A integração de pesquisa é configurada associando o XML de configuração de notificação de metadados ao bucket que especifica em quais objetos atuar e o destino dos metadados do objeto.

As notificações de metadados são geradas no formato de um documento JSON nomeado com o nome do bucket, o nome do objeto e o ID da versão, se houver. Cada notificação de metadados contém um conjunto padrão de metadados do sistema para o objeto, além de todas as tags do objeto e metadados do usuário.



Para tags e metadados do usuário, o StorageGRID passa datas e números para o Elasticsearch como strings ou como notificações de eventos do S3. Para configurar o Elasticsearch para interpretar essas strings como datas ou números, siga as instruções do Elasticsearch para mapeamento de campos dinâmicos e para mapeamento de formatos de data. Você deve habilitar os mapeamentos de campos dinâmicos no índice antes de configurar o serviço de integração de pesquisa. Depois que um documento é indexado, você não pode editar os tipos de campo do documento no índice.

Notificações de pesquisa

Notificações de metadados são geradas e enfileiradas para entrega sempre que:

- Um objeto é criado.
- Um objeto é excluído, inclusive quando objetos são excluídos como resultado da operação da política ILM da grade.
- Metadados ou tags de objetos são adicionados, atualizados ou excluídos. O conjunto completo de metadados e tags é sempre enviado na atualização — não apenas os valores alterados.

Depois de adicionar o XML de configuração de notificação de metadados a um bucket, as notificações são enviadas para quaisquer novos objetos que você criar e para quaisquer objetos que você modificar atualizando seus dados, metadados do usuário ou tags. No entanto, as notificações não são enviadas para nenhum objeto que já estava no bucket. Para garantir que os metadados de todos os objetos no bucket sejam enviados ao destino, você deve fazer um dos seguintes procedimentos:

- Configure o serviço de integração de pesquisa imediatamente após criar o bucket e antes de adicionar qualquer objeto.
- Execute uma ação em todos os objetos já existentes no bucket que acionará uma mensagem de notificação de metadados a ser enviada ao destino.

Serviço de integração de pesquisa e Elasticsearch

O serviço de integração de pesquisa StorageGRID oferece suporte a um cluster Elasticsearch como destino. Assim como nos outros serviços da plataforma, o destino é especificado no ponto de extremidade cujo URN é usado no XML de configuração do serviço. Use o ["Ferramenta de Matriz de Interoperabilidade da NetApp"](#) para determinar as versões suportadas do Elasticsearch.

Gerenciar endpoints de serviços de plataforma

Configurar pontos de extremidade de serviços de plataforma

Antes de configurar um serviço de plataforma para um bucket, você deve configurar pelo menos um endpoint para ser o destino do serviço de plataforma.

O acesso aos serviços da plataforma é habilitado por locatário por um administrador do StorageGRID. Para criar ou usar um ponto de extremidade de serviços de plataforma, você deve ser um usuário locatário com permissão de acesso Gerenciar pontos de extremidade ou Raiz, em uma grade cuja rede foi configurada para permitir que os Nós de Armazenamento acessem recursos de ponto de extremidade externos. Para um único locatário, você pode configurar no máximo 500 pontos de extremidade de serviços de plataforma. Entre em contato com o administrador do StorageGRID para obter mais informações.

O que é um ponto de extremidade de serviços de plataforma?

Um ponto de extremidade de serviços de plataforma especifica as informações que o StorageGRID precisa para acessar o destino externo.

Por exemplo, se você quiser replicar objetos de um bucket do StorageGRID para um bucket do Amazon S3, crie um ponto de extremidade de serviços de plataforma que inclua as informações e credenciais que o StorageGRID precisa para acessar o bucket de destino na Amazon.

Cada tipo de serviço de plataforma requer seu próprio ponto de extremidade, portanto, você deve configurar pelo menos um ponto de extremidade para cada serviço de plataforma que planeja usar. Depois de definir um ponto de extremidade de serviços de plataforma, use o URN do ponto de extremidade como destino no XML de configuração usado para habilitar o serviço.

Você pode usar o mesmo ponto de extremidade como destino para mais de um bucket de origem. Por exemplo, você pode configurar vários buckets de origem para enviar metadados de objetos ao mesmo ponto de extremidade de integração de pesquisa para que você possa realizar pesquisas em vários buckets. Você também pode configurar um bucket de origem para usar mais de um endpoint como destino, o que permite fazer coisas como enviar notificações sobre a criação de objetos para um tópico do Amazon Simple Notification Service (Amazon SNS) e notificações sobre a exclusão de objetos para um segundo tópico do Amazon SNS.

Pontos de extremidade para replicação do CloudMirror

O StorageGRID oferece suporte a endpoints de replicação que representam buckets do S3. Esses buckets podem ser hospedados no Amazon Web Services, na mesma implantação ou em uma implantação remota do StorageGRID ou em outro serviço.

Pontos finais para notificações

O StorageGRID oferece suporte aos endpoints do Amazon SNS e do Kafka. Os endpoints do Simple Queue Service (SQS) ou do AWS Lambda não são suportados.

Para endpoints do Kafka, o TLS mútuo não é suportado. Como resultado, se você tiver `ssl.client.auth` definido para `required` na configuração do seu broker Kafka, isso pode causar problemas de configuração do endpoint Kafka.

Pontos de extremidade para o serviço de integração de pesquisa

O StorageGRID oferece suporte a endpoints de integração de pesquisa que representam clusters do Elasticsearch. Esses clusters do Elasticsearch podem estar em um data center local ou hospedados em uma nuvem AWS ou em outro lugar.

O ponto de extremidade de integração de pesquisa refere-se a um índice e tipo específicos do Elasticsearch. Você deve criar o índice no Elasticsearch antes de criar o endpoint no StorageGRID, ou a criação do endpoint falhará. Você não precisa criar o tipo antes de criar o ponto de extremidade. O StorageGRID criará o tipo, se necessário, quando enviar metadados do objeto para o ponto de extremidade.

Informações relacionadas

["Administrar StorageGRID"](#)

Especifique URN para o ponto de extremidade dos serviços de plataforma

Ao criar um ponto de extremidade de serviços de plataforma, você deve especificar um

Nome de Recurso Exclusivo (URN). Você usará o URN para referenciar o ponto de extremidade ao criar um XML de configuração para o serviço da plataforma. O URN para cada ponto de extremidade deve ser exclusivo.

O StorageGRID valida os pontos de extremidade dos serviços da plataforma conforme você os cria. Antes de criar um ponto de extremidade de serviços de plataforma, confirme se o recurso especificado no ponto de extremidade existe e se pode ser acessado.

Elementos URN

O URN para um ponto de extremidade de serviços de plataforma deve começar com `arn:aws` ou `urn:mysite`, do seguinte modo:

- Se o serviço estiver hospedado na Amazon Web Services (AWS), use `arn:aws`
- Se o serviço estiver hospedado no Google Cloud Platform (GCP), use `arn:aws`
- Se o serviço estiver hospedado localmente, use `urn:mysite`

Por exemplo, se você estiver especificando o URN para um endpoint do CloudMirror hospedado no StorageGRID, o URN pode começar com `urn:sgws`.

O próximo elemento do URN especifica o tipo de serviço de plataforma, da seguinte forma:

Serviço	Tipo
Replicação do CloudMirror	s3
Notificações	sns`ou `kafka
Integração de pesquisa	es

Por exemplo, para continuar especificando o URN para um endpoint do CloudMirror hospedado no StorageGRID, você adicionaria `s3` obter `urn:sgws:s3`.

O elemento final do URN identifica o recurso de destino específico no URI de destino.

Serviço	Recurso específico
Replicação do CloudMirror	bucket-name
Notificações	sns-topic-name`ou `kafka-topic-name
Integração de pesquisa	domain-name/index-name/type-name Observação: se o cluster do Elasticsearch não estiver configurado para criar índices automaticamente, você deverá criar o índice manualmente antes de criar o endpoint.

URNs para serviços hospedados na AWS e GCP

Para entidades AWS e GCP, o URN completo é um ARN AWS válido. Por exemplo:

- Replicação do CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notificações:

```
arn:aws:sns:region:account-id:topic-name
```

- Integração de pesquisa:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



Para um ponto de extremidade de integração de pesquisa da AWS, o domain-name deve incluir a string literal `domain/`, como mostrado aqui.

URNs para serviços hospedados localmente

Ao usar serviços hospedados localmente em vez de serviços em nuvem, você pode especificar o URN de qualquer maneira que crie um URN válido e exclusivo, desde que o URN inclua os elementos necessários na terceira e última posição. Você pode deixar os elementos indicados como opcionais em branco ou especificá-los de qualquer forma que ajude a identificar o recurso e tornar a URN única. Por exemplo:

- Replicação do CloudMirror:

```
urn:mysite:s3:optional:optional:bucket-name
```

Para um endpoint do CloudMirror hospedado no StorageGRID, você pode especificar um URN válido que comece com `urn:sgws`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notificações:

Especifique um ponto de extremidade do Amazon Simple Notification Service:

```
urn:mysite:sns:optional:optional:sns-topic-name
```

Especifique um ponto de extremidade do Kafka:

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

- Integração de pesquisa:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```



Para pontos de extremidade de integração de pesquisa hospedados localmente, o `domain-name` element pode ser qualquer string, desde que o URN do ponto final seja único.

Criar ponto de extremidade de serviços de plataforma

Você deve criar pelo menos um ponto de extremidade do tipo correto antes de poder habilitar um serviço de plataforma.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Os serviços da plataforma foram habilitados para sua conta de locatário por um administrador do StorageGRID .
- Você pertence a um grupo de usuários que tem o ["Gerenciar endpoints ou permissão de acesso root"](#) .
- O recurso referenciado pelo ponto de extremidade dos serviços da plataforma foi criado:
 - Replicação do CloudMirror: bucket S3
 - Notificação de evento: Amazon Simple Notification Service (Amazon SNS) ou tópico Kafka
 - Notificação de pesquisa: índice do Elasticsearch, se o cluster de destino não estiver configurado para criar índices automaticamente.
- Você tem as informações sobre o recurso de destino:
 - Host e porta para o Uniform Resource Identifier (URI)



Se você planeja usar um bucket hospedado em um sistema StorageGRID como um ponto de extremidade para replicação do CloudMirror, entre em contato com o administrador da grade para determinar os valores que você precisa inserir.

- Nome de Recurso Único (URN)

["Especifique URN para o ponto de extremidade dos serviços de plataforma"](#)

- Credenciais de autenticação (se necessário):

Pontos de extremidade de integração de pesquisa

Para endpoints de integração de pesquisa, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta
- HTTP básico: nome de usuário e senha

Pontos de extremidade de replicação do CloudMirror

Para endpoints de replicação do CloudMirror, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta
- CAP (C2S Access Portal): URL de credenciais temporárias, certificados de servidor e cliente, chaves de cliente e uma senha de chave privada de cliente opcional.

Pontos de extremidade do Amazon SNS

Para endpoints do Amazon SNS, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta

Pontos finais do Kafka

Para endpoints do Kafka, você pode usar as seguintes credenciais:

- SASL/PLAIN: Nome de usuário e senha
- SASL/SCRAM-SHA-256: Nome de usuário e senha
- SASL/SCRAM-SHA-512: Nome de usuário e senha

- Certificado de segurança (se estiver usando um certificado CA personalizado)
- Se os recursos de segurança do Elasticsearch estiverem habilitados, você terá o privilégio de monitorar cluster para testes de conectividade e o privilégio de gravar índice ou os privilégios de indexar e excluir índice para atualizações de documentos.

Passos

1. Selecione **ARMAZENAMENTO (S3) > Pontos de extremidade de serviços de plataforma**. A página de pontos de extremidade dos serviços da plataforma é exibida.
2. Selecione **Criar ponto de extremidade**.
3. Insira um nome de exibição para descrever brevemente o ponto de extremidade e sua finalidade.

O tipo de serviço de plataforma que o endpoint suporta é mostrado ao lado do nome do endpoint quando ele é listado na página Endpoints, portanto você não precisa incluir essa informação no nome.

4. No campo **URI**, especifique o Identificador de Recurso Único (URI) do ponto de extremidade.

Use um dos seguintes formatos:

```
https://host:port  
http://host:port
```

Se você não especificar uma porta, as seguintes portas padrão serão usadas:

- Porta 443 para URIs HTTPS e porta 80 para URIs HTTP (a maioria dos endpoints)
- Porta 9092 para HTTPS e URIs HTTP (somente endpoints do Kafka)

Por exemplo, o URI para um bucket hospedado no StorageGRID pode ser:

```
https://s3.example.com:10443
```

Neste exemplo, `s3.example.com` representa a entrada DNS para o IP virtual (VIP) do grupo de alta disponibilidade (HA) do StorageGRID e `10443` representa a porta definida no ponto de extremidade do balanceador de carga.



Sempre que possível, você deve se conectar a um grupo HA de nós de balanceamento de carga para evitar um único ponto de falha.

Da mesma forma, o URI para um bucket hospedado na AWS pode ser:

```
https://s3-aws-region.amazonaws.com
```



Se o ponto de extremidade for usado para o serviço de replicação do CloudMirror, não inclua o nome do bucket no URI. Inclua o nome do bucket no campo **URN**.

5. Insira o Nome de Recurso Exclusivo (URN) para o ponto de extremidade.



Não é possível alterar o URN de um endpoint depois que ele for criado.

6. Selecione **Continuar**.

7. Selecione um valor para **Tipo de autenticação**.

Pontos de extremidade de integração de pesquisa

Insira ou carregue as credenciais para um ponto de extremidade de integração de pesquisa.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
Chave de acesso	Usa credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta
HTTP básico	Usa um nome de usuário e uma senha para autenticar conexões com o destino.	• Nome de usuário • Senha

Pontos de extremidade de replicação do CloudMirror

Insira ou carregue as credenciais para um ponto de extremidade de replicação do CloudMirror.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
Chave de acesso	Usa credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta
CAP (Portal de Acesso C2S)	Usa certificados e chaves para autenticar conexões com o destino.	• URL de credenciais temporárias • Certificado CA do servidor (upload de arquivo PEM) • Certificado do cliente (upload de arquivo PEM) • Chave privada do cliente (upload de arquivo PEM, formato criptografado OpenSSL ou formato de chave privada não criptografada) • Senha da chave privada do cliente (opcional)

Pontos de extremidade do Amazon SNS

Insira ou carregue as credenciais para um endpoint do Amazon SNS.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
Chave de acesso	Usa credenciais no estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreta

Pontos finais do Kafka

Insira ou carregue as credenciais para um ponto de extremidade do Kafka.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona somente para endpoints que tenham a segurança desabilitada.	Sem autenticação.
SASL/SIM	Usa um nome de usuário e uma senha com texto simples para autenticar conexões com o destino.	• Nome de usuário • Senha
SASL/SCRAM-SHA-256	Usa um nome de usuário e uma senha usando um protocolo de desafio-resposta e hash SHA-256 para autenticar conexões com o destino.	• Nome de usuário • Senha
SASL/SCRAM-SHA-512	Usa um nome de usuário e uma senha usando um protocolo de desafio-resposta e hash SHA-512 para autenticar conexões com o destino.	• Nome de usuário • Senha

Selecione **Usar autenticação de delegação** se o nome de usuário e a senha forem derivados de um token de delegação obtido de um cluster Kafka.

8. Selecione **Continuar**.

9. Selecione um botão de opção para **Verificar servidor** para escolher como a conexão TLS com o ponto de extremidade será verificada.

Tipo de verificação do certificado	Descrição
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 CA .
Usar certificado CA do sistema operacional	Use o certificado Grid CA padrão instalado no sistema operacional para proteger conexões.
Não verificar certificado	O certificado usado para a conexão TLS não foi verificado. Esta opção não é segura.

10. Selecione **Testar e criar ponto de extremidade**.

- Uma mensagem de sucesso será exibida se o ponto de extremidade puder ser alcançado usando as credenciais especificadas. A conexão com o ponto de extremidade é validada a partir de um nó em cada site.
- Uma mensagem de erro será exibida se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **Retornar aos detalhes do endpoint** e atualize as informações. Em seguida, selecione **Testar e criar endpoint**.



A criação do endpoint falhará se os serviços da plataforma não estiverem habilitados para sua conta de locatário. Entre em contato com o administrador do StorageGRID .

Depois de configurar um ponto de extremidade, você pode usar seu URN para configurar um serviço de plataforma.

Informações relacionadas

- ["Especifique URN para o ponto de extremidade dos serviços de plataforma"](#)
- ["Configurar a replicação do CloudMirror"](#)
- ["Configurar notificações de eventos"](#)
- ["Configurar serviço de integração de pesquisa"](#)

Teste de conexão para ponto de extremidade de serviços de plataforma

Se a conexão com um serviço de plataforma tiver sido alterada, você poderá testar a conexão do ponto de extremidade para validar se o recurso de destino existe e se pode ser acessado usando as credenciais especificadas.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#) .
- Você pertence a um grupo de usuários que tem o ["Gerenciar endpoints ou permissão de acesso root"](#) .

Sobre esta tarefa

O StorageGRID não valida se as credenciais têm as permissões corretas.

Passos

1. Selecione **ARMAZENAMENTO (S3) > Pontos de extremidade de serviços de plataforma**.

A página Pontos de extremidade dos serviços da plataforma é exibida e mostra a lista de pontos de extremidade dos serviços da plataforma que já foram configurados.

2. Selecione o ponto de extremidade cuja conexão você deseja testar.

A página de detalhes do endpoint é exibida.

3. Selecione **Testar conexão**.

- Uma mensagem de sucesso será exibida se o ponto de extremidade puder ser alcançado usando as credenciais especificadas. A conexão com o ponto de extremidade é validada a partir de um nó em cada site.
- Uma mensagem de erro será exibida se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **Configuração** e atualize as informações. Em seguida, selecione **Testar e salvar alterações**.

Editar ponto de extremidade dos serviços da plataforma

Você pode editar a configuração de um ponto de extremidade de serviços de plataforma para alterar seu nome, URI ou outros detalhes. Por exemplo, talvez você precise atualizar credenciais expiradas ou alterar o URI para apontar para um índice de backup do Elasticsearch para failover. Não é possível alterar o URN de um ponto de extremidade de serviços de plataforma.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Gerenciar endpoints ou permissão de acesso root"](#).

Passos

1. Selecione **ARMAZENAMENTO (S3) > Pontos de extremidade de serviços de plataforma**.

A página Pontos de extremidade dos serviços da plataforma é exibida e mostra a lista de pontos de extremidade dos serviços da plataforma que já foram configurados.

2. Selecione o ponto de extremidade que você deseja editar.

A página de detalhes do endpoint é exibida.

3. Selecione **Configuração**.

4. Conforme necessário, altere a configuração do ponto de extremidade.



Não é possível alterar o URN de um endpoint depois que ele for criado.

- a. Para alterar o nome de exibição do ponto de extremidade, selecione o ícone de edição
- b. Conforme necessário, altere o URI.
- c. Conforme necessário, altere o tipo de autenticação.

- Para autenticação de chave de acesso, altere a chave conforme necessário selecionando **Editar chave S3** e colando uma nova ID de chave de acesso e uma chave de acesso secreta. Se precisar cancelar suas alterações, selecione **Reverter edição da chave S3**.

- Para autenticação CAP (C2S Access Portal), altere a URL de credenciais temporárias ou a senha da chave privada do cliente opcional e carregue novos arquivos de certificado e chave conforme necessário.



A chave privada do cliente deve estar no formato criptografado OpenSSL ou no formato de chave privada não criptografada.

d. Conforme necessário, altere o método de verificação do servidor.

5. Selecione **Testar e salvar alterações**.

- Uma mensagem de sucesso será exibida se o ponto de extremidade puder ser alcançado usando as credenciais especificadas. A conexão com o ponto de extremidade é verificada a partir de um nó em cada site.
- Uma mensagem de erro será exibida se a validação do endpoint falhar. Modifique o ponto de extremidade para corrigir o erro e selecione **Testar e salvar alterações**.

Excluir ponto de extremidade de serviços de plataforma

Você pode excluir um ponto de extremidade se não quiser mais usar o serviço de plataforma associado.

Antes de começar

- Você está conectado ao Gerenciador de Inquilinos usando um ["navegador da web compatível"](#).
- Você pertence a um grupo de usuários que tem o ["Gerenciar endpoints ou permissão de acesso root"](#).

Passos

1. Selecione **ARMAZENAMENTO (S3) > Pontos de extremidade de serviços de plataforma**.

A página Pontos de extremidade dos serviços da plataforma é exibida e mostra a lista de pontos de extremidade dos serviços da plataforma que já foram configurados.

2. Marque a caixa de seleção de cada ponto de extremidade que você deseja excluir.



Se você excluir um ponto de extremidade de serviços de plataforma que está em uso, o serviço de plataforma associado será desabilitado para todos os buckets que usarem o ponto de extremidade. Quaisquer solicitações que ainda não tenham sido concluídas serão descartadas. Quaisquer novas solicitações continuarão a ser geradas até que você altere a configuração do seu bucket para não fazer mais referência ao URN excluído. O StorageGRID relatará essas solicitações como erros irreversíveis.

3. Selecione **Ações > Excluir ponto de extremidade**.

Uma mensagem de confirmação é exibida.

4. Selecione **Excluir ponto de extremidade**.

Solucionar erros de endpoint de serviços de plataforma

Se ocorrer um erro quando o StorageGRID tentar se comunicar com um ponto de extremidade de serviços da plataforma, uma mensagem será exibida no painel. Na página Pontos de extremidade dos serviços da plataforma, a coluna Último erro indica há

quanto tempo o erro ocorreu. Nenhum erro será exibido se as permissões associadas às credenciais de um endpoint estiverem incorretas.

Determinar se ocorreu um erro

Se algum erro de ponto de extremidade de serviços de plataforma tiver ocorrido nos últimos 7 dias, o painel do Gerenciador de Tenants exibirá uma mensagem de alerta. Você pode acessar a página de endpoints dos serviços da plataforma para ver mais detalhes sobre o erro.



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.

O mesmo erro que aparece no painel também aparece na parte superior da página de pontos de extremidade dos serviços da plataforma. Para ver uma mensagem de erro mais detalhada:

Passos

1. Na lista de endpoints, selecione o endpoint que apresenta o erro.
2. Na página de detalhes do endpoint, selecione **Conexão**. Esta guia exibe apenas o erro mais recente de um ponto de extremidade e indica há quanto tempo o erro ocorreu. Erros que incluem o ícone X vermelho  ocorreu nos últimos 7 dias.

Verifique se o erro ainda está presente

Alguns erros podem continuar a ser exibidos na coluna **Último erro** mesmo depois de serem resolvidos. Para verificar se um erro é atual ou para forçar a remoção de um erro resolvido da tabela:

Passos

1. Selecione o ponto final.

A página de detalhes do endpoint é exibida.

2. Selecione **Conexão > Testar conexão**.

Selecionar **Testar conexão** faz com que o StorageGRID valide se o ponto de extremidade dos serviços da plataforma existe e se pode ser acessado com as credenciais atuais. A conexão com o ponto de extremidade é validada a partir de um nó em cada site.

Resolver erros de endpoint

Você pode usar a mensagem **Último erro** na página de detalhes do endpoint para ajudar a determinar o que está causando o erro. Alguns erros podem exigir que você edite o endpoint para resolver o problema. Por exemplo, um erro de CloudMirroring pode ocorrer se o StorageGRID não conseguir acessar o bucket S3 de destino porque não tem as permissões de acesso corretas ou a chave de acesso expirou. A mensagem é "As credenciais do endpoint ou o acesso ao destino precisam ser atualizados" e os detalhes são "AccessDenied" ou "InvalidAccessKeyId".

Se você precisar editar o endpoint para resolver um erro, selecionar **Testar e salvar alterações** fará com que o StorageGRID valide o endpoint atualizado e confirme que ele pode ser acessado com as credenciais atuais. A conexão com o ponto de extremidade é validada a partir de um nó em cada site.

Passos

1. Selecione o ponto final.
2. Na página de detalhes do endpoint, selecione **Configuração**.
3. Edite a configuração do endpoint conforme necessário.
4. Selecione **Conexão > Testar conexão**.

Credenciais de endpoint com permissões insuficientes

Quando o StorageGRID valida um ponto de extremidade de serviços de plataforma, ele confirma que as credenciais do ponto de extremidade podem ser usadas para entrar em contato com o recurso de destino e realiza uma verificação básica de permissões. No entanto, o StorageGRID não valida todas as permissões necessárias para determinadas operações de serviços da plataforma. Por esse motivo, se você receber um erro ao tentar usar um serviço de plataforma (como "403 Forbidden"), verifique as permissões associadas às credenciais do endpoint.

Informações relacionadas

- [Administrar StorageGRID > Solucionar problemas de serviços de plataforma](#)
- ["Criar ponto de extremidade de serviços de plataforma"](#)
- ["Teste de conexão para ponto de extremidade de serviços de plataforma"](#)
- ["Editar ponto de extremidade dos serviços da plataforma"](#)

Configurar a replicação do CloudMirror

Para habilitar a replicação do CloudMirror para um bucket, crie e aplique um XML de configuração de replicação de bucket válido.

Antes de começar

- Os serviços da plataforma foram habilitados para sua conta de locatário por um administrador do StorageGRID .
- Você já criou um bucket para atuar como fonte de replicação.
- O ponto de extremidade que você pretende usar como destino para a replicação do CloudMirror já existe e você tem seu URN.
- Você pertence a um grupo de usuários que tem o ["Gerenciar todos os buckets ou permissão de acesso root"](#) . Essas permissões substituem as configurações de permissão em políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Tenants.

Sobre esta tarefa

A replicação do CloudMirror copia objetos de um bucket de origem para um bucket de destino especificado em um endpoint.

Para obter informações gerais sobre a replicação de bucket e como configurá-la, consulte ["Documentação do Amazon Simple Storage Service \(S3\): Replicando objetos"](#) . Para obter informações sobre como o StorageGRID implementa GetBucketReplication, DeleteBucketReplication e PutBucketReplication, consulte o ["Operações em baldes"](#) .



A replicação do CloudMirror tem 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"](#) .

Observe os seguintes requisitos e características ao configurar a replicação do CloudMirror:

- Ao criar e aplicar um XML de configuração de replicação de bucket válido, ele deve usar o URN de um ponto de extremidade de bucket do S3 para cada destino.
- A replicação não é suportada para buckets de origem ou destino com o S3 Object Lock habilitado.
- Se você habilitar a replicação do CloudMirror em um bucket que contém objetos, os novos objetos adicionados ao bucket serão replicados, mas os objetos existentes no bucket não serão replicados. Você deve atualizar os objetos existentes para acionar a replicação.
- Se você especificar uma classe de armazenamento no XML de configuração de replicação, o StorageGRID usará essa classe ao executar operações no ponto de extremidade S3 de destino. O ponto de extremidade de destino também deve suportar a classe de armazenamento especificada. Certifique-se de seguir todas as recomendações fornecidas pelo fornecedor do sistema de destino.

Passos

1. Habilite a replicação para seu bucket de origem:

- Use um editor de texto para criar o XML de configuração de replicação necessário para habilitar a replicação, conforme especificado na API de replicação do S3.
- Ao configurar o XML:
 - Observe que o StorageGRID suporta apenas a V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do `Filter` elemento para regras e segue as convenções V1 para exclusão de versões de objetos. Consulte a documentação da Amazon sobre configuração de replicação para obter detalhes.
 - Use o URN de um ponto de extremidade do bucket S3 como destino.
 - Opcionalmente, adicione o `<StorageClass>` elemento e especifique um dos seguintes:
 - `STANDARD`: A classe de armazenamento padrão. Se você não especificar uma classe de armazenamento ao carregar um objeto, o `STANDARD` classe de armazenamento é usada.
 - `STANDARD_IA`: (Padrão - acesso pouco frequente.) Use esta classe de armazenamento para dados que são acessados com menos frequência, mas que ainda exigem acesso rápido quando necessário.
 - `REDUCED_REDUNDANCY`: Use esta classe de armazenamento para dados não críticos e reproduzíveis que podem ser armazenados com menos redundância do que os `STANDARD` classe de armazenamento.
 - Se você especificar um `Role` no XML de configuração ele será ignorado. Este valor não é usado pelo StorageGRID.

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

2. Selecione **Exibir buckets** no painel ou selecione **ARMAZENAMENTO (S3) > Buckets**.
3. Selecione o nome do bucket de origem.

A página de detalhes do bucket é exibida.

4. Selecione **Serviços de plataforma > Replicação**.
5. Marque a caixa de seleção **Ativar replicação**.
6. Cole o XML de configuração de replicação na caixa de texto e selecione **Salvar alterações**.



Os serviços da plataforma devem ser habilitados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a API de gerenciamento de grade. Entre em contato com o administrador do StorageGRID se ocorrer um erro ao salvar o XML de configuração.

7. Verifique se a replicação está configurada corretamente:
 - a. Adicione um objeto ao bucket de origem que atenda aos requisitos de replicação, conforme especificado na configuração de replicação.

No exemplo mostrado anteriormente, os objetos que correspondem ao prefixo "2020" são replicados.

- b. Confirme se o objeto foi replicado para o bucket de destino.

Para objetos pequenos, a replicação acontece rapidamente.

Informações relacionadas

["Criar ponto de extremidade de serviços de plataforma"](#)

Configurar notificações de eventos

Você habilita notificações para um bucket criando um XML de configuração de notificação e usando o Tenant Manager para aplicar o XML a um bucket.

Antes de começar

- Os serviços da plataforma foram habilitados para sua conta de locatário por um administrador do StorageGRID .
- Você já criou um bucket para atuar como fonte de notificações.
- O ponto de extremidade que você pretende usar como destino para notificações de eventos já existe e você tem seu URN.
- Você pertence a um grupo de usuários que tem o ["Gerenciar todos os buckets ou permissão de acesso root"](#) . Essas permissões substituem as configurações de permissão em políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Tenants.

Sobre esta tarefa

Você configura notificações de eventos associando o XML de configuração de notificação a um bucket de origem. O XML de configuração de notificação segue as convenções do S3 para configurar notificações de bucket, com o tópico de destino do Kafka ou do Amazon SNS especificado como o URN de um endpoint.

Para obter informações gerais sobre notificações de eventos e como configurá-las, consulte o ["Documentação da Amazon"](#) . Para obter informações sobre como o StorageGRID implementa a API de configuração de notificação do bucket S3, consulte o ["instruções para implementar aplicativos cliente S3"](#) .

Observe os seguintes requisitos e características ao configurar notificações de eventos para um bucket:

- Ao criar e aplicar um XML de configuração de notificação válido, ele deve usar o URN de um ponto de extremidade de notificações de eventos para cada destino.
- 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.
- Depois de configurar as notificações de eventos, sempre que um evento especificado ocorrer para um objeto no bucket de origem, uma notificação será gerada e enviada ao tópico do Amazon SNS ou Kafka usado como endpoint de destino.
- Se você habilitar notificações de eventos para um bucket que contém objetos, as notificações serão enviadas somente para ações executadas após a configuração de notificação ser salva.

Passos

1. Habilite notificações para seu bucket de origem:

- Use um editor de texto para criar o XML de configuração de notificação necessário para habilitar notificações de eventos, conforme especificado na API de notificação do S3.
- Ao configurar o XML, use o URN de um ponto de extremidade de notificações de eventos como o tópico de destino.

```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
  </TopicConfiguration>
</NotificationConfiguration>
```

2. No Gerenciador de locatários, selecione **ARMAZENAMENTO (S3) > Buckets**.

3. Selecione o nome do bucket de origem.

A página de detalhes do bucket é exibida.

4. Selecione **Serviços de plataforma > Notificações de eventos**.

5. Marque a caixa de seleção **Ativar notificações de eventos**.

6. Cole o XML de configuração de notificação na caixa de texto e selecione **Salvar alterações**.



Os serviços da plataforma devem ser habilitados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a API de gerenciamento de grade. Entre em contato com o administrador do StorageGRID se ocorrer um erro ao salvar o XML de configuração.

7. Verifique se as notificações de eventos estão configuradas corretamente:

- a. Execute uma ação em um objeto no bucket de origem que atenda aos requisitos para acionar uma notificação, conforme configurado no XML de configuração.

No exemplo, uma notificação de evento é enviada sempre que um objeto é criado com o `images/` prefixo.

- b. Confirme se uma notificação foi entregue ao tópico de destino do Amazon SNS ou do Kafka.

Por exemplo, se o seu tópico de destino estiver hospedado no Amazon SNS, você poderá configurar o serviço para lhe enviar um e-mail quando a notificação for entregue.

```

{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}

```

+

Se a notificação for recebida no tópico de destino, você configurou com sucesso seu bucket de origem para notificações do StorageGRID .

Informações relacionadas

["Entenda as notificações para buckets"](#)

["Usar API REST do S3"](#)

Configurar o serviço de integração de pesquisa

Você habilita a integração de pesquisa para um bucket criando um XML de integração de pesquisa e usando o Tenant Manager para aplicar o XML ao bucket.

Antes de começar

- Os serviços da plataforma foram habilitados para sua conta de locatário por um administrador do StorageGRID .
- Você já criou um bucket S3 cujo conteúdo deseja indexar.
- O ponto de extremidade que você pretende usar como destino para o serviço de integração de pesquisa já existe e você tem seu URN.
- Você pertence a um grupo de usuários que tem o "[Gerenciar todos os buckets ou permissão de acesso root](#)". Essas permissões substituem as configurações de permissão em políticas de grupo ou bucket ao configurar o bucket usando o Gerenciador de Tenants.

Sobre esta tarefa

Depois de configurar o serviço de integração de pesquisa para um bucket de origem, a criação de um objeto ou a atualização dos metadados ou tags de um objeto aciona o envio de metadados do objeto para o ponto de extremidade de destino.

Se você habilitar o serviço de integração de pesquisa para um bucket que já contém objetos, as notificações de metadados não serão enviadas automaticamente para objetos existentes. Atualize esses objetos existentes para garantir que seus metadados sejam adicionados ao índice de pesquisa de destino.

Passos

1. Habilitar integração de pesquisa para um bucket:

- Use um editor de texto para criar o XML de notificação de metadados necessário para habilitar a integração de pesquisa.
- Ao configurar o XML, use o URN de um ponto de extremidade de integração de pesquisa como destino.

Os objetos podem ser filtrados pelo prefixo do nome do objeto. Por exemplo, você pode enviar metadados para objetos com o prefixo `images` para um destino e metadados para objetos com o prefixo `videos` para outro. Configurações que têm prefixos sobrepostos não são válidas e são rejeitadas quando enviadas. Por exemplo, uma configuração que inclui uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não é permitido.

Conforme necessário, consulte o [exemplos para a configuração de metadados XML](#) .

```

<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>/Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Elementos no XML de configuração de notificação de metadados:

Nome	Descrição	Obrigatório
Configuração de Notificação de Metadados	Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos Rule.	Sim
Regra	Tag de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
EU IA	Identificador exclusivo para a regra. Incluído no elemento Rule.	Não
Status	O status pode ser "Habilitado" ou "Desabilitado". Nenhuma ação é tomada para regras que estão desabilitadas. Incluído no elemento Rule.	Sim
Prefixo	Objetos que correspondem ao prefixo são afetados pela regra, e seus metadados são enviados ao destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento Rule.	Sim
Destino	Tag de contêiner para o destino de uma regra. Incluído no elemento Rule.	Sim

Nome	Descrição	Obrigatório
Urna	URN do destino para onde os metadados do objeto são enviados. Deve ser a URN de um ponto de extremidade StorageGRID com as seguintes propriedades: • `es` deve ser o terceiro elemento. • A URN deve terminar com o índice e o tipo onde os metadados são armazenados, no formato <code>domain-name/myindex/mytype</code>. Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles assumem a seguinte forma: • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> O ponto de extremidade deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. URN está incluído no elemento Destino.	Sim

2. No Gerenciador de inquilinos, selecione **ARMAZENAMENTO (S3) > Buckets**.

3. Selecione o nome do bucket de origem.

A página de detalhes do bucket é exibida.

4. Selecione **Serviços de plataforma > Integração de pesquisa**

5. Marque a caixa de seleção **Ativar integração de pesquisa**.

6. Cole a configuração de notificação de metadados na caixa de texto e selecione **Salvar alterações**.



Os serviços da plataforma devem ser habilitados para cada conta de locatário por um administrador do StorageGRID usando o Grid Manager ou a API de gerenciamento. Entre em contato com o administrador do StorageGRID se ocorrer um erro ao salvar o XML de configuração.

7. Verifique se o serviço de integração de pesquisa está configurado corretamente:

- Adicione um objeto ao bucket de origem que atenda aos requisitos para acionar uma notificação de metadados, conforme especificado no XML de configuração.

No exemplo mostrado anteriormente, todos os objetos adicionados ao bucket acionam uma notificação de metadados.

- Confirme se um documento JSON que contém os metadados e as tags do objeto foi adicionado ao índice de pesquisa especificado no ponto de extremidade.

Depois que você terminar

Conforme necessário, você pode desabilitar a integração de pesquisa para um bucket usando um dos

seguintes métodos:

- Selecione **ARMAZENAMENTO (S3) > Buckets** e desmarque a caixa de seleção **Ativar integração de pesquisa**.
- Se você estiver usando a API do S3 diretamente, use uma solicitação de notificação de metadados DELETE Bucket. Veja as instruções para implementar aplicativos cliente S3.

Exemplo: configuração de notificação de metadados que se aplica a todos os objetos

Neste exemplo, os metadados de todos os objetos são enviados para o mesmo destino.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Exemplo: configuração de notificação de metadados com duas regras

Neste exemplo, metadados de objetos para objetos que correspondem ao prefixo `/images` é enviado para um destino, enquanto metadados de objeto para objetos que correspondem ao prefixo `/videos` é enviado para um segundo destino.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Formato de notificação de metadados

Quando você habilita o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado ao ponto de extremidade de destino sempre que metadados ou tags de objeto são adicionados, atualizados ou excluídos.

Este exemplo mostra um exemplo do JSON que pode ser gerado quando um objeto com a chave `SGWS/Tagging.txt` é criado em um bucket chamado `test`. O `test` o bucket não é versionado, então o `versionId` a tag está vazia.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Campos incluídos no documento JSON

O nome do documento inclui o nome do bucket, o nome do objeto e o ID da versão, se presente.

Informações sobre bucket e objeto

bucket: Nome do balde

key: Nome da chave do objeto

versionID: Versão do objeto, para objetos em buckets versionados

region: Região de balde, por exemplo us-east-1

Metadados do sistema

size: Tamanho do objeto (em bytes) conforme visível para um cliente HTTP

md5: Hash do objeto

Metadados do usuário

metadata: Todos os metadados do usuário para o objeto, como pares chave-valor

key:value

Etiquetas

tags: Todas as tags de objeto definidas para o objeto, como pares chave-valor

key:value

Como visualizar resultados no Elasticsearch

Para tags e metadados do usuário, o StorageGRID passa datas e números para o Elasticsearch como strings ou como notificações de eventos do S3. Para configurar o Elasticsearch para interpretar essas strings como

datas ou números, siga as instruções do Elasticsearch para mapeamento de campos dinâmicos e para mapeamento de formatos de data. Habilite os mapeamentos de campos dinâmicos no índice antes de configurar o serviço de integração de pesquisa. Depois que um documento é indexado, você não pode editar os tipos de campo do documento no índice.

Usar API REST do S3

Versões e atualizações suportadas pela API REST do S3

O StorageGRID oferece suporte à API Simple Storage Service (S3), que é implementada como um conjunto de serviços web Representational State Transfer (REST).

O suporte para a API REST do S3 permite que você conecte aplicativos orientados a serviços desenvolvidos para serviços da Web do S3 com armazenamento de objetos local que usa o sistema StorageGRID . São necessárias alterações mínimas no uso atual de chamadas da API REST do S3 por um aplicativo cliente.

Versões suportadas

O StorageGRID suporta as seguintes versões específicas do S3 e HTTP.

Item	Versão
Especificação da API S3	"Documentação da Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service"
HTTP	1,1 Para obter mais informações sobre HTTP, consulte HTTP/1.1 (RFCs 7230-35). "IETF RFC 2616: Protocolo de Transferência de Hipertexto (HTTP/1.1)" Observação: O StorageGRID não oferece suporte a pipeline HTTP/1.1.

Atualizações no suporte à API REST do S3

Liberar	Comentários
11,9	• Adicionado suporte para valores de soma de verificação SHA-256 pré-calculados para as seguintes solicitações e cabeçalhos suportados. Você pode usar este recurso para verificar a integridade dos objetos enviados: ◦ Upload completo de várias partes: <code>x-amz-checksum-sha256</code> ◦ CriarMultipartUpload: <code>x-amz-checksum-algorithm</code> ◦ ObterObjeto: <code>x-amz-checksum-mode</code> ◦ HeadObject: <code>x-amz-checksum-mode</code> ◦ ListarPartes ◦ ColocarObjeto: <code>x-amz-checksum-sha256</code> ◦ UploadPart: <code>x-amz-checksum-sha256</code> • Foi adicionada a capacidade do administrador da grade de controlar as configurações de conformidade e retenção no nível do locatário. Essas configurações afetam as configurações de bloqueio de objeto do S3. ◦ Modo de retenção padrão do bucket e modo de retenção de objeto: Governança ou Conformidade, se permitido pelo administrador da grade. ◦ Período de retenção padrão do bucket e data de retenção do objeto: deve ser menor ou igual ao permitido pelo período máximo de retenção definido pelo administrador da grade. • Suporte aprimorado para <code>aws-chunked</code> codificação e streaming de conteúdo <code>x-amz-content-sha256</code> valores. Limitações: ◦ Se presente, <code>chunk-signature</code> é opcional e não validado ◦ Se presente, <code>x-amz-trailer</code> o conteúdo é ignorado
11,8	Atualizou os nomes das operações do S3 para corresponder aos nomes usados no "Documentação da Amazon Web Services (AWS): Referência da API do Amazon Simple Storage Service" .
11,7	• Adicionado "Referência rápida: solicitações de API do S3 suportadas" . • Adicionado suporte para usar o modo GOVERNANCE com o S3 Object Lock. • Adicionado suporte para StorageGRID específico <code>x-ntap-sg-cgr-replication-status</code> cabeçalho de resposta para solicitações GET Object e HEAD Object. Este cabeçalho fornece o status de replicação de um objeto para replicação entre grades. • Solicitações SelectObjectContent agora oferecem suporte a objetos Parquet.

Liberar	Comentários
11,6	• Adicionado suporte para usar o <code>partNumber</code> parâmetro de solicitação em solicitações GET Object e HEAD Object. • Adicionado suporte para um modo de retenção padrão e um período de retenção padrão no nível do bucket para o S3 Object Lock. • Adicionado suporte para o <code>s3:object-lock-remaining-retention-days</code> chave de condição de política para definir o intervalo de períodos de retenção permitidos para seus objetos. • Foi alterado o tamanho máximo <i>recomendado</i> para uma única operação PUT Object para 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use o upload multiparte.
11,5	• Adicionado suporte para gerenciamento de criptografia de bucket. • Suporte adicionado para bloqueio de objeto S3 e solicitações de conformidade legadas obsoletas. • Adicionado suporte para usar DELETE Multiple Objects em buckets versionados. • O <code>Content-MD5</code> O cabeçalho da solicitação agora é suportado corretamente.
11,4	• Adicionado suporte para marcação de Bucket DELETE, marcação de Bucket GET e marcação de Bucket PUT. Tags de alocação de custos não são suportadas. • Para buckets criados no StorageGRID 11.4, não é mais necessário restringir nomes de chaves de objeto para atender às práticas recomendadas de desempenho. • Adicionado suporte para notificações de bucket no <code>s3:ObjectRestore:Post</code> tipo de evento. • Os limites de tamanho da AWS para partes multipartes agora são aplicados. Cada parte em um upload multiparte deve ter entre 5 MiB e 5 GiB. A última parte pode ser menor que 5 MiB. • Adicionado suporte para TLS 1.3
11,3	• Adicionado suporte para criptografia do lado do servidor de dados de objetos com chaves fornecidas pelo cliente (SSE-C). • Adicionado suporte para operações de ciclo de vida de bucket DELETE, GET e PUT (somente ação de expiração) e para <code>x-amz-expiration</code> cabeçalho de resposta. • Objeto PUT atualizado, Objeto PUT - Cópia e Upload Multipartes para descrever o impacto das regras do ILM que usam posicionamento síncrono na ingestão. • As cifras TLS 1.1 não são mais suportadas.

Liberar	Comentários
11,2	Adicionado suporte para restauração de objetos POST para uso com pools de armazenamento em nuvem. Adicionado suporte para usar a sintaxe da AWS para ARN, chaves de condição de política e variáveis de política em políticas de grupo e bucket. As políticas de grupo e bucket existentes que usam a sintaxe StorageGRID continuarão a ser suportadas. Observação: Os usos de ARN/URN em outras configurações JSON/XML, incluindo aqueles usados em recursos personalizados do StorageGRID , não foram alterados.
11,1	Adicionado suporte para compartilhamento de recursos entre origens (CORS), HTTP para conexões de cliente S3 com nós de grade e configurações de conformidade em buckets.
11,0	Adicionado suporte para configuração de serviços de plataforma (replicação do CloudMirror, notificações e integração de pesquisa do Elasticsearch) para buckets. Também foi adicionado suporte para restrições de localização de marcação de objetos para buckets e consistência disponível.
10,4	Adicionado suporte para alterações de verificação de ILM no controle de versão, atualizações da página Nomes de Domínio de Endpoint, condições e variáveis em políticas, exemplos de políticas e a permissão PutOverwriteObject.
10,3	Adicionado suporte para controle de versão.
10,2	Adicionado suporte para políticas de acesso de grupo e bucket, e para cópia multiparte (Upload Part - Copy).
10,1	Adicionado suporte para upload multiparte, solicitações de estilo de hospedagem virtual e autenticação v4.
10,0	Suporte inicial da API REST do S3 pelo sistema StorageGRID . A versão atualmente suportada da <i>Simple Storage Service API Reference</i> é 2006-03-01.

Referência rápida: solicitações de API do S3 suportadas

Esta página resume como o StorageGRID oferece suporte às APIs do Amazon Simple Storage Service (S3).

Esta página inclui apenas as operações do S3 suportadas pelo StorageGRID.



Para ver a documentação da AWS para cada operação, selecione o link no título.

Parâmetros de consulta URI comuns e cabeçalhos de solicitação

A menos que indicado, os seguintes parâmetros comuns de consulta de URI são suportados:

- `versionId`(conforme necessário para operações de objeto)

A menos que indicado, os seguintes cabeçalhos de solicitação comuns são suportados:

- Authorization
- Connection
- Content-Length
- Content-MD5
- Content-Type
- Date
- Expect
- Host
- x-amz-date

Informações relacionadas

- ["Detalhes da implementação da API REST S3"](#)
- ["Referência da API do Amazon Simple Storage Service: Cabeçalhos de solicitação comuns"](#)

"AbortarMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, mais este parâmetro de consulta URI adicional:

- uploadId

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações para uploads multipartes"](#)

"Upload completo de várias partes"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, mais este parâmetro de consulta URI adicional:

- uploadId
- x-amz-checksum-sha256

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- ChecksumSHA256
- CompleteMultipartUpload
- ETag

- Part
- PartNumber

Documentação do StorageGRID

["Upload completo de várias partes"](#)

"CopiarObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes cabeçalhos adicionais:

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-`<metadata-name>`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["CopiarObjeto"](#)

"CriarBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes cabeçalhos adicionais:

- x-amz-bucket-object-lock-enabled

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

["Operações em baldes"](#)

"CriarMultipartUpload"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes cabeçalhos adicionais:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["CriarMultipartUpload"](#)

"ExcluirBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Documentação do StorageGRID

["Operações em baldes"](#)

"ExcluirBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"DeleteBucketEncryption"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"Ciclo de vida do DeleteBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

- ["Operações em baldes"](#)
- ["Criar configuração do ciclo de vida do S3"](#)

"Política de exclusão de balde"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"DeleteBucketReplication"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ExcluirBucketTagging"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ExcluirObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, mais este cabeçalho de solicitação adicional:

- `x-amz-bypass-governance-retention`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em objetos"](#)

"ExcluirObjetos"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, mais este cabeçalho de solicitação adicional:

- `x-amz-bypass-governance-retention`

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

["Operações em objetos"](#)

"ExcluirMarcaçãoDeObjeto"

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em objetos"](#)

"ObterBucketAcl"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ObterBucketCors"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"Obter criptografia do Bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"Obter configuração do ciclo de vida do Bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

- ["Operações em baldes"](#)
- ["Criar configuração do ciclo de vida do S3"](#)

"ObterBucketLocation"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"Obter configuração de notificação de bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ObterBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"Obter replicação do Bucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"Obter marcação de balde"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ObterVersionamento doBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ObterObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros de consulta URI adicionais:

- x-amz-checksum-mode
- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

E estes cabeçalhos de solicitação adicionais:

- Range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["ObterObjeto"](#)

"ObterAclObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em objetos"](#)

"ObterObjetoLegalHold"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)

"ObterConfiguraçãoObjectLock"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)

"ObterRetençãoDeObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)

"Obter marcação de objeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em objetos"](#)

"Balde de cabeça"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"CabeçaObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes cabeçalhos adicionais:

- x-amz-checksum-mode
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["CabeçaObjeto"](#)

"ListBuckets"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Nenhum

Documentação do StorageGRID

[Operações no serviço](#) > [ListBuckets](#)

"ListarMultipartUploads"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros adicionais:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["ListarMultipartUploads"](#)

"Objetos de Lista"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros adicionais:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ListObjectsV2"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros adicionais:

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"Versões do objeto de lista"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros adicionais:

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["Operações em baldes"](#)

"ListarPartes"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros adicionais:

- max-parts

- part-number-marker
- uploadId

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["ListarMultipartUploads"](#)

["ColoqueBucketCors"](#)

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

["Operações em baldes"](#)

["PutBucketEncryption"](#)

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentação do StorageGRID

["Operações em baldes"](#)

["Configuração do ciclo de vida do PutBucket"](#)

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- And
- Days
- Expiration

- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

Documentação do StorageGRID

- ["Operações em baldes"](#)
- ["Criar configuração do ciclo de vida do S3"](#)

"Configuração de notificação PutBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Tags XML do corpo da solicitação

O StorageGRID suporta estas tags XML do corpo da solicitação:

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

Documentação do StorageGRID

["Operações em baldes"](#)

"PutBucketPolicy"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Para obter detalhes sobre os campos de corpo JSON suportados, consulte ["Use políticas de acesso a buckets e grupos"](#).

"PutBucketReplicação"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Tags XML do corpo da solicitação

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

Documentação do StorageGRID

["Operações em baldes"](#)

"Colocar marcação de balde"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

["Operações em baldes"](#)

"Versão PutBucket"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Parâmetros do corpo da solicitação

O StorageGRID suporta estes parâmetros do corpo da solicitação:

- VersioningConfiguration
- Status

Documentação do StorageGRID

"Operações em baldes"

"ColocarObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes cabeçalhos adicionais:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-sha256
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

Corpo da solicitação

- Dados binários do objeto

Documentação do StorageGRID

"ColocarObjeto"

"ColocarObjetoLegalHold"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)

"PutObjectLockConfiguration"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)

"ColocarRetençãoDeObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, mais este cabeçalho adicional:

- x-amz-bypass-governance-retention

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)

"Colocar marcação de objeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

O StorageGRID oferece suporte a todos os parâmetros do corpo da solicitação definidos pela API REST do Amazon S3 no momento da implementação.

Documentação do StorageGRID

["Operações em objetos"](#)

"RestaurarObjeto"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Para obter detalhes sobre os campos corporais suportados, consulte ["RestaurarObjeto"](#) .

"SelecionarObjetoConteúdo"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação.

Corpo da solicitação

Para obter detalhes sobre os campos corporais suportados, consulte o seguinte:

- ["Use o S3 Select"](#)
- ["SelecionarObjetoConteúdo"](#)

"UploadPart"

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `partNumber`
- `uploadId`

E estes cabeçalhos de solicitação adicionais:

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corpo da solicitação

- Dados binários da peça

Documentação do StorageGRID

["UploadPart"](#)

["UploadPartCopy"](#)

Parâmetros de consulta URI e cabeçalhos de solicitação

O StorageGRID oferece suporte a todos [parâmetros e cabeçalhos comuns](#) para esta solicitação, além destes parâmetros de consulta URI adicionais:

- `partNumber`
- `uploadId`

E estes cabeçalhos de solicitação adicionais:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`

- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

Corpo da solicitação

Nenhum

Documentação do StorageGRID

["UploadPartCopy"](#)

Testar configuração da API REST do S3

Você pode usar a Amazon Web Services Command Line Interface (AWS CLI) para testar sua conexão com o sistema e verificar se você consegue ler e gravar objetos.

Antes de começar

- Você baixou e instalou o AWS CLI de ["aws.amazon.com/cli"](https://aws.amazon.com/cli/) .
- Opcionalmente, você tem ["criou um ponto de extremidade do balanceador de carga"](#) . Caso contrário, você sabe o endereço IP do nó de armazenamento ao qual deseja se conectar e o número da porta a ser usada. Ver ["Endereços IP e portas para conexões de clientes"](#) .
- Você tem ["criou uma conta de locatário S3"](#) .
- Você fez login no inquilino e ["criou uma chave de acesso"](#) .

Para obter detalhes sobre essas etapas, consulte ["Configurar conexões do cliente"](#) .

Passos

1. Configure as definições da AWS CLI para usar a conta que você criou no sistema StorageGRID :
 - a. Entre no modo de configuração: `aws configure`
 - b. Digite o ID da chave de acesso da conta que você criou.
 - c. Digite a chave de acesso secreta da conta que você criou.
 - d. Digite a região padrão a ser usada. Por exemplo, `us-east-1` .
 - e. Digite o formato de saída padrão a ser usado ou pressione **Enter** para selecionar JSON.
2. Crie um bucket.

Este exemplo pressupõe que você configurou um ponto de extremidade do balanceador de carga para usar o endereço IP 10.96.101.17 e a porta 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Se o bucket for criado com sucesso, o local do bucket será retornado, conforme visto no exemplo a seguir:

```
"Location": "/testbucket"
```

3. Carregar um objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Se o objeto for carregado com sucesso, uma Etag será retornada, que é um hash dos dados do objeto.

4. Liste o conteúdo do bucket para verificar se o objeto foi carregado.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Exclua o objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Exclua o bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Como o StorageGRID implementa a API REST do S3

Solicitações conflitantes de clientes

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos".

O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

Valores de consistência

A consistência fornece um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de armazenamento e sites. Você pode alterar a consistência conforme exigido pelo seu aplicativo.

Por padrão, o StorageGRID garante consistência de leitura após gravação para objetos recém-criados. Qualquer GET após um PUT concluído com sucesso poderá ler os dados recém-gravados. Substituições de objetos existentes, atualizações de metadados e exclusões são eventualmente consistentes. As substituições geralmente levam segundos ou minutos para se propagar, mas podem levar até 15 dias.

Se você quiser executar operações de objeto com uma consistência diferente, você pode:

- Especifique uma consistência para [cada balde](#) .
- Especifique uma consistência para [cada operação de API](#) .
- Altere a consistência padrão em toda a grade executando uma das seguintes tarefas:
 - No Grid Manager, vá para **CONFIGURAÇÃO > Sistema > Configurações de armazenamento > Consistência padrão**.
 - .



Uma alteração na consistência de toda a grade se aplica somente aos buckets criados após a configuração ter sido alterada. Para determinar os detalhes de uma alteração, consulte o log de auditoria localizado em `/var/local/log` (pesquise por **consistencyLevel**).

Valores de consistência

A consistência afeta como os metadados que o StorageGRID usa para rastrear objetos são distribuídos entre os nós e, portanto, a disponibilidade dos objetos para solicitações do cliente.

Você pode definir a consistência de um bucket ou de uma operação de API para um dos seguintes valores:

- **Todos**: Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
- **Strong-global**: Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
- **Strong-site**: Garante consistência de leitura após gravação para todas as solicitações de clientes dentro de um site.
- **Leitura após nova gravação**: (Padrão) 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 .

Use a consistência "Leitura após nova gravação" e "Disponível"

Quando uma operação HEAD ou GET usa a consistência "Leitura após nova gravação", o StorageGRID executa a pesquisa em várias etapas, da seguinte maneira:

- Primeiro, ele procura o objeto usando uma consistência baixa.
- Se essa pesquisa falhar, ela será repetida no próximo valor de consistência até atingir uma consistência equivalente ao comportamento de strong-global.

Se uma operação HEAD ou GET usar a consistência "Leitura após nova gravação", mas o objeto não existir, a pesquisa de objetos sempre alcançará uma consistência equivalente ao comportamento de strong-global. Como essa consistência exige que várias cópias dos metadados do objeto estejam disponíveis em cada site, você poderá receber um alto número de erros 500 do servidor interno se dois ou mais nós de armazenamento no mesmo site estiverem indisponíveis.

A menos que você precise de garantias de consistência semelhantes às do Amazon S3, você pode evitar esses erros para operações HEAD e GET definindo a consistência como "Disponível". Quando uma operação HEAD ou GET usa a consistência "Disponível", o StorageGRID fornece apenas consistência eventual. Ele não tenta novamente uma operação com falha para aumentar a consistência, portanto, não exige que várias cópias dos metadados do objeto estejam disponíveis.

Especificar consistência para operação de API

Para definir a consistência de uma operação de API individual, os valores de consistência devem ser suportados para a operação e você deve especificar a consistência no cabeçalho da solicitação. Este exemplo define a consistência como "Strong-site" para uma operação GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



Você deve usar a mesma consistência para as operações PutObject e GetObject.

Especificar consistência para bucket

Para definir a consistência do bucket, você pode usar o StorageGRID ["Consistência do balde PUT"](#) solicitar. Ou você pode ["alterar a consistência de um balde"](#) do gerente do inquilino.

Ao definir a consistência de um bucket, esteja ciente do seguinte:

- Definir a consistência de um bucket determina qual consistência será usada para operações do S3 executadas nos objetos no bucket ou na configuração do bucket. Não afeta as operações no próprio bucket.
- A consistência de uma operação de API individual substitui a consistência do bucket.
- Em geral, os buckets devem usar a consistência padrão, "Leitura após nova gravação". Se as solicitações não estiverem funcionando corretamente, altere o comportamento do cliente do aplicativo, se possível. Ou configure o cliente para especificar a consistência para cada solicitação de API. Defina a consistência no nível do bucket somente como último recurso.

Como a consistência e as regras de ILM interagem para afetar a proteção de dados

Tanto sua escolha de consistência quanto sua regra de ILM afetam como os objetos são protegidos. Essas configurações podem interagir.

Por exemplo, a consistência usada quando um objeto é armazenado afeta o posicionamento inicial dos metadados do objeto, enquanto o comportamento de ingestão selecionado para a regra ILM afeta o posicionamento inicial das cópias do objeto. Como o StorageGRID requer acesso aos metadados de um objeto e seus dados 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 do sistema mais previsíveis.

A seguir "[opções de ingestão](#)" estão disponíveis para regras ILM:

Comprometimento duplo

O StorageGRID faz imediatamente cópias provisórias do objeto e retorna sucesso ao cliente. Cópias especificadas na regra ILM são feitas quando possível.

Estrito

Todas as cópias especificadas na regra ILM devem ser feitas antes que o sucesso seja retornado ao cliente.

Equilibrado

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.

Exemplo de como a consistência e a regra 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.

Controle de versão de objetos

Você pode definir o estado de controle de versão de um bucket se quiser manter várias versões de cada objeto. Habilitar o controle de versão para um bucket pode ajudar a proteger contra a exclusão acidental de objetos e permite que você recupere e restaure versões anteriores de um objeto.

O sistema StorageGRID implementa o controle de versão com suporte para a maioria dos recursos e com algumas limitações. O StorageGRID suporta até 10.000 versões de cada objeto.

O controle de versão de objetos pode ser combinado com o gerenciamento do ciclo de vida das informações (ILM) do StorageGRID ou com a configuração do ciclo de vida do bucket do S3. Você deve habilitar explicitamente o controle de versão para cada bucket. Quando o controle de versão é habilitado para um bucket, cada objeto adicionado ao bucket recebe um ID de versão, que é gerado pelo sistema StorageGRID .

O uso de MFA (autenticação multifator) não é suportado.



O controle de versão pode ser habilitado somente em buckets criados com o StorageGRID versão 10.3 ou posterior.

ILM e controle de versão

As políticas de ILM são aplicadas a cada versão de um objeto. Um processo de verificação de ILM verifica continuamente todos os objetos e os reavalia em relação à política de ILM atual. Quaisquer alterações feitas nas políticas do ILM serão aplicadas a todos os objetos ingeridos anteriormente. Isso inclui versões ingeridas anteriormente se o controle de versão estiver habilitado. A verificação de ILM aplica novas alterações de ILM a objetos ingeridos anteriormente.

Para objetos S3 em buckets habilitados para controle de versão, o suporte ao controle de versão permite que você crie regras ILM que usam "Tempo não atual" como o Tempo de referência (selecione **Sim** para a pergunta "Aplicar esta regra somente a versões de objetos mais antigas?" em ["Etapa 1 do assistente Criar uma regra ILM"](#)). Quando um objeto é atualizado, suas versões anteriores se tornam obsoletas. Usar um filtro "Tempo não atual" permite criar políticas que reduzem o impacto de armazenamento de versões anteriores de objetos.



Ao carregar uma nova versão de um objeto usando uma operação de upload multipartes, o tempo não atual para a versão original do objeto reflete quando o upload multipartes foi criado para a nova versão, não quando o upload multipartes foi concluído. Em casos limitados, o horário não atual da versão original pode ser horas ou dias anterior ao horário da versão atual.

Informações relacionadas

- ["Como objetos versionados do S3 são excluídos"](#)
- ["Regras e políticas do ILM para objetos versionados do S3 \(Exemplo 4\)"](#) .

Use a API REST do S3 para configurar o bloqueio de objeto do S3

Se a configuração global do S3 Object Lock estiver habilitada para seu sistema StorageGRID , você poderá criar buckets com o S3 Object Lock habilitado. Você pode especificar a retenção padrão para cada bucket ou configurações de retenção para cada versão do objeto.

Como habilitar o bloqueio de objeto S3 para um bucket

Se a configuração global S3 Object Lock estiver habilitada para seu sistema StorageGRID , você poderá habilitar o S3 Object Lock ao criar cada bucket.

O bloqueio de objeto do S3 é uma configuração permanente que só pode ser ativada quando você cria um bucket. Não é possível adicionar ou desabilitar o S3 Object Lock após a criação de um bucket.

Para habilitar o bloqueio de objeto S3 para um bucket, use um destes métodos:

- Crie o bucket usando o Tenant Manager. Ver "[Criar bucket S3](#)".
- Crie o bucket usando uma solicitação `CreateBucket` com o `x-amz-bucket-object-lock-enabled` cabeçalho da solicitação. Ver "[Operações em baldes](#)".

O S3 Object Lock requer controle de versão do bucket, que é ativado automaticamente quando o bucket é criado. Não é possível suspender o controle de versão do bucket. Ver "[Controle de versão de objetos](#)".

Configurações de retenção padrão para um bucket

Quando o Bloqueio de Objeto S3 estiver habilitado para um bucket, você poderá, opcionalmente, habilitar a retenção padrão para o bucket e especificar um modo de retenção padrão e um período de retenção padrão.

Modo de retenção padrão

- No modo 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 GOVERNANÇA:
 - Usuários com o `s3:BypassGovernanceRetention` permissão pode usar o `x-amz-bypass-governance-retention: true` cabeçalho de solicitação para ignorar as 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.

Período de retenção padrão

Cada bucket pode ter um período de retenção padrão especificado em anos ou dias.

Como definir a retenção padrão para um bucket

Para definir a retenção padrão para um bucket, use um destes métodos:

- Gerencie as configurações do bucket no Gerenciador de locatários. Ver "[Criar um bucket S3](#)" e "[Atualizar retenção padrão do bloqueio de objeto S3](#)".
- Emita uma solicitação `PutObjectLockConfiguration` para o bucket para especificar o modo padrão e o número padrão de dias ou anos.

PutObjectLockConfiguration

A solicitação `PutObjectLockConfiguration` permite que você defina e modifique o modo de retenção padrão e o período de retenção padrão para um bucket que tenha o S3 Object Lock habilitado. Você também pode remover as configurações de retenção padrão configuradas anteriormente.

Quando novas versões de objetos são ingeridas no bucket, o modo de retenção padrão é aplicado se `x-amz-object-lock-mode` e `x-amz-object-lock-retain-until-date` não são especificados. O período de retenção padrão é usado para calcular a data de retenção se `x-amz-object-lock-retain-until-date` não é especificado.

Se o período de retenção padrão for modificado após a ingestão de uma versão do objeto, a data de retenção da versão do objeto permanecerá a mesma e não será recalculada usando o novo período de retenção padrão.

Você deve ter o `s3:PutBucketObjectLockConfiguration` permissão, ou ser root da conta, para concluir esta operação.

O `Content-MD5` O cabeçalho da solicitação deve ser especificado na solicitação PUT.

Exemplo de solicitação

Este exemplo habilita o S3 Object Lock para um bucket e define o modo de retenção padrão como COMPLIANCE e o período de retenção padrão como 6 anos.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Como determinar a retenção padrão para um bucket

Para determinar se o S3 Object Lock está habilitado para um bucket e para ver o modo de retenção padrão e o período de retenção, use um destes métodos:

- Visualize o bucket no Gerenciador de locatários. Ver ["Exibir buckets S3"](#) .
- Emita uma solicitação `GetObjectLockConfiguration`.

ObterConfiguraçãoObjectLock

A solicitação `GetObjectLockConfiguration` permite que você determine se o S3 Object Lock está habilitado para um bucket e, se estiver, veja se há um modo de retenção padrão e um período de retenção configurados para o bucket.

Quando novas versões de objetos são ingeridas no bucket, o modo de retenção padrão é aplicado se `x-amz-`

object-lock-mode não é especificado. O período de retenção padrão é usado para calcular a data de retenção se x-amz-object-lock-retain-until-date não é especificado.

Você deve ter o s3:GetBucketObjectLockConfiguration permissão, ou ser root da conta, para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Exemplo de resposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Como especificar configurações de retenção para um objeto

Um bucket com o S3 Object Lock ativado pode conter uma combinação de objetos com e sem configurações de retenção do S3 Object Lock.

As configurações de retenção no nível do objeto são especificadas usando a API REST do S3. As configurações de retenção de um objeto substituem quaisquer configurações de retenção padrão do bucket.

Você pode especificar as seguintes configurações para cada objeto:

- **Modo de retenção:** CONFORMIDADE ou GOVERNANÇA.
- **Retain-until-date:** Uma data que especifica por quanto tempo a versão do objeto deve ser retida pelo StorageGRID.
 - No modo CONFORMIDADE, se a data de retenção for no futuro, o objeto poderá ser recuperado, mas não poderá ser modificado ou excluído. A data de retenção pode ser aumentada, mas esta data não pode ser diminuída ou removida.
 - No modo GOVERNANÇA, usuários com permissão especial podem ignorar a configuração de retenção até a data. Eles podem excluir uma versão do objeto antes que seu período de retenção termine. Eles também podem aumentar, diminuir ou até mesmo remover a data de retenção.
- **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.

A configuração de retenção legal para um objeto é independente do modo de retenção e da data de retenção. Se uma versão do objeto estiver sob retenção legal, ninguém poderá excluí-la.

Para especificar as configurações de bloqueio de objeto do S3 ao adicionar uma versão de objeto a um bucket, emita um `"ColocarObjeto"`, `"CopiarObjeto"`, ou `"CriarMultipartUpload"` solicitar.

Você pode usar o seguinte:

- `x-amz-object-lock-mode`, que pode ser COMPLIANCE ou GOVERNANCE (diferencia maiúsculas de minúsculas).



Se você especificar `x-amz-object-lock-mode`, você também deve especificar `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
 - O valor reter-até-data deve estar no formato `2020-08-10T21:46:00Z`. Segundos fracionários são permitidos, mas apenas 3 dígitos decimais são preservados (precisão de milissegundos). Outros formatos ISO 8601 não são permitidos.
 - A data de retenção deve ser no futuro.
- `x-amz-object-lock-legal-hold`

Se a retenção legal estiver LIGADA (diferencia maiúsculas de minúsculas), o objeto será colocado sob retenção legal. Se a retenção legal estiver DESLIGADA, nenhuma retenção legal será aplicada. Qualquer outro valor resulta em um erro 400 Bad Request (InvalidArgument).

Se você usar qualquer um desses cabeçalhos de solicitação, esteja ciente destas restrições:

- O `Content-MD5` o cabeçalho da solicitação é necessário se houver `x-amz-object-lock-*` O cabeçalho da solicitação está presente na solicitação PutObject. Content-MD5 não é necessário para CopyObject ou CreateMultipartUpload.
- Se o bucket não tiver o S3 Object Lock habilitado e um `x-amz-object-lock-*` Se o cabeçalho da solicitação estiver presente, um erro 400 Bad Request (InvalidRequest) será retornado.

- A solicitação PutObject suporta o uso de `x-amz-storage-class: REDUCED_REDUNDANCY` para corresponder ao comportamento da AWS. No entanto, quando um objeto é ingerido em um bucket com o S3 Object Lock habilitado, o StorageGRID sempre executará uma ingestão de confirmação dupla.
- Uma resposta de versão GET ou HeadObject subsequente incluirá os cabeçalhos `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e `x-amz-object-lock-legal-hold`, se configurado e se o remetente da solicitação tiver o correto `s3:Get*` permissões.

Você pode usar o `s3:object-lock-remaining-retention-days` chave de condição de política para limitar os períodos mínimos e máximos de retenção permitidos para seus objetos.

Como atualizar as configurações de retenção de um objeto

Se precisar atualizar as configurações de retenção ou retenção legal para uma versão de objeto existente, você pode executar as seguintes operações de sub-recursos do objeto:

- PutObjectLegalHold

Se o novo valor de retenção legal for LIGADO, o objeto será colocado sob retenção legal. Se o valor de retenção legal estiver DESLIGADO, a retenção legal será suspensa.

- PutObjectRetention
 - O valor do modo pode ser CONFORMIDADE ou GOVERNANÇA (diferencia maiúsculas de minúsculas).
 - O valor reter-até-data deve estar no formato 2020-08-10T21:46:00Z . Segundos fracionários são permitidos, mas apenas 3 dígitos decimais são preservados (precisão de milissegundos). Outros formatos ISO 8601 não são permitidos.
 - Se uma versão do objeto tiver uma data de retenção existente, você só poderá aumentá-la. O novo valor deve estar no futuro.

Como usar o modo GOVERNANÇA

Usuários que possuem o `s3:BypassGovernanceRetention` a permissão pode ignorar as configurações de retenção ativas de um objeto que usa o modo GOVERNANCE. Qualquer operação DELETE ou PutObjectRetention deve incluir o `x-amz-bypass-governance-retention:true` cabeçalho da solicitação. Esses usuários podem executar estas operações adicionais:

- Execute as operações DeleteObject ou DeleteObjects para excluir uma versão do objeto antes que seu período de retenção termine.

Objetos que estão sob retenção legal não podem ser excluídos. A retenção legal deve estar DESLIGADA.

- Execute operações PutObjectRetention que alterem o modo de versão de um objeto de GOVERNANCE para COMPLIANCE antes que o período de retenção do objeto tenha decorrido.

Alterar o modo de CONFORMIDADE para GOVERNANÇA nunca é permitido.

- Execute operações PutObjectRetention para aumentar, diminuir ou remover o período de retenção de uma versão do objeto.

Informações relacionadas

- ["Gerenciar objetos com o S3 Object Lock"](#)

- ["Use o S3 Object Lock para reter objetos"](#)
- ["Guia do usuário do Amazon Simple Storage Service: Bloqueio de objetos"](#)

Criar configuração do ciclo de vida do S3

Você pode criar uma configuração de ciclo de vida do S3 para controlar quando objetos específicos são excluídos do sistema StorageGRID .

O exemplo simples nesta seção ilustra como uma configuração de ciclo de vida do S3 pode controlar quando determinados objetos são excluídos (expirados) de buckets específicos do S3. O exemplo nesta seção é apenas para fins ilustrativos. Para obter detalhes completos sobre a criação de configurações do ciclo de vida do S3, consulte ["Guia do usuário do Amazon Simple Storage Service: gerenciamento do ciclo de vida do objeto"](#) . Observe que o StorageGRID suporta apenas ações de expiração; ele não suporta ações de transição.

O que é configuração de ciclo de vida

Uma configuração de ciclo de vida é um conjunto de regras aplicadas aos objetos em buckets específicos do S3. Cada regra especifica quais objetos são afetados e quando esses objetos expirarão (em uma data específica ou após um determinado número de dias).

O StorageGRID suporta até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML:

- Expiração: Exclua um objeto quando uma data especificada for atingida ou quando um número especificado de dias for atingido, a partir do momento em que o objeto foi ingerido.
- NoncurrentVersionExpiration: Exclui um objeto quando um número especificado de dias é atingido, começando em quando o objeto se tornou não atual.
- Filtro (Prefixo, Tag)
- Status
- EU IA

Cada objeto segue as configurações de retenção de um ciclo de vida de bucket do S3 ou de uma política do ILM. 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 de ciclo de vida do bucket. Objetos que não correspondem ao filtro de ciclo de vida do bucket usam as configurações de retenção da política do ILM. Se um objeto corresponder a um filtro de ciclo de vida de bucket e nenhuma ação de expiração for explicitamente especificada, as configurações de retenção da política ILM não serão usadas e ficará implícito que as versões do objeto serão retidas para sempre. Ver ["Exemplo de prioridades para o ciclo de vida do bucket S3 e política de ILM"](#) .

Como resultado, um objeto pode ser removido da grade mesmo que as instruções de posicionamento em uma regra ILM ainda se apliquem ao objeto. Ou um objeto pode ser retido na grade mesmo depois que quaisquer instruções de posicionamento do ILM para o objeto tenham expirado. Para obter detalhes, consulte ["Como o ILM opera ao longo da vida de um objeto"](#) .



A configuração do ciclo de vida do bucket pode ser usada com buckets que tenham o S3 Object Lock habilitado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis legados.

O StorageGRID oferece suporte ao uso das seguintes operações de bucket para gerenciar configurações de ciclo de vida:

- Ciclo de vida do DeleteBucket
- Obter configuração do ciclo de vida do Bucket
- Configuração do ciclo de vida do PutBucket

Criar configuração de ciclo de vida

Como primeira etapa na criação de uma configuração de ciclo de vida, você cria um arquivo JSON que inclui uma ou mais regras. Por exemplo, este arquivo JSON inclui três regras, como segue:

1. A regra 1 se aplica somente a objetos que correspondem ao prefixo `category1 /` e que tenham uma `key2` valor de `tag2`. O `Expiration` O parâmetro especifica que os objetos que correspondem ao filtro expirarão à meia-noite de 22 de agosto de 2020.
2. A regra 2 se aplica somente a objetos que correspondem ao prefixo `category2 /`. O `Expiration` O parâmetro especifica que os objetos que correspondem ao filtro expirarão 100 dias após serem ingeridos.



Regras que especificam um número de dias são relativas a quando o objeto foi ingerido. Se a data atual exceder a data de ingestão mais o número de dias, alguns objetos poderão ser removidos do bucket assim que a configuração do ciclo de vida for aplicada.

3. A regra 3 se aplica somente a objetos que correspondem ao prefixo `category3 /`. O `Expiration` O parâmetro especifica que quaisquer versões não atuais de objetos correspondentes expirarão 50 dias após se tornarem não atuais.

```

{
  "Rules": [
    {
      "ID": "rule1",
      "Filter": {
        "And": {
          "Prefix": "category1/",
          "Tags": [
            {
              "Key": "key2",
              "Value": "tag2"
            }
          ]
        }
      },
      "Expiration": {
        "Date": "2020-08-22T00:00:00Z"
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule2",
      "Filter": {
        "Prefix": "category2/"
      },
      "Expiration": {
        "Days": 100
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule3",
      "Filter": {
        "Prefix": "category3/"
      },
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 50
      },
      "Status": "Enabled"
    }
  ]
}

```

Aplicar configuração de ciclo de vida ao bucket

Depois de criar o arquivo de configuração do ciclo de vida, aplique-o a um bucket emitindo uma solicitação `PutBucketLifecycleConfiguration`.

Esta solicitação aplica a configuração do ciclo de vida no arquivo de exemplo a objetos em um bucket denominado `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar se uma configuração de ciclo de vida foi aplicada com sucesso ao bucket, emita uma solicitação `GetBucketLifecycleConfiguration`. Por exemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Uma resposta bem-sucedida lista a configuração do ciclo de vida que você acabou de aplicar.

Validar se a expiração do ciclo de vida do bucket se aplica ao objeto

Você pode determinar se uma regra de expiração na configuração do ciclo de vida se aplica a um objeto específico ao emitir uma solicitação `PutObject`, `HeadObject` ou `GetObject`. Se uma regra se aplicar, a resposta inclui uma `Expiration` parâmetro que indica quando o objeto expira e qual regra de expiração foi correspondida.



Como o ciclo de vida do bucket substitui o ILM, o `expiry-date` é mostrada a data real em que o objeto será excluído. Para obter detalhes, consulte ["Como a retenção de objetos é determinada"](#).

Por exemplo, esta solicitação `PutObject` foi emitida em 22 de junho de 2020 e coloca um objeto no `testbucket` balde.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

A resposta de sucesso indica que o objeto irá expirar em 100 dias (01 de outubro de 2020) e que correspondeu à Regra 2 da configuração do ciclo de vida.

```
{
  *Expiration: "expiry-date=\\"Thu, 01 Oct 2020 09:07:49 GMT\\", rule-
id=\\"rule2\\",
  ETag: "\\"9762f8a803bc34f5340579d4446076f7\\""}
}
```

Por exemplo, esta solicitação HeadObject foi usada para obter metadados para o mesmo objeto no bucket testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

A resposta de sucesso inclui os metadados do objeto e indica que o objeto irá expirar em 100 dias e que correspondeu à Regra 2.

```
{
  "AcceptRanges": "bytes",
  *Expiration: "expiry-date=\\"Thu, 01 Oct 2020 09:07:48 GMT\\", rule-
id=\\"rule2\\",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\\"9762f8a803bc34f5340579d4446076f7\\""}
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```



Para buckets habilitados para controle de versão, o x-amz-expiration O cabeçalho de resposta se aplica somente às versões atuais dos objetos.

Recomendações para implementar a API REST do S3

Você deve seguir estas recomendações ao implementar a API REST do S3 para uso com o StorageGRID.

Recomendações para HEADs para objetos inexistentes

Se o seu aplicativo verifica rotineiramente se um objeto existe em um caminho onde você não espera que o objeto realmente exista, você deve usar o "Disponível"[consistência](#) . Por exemplo, você deve usar a consistência "Disponível" se seu aplicativo fizer HEAD de um local antes de fazer PUT nele.

Caso contrário, se a operação HEAD não encontrar o objeto, você poderá receber um alto número de erros 500 do Servidor Interno se dois ou mais Nós de Armazenamento no mesmo site estiverem indisponíveis ou um site remoto estiver inacessível.

Você pode definir a consistência "Disponível" para cada bucket usando o [Consistência do balde PUT](#) solicitação, ou você pode especificar a consistência no cabeçalho da solicitação para uma operação de API

individual.

Recomendações para chaves de objeto

Siga estas recomendações para nomes de chaves de objeto, com base em quando o bucket foi criado pela primeira vez.

Buckets criados no StorageGRID 11.4 ou anterior

- Não use valores aleatórios como os quatro primeiros caracteres das chaves do objeto. Isso contrasta com a antiga recomendação da AWS para prefixos de chaves. Em vez disso, use prefixos não aleatórios e não exclusivos, como `image`.
- Se você seguir a antiga recomendação da AWS de usar caracteres aleatórios e exclusivos em prefixos de chave, prefixe as chaves de objeto com um nome de diretório. Ou seja, use este formato:

```
mybucket/mydir/f8e3-image3132.jpg
```

Em vez deste formato:

```
mybucket/f8e3-image3132.jpg
```

Buckets criados no StorageGRID 11.4 ou posterior

Não é necessário restringir nomes de chaves de objetos para atender às melhores práticas de desempenho. Na maioria dos casos, você pode usar valores aleatórios para os quatro primeiros caracteres dos nomes das chaves do objeto.



Uma exceção a isso é uma carga de trabalho do S3 que remove continuamente todos os objetos após um curto período de tempo. Para minimizar o impacto no desempenho deste caso de uso, varie uma parte inicial do nome da chave a cada vários milhares de objetos com algo como a data. Por exemplo, suponha que um cliente S3 normalmente grava 2.000 objetos/segundo e a política de ciclo de vida do ILM ou do bucket remove todos os objetos após três dias. Para minimizar o impacto no desempenho, você pode nomear as chaves usando um padrão como este: `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Recomendações para "leituras de intervalo"

Se o ["opção global para compactar objetos armazenados"](#) estiver habilitado, os aplicativos cliente S3 devem 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.

Suporte para API REST do Amazon S3

Detalhes da implementação da API REST S3

O sistema StorageGRID implementa a API do Simple Storage Service (versão da API 2006-03-01) com suporte para a maioria das operações e com algumas limitações. Você precisa entender os detalhes de implementação ao integrar aplicativos cliente da API REST do S3.

O sistema StorageGRID oferece suporte a solicitações no estilo de hospedagem virtual e solicitações no estilo de caminho.

Manuseio de data

A implementação StorageGRID da API REST do S3 suporta apenas formatos de data HTTP válidos.

O sistema StorageGRID suporta apenas formatos de data HTTP válidos para quaisquer cabeçalhos que aceitem valores de data. A parte de hora da data pode ser especificada no formato Greenwich Mean Time (GMT) ou no formato Universal Coordinated Time (UTC) sem deslocamento de fuso horário (+0000 deve ser especificado). Se você incluir o `x-amz-date` cabeçalho na sua solicitação, ele substitui qualquer valor especificado no cabeçalho da solicitação `Date`. Ao usar o AWS Signature versão 4, o `x-amz-date` O cabeçalho deve estar presente na solicitação assinada porque o cabeçalho de data não é suportado.

Cabeçalhos de solicitação comuns

O sistema StorageGRID suporta os cabeçalhos de solicitação comuns definidos por ["Referência da API do Amazon Simple Storage Service: Cabeçalhos de solicitação comuns"](#), com uma exceção.

Cabeçalho da solicitação	Implementação
Autorização	Suporte total para AWS Signature versão 2 Suporte para AWS Signature versão 4, com as seguintes exceções: Quando você fornece o valor real da soma de verificação da carga útil em <code>x-amz-content-sha256</code>, o valor é aceito sem validação, como se o valor <code>UNSIGNED-PAYLOAD</code> tinha sido fornecido para o cabeçalho. Quando você fornece um <code>x-amz-content-sha256</code> valor do cabeçalho que implica <code>aws-chunked streaming</code> (por exemplo, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), as assinaturas dos blocos não são verificadas em relação aos dados dos blocos.
token de segurança x-amz	Não implementado. Devoluções <code>XNotImplemented</code> .

Cabeçalhos de resposta comuns

O sistema StorageGRID suporta todos os cabeçalhos de resposta comuns definidos pela *Simple Storage Service API Reference*, com uma exceção.

Cabeçalho de resposta	Implementação
<code>x-amz-id-2</code>	Não utilizado

Autenticar solicitações

O sistema StorageGRID oferece suporte ao acesso autenticado e anônimo a objetos usando a API S3.

A API do S3 oferece suporte ao Signature versão 2 e ao Signature versão 4 para autenticação de solicitações da API do S3.

Solicitações autenticadas devem ser assinadas usando seu ID de chave de acesso e sua chave de acesso secreta.

O sistema StorageGRID suporta dois métodos de autenticação: HTTP `Authorization` cabeçalho e usando parâmetros de consulta.

Use o cabeçalho de autorização HTTP

O HTTP `Authorization` O cabeçalho é usado por todas as operações da API do S3, exceto solicitações anônimas, quando permitido pela política de bucket. O `Authorization` O cabeçalho contém todas as informações de assinatura necessárias para autenticar uma solicitação.

Usar parâmetros de consulta

Você pode usar parâmetros de consulta para adicionar informações de autenticação a uma URL. Isso é conhecido como pré-assinatura de URL, que pode ser usado para conceder acesso temporário a recursos específicos. Usuários com a URL pré-assinada não precisam saber a chave de acesso secreta para acessar o recurso, o que permite que você forneça acesso restrito de terceiros a um recurso.

Operações no serviço

O sistema StorageGRID suporta as seguintes operações no serviço.

Operação	Implementação
ListBuckets (anteriormente chamado de Serviço GET)	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
Uso de armazenamento GET	O StorageGRID " Uso de armazenamento GET " A solicitação informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta. Esta é uma operação no serviço com um caminho de / e um parâmetro de consulta personalizado(<code>?x-ntap-sg-usage</code>) adicionado.
OPÇÕES /	Os aplicativos clientes podem emitir <code>OPTIONS</code> / solicitações para a porta S3 em um nó de armazenamento, sem fornecer credenciais de autenticação S3, para determinar se o nó de armazenamento está disponível. Você pode usar essa solicitação para monitoramento ou para permitir que balanceadores de carga externos identifiquem quando um nó de armazenamento está inativo.

Operações em baldes

O sistema StorageGRID suporta no máximo 5.000 buckets para cada conta de locatário do S3.

Cada grade pode ter no máximo 100.000 buckets.

Para dar suporte a 5.000 buckets, cada nó de armazenamento na grade deve ter no mínimo 64 GB de RAM.

As restrições de nome de bucket seguem as restrições de região padrão dos EUA da AWS, mas você deve restringi-las ainda mais às convenções de nomenclatura de DNS para oferecer suporte a solicitações de estilo de hospedagem virtual do S3.

Veja o seguinte para mais informações:

- ["Guia do usuário do Amazon Simple Storage Service: cotas, restrições e limitações de bucket"](#)
- ["Configurar nomes de domínio de endpoint S3"](#)

As operações ListObjects (GET Bucket) e ListObjectVersions (versões do objeto GET Bucket) oferecem suporte ao StorageGRID ["valores de consistência"](#).

Você pode verificar se as atualizações do último horário de acesso estão habilitadas ou desabilitadas para buckets individuais. Ver ["Último horário de acesso do Bucket GET"](#).

A tabela a seguir descreve como o StorageGRID implementa as operações de bucket da API REST do S3. Para executar qualquer uma dessas operações, é necessário fornecer as credenciais de acesso necessárias para a conta.

Operação	Implementação
CriarBucket	Cria um novo bucket. Ao criar o bucket, você se torna o proprietário do bucket. - Os nomes dos buckets devem obedecer às seguintes regras: - Deve ser exclusivo em cada sistema StorageGRID (não apenas exclusivo na conta do locatário). - Deve ser compatível com DNS. - Deve conter no mínimo 3 e no máximo 63 caracteres. - Pode ser uma série de um ou mais rótulos, com rótulos adjacentes separados por um ponto. Cada rótulo deve começar e terminar com uma letra minúscula ou um número e só pode usar letras minúsculas, números e hifens. - Não deve parecer um endereço IP formatado em texto. - Não deve usar pontos em solicitações de estilo de hospedagem virtual. Os períodos causarão problemas com a verificação do certificado curinga do servidor. - Por padrão, os buckets são criados no <code>us-east-1</code> região; no entanto, você pode usar o <code>LocationConstraint</code> elemento request no corpo da solicitação para especificar uma região diferente. Ao usar o <code>LocationConstraint</code> elemento, você deve especificar o nome exato de uma região que foi definida usando o Grid Manager ou a Grid Management API. Entre em contato com o administrador do sistema se você não souber o nome da região que deve usar. Observação: Ocorrerá um erro se sua solicitação <code>CreateBucket</code> usar uma região que não foi definida em StorageGRID. - Você pode incluir o <code>x-amz-bucket-object-lock-enabled</code> cabeçalho de solicitação para criar um bucket com o S3 Object Lock habilitado. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3". Você deve habilitar o S3 Object Lock ao criar o bucket. Não é possível adicionar ou desabilitar o S3 Object Lock após a criação de um bucket. O S3 Object Lock requer controle de versão do bucket, que é ativado automaticamente quando você cria o bucket.
ExcluirBucket	Exclui o bucket.
ExcluirBucketCors	Exclui a configuração CORS do bucket.
DeleteBucketEncryption	Exclui a criptografia padrão do bucket. Os objetos criptografados existentes permanecem criptografados, mas quaisquer novos objetos adicionados ao bucket não são criptografados.
Ciclo de vida do DeleteBucket	Exclui a configuração do ciclo de vida do bucket. Ver "Criar configuração do ciclo de vida do S3" .

Operação	Implementação
Política de exclusão de balde	Exclui a política anexada ao bucket.
DeleteBucketReplication	Exclui a configuração de replicação anexada ao bucket.
ExcluirBucketTagging	Usa o <code>tagging</code> sub-recurso para remover todas as tags de um bucket. Cuidado: Se uma tag de política ILM não padrão for definida para este bucket, haverá um <code>NTAP-SG-ILM-BUCKET-TAG</code> tag de bucket com um valor atribuído a ela. Não emita uma solicitação <code>DeleteBucketTagging</code> se houver um <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de balde. Em vez disso, emita uma solicitação <code>PutBucketTagging</code> apenas com o <code>NTAP-SG-ILM-BUCKET-TAG</code> tag e seu valor atribuído para remover todas as outras tags do bucket. Não modifique ou remova o <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de balde.
ObterBucketAcl	Retorna uma resposta positiva e o ID, DisplayName e Permissão do proprietário do bucket, indicando que o proprietário tem acesso total ao bucket.
ObterBucketCors	Retorna o <code>cors</code> configuração para o bucket.
Obter criptografia do Bucket	Retorna a configuração de criptografia padrão para o bucket.
Obter configuração do ciclo de vida do Bucket (anteriormente chamado de ciclo de vida do GET Bucket)	Retorna a configuração do ciclo de vida do bucket. Ver " Criar configuração do ciclo de vida do S3 ".
ObterBucketLocation	Retorna a região que foi definida usando o <code>LocationConstraint</code> elemento na solicitação <code>CreateBucket</code> . Se a região do balde for <code>us-east-1</code> , uma string vazia é retornada para a região.
Obter configuração de notificação de bucket (anteriormente chamado de notificação GET Bucket)	Retorna a configuração de notificação anexada ao bucket.
ObterBucketPolicy	Retorna a política anexada ao bucket.
Obter replicação do Bucket	Retorna a configuração de replicação anexada ao bucket.

Operação	Implementação
Obter marcação de balde	Usa o <code>tagging</code> sub-recurso para retornar todas as tags de um bucket. Cuidado: Se uma tag de política ILM não padrão for definida para este bucket, haverá um <code>NTAP-SG-ILM-BUCKET-TAG</code> tag de bucket com um valor atribuído a ela. Não modifique ou remova esta tag.
ObterVersionamento doBucket	Esta implementação utiliza o <code>versioning</code> sub-recurso para retornar o estado de controle de versão de um bucket. • <i>blank</i>: O controle de versão nunca foi habilitado (o bucket é "Sem versão") • Habilitado: o controle de versão está habilitado • Suspenso: o controle de versão foi habilitado anteriormente e está suspenso
ObterConfiguraçãoObject Lock	Retorna o modo de retenção padrão do bucket e o período de retenção padrão, se configurado. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3".
Balde de cabeça	Determina se um bucket existe e se você tem permissão para acessá-lo. Esta operação retorna: • <code>x-ntap-sg-bucket-id</code>: O UUID do bucket no formato UUID. • <code>x-ntap-sg-trace-id</code>: O ID de rastreamento exclusivo da solicitação associada.
ListObjects e ListObjectsV2 (anteriormente chamado de GET Bucket)	Retorna alguns ou todos (até 1.000) objetos em um bucket. A classe de armazenamento para objetos pode ter um dos dois valores, mesmo que o objeto tenha sido ingerido com o <code>REDUCED_REDUNDANCY</code> opção de classe de armazenamento: • <code>STANDARD</code>, que indica que o objeto está armazenado em um pool de armazenamento composto por nós de armazenamento. • <code>GLACIER</code>, que indica que o objeto foi movido para o bucket externo especificado pelo Cloud Storage Pool. Se o bucket contiver um grande número de chaves excluídas com o mesmo prefixo, a resposta poderá incluir algumas <code>CommonPrefixes</code> que não contêm chaves.
Versões do objeto de lista (anteriormente chamadas de versões do objeto GET Bucket)	Com acesso <code>READ</code> em um bucket, usando esta operação com o <code>versions</code> subresource lista metadados de todas as versões de objetos no bucket.

Operação	Implementação
ColoqueBucketCors	Define a configuração CORS para um bucket para que o bucket possa atender a solicitações de origem cruzada. O compartilhamento de recursos entre origens (CORS) é um mecanismo de segurança que permite que aplicativos web clientes em um domínio acessem recursos em um domínio diferente. Por exemplo, suponha que você use um bucket S3 chamado <code>images</code> para armazenar gráficos. Ao definir a configuração CORS para o <code>images</code> bucket, você pode permitir que as imagens nesse bucket sejam exibidas no site <code>http://www.example.com</code> .
PutBucketEncryption	Define o estado de criptografia padrão de um bucket existente. Quando a criptografia em nível de bucket está habilitada, todos os novos objetos adicionados ao bucket são criptografados. O StorageGRID oferece suporte à criptografia do lado do servidor com chaves gerenciadas StorageGRID. Ao especificar a regra de configuração de criptografia do lado do servidor, defina o <code>SSEAlgorithm</code> parâmetro para <code>AES256</code>, e não use o <code>KMSMasterKeyID</code> parâmetro. A configuração de criptografia padrão do bucket será ignorada se a solicitação de upload do objeto já especificar a criptografia (ou seja, se a solicitação incluir o <code>x-amz-server-side-encryption-*</code> cabeçalho da solicitação).
Configuração do ciclo de vida do PutBucket (anteriormente chamado de ciclo de vida do PUT Bucket)	Cria uma nova configuração de ciclo de vida para o bucket ou substitui uma configuração de ciclo de vida existente. O StorageGRID suporta até 1.000 regras de ciclo de vida em uma configuração de ciclo de vida. Cada regra pode incluir os seguintes elementos XML: • Expiração (Dias, Data, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtro (Prefixo, Tag) • Status • EU IA O StorageGRID não oferece suporte a estas ações: • AbortarIncompletoMultipartUpload • Transição Ver "Criar configuração do ciclo de vida do S3". Para entender como a ação Expiração em um ciclo de vida de bucket interage com as instruções de posicionamento do ILM, consulte "Como o ILM opera ao longo da vida de um objeto". Observação: a configuração do ciclo de vida do bucket pode ser usada com buckets que tenham o S3 Object Lock habilitado, mas a configuração do ciclo de vida do bucket não é suportada para buckets compatíveis legados.

Operação	Implementação
Configuração de notificação PutBucket (anteriormente chamado de notificação PUT Bucket)	Configura notificações para o bucket usando o XML de configuração de notificação incluído no corpo da solicitação. Você deve estar ciente dos seguintes detalhes de implementação: • O StorageGRID oferece suporte ao Amazon Simple Notification Service (Amazon SNS) ou a tópicos do Kafka como destinos. Os endpoints do Simple Queue Service (SQS) ou do Amazon Lambda não são suportados. • O destino das notificações deve ser especificado como o URN de um ponto de extremidade do StorageGRID . Os endpoints podem ser criados usando o Tenant Manager ou a Tenant Management API. O ponto de extremidade deve existir para que a configuração da notificação seja bem-sucedida. Se o ponto final não existir, um 400 Bad Request erro é retornado com o código <code>InvalidArgument</code> . • Não é possível configurar uma notificação para os seguintes tipos de eventos. Esses tipos de eventos não são suportados. ◦ <code>s3:ReducedRedundancyLostObject</code> ◦ <code>s3:ObjectRestore:Completed</code> • As notificações de eventos enviadas do StorageGRID usam o formato JSON padrão, exceto que elas não incluem algumas chaves e usam valores específicos para outras, conforme mostrado na lista a seguir: ◦ fonte do evento <pre>sgws:s3</pre> ◦ Região aws não incluído ◦ x-amz-id-2 não incluído ◦ arn <pre>urn:sgws:s3:::bucket_name</pre>
PutBucketPolicy	Define a política anexada ao bucket. Ver "Use políticas de acesso a buckets e grupos".

Operação	Implementação
PutBucketReplicação	Configura "Replicação do StorageGRID CloudMirror" para o bucket usando o XML de configuração de replicação fornecido no corpo da solicitação. Para replicação do CloudMirror, você deve estar ciente dos seguintes detalhes de implementação: • O StorageGRID suporta apenas a V1 da configuração de replicação. Isso significa que o StorageGRID não suporta o uso do <code>Filter</code> elemento para regras e segue as convenções V1 para exclusão de versões de objetos. Para mais detalhes, veja "Guia do usuário do Amazon Simple Storage Service: configuração de replicação". • A replicação de buckets pode ser configurada em buckets versionados ou não versionados. • Você pode especificar um bucket de destino diferente em cada regra do XML de configuração de replicação. Um bucket de origem pode ser replicado para mais de um bucket de destino. • Os buckets de destino devem ser especificados como o URN dos endpoints do StorageGRID, conforme especificado no Tenant Manager ou na Tenant Management API. Ver "Configurar a replicação do CloudMirror". O ponto de extremidade deve existir para que a configuração da replicação seja bem-sucedida. Se o ponto final não existir, a solicitação falhará como um 400 Bad Request. A mensagem de erro diz: Unable to save the replication policy. The specified endpoint URN does not exist: <i>URN</i>. • Você não precisa especificar um <code>Role</code> no XML de configuração. Este valor não é usado pelo StorageGRID e será ignorado se enviado. • Se você omitir a classe de armazenamento do XML de configuração, o StorageGRID usará o <code>STANDARD</code> classe de armazenamento por padrão. • Se você excluir um objeto do bucket de origem ou excluir o próprio bucket de origem, o comportamento de replicação entre regiões será o seguinte: ◦ Se você excluir o objeto ou bucket antes que ele seja replicado, o objeto/bucket não será replicado e você não será notificado. ◦ Se você excluir o objeto ou bucket após ele ter sido replicado, o StorageGRID seguirá o comportamento de exclusão padrão do Amazon S3 para a V1 da replicação entre regiões.

Operação	Implementação
Colocar marcação de balde	Usa o <code>tagging</code> sub-recurso para adicionar ou atualizar um conjunto de tags para um bucket. Ao adicionar tags de bucket, esteja ciente das seguintes limitações: • Tanto o StorageGRID quanto o Amazon S3 suportam até 50 tags para cada bucket. • As tags associadas a um bucket devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento. • Os valores das tags podem ter até 256 caracteres Unicode. • Chaves e valores diferenciam maiúsculas de minúsculas. Cuidado: Se uma tag de política ILM não padrão for definida para este bucket, haverá um <code>NTAP-SG-ILM-BUCKET-TAG</code> tag de bucket com um valor atribuído a ela. Certifique-se de que o <code>NTAP-SG-ILM-BUCKET-TAG</code> A tag bucket é incluída com o valor atribuído em todas as solicitações <code>PutBucketTagging</code>. Não modifique ou remova esta tag. Observação: esta operação substituirá quaisquer tags atuais que o bucket já tenha. Se alguma tag existente for omitida do conjunto, essas tags serão removidas do bucket.
Versão PutBucket	Usa o <code>versioning</code> sub-recurso para definir o estado de controle de versão de um bucket existente. Você pode definir o estado de controle de versão com um dos seguintes valores: • Habilitado: habilita o controle de versão para os objetos no bucket. Todos os objetos adicionados ao bucket recebem um ID de versão exclusivo. • Suspensão: desabilita o controle de versão dos objetos no bucket. Todos os objetos adicionados ao bucket recebem o ID da versão <code>null</code>.
PutObjectLockConfiguration	Configura ou remove o modo de retenção padrão do bucket e o período de retenção padrão. Se o período de retenção padrão for modificado, a data de retenção das versões de objetos existentes permanecerá a mesma e não será recalculada usando o novo período de retenção padrão. Ver "Use a API REST do S3 para configurar o bloqueio de objeto do S3" para informações detalhadas.

Operações em objetos

Operações em objetos

Esta seção descreve como o sistema StorageGRID implementa operações da API REST do S3 para objetos.

As seguintes condições se aplicam a todas as operações de objeto:

- StorageGRID "**valores de consistência**" são suportados por todas as operações em objetos, com exceção das seguintes:
 - ObterAclObjeto
 - OPTIONS /
 - ColocarObjetoLegalHold
 - ColocarRetençãoDeObjeto
 - SelecionarObjetoConteúdo
- Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.
- Todos os objetos em um bucket StorageGRID são de propriedade do proprietário do bucket, incluindo objetos criados por um usuário anônimo ou por outra conta.
- Objetos de dados ingeridos no sistema StorageGRID por meio do Swift não podem ser acessados pelo S3.

A tabela a seguir descreve como o StorageGRID implementa operações de objeto da API REST do S3.

Operação	Implementação
ExcluirObjeto	Autenticação multifator (MFA) e o cabeçalho de resposta <code>x-amz-mfa</code> não são suportados. Ao processar uma solicitação <code>DeleteObject</code>, o StorageGRID tenta remover imediatamente todas as cópias do objeto de todos os locais armazenados. Se bem-sucedido, o StorageGRID retornará uma resposta ao cliente imediatamente. Se todas as cópias não puderem ser removidas em 30 segundos (por exemplo, porque um local está temporariamente indisponível), o StorageGRID enfileira as cópias para remoção e então indica o sucesso ao cliente. Controle de versão Para remover uma versão específica, o solicitante deve ser o proprietário do bucket e usar o <code>versionId</code> sub-recurso. Usar este sub-recurso exclui permanentemente a versão. Se o <code>versionId</code> corresponde a um marcador de exclusão, o cabeçalho de resposta <code>x-amz-delete-marker</code> é retornado definido para <code>true</code>. • Se um objeto for excluído sem o <code>versionId</code> sub-recurso em um bucket com controle de versão habilitado, isso resulta na geração de um marcador de exclusão. O <code>versionId</code> para o marcador de exclusão é retornado usando o <code>x-amz-version-id</code> cabeçalho de resposta e o <code>x-amz-delete-marker</code> o cabeçalho de resposta é retornado definido como <code>true</code>. • Se um objeto for excluído sem o <code>versionId</code> sub-recurso em um bucket com controle de versão suspenso, isso resulta em uma exclusão permanente de uma versão 'nula' já existente ou de um marcador de exclusão 'nulo' e na geração de um novo marcador de exclusão 'nulo'. O <code>x-amz-delete-marker</code> o cabeçalho de resposta é retornado definido como <code>true</code>. Observação: Em certos casos, podem existir vários marcadores de exclusão para um objeto. Ver"Use a API REST do S3 para configurar o bloqueio de objeto do S3" para aprender como excluir versões de objetos no modo GOVERNANCE.
ExcluirObjetos (anteriormente chamado de DELETE Multiple Objects)	Autenticação multifator (MFA) e o cabeçalho de resposta <code>x-amz-mfa</code> não são suportados. Vários objetos podem ser excluídos na mesma mensagem de solicitação. Ver"Use a API REST do S3 para configurar o bloqueio de objeto do S3" para aprender como excluir versões de objetos no modo GOVERNANCE.

Operação	Implementação
ExcluirMarcaçãoDeObjeto	Usa o <code>tagging</code> sub-recurso para remover todas as tags de um objeto. Controle de versão Se o <code>versionId</code> se o parâmetro de consulta não for especificado na solicitação, a operação excluirá todas as tags da versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status "MethodNotAllowed" será retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.
ObterObjeto	"ObterObjeto"
ObterAclObjeto	Se as credenciais de acesso necessárias forem fornecidas para a conta, a operação retornará uma resposta positiva e o ID, o <code>DisplayName</code> e a Permissão do proprietário do objeto, indicando que o proprietário tem acesso total ao objeto.
ObterObjetoLegalHold	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"
ObterRetençãoDeObjeto	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"
Obter marcação de objeto	Usa o <code>tagging</code> sub-recurso para retornar todas as tags de um objeto. Controle de versão Se o <code>versionId</code> se o parâmetro de consulta não for especificado na solicitação, a operação retornará todas as tags da versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status "MethodNotAllowed" será retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.
CabeçaObjeto	"CabeçaObjeto"
RestaurarObjeto	"RestaurarObjeto"
ColocarObjeto	"ColocarObjeto"
CopiarObjeto (anteriormente chamado de Objeto PUT - Copiar)	"CopiarObjeto"
ColocarObjetoLegalHold	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"
ColocarRetençãoDeObjeto	"Use a API REST do S3 para configurar o bloqueio de objeto do S3"

Operação	Implementação
Colocar marcação de objeto	Usa o <code>tagging</code> sub-recurso para adicionar um conjunto de tags a um objeto existente. Limites de tags de objeto Você pode adicionar tags a novos objetos ao carregá-los ou adicioná-las a objetos existentes. Tanto o StorageGRID quanto o Amazon S3 suportam até 10 tags para cada objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento e os valores de tag podem ter até 256 caracteres Unicode de comprimento. Chaves e valores diferenciam maiúsculas de minúsculas. Atualizações de tags e comportamento de ingestão Quando você usa <code>PutObjectTagging</code> para atualizar as tags de um objeto, o StorageGRID não ingere novamente o objeto. Isso significa que a opção para Comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento do objeto que sejam acionadas pela atualização são feitas quando o ILM é reavaliado pelos processos normais de ILM em segundo plano. Isso significa que, se a regra ILM usar a opção Estrita para comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objetos necessários não puderem ser feitos (por exemplo, porque um local recém-necessário não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível. Resolução de conflitos Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação. Controle de versão Se o <code>versionId</code> o parâmetro de consulta não é especificado na solicitação, a operação adiciona tags à versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status <code>"MethodNotAllowed"</code> será retornado com o <code>x-amz-delete-marker</code> cabeçalho de resposta definido como <code>true</code>.
SelecionarObjetoConteúdo	"SelecionarObjetoConteúdo"

Use o S3 Select

O StorageGRID oferece suporte às seguintes cláusulas, tipos de dados e operadores do Amazon S3 Select para o ["Comando SelectObjectContent"](#).



Itens não listados não são suportados.

Para sintaxe, veja ["Selecionar Objeto Conteúdo"](#) . Para obter mais informações sobre o S3 Select, consulte o ["Documentação da AWS para S3 Select"](#) .

Somente contas de locatários que tenham o S3 Select habilitado podem emitir consultas SelectObjectContent. Veja o ["considerações e requisitos para usar o S3 Select"](#) .

Cláusulas

- Lista SELECIONAR
- cláusula FROM
- Cláusula WHERE
- Cláusula LIMIT

Tipos de dados

- bool
- inteiro
- corda
- flutuador
- decimal, numérico
- carimbo de data/hora

Operadores

Operadores lógicos

- E
- NÃO
- OU

Operadores de comparação

- <
- >
- <=
- >=
- =
- =
- <>
- !=
- ENTRE
- EM

Operadores de correspondência de padrões

- COMO
- _
- %

Operadores unitários

- É NULO
- NÃO É NULO

Operadores matemáticos

- +
- -
- *
- /
- %

O StorageGRID segue a precedência do operador Amazon S3 Select.

Funções agregadas

- MÉDIA()
- CONTAR(*)
- MÁXIMO()
- MÍNIMO()
- SOMA()

Funções condicionais

- CASO
- COALESCE
- NULLIF

Funções de conversão

- CAST (para tipo de dados suportado)

Funções de data

- DATA_ADICIONADA
- DATA_DIFF
- EXTRAIR
- PARA_STRING
- PARA_CARIMBO_DE_HORA

- UTCNOW

Funções de string

- COMPRIMENTO_CARACTERE, COMPRIMENTO_CARACTERE
- MAIS BAIXO
- SUBSTRING
- APARAR
- SUPERIOR

Use criptografia do lado do servidor

A criptografia do lado do servidor permite que você proteja os dados do seu objeto em repouso. O StorageGRID criptografa os dados enquanto grava o objeto e descriptografa os dados quando você acessa o objeto.

Se você quiser usar a criptografia do lado do servidor, poderá escolher uma das duas opções mutuamente exclusivas, com base em como as chaves de criptografia são gerenciadas:

- **SSE (criptografia do lado do servidor com chaves gerenciadas StorageGRID):** quando você emite uma solicitação S3 para armazenar um objeto, o StorageGRID criptografa o objeto com uma chave exclusiva. Quando você emite uma solicitação S3 para recuperar o objeto, o StorageGRID usa a chave armazenada para descriptografar o objeto.
- **SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente):** Quando você emite uma solicitação S3 para armazenar um objeto, você fornece sua própria chave de criptografia. Ao recuperar um objeto, você fornece a mesma chave de criptografia como parte de sua solicitação. Se as duas chaves de criptografia corresponderem, o objeto será descriptografado e os dados do objeto serão retornados.

Embora o StorageGRID gerencie todas as operações de criptografia e descriptografia de objetos, você deve gerenciar as chaves de criptografia fornecidas.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente.



Se um objeto for criptografado com SSE ou SSE-C, todas as configurações de criptografia em nível de bucket ou de grade serão ignoradas.

Usar SSE

Para criptografar um objeto com uma chave exclusiva gerenciada pelo StorageGRID, use o seguinte cabeçalho de solicitação:

```
x-amz-server-side-encryption
```

O cabeçalho de solicitação SSE é suportado pelas seguintes operações de objeto:

- "ColocarObjeto"
- "CopiarObjeto"

- ["CriarMultipartUpload"](#)

Usar SSE-C

Para criptografar um objeto com uma chave exclusiva que você gerencia, use três cabeçalhos de solicitação:

Cabeçalho da solicitação	Descrição
x-amz-server-side-encryption-customer-algorithm	Especifique o algoritmo de criptografia. O valor do cabeçalho deve ser AES256 .
x-amz-server-side-encryption-customer-key	Especifique a chave de criptografia que será usada para criptografar ou descriptografar o objeto. O valor da chave deve ser de 256 bits, codificado em base64.
x-amz-server-side-encryption-customer-key-MD5	Especifique o resumo MD5 da chave de criptografia de acordo com o RFC 1321, que é usado para garantir que a chave de criptografia foi transmitida sem erros. O valor do resumo MD5 deve ser codificado em base64 de 128 bits.

Os cabeçalhos de solicitação SSE-C são suportados pelas seguintes operações de objeto:

- ["ObterObjeto"](#)
- ["CabeçaObjeto"](#)
- ["ColocarObjeto"](#)
- ["CopiarObjeto"](#)
- ["CriarMultipartUpload"](#)
- ["UploadPart"](#)
- ["UploadPartCopy"](#)

Considerações sobre o uso de criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

Antes de usar o SSE-C, esteja ciente das seguintes considerações:

- Você deve usar https.



O StorageGRID rejeita quaisquer solicitações feitas via http ao usar SSE-C. Por questões de segurança, considere que qualquer chave enviada acidentalmente via http estará comprometida. Descarte a chave e gire conforme apropriado.

- O ETag na resposta não é o MD5 dos dados do objeto.
- Você deve gerenciar o mapeamento de chaves de criptografia para objetos. O StorageGRID não armazena chaves de criptografia. Você é responsável por rastrear a chave de criptografia fornecida para cada objeto.
- Se o seu bucket tiver controle de versão habilitado, cada versão do objeto deverá ter sua própria chave de criptografia. Você é responsável por rastrear a chave de criptografia usada para cada versão do objeto.

- Como você gerencia chaves de criptografia no lado do cliente, também deve gerenciar quaisquer proteções adicionais, como rotação de chaves, no lado do cliente.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente.

- Se a replicação entre grades ou a replicação do CloudMirror estiver configurada para o bucket, você não poderá ingerir objetos SSE-C. A operação de ingestão falhará.

Informações relacionadas

["Guia do usuário do Amazon S3: usando criptografia do lado do servidor com chaves fornecidas pelo cliente \(SSE-C\)"](#)

CopiarObjeto

Você pode usar a solicitação S3 CopyObject para criar uma cópia de um objeto que já está armazenado no S3. Uma operação CopyObject é o mesmo que executar GetObject seguido de PutObject.

Resolver conflitos

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

Tamanho do objeto

O tamanho máximo *recomendado* para uma única operação PutObject é 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use ["upload multiparte"](#) em vez de.

O tamanho máximo *compatível* para uma única operação PutObject é 5 TiB (5.497.558.138.880 bytes).



Se você atualizou do StorageGRID 11.6 ou anterior, o alerta de tamanho de objeto S3 PUT muito grande será acionado se você tentar carregar um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11.7 ou 11.8, o alerta não será acionado neste caso. No entanto, para se alinhar ao padrão AWS S3, versões futuras do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

Caracteres UTF-8 em metadados do usuário

Se uma solicitação incluir valores UTF-8 (sem escape) no nome da chave ou no valor dos metadados definidos pelo usuário, o comportamento do StorageGRID será indefinido.

O StorageGRID não analisa nem interpreta caracteres UTF-8 de escape incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Caracteres UTF-8 escapados são tratados como caracteres ASCII:

- As solicitações serão bem-sucedidas se os metadados definidos pelo usuário incluírem caracteres UTF-8 de escape.
- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome da chave ou valor incluir caracteres não imprimíveis.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- Content-Type
- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since
- x-amz-meta-, seguido por um par nome-valor contendo metadados definidos pelo usuário
- x-amz-metadata-directive: O valor padrão é COPY , que permite copiar o objeto e os metadados associados.

Você pode especificar REPLACE para substituir os metadados existentes ao copiar o objeto ou para atualizar os metadados do objeto.

- x-amz-storage-class
- x-amz-tagging-directive: O valor padrão é COPY , que permite copiar o objeto e todas as tags.

Você pode especificar REPLACE para substituir as tags existentes ao copiar o objeto ou para atualizar as tags.

- Cabeçalhos de solicitação de bloqueio de objeto S3:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular o modo de versão do objeto e reter até a data. Ver ["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#) .

- Cabeçalhos de solicitação SSE:

- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

Ver [Cabeçalhos de solicitação para criptografia do lado do servidor](#)

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm

Quando você copia um objeto, se o objeto de origem tiver uma soma de verificação, o StorageGRID não copia esse valor de soma de verificação para o novo objeto. Este comportamento se aplica independentemente de você tentar usar ou não `x-amz-checksum-algorithm` na solicitação do objeto.

- x-amz-website-redirect-location

Opções de classe de armazenamento

O `x-amz-storage-class` O cabeçalho de solicitação é suportado e afeta quantas cópias de objeto o StorageGRID cria se a regra ILM correspondente usa o Dual commit ou Balanced "opção de ingestão".

- STANDARD

(Padrão) Especifica uma operação de ingestão de confirmação dupla quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

- REDUCED_REDUNDANCY

Especifica uma operação de ingestão de confirmação única quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.



Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o REDUCED_REDUNDANCY a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o REDUCED_REDUNDANCY opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Usando x-amz-copy-source em CopyObject

Se o bucket de origem e a chave, especificados no `x-amz-copy-source` cabeçalho, são diferentes do bucket de destino e da chave, uma cópia dos dados do objeto de origem é gravada no destino.

Se a origem e o destino corresponderem, e o `x-amz-metadata-directive` cabeçalho é especificado como REPLACE, os metadados do objeto são atualizados com os valores de metadados fornecidos na solicitação. Nesse caso, o StorageGRID não ingere novamente o objeto. Isto tem duas consequências importantes:

- Você não pode usar CopyObject para criptografar um objeto existente no local ou para alterar a criptografia de um objeto existente no local. Se você fornecer o `x-amz-server-side-encryption` cabeçalho ou o `x-amz-server-side-encryption-customer-algorithm` cabeçalho, StorageGRID

rejeita a solicitação e retorna `XNotImplemented`.

- A opção para Comportamento de ingestão especificada na regra ILM correspondente não é usada. Quaisquer alterações no posicionamento do objeto que sejam acionadas pela atualização são feitas quando o ILM é reavaliado pelos processos normais de ILM em segundo plano.

Isso significa que, se a regra ILM usar a opção Estrita para comportamento de ingestão, nenhuma ação será tomada se os posicionamentos de objetos necessários não puderem ser feitos (por exemplo, porque um local recém-necessário não está disponível). O objeto atualizado mantém seu posicionamento atual até que o posicionamento necessário seja possível.

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você "[usar criptografia do lado do servidor](#)", os cabeçalhos de solicitação que você fornece dependem se o objeto de origem está criptografado e se você planeja criptografar o objeto de destino.

- Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deverá incluir os três cabeçalhos a seguir na solicitação `CopyObject` para que o objeto possa ser descriptografado e copiado:
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especifique `AES256`.
 - `x-amz-copy-source-server-side-encryption-customer-key`: Especifique a chave de criptografia que você forneceu quando criou o objeto de origem.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 que você forneceu quando criou o objeto de origem.
- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva que você fornece e gerencia, inclua os três cabeçalhos a seguir:
 - `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256`.
 - `x-amz-server-side-encryption-customer-key`: Especifique uma nova chave de criptografia para o objeto de destino.
 - `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da nova chave de criptografia.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para "[usando criptografia do lado do servidor](#)".

- Se você quiser criptografar o objeto de destino (a cópia) com uma chave exclusiva gerenciada pelo `StorageGRID` (SSE), inclua este cabeçalho na solicitação `CopyObject`:
 - `x-amz-server-side-encryption`



O `server-side-encryption` o valor do objeto não pode ser atualizado. Em vez disso, faça uma cópia com um novo `server-side-encryption` valor usando `x-amz-metadata-directive: REPLACE`.

Controle de versão

Se o bucket de origem for versionado, você pode usar o `x-amz-copy-source` cabeçalho para copiar a

versão mais recente de um objeto. Para copiar uma versão específica de um objeto, você deve especificar explicitamente a versão a ser copiada usando o `versionId` sub-recurso. Se o bucket de destino for versionado, a versão gerada será retornada no `x-amz-version-id` cabeçalho de resposta. Se o controle de versão for suspenso para o bucket de destino, então `x-amz-version-id` retorna um valor "nulo".

ObterObjeto

Você pode usar a solicitação S3 `GetObject` para recuperar um objeto de um bucket S3.

GetObject e objetos multipartes

Você pode usar o `partNumber` parâmetro de solicitação para recuperar uma parte específica de um objeto multiparte ou segmentado. O `x-amz-mp-parts-count` O elemento de resposta indica quantas partes o objeto possui.

Você pode definir `partNumber` para 1 para objetos segmentados/multipartes e objetos não segmentados/não multipartes; no entanto, o `x-amz-mp-parts-count` O elemento de resposta é retornado somente para objetos segmentados ou multipartes.

Caracteres UTF-8 em metadados do usuário

O StorageGRID não analisa nem interpreta caracteres UTF-8 de escape em metadados definidos pelo usuário. As solicitações GET para um objeto com caracteres UTF-8 de escape em metadados definidos pelo usuário não retornam o `x-amz-missing-meta` cabeçalho se o nome da chave ou valor incluir caracteres não imprimíveis.

Cabeçalho de solicitação suportado

O seguinte cabeçalho de solicitação é suportado:

- `x-amz-checksum-mode`: Especifique `ENABLED`

O Range cabeçalho não é suportado com `x-amz-checksum-mode` para `GetObject`. Quando você inclui Range no pedido com `x-amz-checksum-mode` habilitado, o StorageGRID não retorna um valor de soma de verificação na resposta.

Cabeçalho de solicitação não suportado

O seguinte cabeçalho de solicitação não é suportado e retorna `XNotImplemented`:

- `x-amz-website-redirect-location`

Controle de versão

Se um `versionId` sub-recurso não for especificado, a operação buscará a versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status "Não encontrado" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Cabeçalhos de solicitação para criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use todos os três cabeçalhos se o objeto estiver criptografado com uma chave exclusiva fornecida por você.

- `x-amz-server-side-encryption-customer-algorithm`: Especifique AES256 .
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do objeto.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em "[Use criptografia do lado do servidor](#)" .

Comportamento de GetObject para objetos do Cloud Storage Pool

Se um objeto foi armazenado em um "[Pool de armazenamento em nuvem](#)" , o comportamento de uma solicitação GetObject depende do estado do objeto. Ver "[CabeçaObjeto](#)" para mais detalhes.



Se um objeto estiver armazenado em um Cloud Storage Pool e uma ou mais cópias do objeto também existirem na grade, as solicitações GetObject tentarão recuperar dados da grade antes de recuperá-los do Cloud Storage Pool.

Estado do objeto	Comportamento de GetObject
Objeto ingerido no StorageGRID , mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de armazenamento tradicional ou usando codificação de eliminação	200 OK Uma cópia do objeto é recuperada.
Objeto no Cloud Storage Pool, mas ainda não transitado para um estado não recuperável	200 OK Uma cópia do objeto é recuperada.
Objeto transitado para um estado não recuperável	403 Forbidden , InvalidObjectState Use um " RestaurarObjeto " solicitação para restaurar o objeto a um estado recuperável.
Objeto em processo de restauração de um estado não recuperável	403 Forbidden , InvalidObjectState Aguarde a conclusão da solicitação RestoreObject.
Objeto totalmente restaurado no Cloud Storage Pool	200 OK Uma cópia do objeto é recuperada.

Objetos multipartes ou segmentados em um pool de armazenamento em nuvem

Se você carregou um objeto multiparte ou se o StorageGRID dividiu um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no Cloud Storage Pool por meio da amostragem de um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação GetObject pode retornar

incorretamente 200 OK quando algumas partes do objeto já foram transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não foram restauradas.

Nestes casos:

- A solicitação GetObject pode retornar alguns dados, mas parar no meio da transferência.
- Uma solicitação GetObject subsequente pode retornar 403 Forbidden .

GetObject e replicação entre grades

Se você estiver usando "federação de grade" e "replicação entre grades" estiver habilitado para um bucket, o cliente S3 poderá verificar o status de replicação de um objeto emitindo uma solicitação GetObject. 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.



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

CabeçaObjeto

Você pode usar a solicitação S3 HeadObject para recuperar metadados de um objeto sem retornar o próprio objeto. Se o objeto estiver armazenado em um Cloud Storage Pool, você poderá usar o HeadObject para determinar o estado de transição do objeto.

HeadObject e objetos multipartes

Você pode usar o partNumber parâmetro de solicitação para recuperar metadados para uma parte específica de um objeto multiparte ou segmentado. O x-amz-mp-parts-count O elemento de resposta indica quantas partes o objeto possui.

Você pode definir partNumber para 1 para objetos segmentados/multipartes e objetos não segmentados/não multipartes; no entanto, o x-amz-mp-parts-count O elemento de resposta é retornado somente para objetos segmentados ou multipartes.

Caracteres UTF-8 em metadados do usuário

O StorageGRID não analisa nem interpreta caracteres UTF-8 de escape em metadados definidos pelo usuário. As solicitações HEAD para um objeto com caracteres UTF-8 escapados em metadados definidos pelo usuário não retornam o x-amz-missing-meta cabeçalho se o nome da chave ou valor incluir caracteres não imprimíveis.

Cabeçalho de solicitação suportado

O seguinte cabeçalho de solicitação é suportado:

- `x-amz-checksum-mode`

O `partNumber` parâmetro e `Range` cabeçalho não é suportado com `x-amz-checksum-mode` para `HeadObject`. Quando você os inclui na solicitação com `x-amz-checksum-mode` habilitado, o `StorageGRID` não retorna um valor de soma de verificação na resposta.

Cabeçalho de solicitação não suportado

O seguinte cabeçalho de solicitação não é suportado e retorna `XNotImplemented`:

- `x-amz-website-redirect-location`

Controle de versão

Se um `versionId` sub-recurso não for especificado, a operação buscará a versão mais recente do objeto em um bucket versionado. Se a versão atual do objeto for um marcador de exclusão, um status "Não encontrado" será retornado com o `x-amz-delete-marker` cabeçalho de resposta definido como `true`.

Cabeçalhos de solicitação para criptografia do lado do servidor com chaves de criptografia fornecidas pelo cliente (SSE-C)

Use todos esses três cabeçalhos se o objeto estiver criptografado com uma chave exclusiva fornecida por você.

- `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do objeto.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em ["Use criptografia do lado do servidor"](#).

Respostas do HeadObject para objetos do Cloud Storage Pool

Se o objeto for armazenado em um ["Pool de armazenamento em nuvem"](#), os seguintes cabeçalhos de resposta são retornados:

- `x-amz-storage-class`: `GLACIER`
- `x-amz-restore`

Os cabeçalhos de resposta fornecem informações sobre o estado de um objeto à medida que ele é movido para um pool de armazenamento em nuvem, opcionalmente transferido para um estado não recuperável e restaurado.

Estado do objeto	Resposta ao HeadObject
Objeto ingerido no StorageGRID , mas ainda não avaliado pelo ILM, ou objeto armazenado em um pool de armazenamento tradicional ou usando codificação de eliminação	200 OK(Nenhum cabeçalho de resposta especial é retornado.)
Objeto no Cloud Storage Pool, mas ainda não transitado para um estado não recuperável	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" Até que o objeto seja transferido para um estado não recuperável, o valor para <code>expiry-date</code> está definido para um tempo distante no futuro. O tempo exato da transição não é controlado pelo sistema StorageGRID .
O objeto passou para um estado não recuperável, mas pelo menos uma cópia também existe na grade	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" O valor para <code>expiry-date</code> está definido para um tempo distante no futuro. Observação: Se a cópia na grade não estiver disponível (por exemplo, um nó de armazenamento estiver inativo), você deverá emitir uma "RestaurarObjeto" solicite a restauração da cópia do Cloud Storage Pool antes de poder recuperar o objeto com sucesso.
O objeto passou para um estado não recuperável e não há nenhuma cópia na grade	200 OK x-amz-storage-class: GLACIER
Objeto em processo de restauração de um estado não recuperável	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"

Estado do objeto	Resposta ao HeadObject
Objeto totalmente restaurado no Cloud Storage Pool	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 2018 00:00:00 GMT" O expiry-date indica quando o objeto no Cloud Storage Pool será retornado a um estado não recuperável.

Objetos multipartes ou segmentados no Cloud Storage Pool

Se você carregou um objeto multiparte ou se o StorageGRID dividiu um objeto grande em segmentos, o StorageGRID determina se o objeto está disponível no Cloud Storage Pool por meio da amostragem de um subconjunto das partes ou segmentos do objeto. Em alguns casos, uma solicitação HeadObject pode retornar incorretamente `x-amz-restore: ongoing-request="false"` quando algumas partes do objeto já foram transferidas para um estado não recuperável ou quando algumas partes do objeto ainda não foram restauradas.

HeadObject e replicação entre grades

Se você estiver usando "[federação de grade](#)" e "[replicação entre grades](#)" estiver habilitado para um bucket, o cliente S3 poderá verificar o status de replicação de um objeto emitindo uma solicitação HeadObject. 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.



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

Colocar Objeto

Você pode usar a solicitação PutObject do S3 para adicionar um objeto a um bucket.

Resolver conflitos

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma

operação.

Tamanho do objeto

O tamanho máximo *recomendado* para uma única operação PutObject é 5 GiB (5.368.709.120 bytes). Se você tiver objetos maiores que 5 GiB, use ["upload multiparte"](#) em vez de.

O tamanho máximo *compatível* para uma única operação PutObject é 5 TiB (5.497.558.138.880 bytes).



Se você atualizou do StorageGRID 11.6 ou anterior, o alerta de tamanho de objeto S3 PUT muito grande será acionado se você tentar carregar um objeto que exceda 5 GiB. Se você tiver uma nova instalação do StorageGRID 11.7 ou 11.8, o alerta não será acionado neste caso. No entanto, para se alinhar ao padrão AWS S3, versões futuras do StorageGRID não suportarão uploads de objetos maiores que 5 GiB.

Tamanho dos metadados do usuário

O Amazon S3 limita o tamanho dos metadados definidos pelo usuário em cada cabeçalho de solicitação PUT a 2 KB. O StorageGRID limita os metadados do usuário a 24 KiB. O tamanho dos metadados definidos pelo usuário é medido pela soma do número de bytes na codificação UTF-8 de cada chave e valor.

Caracteres UTF-8 em metadados do usuário

Se uma solicitação incluir valores UTF-8 (sem escape) no nome da chave ou no valor dos metadados definidos pelo usuário, o comportamento do StorageGRID será indefinido.

O StorageGRID não analisa nem interpreta caracteres UTF-8 de escape incluídos no nome da chave ou no valor dos metadados definidos pelo usuário. Caracteres UTF-8 escapados são tratados como caracteres ASCII:

- As solicitações PutObject, CopyObject, GetObject e HeadObject serão bem-sucedidas se os metadados definidos pelo usuário incluírem caracteres UTF-8 de escape.
- O StorageGRID não retorna o `x-amz-missing-meta` cabeçalho se o valor interpretado do nome da chave ou valor incluir caracteres não imprimíveis.

Limites de tags de objeto

Você pode adicionar tags a novos objetos ao carregá-los ou adicioná-las a objetos existentes. Tanto o StorageGRID quanto o Amazon S3 suportam até 10 tags para cada objeto. As tags associadas a um objeto devem ter chaves de tag exclusivas. Uma chave de tag pode ter até 128 caracteres Unicode de comprimento e os valores de tag podem ter até 256 caracteres Unicode de comprimento. Chaves e valores diferenciam maiúsculas de minúsculas.

Propriedade do objeto

No StorageGRID, todos os objetos são de propriedade da conta do proprietário do bucket, incluindo objetos criados por uma conta não proprietária ou um usuário anônimo.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- Cache-Control

- Content-Disposition
- Content-Encoding

Quando você especifica `aws-chunked` para `Content-Encoding` O StorageGRID não verifica os seguintes itens:

- O StorageGRID não verifica o `chunk-signature` contra os dados do bloco.
- O StorageGRID não verifica o valor que você fornece para `x-amz-decoded-content-length` contra o objeto.
- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

A codificação de transferência em blocos é suportada se `aws-chunked` a assinatura de carga útil também é usada.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguido por um par nome-valor contendo metadados definidos pelo usuário.

Ao especificar o par nome-valor para metadados definidos pelo usuário, use este formato geral:

```
x-amz-meta-name: value
```

Se você quiser usar a opção **Tempo de criação definido pelo usuário** como o Tempo de referência para uma regra ILM, você deve usar `creation-time` como o nome dos metadados que registram quando o objeto foi criado. Por exemplo:

```
x-amz-meta-creation-time: 1443399726
```

O valor para `creation-time` é avaliado como segundos desde 1º de janeiro de 1970.



Uma regra de ILM não pode usar um **horário de criação definido pelo usuário** para o horário de referência e a opção de ingestão balanceada ou restrita. Um erro é retornado quando a regra ILM é criada.

- `x-amz-tagging`
- Cabeçalhos de solicitação de bloqueio de objeto S3
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`

- `x-amz-object-lock-legal-hold`

Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular o modo de versão do objeto e reter até a data. Ver ["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#).

- Cabeçalhos de solicitação SSE:

- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

Ver [Cabeçalhos de solicitação para criptografia do lado do servidor](#)

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

O `x-amz-website-redirect-location` retornos de cabeçalho `XNotImplemented`.

Opções de classe de armazenamento

O `x-amz-storage-class` O cabeçalho da solicitação é suportado. O valor submetido para `x-amz-storage-class` afeta como o StorageGRID protege os dados do objeto durante a ingestão e não quantas cópias persistentes do objeto são armazenadas no sistema StorageGRID (o que é determinado pelo ILM).

Se a regra ILM correspondente a um objeto ingerido usar a opção de ingestão estrita, o `x-amz-storage-class` cabeçalho não tem efeito.

Os seguintes valores podem ser usados para `x-amz-storage-class`:

- STANDARD(Padrão)
 - **Confirmação dupla:** se a regra do ILM especificar a opção Confirmação dupla para o comportamento de ingestão, assim que um objeto for ingerido, uma segunda cópia desse objeto será criada e distribuída para um nó de armazenamento diferente (confirmação dupla). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais atendem às instruções de posicionamento na regra. Caso contrário, talvez seja necessário fazer novas cópias de objetos em locais diferentes e as cópias provisórias iniciais talvez precisem ser excluídas.
 - **Balanceado:** Se a regra do ILM especificar a opção Balanceado e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes Nós de Armazenamento.

Se o StorageGRID puder criar imediatamente todas as cópias de objetos especificadas na regra ILM

(posicionamento síncrono), o `x-amz-storage-class` cabeçalho não tem efeito.

- `REDUCED_REDUNDANCY`
 - **Confirmação dupla:** se a regra do ILM especificar a opção Confirmação dupla para o comportamento de ingestão, o StorageGRID criará uma única cópia provisória à medida que o objeto for ingerido (confirmação única).
 - **Balanceado:** Se a regra ILM especificar a opção Balanceado, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito. O `REDUCED_REDUNDANCY` A opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso usando `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia extra do objeto para cada operação de ingestão.

Usando o `REDUCED_REDUNDANCY` opção não é recomendada em outras circunstâncias.

`REDUCED_REDUNDANCY` aumenta o risco de perda de dados do objeto durante a ingestão. Por exemplo, você pode perder dados se a cópia única for armazenada inicialmente em um nó de armazenamento que falhe antes que a avaliação do ILM possa ocorrer.



Ter 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.

Especificando `REDUCED_REDUNDANCY` afeta apenas quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Isso não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas de ILM ativas e não resulta no armazenamento de dados em níveis mais baixos de redundância no sistema StorageGRID .



Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Cabeçalhos de solicitação para criptografia do lado do servidor

Você pode usar os seguintes cabeçalhos de solicitação para criptografar um objeto com criptografia do lado do servidor. As opções SSE e SSE-C são mutuamente exclusivas.

- **SSE:** Use o cabeçalho a seguir se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID.

- `x-amz-server-side-encryption`

Quando o `x-amz-server-side-encryption` o cabeçalho não está incluído na solicitação `PutObject`, a grade inteira "[configuração de criptografia de objeto armazenado](#)" é omitido da resposta `PutObject`.

- **SSE-C:** Use todos esses três cabeçalhos se quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.

- `x-amz-server-side-encryption-customer-algorithm`: Especifique AES256 .
- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para ["usando criptografia do lado do servidor"](#) .



Se um objeto for criptografado com SSE ou SSE-C, todas as configurações de criptografia em nível de bucket ou de grade serão ignoradas.

Controle de versão

Se o controle de versão estiver habilitado para um bucket, um único `versionId` é gerado automaticamente para a versão do objeto que está sendo armazenado. Esse `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho de resposta.

Se o controle de versão for suspenso, a versão do objeto será armazenada com um valor nulo `versionId` e se uma versão nula já existir, ela será substituída.

Cálculos de assinatura para o cabeçalho de autorização

Ao usar o `Authorization` cabeçalho para autenticar solicitações, o StorageGRID difere do AWS nas seguintes maneiras:

- StorageGRID não requer `host` cabeçalhos a serem incluídos dentro `CanonicalHeaders` .
- StorageGRID não requer `Content-Type` para ser incluído dentro `CanonicalHeaders` .
- StorageGRID não requer `x-amz-*` cabeçalhos a serem incluídos dentro `CanonicalHeaders` .



Como prática recomendada geral, sempre inclua esses cabeçalhos dentro `CanonicalHeaders` para garantir que eles sejam verificados; no entanto, se você excluir esses cabeçalhos, o StorageGRID não retornará um erro.

Para mais detalhes, consulte ["Cálculos de assinatura para o cabeçalho de autorização: transferindo carga útil em um único bloco \(AWS Signature versão 4\)"](#) .

Informações relacionadas

- ["Gerenciar objetos com ILM"](#)
- ["Referência da API do Amazon Simple Storage Service: PutObject"](#)

RestaurarObjeto

Você pode usar a solicitação S3 `RestoreObject` para restaurar um objeto armazenado em um pool de armazenamento em nuvem.

Tipo de solicitação suportado

O StorageGRID suporta apenas solicitações `RestoreObject` para restaurar um objeto. Não suporta o `SELECT` tipo de restauração. Selecione solicitações de retorno `XNotImplemented`.

Controle de versão

Opcionalmente, especifique `versionId` para restaurar uma versão específica de um objeto em um bucket versionado. Se você não especificar `versionId`, a versão mais recente do objeto é restaurada.

Comportamento de `RestoreObject` em objetos do Cloud Storage Pool

Se um objeto foi armazenado em um ["Pool de armazenamento em nuvem"](#), uma solicitação `RestoreObject` tem o seguinte comportamento, com base no estado do objeto. Ver ["CabeçaObjeto"](#) para mais detalhes.



Se um objeto estiver armazenado em um Cloud Storage Pool e uma ou mais cópias do objeto também existirem na grade, não haverá necessidade de restaurar o objeto emitindo uma solicitação `RestoreObject`. Em vez disso, a cópia local pode ser recuperada diretamente, usando uma solicitação `GetObject`.

Estado do objeto	Comportamento de <code>RestoreObject</code>
Objeto ingerido no StorageGRID, mas ainda não avaliado pelo ILM, ou o objeto não está em um pool de armazenamento em nuvem	<code>403 Forbidden, InvalidObjectState</code>
Objeto no Cloud Storage Pool, mas ainda não transitado para um estado não recuperável	<code>`200 OK`</code> Nenhuma alteração é feita. Nota: Antes que um objeto seja transferido para um estado não recuperável, você não pode alterar sua <code>expiry-date</code> .
Objeto transitado para um estado não recuperável	<code>`202 Accepted`</code> Restaura uma cópia recuperável do objeto para o Cloud Storage Pool pelo número de dias especificado no corpo da solicitação. No final desse período, o objeto é devolvido a um estado não recuperável. Opcionalmente, use o <code>Tier</code> elemento de solicitação para determinar quanto tempo o trabalho de restauração levará para terminar(<code>Expedited</code> , <code>Standard</code> , ou <code>Bulk</code>). Se você não especificar <code>Tier</code> , o <code>Standard</code> camada é usada. Importante: Se um objeto tiver sido transferido para o S3 Glacier Deep Archive ou o Cloud Storage Pool usar o armazenamento de Blobs do Azure, você não poderá restaurá-lo usando o <code>Expedited</code> nível. O seguinte erro é retornado <code>403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class</code> .

Estado do objeto	Comportamento de RestoreObject
Objeto em processo de restauração de um estado não recuperável	409 Conflict , RestoreAlreadyInProgress
Objeto totalmente restaurado no Cloud Storage Pool	200 OK Observação: Se um objeto foi restaurado para um estado recuperável, você pode alterá-lo <code>expiry-date</code> reemitindo a solicitação <code>RestoreObject</code> com um novo valor para <code>Days</code> . A data de restauração é atualizada em relação ao horário da solicitação.

SelecionarObjetoConteúdo

Você pode usar a solicitação `SelectObjectContent` do S3 para filtrar o conteúdo de um objeto do S3 com base em uma instrução SQL simples.

Para mais informações, consulte ["Referência da API do Amazon Simple Storage Service: SelectObjectContent"](#) .

Antes de começar

- A conta do locatário tem a permissão S3 Select.
- Você tem `s3:GetObject` permissão para o objeto que você deseja consultar.
- 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.
- Sua expressão SQL tem um comprimento máximo de 256 KB.
- Qualquer registro na entrada ou nos resultados tem um comprimento máximo de 1 MiB.

Exemplo de sintaxe de solicitação CSV


```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

Exemplo de sintaxe de solicitação Parquet

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

Exemplo de consulta SQL

Esta consulta obtém o nome do estado, as populações de 2010, as populações estimadas de 2015 e a porcentagem de alteração dos dados do censo dos EUA. Registros no arquivo que não são estados são ignorados.

```

SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME

```

As primeiras linhas do arquivo a ser consultado, SUB-EST2020_ALL.csv , fica assim:

```
SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040, 01, 000, 00000, 00000, 00000, 0, A, Alabama, Alabama, 4779736, 4780118, 4785514, 4
799642, 4816632, 4831586,
4843737, 4854803, 4866824, 4877989, 4891628, 4907965, 4920706, 4921532
162, 01, 000, 00124, 00000, 00000, 0, A, Abbeville
city, Alabama, 2688, 2705, 2699, 2694, 2645, 2629, 2610, 2602,
2587, 2578, 2565, 2555, 2555, 2553
162, 01, 000, 00460, 00000, 00000, 0, A, Adamsville
city, Alabama, 4522, 4487, 4481, 4474, 4453, 4430, 4399, 4371,
4335, 4304, 4285, 4254, 4224, 4211
162, 01, 000, 00484, 00000, 00000, 0, A, Addison
town, Alabama, 758, 754, 751, 750, 745, 744, 742, 734, 734, 728,
725, 723, 719, 717
```

Exemplo de uso do AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

As primeiras linhas do arquivo de saída, changes.csv, fica assim:

```
Alabama, 4779736, 4854803, 1.5705260708959658022953568983726297854
Alaska, 710231, 738430, 3.9703983633493891424057806544631253775
Arizona, 6392017, 6832810, 6.8959922978928247531256565807005832431
Arkansas, 2915918, 2979732, 2.1884703204959810255295244928012378949
California, 37253956, 38904296, 4.4299724839960620557988526104449148971
Colorado, 5029196, 5454328, 8.4532796097030221132761578590295546246
```

Exemplo de uso do AWS-CLI (Parquet)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV":{}}' changes.csv
```

As primeiras linhas do arquivo de saída, changes.csv, se parecem com isto:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operações para uploads multipartes

Operações para uploads multipartes

Esta seção descreve como o StorageGRID oferece suporte a operações para uploads multipartes.

As seguintes condições e notas se aplicam a todas as operações de upload multipartes:

- Você não deve exceder 1.000 uploads multipartes simultâneos para um único bucket porque os resultados das consultas ListMultipartUploads para esse bucket podem retornar resultados incompletos.
- O StorageGRID impõe limites de tamanho da AWS para partes multipartes. Os clientes do S3 devem seguir estas diretrizes:
 - Cada parte em um upload multiparte deve ter entre 5 MiB (5.242.880 bytes) e 5 GiB (5.368.709.120 bytes).
 - A última parte pode ser menor que 5 MiB (5.242.880 bytes).
 - Em geral, os tamanhos das peças devem ser os maiores possíveis. Por exemplo, use tamanhos de peça de 5 GiB para um objeto de 100 GiB. Como cada parte é considerada um objeto único, o uso de tamanhos de parte grandes reduz a sobrecarga de metadados do StorageGRID .
 - Para objetos menores que 5 GiB, considere usar o upload não multiparte.
- O ILM é avaliado para cada parte de um objeto multiparte à medida que é ingerido e para o objeto como um todo quando o upload multiparte é concluído, se a regra ILM usar o Balanceado ou o Estrito ["opção de ingestão"](#) . Você deve estar ciente de como isso afeta o posicionamento de objetos e peças:
 - Se o ILM for alterado enquanto um upload multiparte do S3 estiver em andamento, algumas partes do objeto poderão não atender aos requisitos atuais do ILM quando o upload multiparte for concluído. Qualquer peça que não seja colocada corretamente é colocada na fila para reavaliação do ILM e

movida para o local correto posteriormente.

- Ao avaliar o ILM para uma peça, o StorageGRID filtra o tamanho da peça, não o 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, cada parte de 1 GB de um upload multiparte de 10 partes será armazenada no DC2 na ingestão. Entretanto, quando o ILM é avaliado para o objeto como um todo, todas as partes do objeto são movidas para DC1.
- Todas as operações de upload multipartes oferecem suporte ao StorageGRID ["valores de consistência"](#).
- Quando um objeto é ingerido usando upload multipartes, o ["limite de segmentação de objetos \(1 GiB\)"](#) não é aplicado.
- Conforme necessário, você pode usar ["criptografia do lado do servidor"](#) com uploads multipartes. Para usar SSE (criptografia do lado do servidor com chaves gerenciadas StorageGRID), você inclui o `x-amz-server-side-encryption` cabeçalho de solicitação somente na solicitação `CreateMultipartUpload`. Para usar SSE-C (criptografia do lado do servidor com chaves fornecidas pelo cliente), especifique os mesmos três cabeçalhos de solicitação de chave de criptografia na solicitação `CreateMultipartUpload` e em cada solicitação `UploadPart` subsequente.

Operação	Implementação
<code>AbortMultipartUpload</code>	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
Upload completo de várias partes	Ver "Upload completo de várias partes"
<code>CriarMultipartUpload</code> (anteriormente chamado de Iniciar Upload Multipartes)	Ver "CriarMultipartUpload"
<code>ListarMultipartUploads</code>	Ver "ListarMultipartUploads"
<code>ListarPartes</code>	Implementado com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.
<code>UploadPart</code>	Ver "UploadPart"
<code>UploadPartCopy</code>	Ver "UploadPartCopy"

Upload completo de várias partes

A operação `CompleteMultipartUpload` conclui um upload multiparte de um objeto reunindo as partes carregadas anteriormente.



O StorageGRID suporta valores não consecutivos em ordem crescente para `partNumber` parâmetro de solicitação com `CompleteMultipartUpload`. O parâmetro pode começar com qualquer valor.

Resolver conflitos

Solicitações de clientes conflitantes, como dois clientes gravando na mesma chave, são resolvidas com base no princípio de "últimos ganhos". O tempo para a avaliação de "últimas vitórias" é baseado em quando o sistema StorageGRID conclui uma determinada solicitação, e não em quando os clientes S3 iniciam uma operação.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

O `x-amz-storage-class` cabeçalho afeta quantas cópias de objeto o StorageGRID cria se a regra ILM correspondente especificar o "[Opção de confirmação dupla ou ingestão balanceada](#)".

- STANDARD

(Padrão) Especifica uma operação de ingestão de confirmação dupla quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.

- REDUCED_REDUNDANCY

Especifica uma operação de ingestão de confirmação única quando a regra ILM usa a opção Confirmação dupla ou quando a opção Balanceada retorna para a criação de cópias provisórias.



Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o REDUCED_REDUNDANCY a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o REDUCED_REDUNDANCY opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.



Se um upload multipart não for concluído em 15 dias, a operação será marcada como inativa e todos os dados associados serão excluídos do sistema.



O ETag o valor retornado não é uma soma MD5 dos dados, mas segue a implementação da API do Amazon S3 ETag valor para objetos multipartes.

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controle de versão

Esta operação conclui um upload multipart. Se o controle de versão estiver habilitado para um bucket, a versão do objeto será criada após a conclusão do upload multipart.

Se o controle de versão estiver habilitado para um bucket, um único `versionId` é gerado automaticamente para a versão do objeto que está sendo armazenado. Esse `versionId` também é retornado na resposta usando o `x-amz-version-id` cabeçalho de resposta.

Se o controle de versão for suspenso, a versão do objeto será armazenada com um valor nulo `versionId` e se uma versão nula já existir, ela será substituída.



Quando o controle de versão está habilitado para um bucket, a conclusão de um upload multipart sempre cria uma nova versão, mesmo que haja uploads multipart simultâneos concluídos na mesma chave de objeto. Quando o controle de versão não está habilitado para um bucket, é possível iniciar um upload multipart e, em seguida, fazer com que outro upload multipart seja iniciado e concluído primeiro na mesma chave de objeto. Em buckets não versionados, o upload multipart concluído por último tem precedência.

Falha na replicação, notificação ou notificação de metadados

Se o bucket onde o upload multipart ocorre estiver configurado para um serviço de plataforma, o upload multipart será bem-sucedido mesmo se a ação de replicação ou notificação associada falhar.

Um locatário pode acionar a replicação com falha ou a notificação atualizando os metadados ou as tags do objeto. Um locatário pode reenviar os valores existentes para evitar fazer alterações indesejadas.

Consulte "[Solucionar problemas de serviços de plataforma](#)".

CriarMultipartUpload

A operação `CreateMultipartUpload` (anteriormente chamada de `Initiate Multipart Upload`) inicia um upload multipart para um objeto e retorna um ID de upload.

O `x-amz-storage-class` O cabeçalho da solicitação é suportado. O valor submetido para `x-amz-storage-class` afeta como o StorageGRID protege os dados do objeto durante a ingestão e não quantas cópias persistentes do objeto são armazenadas no sistema StorageGRID (o que é determinado pelo ILM).

Se a regra ILM correspondente a um objeto ingerido usar o Strict"[opção de ingestão](#)", o `x-amz-storage-class` cabeçalho não tem efeito.

Os seguintes valores podem ser usados para `x-amz-storage-class`:

- **STANDARD(Padrão)**
 - **Confirmação dupla:** se a regra do ILM especificar a opção de ingestão de confirmação dupla, assim que um objeto for ingerido, uma segunda cópia desse objeto será criada e distribuída para um nó de armazenamento diferente (confirmação dupla). Quando o ILM é avaliado, o StorageGRID determina se essas cópias provisórias iniciais atendem às instruções de posicionamento na regra. Caso contrário, talvez seja necessário fazer novas cópias de objetos em locais diferentes e as cópias provisórias iniciais talvez precisem ser excluídas.
 - **Balanceado:** Se a regra do ILM especificar a opção Balanceado e o StorageGRID não puder fazer imediatamente todas as cópias especificadas na regra, o StorageGRID fará duas cópias provisórias em diferentes Nós de Armazenamento.

Se o StorageGRID puder criar imediatamente todas as cópias de objetos especificadas na regra ILM (posicionamento síncrono), o `x-amz-storage-class` cabeçalho não tem efeito.

- `REDUCED_REDUNDANCY`

- **Confirmação dupla:** se a regra do ILM especificar a opção Confirmação dupla, o StorageGRID criará uma única cópia provisória à medida que o objeto for ingerido (confirmação única).
- **Balanceado:** Se a regra ILM especificar a opção Balanceado, o StorageGRID fará uma única cópia provisória somente se o sistema não puder fazer imediatamente todas as cópias especificadas na regra. Se o StorageGRID puder executar o posicionamento síncrono, este cabeçalho não terá efeito. O `REDUCED_REDUNDANCY` A opção é melhor usada quando a regra ILM que corresponde ao objeto cria uma única cópia replicada. Neste caso usando `REDUCED_REDUNDANCY` elimina a criação e exclusão desnecessárias de uma cópia extra do objeto para cada operação de ingestão.

Usando o `REDUCED_REDUNDANCY` opção não é recomendada em outras circunstâncias.

`REDUCED_REDUNDANCY` aumenta o risco de perda de dados do objeto durante a ingestão. Por exemplo, você pode perder dados se a cópia única for armazenada inicialmente em um nó de armazenamento que falhe antes que a avaliação do ILM possa ocorrer.



Ter 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.

Especificando `REDUCED_REDUNDANCY` afeta apenas quantas cópias são criadas quando um objeto é ingerido pela primeira vez. Isso não afeta quantas cópias do objeto são feitas quando o objeto é avaliado pelas políticas de ILM ativas e não resulta no armazenamento de dados em níveis mais baixos de redundância no sistema StorageGRID .



Se você estiver ingerindo um objeto em um bucket com o S3 Object Lock habilitado, o `REDUCED_REDUNDANCY` a opção é ignorada. Se você estiver ingerindo um objeto em um bucket compatível legado, o `REDUCED_REDUNDANCY` opção retorna um erro. O StorageGRID sempre executará uma ingestão de confirmação dupla para garantir que os requisitos de conformidade sejam atendidos.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `Content-Type`
- `x-amz-checksum-algorithm`

Atualmente, apenas o valor `SHA256` para `x-amz-checksum-algorithm` é suportado.

- `x-amz-meta-`, seguido por um par nome-valor contendo metadados definidos pelo usuário

Ao especificar o par nome-valor para metadados definidos pelo usuário, use este formato geral:

```
x-amz-meta-_name_: `value`
```

Se você quiser usar a opção **Tempo de criação definido pelo usuário** como o Tempo de referência para uma regra ILM, você deve usar `creation-time` como o nome dos metadados que registram quando o

objeto foi criado. Por exemplo:

```
x-amz-meta-creation-time: 1443399726
```

O valor para `creation-time` é avaliado como segundos desde 1º de janeiro de 1970.



Adicionando `creation-time` pois metadados definidos pelo usuário não são permitidos se você estiver adicionando um objeto a um bucket que tenha a Conformidade legada habilitada. Um erro será retornado.

- Cabeçalhos de solicitação de bloqueio de objeto S3:

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Se uma solicitação for feita sem esses cabeçalhos, as configurações de retenção padrão do bucket serão usadas para calcular a versão do objeto `retain-until-date`.

["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)

- Cabeçalhos de solicitação SSE:

- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

[Cabeçalhos de solicitação para criptografia do lado do servidor](#)



Para obter informações sobre como o StorageGRID lida com caracteres UTF-8, consulte ["ColocarObjeto"](#).

Cabeçalhos de solicitação para criptografia do lado do servidor

Você pode usar os seguintes cabeçalhos de solicitação para criptografar um objeto multiparte com criptografia do lado do servidor. As opções SSE e SSE-C são mutuamente exclusivas.

- **SSE:** Use o seguinte cabeçalho na solicitação `CreateMultipartUpload` se quiser criptografar o objeto com uma chave exclusiva gerenciada pelo StorageGRID. Não especifique este cabeçalho em nenhuma das solicitações `UploadPart`.
 - `x-amz-server-side-encryption`
- **SSE-C:** Use todos esses três cabeçalhos na solicitação `CreateMultipartUpload` (e em cada solicitação `UploadPart` subsequente) se quiser criptografar o objeto com uma chave exclusiva que você fornece e gerencia.
 - `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256`.

- `x-amz-server-side-encryption-customer-key`: Especifique sua chave de criptografia para o novo objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o resumo MD5 da chave de criptografia do novo objeto.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações para ["usando criptografia do lado do servidor"](#).

Cabeçalhos de solicitação não suportados

O seguinte cabeçalho de solicitação não é suportado:

- `x-amz-website-redirect-location`

O `x-amz-website-redirect-location` retornos de cabeçalho `XNotImplemented`.

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação `CompleteMultipartUpload` é executada.

ListarMultipartUploads

A operação `ListMultipartUploads` lista uploads multipartes em andamento para um bucket.

Os seguintes parâmetros de solicitação são suportados:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação `CompleteMultipartUpload` é executada.

UploadPart

A operação UploadPart carrega uma parte em um upload multiparte para um objeto.

Cabeçalhos de solicitação suportados

Os seguintes cabeçalhos de solicitação são suportados:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação CreateMultipartUpload, também deverá incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: Especifique AES256 .
- `x-amz-server-side-encryption-customer-key`: Especifique a mesma chave de criptografia que você forneceu na solicitação CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique o mesmo resumo MD5 que você forneceu na solicitação CreateMultipartUpload.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em ["Use criptografia do lado do servidor"](#) .

Se você especificou uma soma de verificação SHA-256 durante a solicitação CreateMultipartUpload, também deverá incluir o seguinte cabeçalho de solicitação em cada solicitação UploadPart:

- `x-amz-checksum-sha256`: Especifique a soma de verificação SHA-256 para esta parte.

Cabeçalhos de solicitação não suportados

Os seguintes cabeçalhos de solicitação não são suportados:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

UploadPartCopy

A operação UploadPartCopy carrega uma parte de um objeto copiando dados de um objeto existente como fonte de dados.

A operação UploadPartCopy é implementada com todo o comportamento da API REST do Amazon S3. Sujeito a alterações sem aviso.

Esta solicitação lê e grava os dados do objeto especificados em x-amz-copy-source-range dentro do sistema StorageGRID .

Os seguintes cabeçalhos de solicitação são suportados:

- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since

Cabeçalhos de solicitação para criptografia do lado do servidor

Se você especificou a criptografia SSE-C para a solicitação CreateMultipartUpload, também deverá incluir os seguintes cabeçalhos de solicitação em cada solicitação UploadPartCopy:

- x-amz-server-side-encryption-customer-algorithm: Especifique AES256 .
- x-amz-server-side-encryption-customer-key: Especifique a mesma chave de criptografia que você forneceu na solicitação CreateMultipartUpload.
- x-amz-server-side-encryption-customer-key-MD5: Especifique o mesmo resumo MD5 que você forneceu na solicitação CreateMultipartUpload.

Se o objeto de origem for criptografado usando uma chave fornecida pelo cliente (SSE-C), você deverá incluir os três cabeçalhos a seguir na solicitação UploadPartCopy para que o objeto possa ser descriptografado e copiado:

- x-amz-copy-source-server-side-encryption-customer-algorithm: Especifique AES256 .
- x-amz-copy-source-server-side-encryption-customer-key: Especifique a chave de criptografia que você forneceu quando criou o objeto de origem.
- x-amz-copy-source-server-side-encryption-customer-key-MD5: Especifique o resumo MD5 que você forneceu quando criou o objeto de origem.



As chaves de criptografia fornecidas nunca são armazenadas. Se você perder uma chave de criptografia, perderá o objeto correspondente. Antes de usar chaves fornecidas pelo cliente para proteger dados de objetos, revise as considerações em ["Use criptografia do lado do servidor"](#) .

Controle de versão

O upload multipartes consiste em operações separadas para iniciar o upload, listar uploads, carregar partes, montar as partes carregadas e concluir o upload. Os objetos são criados (e versionados, se aplicável) quando a operação CompleteMultipartUpload é executada.

Respostas de erro

O sistema StorageGRID suporta todas as respostas de erro padrão da API REST do S3 aplicáveis. Além disso, a implementação do StorageGRID adiciona várias respostas

personalizadas.

Códigos de erro da API S3 suportados

Nome	Status HTTP
Acesso negado	403 Proibido
BadDigest	400 Solicitação Inválida
BucketAlreadyExists	409 Conflito
BaldeNãoVazio	409 Conflito
Corpo Incompleto	400 Solicitação Inválida
Erro interno	Erro interno do servidor 500
Id de chave de acesso inválido	403 Proibido
Argumento inválido	400 Solicitação Inválida
Nome de Bucket inválido	400 Solicitação Inválida
Estado de Bucket inválido	409 Conflito
InvalidDigest	400 Solicitação Inválida
Erro de Algoritmo de Criptografia Inválido	400 Solicitação Inválida
Parte inválida	400 Solicitação Inválida
Pedido de peça inválido	400 Solicitação Inválida
Intervalo inválido	416 Intervalo solicitado não satisfatório
Solicitação inválida	400 Solicitação Inválida
Classe de armazenamento inválida	400 Solicitação Inválida
Tag inválida	400 Solicitação Inválida
URI inválido	400 Solicitação Inválida
ChaveMuitoLonga	400 Solicitação Inválida

Nome	Status HTTP
XML malformatado	400 Solicitação Inválida
MetadadosMuitoGrandes	400 Solicitação Inválida
MétodoNãoPermitido	Método 405 não permitido
Comprimento do conteúdo ausente	411 Comprimento necessário
Erro de corpo de solicitação ausente	400 Solicitação Inválida
Cabeçalho de segurança ausente	400 Solicitação Inválida
NoSuchBucket	404 Não Encontrado
Nenhuma Chave	404 Não Encontrado
NoSuchUpload	404 Não Encontrado
Não implementado	501 Não Implementado
Política NoSuchBucket	404 Não Encontrado
Erro de configuração de bloqueio de objeto não encontrado	404 Não Encontrado
Pré-condição falhou	412 Pré-condição falhou
RequestTimeTooSkewed	403 Proibido
Serviço não disponível	503 Serviço indisponível
AssinaturaNãoCorresponde	403 Proibido
Muitos Baldes	400 Solicitação Inválida
UserKeyDeveSerEspecificado	400 Solicitação Inválida

Códigos de erro personalizados do StorageGRID

Nome	Descrição	Status HTTP
XBucketLifecycleNãoPermitido	A configuração do ciclo de vida do bucket não é permitida em um bucket compatível legado	400 Solicitação Inválida

Nome	Descrição	Status HTTP
XBucketPolicyParseException	Falha ao analisar o JSON da política de bucket recebida.	400 Solicitação Inválida
XComplianceConflito	Operação negada devido a configurações de conformidade legadas.	403 Proibido
XComplianceRedundância ReduzidaProibido	Redundância reduzida não é permitida no bucket compatível legado	400 Solicitação Inválida
Comprimento da política XMaxBucket excedido	Sua apólice excede o comprimento máximo permitido da apólice.	400 Solicitação Inválida
XMissingInternalRequestHeader	Falta um cabeçalho de uma solicitação interna.	400 Solicitação Inválida
Conformidade com XNoSuchBucket	O bucket especificado não tem a conformidade legada habilitada.	404 Não Encontrado
XNãoAceitável	A solicitação contém um ou mais cabeçalhos de aceitação que não puderam ser atendidos.	406 Não aceitável
XNãoImplementado	A solicitação que você forneceu implica uma funcionalidade que não está implementada.	501 Não Implementado

Operações personalizadas do StorageGRID

Operações personalizadas do StorageGRID

O sistema StorageGRID suporta operações personalizadas que são adicionadas à API REST do S3.

A tabela a seguir lista as operações personalizadas suportadas pelo StorageGRID.

Operação	Descrição
"Consistência do balde GET"	Retorna a consistência que está sendo aplicada a um bucket específico.
"Consistência do balde PUT"	Define a consistência aplicada a um bucket específico.
"Último horário de acesso do Bucket GET"	Retorna se as últimas atualizações de horário de acesso estão habilitadas ou desabilitadas para um bucket específico.
"Hora do último acesso ao bucket PUT"	Permite que você habilite ou desabilite as atualizações do último horário de acesso para um bucket específico.

Operação	Descrição
"EXCLUIR configuração de notificação de metadados do bucket"	Exclui o XML de configuração de notificação de metadados associado a um bucket específico.
"Configuração de notificação de metadados do GET Bucket"	Retorna o XML de configuração de notificação de metadados associado a um bucket específico.
"Configuração de notificação de metadados do PUT Bucket"	Configura o serviço de notificação de metadados para um bucket.
"Uso de armazenamento GET"	Informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta.
"Obsoleto: CreateBucket com configurações de conformidade"	Obsoleto e sem suporte: não é mais possível criar novos buckets com a Conformidade ativada.
"Obsoleto: conformidade com o GET Bucket"	Obsoleto, mas com suporte: retorna as configurações de conformidade atualmente em vigor para um bucket compatível legado existente.
"Obsoleto: conformidade com PUT Bucket"	Obsoleto, mas com suporte: permite modificar as configurações de conformidade de um bucket compatível legado existente.

Consistência do balde GET

A solicitação de consistência GET Bucket permite que você determine a consistência que está sendo aplicada a um bucket específico.

A consistência padrão é definida para garantir leitura após gravação para objetos recém-criados.

Você deve ter a permissão `s3:GetBucketConsistency` ou ser root da conta para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Resposta

No XML de resposta, `<Consistency>` retornará um dos seguintes valores:

Consistência	Descrição
todos	Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
forte-global	Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
site forte	Garante consistência de leitura após gravação para todas as solicitações de clientes em um site.
leitura após nova escrita	(Padrão) 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 .

Exemplo de resposta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Informações relacionadas

["Valores de consistência"](#)

Consistência do balde PUT

A solicitação de consistência do PUT Bucket permite que você especifique a consistência a ser aplicada às operações executadas em um bucket.

A consistência padrão é definida para garantir leitura após gravação para objetos recém-criados.

Antes de começar

Você deve ter a permissão `s3:PutBucketConsistency` ou ser root da conta para concluir esta operação.

Solicitar

O `x-ntap-sg-consistency` o parâmetro deve conter um dos seguintes valores:

Consistência	Descrição
todos	Todos os nós recebem os dados imediatamente, ou a solicitação falhará.
forte-global	Garante consistência de leitura após gravação para todas as solicitações de clientes em todos os sites.
site forte	Garante consistência de leitura após gravação para todas as solicitações de clientes em um site.
leitura após nova escrita	(Padrão) 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 .

Observação: Em geral, você deve usar a consistência "Leitura após nova gravação". Se as solicitações não estiverem funcionando corretamente, altere o comportamento do cliente do aplicativo, se possível. Ou configure o cliente para especificar a consistência para cada solicitação de API. Defina a consistência no nível do bucket somente como último recurso.

Exemplo de solicitação

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informações relacionadas

["Valores de consistência"](#)

Último horário de acesso do Bucket GET

A solicitação de último horário de acesso do GET Bucket permite que você determine se as atualizações de último horário de acesso estão habilitadas ou desabilitadas para buckets individuais.

Você deve ter a permissão `s3:GetBucketLastAccessTime` ou ser root da conta para concluir esta operação.

Exemplo de solicitação

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

Este exemplo mostra que as atualizações do último horário de acesso estão habilitadas para o bucket.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

Hora do último acesso ao bucket PUT

A solicitação de último horário de acesso do PUT Bucket permite que você habilite ou desabilite atualizações de último horário de acesso para buckets individuais. Desabilitar as atualizações do último horário de acesso melhora o desempenho e é a configuração padrão para todos os buckets criados com a versão 10.3.0 ou posterior.

Você deve ter a permissão `s3:PutBucketLastAccessTime` para um bucket ou ser root da conta para concluir esta operação.



A partir da versão 10.3 do StorageGRID, as atualizações do último horário de acesso são desabilitadas por padrão para todos os novos buckets. Se você tiver buckets que foram criados usando uma versão anterior do StorageGRID e quiser corresponder ao novo comportamento padrão, deverá desabilitar explicitamente as atualizações do último horário de acesso para cada um desses buckets anteriores. Você pode habilitar ou desabilitar atualizações para o último horário de acesso usando a solicitação de último horário de acesso do bucket PUT ou na página de detalhes de um bucket no Gerenciador de locatários. Ver ["Habilitar ou desabilitar atualizações do último horário de acesso"](#).

Se as atualizações do último horário de acesso estiverem desabilitadas para um bucket, o seguinte comportamento será aplicado às operações no bucket:

- As solicitações `GetObject`, `GetObjectAcl`, `GetObjectTagging` e `HeadObject` não atualizam o último horário de acesso. O objeto não é adicionado às filas para avaliação do gerenciamento do ciclo de vida das informações (ILM).
- As solicitações `CopyObject` e `PutObjectTagging` que atualizam apenas os metadados também atualizam o horário do último acesso. O objeto é adicionado às filas para avaliação do ILM.
- Se as atualizações do último horário de acesso estiverem desabilitadas para o bucket de origem, as solicitações `CopyObject` não atualizarão o último horário de acesso para o bucket de origem. O objeto que foi copiado não é adicionado às filas para avaliação do ILM para o bucket de origem. Entretanto, para o destino, as solicitações `CopyObject` sempre atualizam o horário do último acesso. A cópia do objeto é adicionada às filas para avaliação do ILM.
- `CompleteMultipartUpload` solicita atualização do último horário de acesso. O objeto concluído é adicionado às filas para avaliação do ILM.

Exemplos de solicitação

Este exemplo habilita o último horário de acesso para um bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Este exemplo desabilita o último horário de acesso para um bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

EXCLUIR configuração de notificação de metadados do bucket

A solicitação de configuração de notificação de metadados `DELETE Bucket` permite que você desabilite o serviço de integração de pesquisa para buckets individuais excluindo o XML de configuração.

Você deve ter a permissão `s3:DeleteBucketMetadataNotification` para um bucket ou ser root da conta para concluir esta operação.

Exemplo de solicitação

Este exemplo mostra a desativação do serviço de integração de pesquisa para um bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configuração de notificação de metadados do GET Bucket

A solicitação de configuração de notificação de metadados do GET Bucket permite que você recupere o XML de configuração usado para configurar a integração de pesquisa para buckets individuais.

Você deve ter a permissão `s3:GetBucketMetadataNotification` ou ser root da conta para concluir esta operação.

Exemplo de solicitação

Esta solicitação recupera a configuração de notificação de metadados para o bucket denominado `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Resposta

O corpo da resposta inclui a configuração de notificação de metadados para o bucket. A configuração de notificação de metadados permite que você determine como o bucket é configurado para integração de pesquisa. Ou seja, ele permite que você determine quais objetos são indexados e para quais endpoints seus metadados de objeto estão sendo enviados.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>

```

Cada configuração de notificação de metadados inclui uma ou mais regras. Cada regra especifica os objetos aos quais se aplica e o destino para onde o StorageGRID deve enviar metadados do objeto. Os destinos devem ser especificados usando o URN de um ponto de extremidade StorageGRID .

Nome	Descrição	Obrigatório
Configuração de Notificação de Metadados	Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos Rule.	Sim
Regra	Tag de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
EU IA	Identificador exclusivo para a regra. Incluído no elemento Rule.	Não
Status	O status pode ser "Habilitado" ou "Desabilitado". Nenhuma ação é tomada para regras que estão desabilitadas. Incluído no elemento Rule.	Sim

Nome	Descrição	Obrigatório
Prefixo	Objetos que correspondem ao prefixo são afetados pela regra, e seus metadados são enviados ao destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento Rule.	Sim
Destino	Tag de contêiner para o destino de uma regra. Incluído no elemento Rule.	Sim
Urna	URN do destino para onde os metadados do objeto são enviados. Deve ser a URN de um ponto de extremidade StorageGRID com as seguintes propriedades: • `es` deve ser o terceiro elemento. • A URN deve terminar com o índice e o tipo onde os metadados são armazenados, no formato <code>domain-name/myindex/mytype</code>. Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles assumem a seguinte forma: • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> O ponto de extremidade deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. A urna está incluída no elemento Destino.	Sim

Exemplo de resposta

O XML incluído entre o

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` **tags** mostra como a integração com um ponto de extremidade de integração de pesquisa é configurada para o bucket. Neste exemplo, os metadados do objeto estão sendo enviados para um índice do Elasticsearch denominado `current` e digite nomeado `2017` que está hospedado em um domínio AWS chamado `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Informações relacionadas

["Use uma conta de inquilino"](#)

Configuração de notificação de metadados do PUT Bucket

A solicitação de configuração de notificação de metadados do PUT Bucket permite que você habilite o serviço de integração de pesquisa para buckets individuais. O XML de configuração de notificação de metadados fornecido no corpo da solicitação especifica os objetos cujos metadados são enviados ao índice de pesquisa de destino.

Você deve ter a permissão `s3:PutBucketMetadataNotification` para um bucket ou ser root da conta para concluir esta operação.

Solicitar

A solicitação deve incluir a configuração de notificação de metadados no corpo da solicitação. Cada configuração de notificação de metadados inclui uma ou mais regras. Cada regra especifica os objetos aos quais se aplica e o destino para onde o StorageGRID deve enviar metadados do objeto.

Os objetos podem ser filtrados pelo prefixo do nome do objeto. Por exemplo, você pode enviar metadados para objetos com o prefixo `/images` para um destino e objetos com o prefixo `/videos` para outro.

Configurações que possuem prefixos sobrepostos não são válidas e são rejeitadas quando enviadas. Por exemplo, uma configuração que incluía uma regra para objetos com o prefixo `test` e uma segunda regra para objetos com o prefixo `test2` não seria permitido.

Os destinos devem ser especificados usando o URN de um ponto de extremidade StorageGRID . O ponto de extremidade deve existir quando a configuração de notificação de metadados for enviada, ou a solicitação

falhará como um 400 Bad Request. A mensagem de erro diz: Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: *URN*.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

A tabela descreve os elementos no XML de configuração de notificação de metadados.

Nome	Descrição	Obrigatório
Configuração de Notificação de Metadados	Tag de contêiner para regras usadas para especificar os objetos e o destino para notificações de metadados. Contém um ou mais elementos Rule.	Sim
Regra	Tag de contêiner para uma regra que identifica os objetos cujos metadados devem ser adicionados a um índice especificado. Regras com prefixos sobrepostos são rejeitadas. Incluído no elemento MetadataNotificationConfiguration.	Sim
EU IA	Identificador exclusivo para a regra. Incluído no elemento Rule.	Não
Status	O status pode ser "Habilitado" ou "Desabilitado". Nenhuma ação é tomada para regras que estão desabilitadas. Incluído no elemento Rule.	Sim

Nome	Descrição	Obrigatório
Prefixo	Objetos que correspondem ao prefixo são afetados pela regra, e seus metadados são enviados ao destino especificado. Para corresponder a todos os objetos, especifique um prefixo vazio. Incluído no elemento Rule.	Sim
Destino	Tag de contêiner para o destino de uma regra. Incluído no elemento Rule.	Sim
Urna	URN do destino para onde os metadados do objeto são enviados. Deve ser a URN de um ponto de extremidade StorageGRID com as seguintes propriedades: • `es` deve ser o terceiro elemento. • A URN deve terminar com o índice e o tipo onde os metadados são armazenados, no formato <code>domain-name/myindex/mytype</code>. Os endpoints são configurados usando o Tenant Manager ou a Tenant Management API. Eles assumem a seguinte forma: • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> O ponto de extremidade deve ser configurado antes que o XML de configuração seja enviado, ou a configuração falhará com um erro 404. A urna está incluída no elemento Destino.	Sim

Exemplos de solicitação

Este exemplo mostra como habilitar a integração de pesquisa para um bucket. Neste exemplo, os metadados de todos os objetos são enviados para o mesmo destino.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Neste exemplo, metadados de objetos para objetos que correspondem ao prefixo `/images` é enviado para um destino, enquanto metadados de objeto para objetos que correspondem ao prefixo `/videos` é enviado para um segundo destino.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

JSON gerado pelo serviço de integração de pesquisa

Quando você habilita o serviço de integração de pesquisa para um bucket, um documento JSON é gerado e enviado ao ponto de extremidade de destino sempre que metadados ou tags de objeto são adicionados, atualizados ou excluídos.

Este exemplo mostra um exemplo do JSON que pode ser gerado quando um objeto com a chave `SGWS/Tagging.txt` é criado em um bucket chamado `test`. O `test` o bucket não é versionado, então o `versionId` a tag está vazia.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadados de objeto incluídos em notificações de metadados

A tabela lista todos os campos incluídos no documento JSON que é enviado ao ponto de extremidade de destino quando a integração de pesquisa está habilitada.

O nome do documento inclui o nome do bucket, o nome do objeto e o ID da versão, se presente.

Tipo	Nome do item	Descrição
Informações sobre bucket e objeto	balde	Nome do balde
Informações sobre bucket e objeto	chave	Nome da chave do objeto
Informações sobre bucket e objeto	ID da versão	Versão do objeto, para objetos em buckets versionados
Informações sobre bucket e objeto	região	Região de balde, por exemplo <code>us-east-1</code>
Metadados do sistema	tamanho	Tamanho do objeto (em bytes) conforme visível para um cliente HTTP
Metadados do sistema	md5	Hash de objeto
Metadados do usuário	metadados <i>key:value</i>	Todos os metadados do usuário para o objeto, como pares de chave-valor

Tipo	Nome do item	Descrição
Etiquetas	etiquetas <i>key:value</i>	Todas as tags de objeto definidas para o objeto, como pares chave-valor



Para tags e metadados do usuário, o StorageGRID passa datas e números para o Elasticsearch como strings ou como notificações de eventos do S3. Para configurar o Elasticsearch para interpretar essas strings como datas ou números, siga as instruções do Elasticsearch para mapeamento de campos dinâmicos e para mapeamento de formatos de data. Você deve habilitar os mapeamentos de campos dinâmicos no índice antes de configurar o serviço de integração de pesquisa. Depois que um documento é indexado, você não pode editar os tipos de campo do documento no índice.

Informações relacionadas

["Use uma conta de inquilino"](#)

Solicitação de uso de armazenamento GET

A solicitação GET Storage Usage informa a quantidade total de armazenamento em uso por uma conta e para cada bucket associado à conta.

A quantidade de armazenamento usada por uma conta e seus buckets pode ser obtida por meio de uma solicitação ListBuckets modificada com o `x-ntap-sg-usage` parâmetro de consulta. O uso do armazenamento do bucket é rastreado separadamente das solicitações PUT e DELETE processadas pelo sistema. Pode haver algum atraso antes que os valores de uso correspondam aos valores esperados com base no processamento de solicitações, principalmente se o sistema estiver sob carga pesada.

Por padrão, o StorageGRID tenta recuperar informações de uso usando consistência global forte. Se a consistência global forte não puder ser alcançada, o StorageGRID tentará recuperar as informações de uso em uma consistência de site forte.

Você deve ter a permissão `s3:ListAllMyBuckets` ou ser root da conta para concluir esta operação.

Exemplo de solicitação

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

Este exemplo mostra uma conta que tem quatro objetos e 12 bytes de dados em dois buckets. Cada bucket contém dois objetos e seis bytes de dados.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Controle de versão

Cada versão do objeto armazenada contribuirá para o `ObjectCount` e `DataBytes` valores na resposta. Os marcadores de exclusão não são adicionados ao `ObjectCount` total.

Informações relacionadas

["Valores de consistência"](#)

Solicitações de bucket obsoletas para conformidade legada

Solicitações de bucket obsoletas para conformidade legada

Talvez seja necessário usar a API REST do StorageGRID S3 para gerenciar buckets que foram criados usando o recurso de conformidade legado.

Recurso de conformidade obsoleto

O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock.

Se você habilitou anteriormente a configuração global de Conformidade, a configuração global de Bloqueio de Objeto S3 será habilitada no StorageGRID 11.6. Não é mais possível criar novos buckets com a Conformidade ativada; no entanto, conforme necessário, você pode usar a API REST do StorageGRID S3 para gerenciar quaisquer buckets compatíveis legados existentes.

- ["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)
- ["Gerenciar objetos com ILM"](#)
- ["Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"](#)

Solicitações de conformidade obsoletas:

- ["Obsoleto - Modificações na solicitação do bucket PUT para conformidade"](#)

O elemento XML SGCompliance está obsoleto. Anteriormente, você podia incluir esse elemento personalizado StorageGRID no corpo de solicitação XML opcional de solicitações PUT Bucket para criar um bucket compatível.

- ["Obsoleto - Conformidade com o GET Bucket"](#)

A solicitação de conformidade do GET Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket compatível legado existente.

- ["Obsoleto - Conformidade com PUT Bucket"](#)

A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para modificar as configurações de conformidade de um bucket compatível legado existente. Por exemplo, você pode colocar um bucket existente em retenção legal ou aumentar seu período de retenção.

Obsoleto: modificações na solicitação CreateBucket para conformidade

O elemento XML SGCompliance está obsoleto. Anteriormente, você podia incluir este elemento personalizado StorageGRID no corpo de solicitação XML opcional das solicitações CreateBucket para criar um bucket compatível.



O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock. Veja o seguinte para mais detalhes:

- ["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)
- ["Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"](#)

Não é mais possível criar novos buckets com a Conformidade ativada. A seguinte mensagem de erro será retornada se você tentar usar as modificações de solicitação CreateBucket para conformidade para criar um novo bucket compatível:

The Compliance feature is deprecated.

Contact your StorageGRID administrator if you need to create new Compliant buckets.

Obsoleto: solicitação de conformidade do GET Bucket

A solicitação de conformidade do GET Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para determinar as configurações de conformidade atualmente em vigor para um bucket compatível legado existente.



O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock. Veja o seguinte para mais detalhes:

- ["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)
- ["Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"](#)

Você deve ter a permissão `s3:GetBucketCompliance` ou ser root da conta para concluir esta operação.

Exemplo de solicitação

Este exemplo de solicitação permite que você determine as configurações de conformidade para o bucket denominado `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemplo de resposta

No XML de resposta, `<SGCompliance>` lista as configurações de conformidade em vigor para o bucket. Este exemplo de resposta mostra as configurações de conformidade para um bucket no qual cada objeto será retido por um ano (525.600 minutos), a partir do momento em que o objeto for ingerido na grade. Atualmente não há retenção legal para este balde. Cada objeto será excluído automaticamente após um ano.

```

HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>

```

Nome	Descrição
Período de retenção em minutos	A duração do período de retenção para objetos adicionados a este bucket, em minutos. O período de retenção começa quando o objeto é ingerido na grade.
Retenção Legal	• Verdadeiro: Este bucket está atualmente sob retenção legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja suspensa, mesmo que o período de retenção tenha expirado. • Falso: Este bucket não está atualmente sob retenção legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Exclusão automática	• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob retenção legal. • Falso: Os objetos neste bucket não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Respostas de erro

Se o bucket não foi criado para ser compatível, o código de status HTTP para a resposta é 404 `Not Found`, com um código de erro S3 de `XNoSuchBucketCompliance`.

Obsoleto: solicitação de conformidade do PUT Bucket

A solicitação de conformidade do PUT Bucket está obsoleta. No entanto, você pode continuar a usar essa solicitação para modificar as configurações de conformidade de um bucket compatível legado existente. Por exemplo, você pode colocar um bucket existente em retenção legal ou aumentar seu período de retenção.



O recurso de conformidade do StorageGRID que estava disponível em versões anteriores do StorageGRID foi descontinuado e substituído pelo S3 Object Lock. Veja o seguinte para mais detalhes:

- ["Use a API REST do S3 para configurar o bloqueio de objeto do S3"](#)
- ["Base de conhecimento da NetApp : Como gerenciar buckets compatíveis legados no StorageGRID 11.5"](#)

Você deve ter a permissão `s3:PutBucketCompliance` ou ser root da conta para concluir esta operação.

Você deve especificar um valor para cada campo das configurações de conformidade ao emitir uma solicitação de conformidade do PUT Bucket.

Exemplo de solicitação

Este exemplo de solicitação modifica as configurações de conformidade para o bucket denominado `mybucket`. Neste exemplo, os objetos em `mybucket` agora serão retidos por dois anos (1.051.200 minutos) em vez de um ano, a partir do momento em que o objeto for inserido na grade. Não há retenção legal para este balde. Cada objeto será excluído automaticamente após dois anos.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrição
Período de retenção em minutos	A duração do período de retenção para objetos adicionados a este bucket, em minutos. O período de retenção começa quando o objeto é ingerido na grade. Importante Ao especificar um novo valor para <code>RetentionPeriodMinutes</code>, você deve especificar um valor que seja igual ou maior que o período de retenção atual do bucket. Depois que o período de retenção do bucket for definido, você não poderá diminuir esse valor; você só poderá aumentá-lo.

Nome	Descrição
Retenção Legal	• Verdadeiro: Este bucket está atualmente sob retenção legal. Os objetos neste bucket não podem ser excluídos até que a retenção legal seja suspensa, mesmo que o período de retenção tenha expirado. • Falso: Este bucket não está atualmente sob retenção legal. Os objetos neste bucket podem ser excluídos quando seu período de retenção expirar.
Exclusão automática	• Verdadeiro: Os objetos neste bucket serão excluídos automaticamente quando seu período de retenção expirar, a menos que o bucket esteja sob retenção legal. • Falso: Os objetos neste bucket não serão excluídos automaticamente quando o período de retenção expirar. Você deve excluir esses objetos manualmente se precisar excluí-los.

Consistência para configurações de conformidade

Quando você atualiza as configurações de conformidade de um bucket do S3 com uma solicitação de conformidade do bucket PUT, o StorageGRID tenta atualizar os metadados do bucket na grade. Por padrão, o StorageGRID usa a consistência **Strong-global** para garantir que todos os sites do data center e todos os nós de armazenamento que contêm metadados de bucket tenham consistência de leitura após gravação para as configurações de conformidade alteradas.

Se o StorageGRID não conseguir atingir a consistência **Strong-global** porque um site de data center ou vários nós de armazenamento em um site não estão disponíveis, o código de status HTTP para a resposta é 503 Service Unavailable.

Se você receber essa resposta, entre em contato com o administrador da rede para garantir que os serviços de armazenamento necessários sejam disponibilizados o mais rápido possível. Se o administrador da grade não conseguir disponibilizar Nós de Armazenamento suficientes em cada site, o suporte técnico poderá instruí-lo a tentar novamente a solicitação com falha, forçando a consistência **Strong-site**.



Nunca force a consistência **Strong-site** para conformidade com o bucket PUT, a menos que você tenha sido instruído a fazê-lo pelo suporte técnico e a menos que você entenda as potenciais consequências do uso desse nível.

Quando a consistência é reduzida para **Strong-site**, o StorageGRID garante que as configurações de conformidade atualizadas terão consistência de leitura após gravação somente para solicitações de clientes dentro de um site. Isso significa que o sistema StorageGRID pode ter temporariamente várias configurações inconsistentes para esse bucket até que todos os sites e nós de armazenamento estejam disponíveis. Configurações inconsistentes podem resultar em comportamento inesperado e indesejado. Por exemplo, se você estiver colocando um bucket sob retenção legal e forçar uma consistência menor, as configurações de conformidade anteriores do bucket (ou seja, retenção legal) poderão continuar em vigor em alguns sites de data center. Como resultado, objetos que você acha que estão em retenção legal podem ser excluídos quando seu período de retenção expirar, pelo usuário ou pela Exclusão Automática, se habilitada.

Para forçar o uso da consistência **Strong-site**, emita novamente a solicitação de conformidade do PUT Bucket e inclua o Consistency-Control Cabeçalho de solicitação HTTP, como segue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Respostas de erro

- Se o bucket não foi criado para ser compatível, o código de status HTTP para a resposta é 404 Not Found.
- Se `RetentionPeriodMinutes` na solicitação for menor que o período de retenção atual do bucket, o código de status HTTP é 400 Bad Request.

Informações relacionadas

["Obsoleto: modificações na solicitação do bucket PUT para conformidade"](#)

Políticas de acesso a grupos e buckets

Use políticas de acesso a buckets e grupos

O StorageGRID usa a linguagem de política da Amazon Web Services (AWS) para permitir que os locatários do S3 controlem o acesso a buckets e objetos dentro desses buckets. O sistema StorageGRID implementa um subconjunto da linguagem de política da API REST do S3. As políticas de acesso para a API do S3 são escritas em JSON.

Visão geral da política de acesso

Há dois tipos de políticas de acesso suportadas pelo StorageGRID.

- **Políticas de bucket**, que são gerenciadas usando as operações da API S3 `GetBucketPolicy`, `PutBucketPolicy` e `DeleteBucketPolicy` ou a API Tenant Manager ou Tenant Management. As políticas de bucket são anexadas aos buckets, portanto, elas são configuradas para controlar o acesso de usuários na conta do proprietário do bucket ou de outras contas ao bucket e aos objetos nele contidos. Uma política de bucket se aplica a apenas um bucket e possivelmente a vários grupos.
- **Políticas de grupo**, que são configuradas usando o Tenant Manager ou a Tenant Management API. As políticas de grupo são anexadas a um grupo na conta, portanto, elas são configuradas para permitir que esse grupo acesse recursos específicos de propriedade dessa conta. Uma política de grupo se aplica a apenas um grupo e possivelmente a vários buckets.



Não há diferença de prioridade entre políticas de grupo e de bucket.

As políticas de grupo e bucket do StorageGRID seguem uma gramática específica definida pela Amazon. Dentro de cada política há uma série de declarações de política, e cada declaração contém os seguintes elementos:

- ID da declaração (Sid) (opcional)
- Efeito
- Principal/Não Principal
- Recurso/NãoRecurso
- Ação/NãoAção

- Condição (opcional)

As declarações de política são criadas usando esta estrutura para especificar permissões: Conceder <Efeito> para permitir/negar que <Principal> execute <Ação> em <Recurso> quando <Condição> se aplicar.

Cada elemento de política é usado para uma função específica:

Elemento	Descrição
Sido	O elemento Sid é opcional. O Sid serve apenas como uma descrição para o usuário. Ele é armazenado, mas não interpretado pelo sistema StorageGRID .
Efeito	Use o elemento Efeito para estabelecer se as operações especificadas são permitidas ou negadas. Você deve identificar as operações que permite (ou nega) em buckets ou objetos usando as palavras-chave do elemento Action suportadas.
Principal/Não Principal	Você pode permitir que usuários, grupos e contas acessem recursos específicos e executem ações específicas. Se nenhuma assinatura S3 for incluída na solicitação, o acesso anônimo será permitido especificando o caractere curinga (*) como principal. Por padrão, somente o root da conta tem acesso aos recursos de propriedade da conta. Você só precisa especificar o elemento Principal em uma política de bucket. Para políticas de grupo, o grupo ao qual a política está anexada é o elemento Principal implícito.
Recurso/NãoRecurso	O elemento Resource identifica buckets e objetos. Você pode permitir ou negar permissões para buckets e objetos usando o Amazon Resource Name (ARN) para identificar o recurso.
Ação/NãoAção	Os elementos Ação e Efeito são os dois componentes das permissões. Quando um grupo solicita um recurso, o acesso ao recurso é concedido ou negado. O acesso será negado, a menos que você atribua permissões especificamente, mas você pode usar a negação explícita para substituir uma permissão concedida por outra política.
Doença	O elemento Condition é opcional. As condições permitem que você crie expressões para determinar quando uma política deve ser aplicada.

No elemento Ação, você pode usar o caractere curinga (*) para especificar todas as operações ou um subconjunto de operações. Por exemplo, esta Ação corresponde a permissões como s3:GetObject, s3:PutObject e s3:DeleteObject.

```
s3:*Object
```

No elemento Recurso, você pode usar os caracteres curinga (*) e (?). Enquanto o asterisco (*) corresponde a 0 ou mais caracteres, o ponto de interrogação (?) corresponde a qualquer caractere único.

No elemento Principal, caracteres curinga não são suportados, exceto para definir acesso anônimo, que concede permissão a todos. Por exemplo, você define o curinga (*) como o valor Principal.

```
"Principal": "*"}
```

```
"Principal": {"AWS": "*"}
```

No exemplo a seguir, a instrução está usando os elementos Effect, Principal, Action e Resource. Este exemplo mostra uma declaração de política de bucket completa que usa o efeito "Permitir" para dar aos Principais, o grupo de administração `federated-group/admin` e o grupo financeiro `federated-group/finance`, permissões para executar a Ação `s3:ListBucket` no balde chamado `mybucket` e a Ação `s3:GetObject` em todos os objetos dentro desse balde.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

A política de bucket tem um limite de tamanho de 20.480 bytes, e a política de grupo tem um limite de tamanho de 5.120 bytes.

Consistência para políticas

Por padrão, todas as atualizações feitas nas políticas de grupo serão consistentes. Quando uma política de grupo se torna consistente, as alterações podem levar mais 15 minutos para entrar em vigor, devido ao cache de políticas. Por padrão, todas as atualizações feitas nas políticas de bucket são fortemente consistentes.

Conforme necessário, você pode alterar as garantias de consistência para atualizações de política de bucket. Por exemplo, você pode querer que uma alteração em uma política de bucket esteja disponível durante uma

interrupção do site.

Neste caso, você pode definir o `Consistency-Control` cabeçalho na solicitação `PutBucketPolicy` ou você pode usar a solicitação de consistência `PUT Bucket`. Quando uma política de bucket se torna consistente, as alterações podem levar mais 8 segundos para entrar em vigor, devido ao cache de políticas.



Se você definir a consistência para um valor diferente para contornar uma situação temporária, certifique-se de definir a configuração do nível do bucket de volta para seu valor original quando terminar. Caso contrário, todas as solicitações futuras de bucket usarão a configuração modificada.

Use ARN em declarações de política

Em declarações de política, o ARN é usado nos elementos `Principal` e `Resource`.

- Use esta sintaxe para especificar o ARN do recurso S3:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Use esta sintaxe para especificar o ARN do recurso de identidade (usuários e grupos):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Outras considerações:

- Você pode usar o asterisco (*) como curinga para corresponder a zero ou mais caracteres dentro da chave do objeto.
- Caracteres internacionais, que podem ser especificados na chave do objeto, devem ser codificados usando JSON UTF-8 ou usando sequências de escape JSON `\u`. A codificação percentual não é suportada.

"Sintaxe URN RFC 2141"

O corpo da solicitação HTTP para a operação `PutBucketPolicy` deve ser codificado com `charset=UTF-8`.

Especificar recursos em uma política

Em declarações de política, você pode usar o elemento `Resource` para especificar o bucket ou objeto para o qual as permissões são permitidas ou negadas.

- Cada declaração de política requer um elemento `Recurso`. Em uma política, os recursos são denotados pelo elemento `Resource`, ou alternativamente, `NotResource` para exclusão.
- Você especifica recursos com um ARN de recurso S3. Por exemplo:


```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Você também pode usar variáveis de política dentro da chave do objeto. Por exemplo:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- O valor do recurso pode especificar um bucket que ainda não existe quando uma política de grupo é criada.

Especificar os principais em uma política

Use o elemento Principal para identificar o usuário, grupo ou conta de locatário que tem acesso permitido/negado ao recurso pela declaração de política.

- Cada declaração de política em uma política de bucket deve incluir um elemento Principal. Declarações de política em uma política de grupo não precisam do elemento Principal porque o grupo é entendido como o principal.
- Em uma política, os principais são indicados pelo elemento "Principal" ou, alternativamente, "NotPrincipal" para exclusão.
- Identidades baseadas em conta devem ser especificadas usando um ID ou um ARN:

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- Este exemplo usa o ID da conta de locatário 27233906934684427525, que inclui a raiz da conta e todos os usuários na conta:

```
"Principal": { "AWS": "27233906934684427525" }
```

- Você pode especificar apenas a raiz da conta:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Você pode especificar um usuário federado específico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
user/Alex" }
```

- Você pode especificar um grupo federado específico ("Gerentes"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-group/Managers" }
```

- Você pode especificar um principal anônimo:

```
"Principal": ""
```

- Para evitar ambiguidade, você pode usar o UUID do usuário em vez do nome de usuário:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

Por exemplo, suponha que Alex deixe a organização e o nome de usuário `Alex` é excluído. Se um novo Alex se juntar à organização e for designado para o mesmo `Alex` nome de usuário, o novo usuário pode herdar involuntariamente as permissões concedidas ao usuário original.

- O valor principal pode especificar um nome de grupo/usuário que ainda não existe quando uma política de bucket é criada.

Especificar permissões em uma política

Em uma política, o elemento Ação é usado para permitir/negar permissões para um recurso. Há um conjunto de permissões que você pode especificar em uma política, que são indicadas pelo elemento "Ação" ou, alternativamente, "NãoAção" para exclusão. Cada um desses elementos mapeia operações específicas da API REST do S3.

As tabelas listam as permissões que se aplicam aos buckets e as permissões que se aplicam aos objetos.



O Amazon S3 agora usa a permissão `s3:PutReplicationConfiguration` para as ações `PutBucketReplication` e `DeleteBucketReplication`. O StorageGRID usa permissões separadas para cada ação, o que corresponde à especificação original do Amazon S3.



Uma exclusão é realizada quando um `put` é usado para substituir um valor existente.

Permissões que se aplicam a buckets

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:CriarBucket	CriarBucket	Sim. Observação: Use somente em políticas de grupo.
s3:ExcluirBucket	ExcluirBucket	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:DeleteBucketMetadataNotification	EXCLUIR configuração de notificação de metadados do bucket	Sim
s3:DeleteBucketPolicy	Política de exclusão de balde	
s3:ExcluirConfiguração de Replicação	DeleteBucketReplication	Sim, permissões separadas para PUT e DELETE
s3:ObterBucketAcl	ObterBucketAcl	
s3:ObterConformidade doBucket	Conformidade com o GET Bucket (obsoleto)	Sim
s3:ObterConsistência doBucket	Consistência do balde GET	Sim
s3:ObterBucketCORS	ObterBucketCors	
s3:ObterConfiguração de Criptografia	Obter criptografia do Bucket	
s3:GetBucketÚltimoAcessoHora	Último horário de acesso do Bucket GET	Sim
s3:ObterLocalização do Balde	ObterBucketLocation	
s3:GetBucketMetadataNotification	Configuração de notificação de metadados do GET Bucket	Sim
s3:GetBucketNotification	Obter configuração de notificação de bucket	
s3:GetBucketObjectLockConfiguration	ObterConfiguraçãoObjectLock	
s3:ObterPolítica deBucket	ObterBucketPolicy	
s3:Obter marcação de balde	Obter marcação de balde	
s3:GetBucketVersionamento	ObterVersionamento doBucket	
s3:ObterConfiguração do Ciclo de Vida	Obter configuração do ciclo de vida do Bucket	
s3:ObterConfiguração de Replicação	Obter replicação do Bucket	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:ListarTodosOsMeusBuckets	- ListBuckets - Uso de armazenamento GET	Sim, para uso de armazenamento GET. Observação: Use somente em políticas de grupo.
s3:ListBucket	- Objetos de Lista - Balde de cabeça - RestaurarObjeto	
s3:ListBucketMultipartUploads	- ListarMultipartUploads - RestaurarObjeto	
s3:ListBucketVersões	Versões do GET Bucket	
s3:Conformidade com PutBucket	Conformidade com o PUT Bucket (obsoleto)	Sim
s3:ConsistênciaPutBucket	Consistência do balde PUT	Sim
s3:ColocarBucketCORS	- ExcluirBucketCors† - ColoqueBucketCors	
s3:PutEncryptionConfiguration	- DeleteBucketEncryption - PutBucketEncryption	
s3:ColocarBucketÚltimoAcessoHora	Hora do último acesso ao bucket PUT	Sim
s3:PutBucketMetadataNotification	Configuração de notificação de metadados do PUT Bucket	Sim
s3:NotificaçãoPutBucket	Configuração de notificação PutBucket	
s3:PutBucketObjectLockConfiguração	- CreateBucket com o x-amz-bucket-object-lock-enabled: true cabeçalho de solicitação (também requer a permissão s3:CreateBucket) - PutObjectLockConfiguration	
s3:PolíticaPutBucket	PutBucketPolicy	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:PutBucketTagging	- ExcluirBucketTagging† - Colocar marcação de balde	
s3:PutBucketVersionamento	Versão PutBucket	
s3:PutLifecycleConfiguration	- Ciclo de vida do DeleteBucket† - Configuração do ciclo de vida do PutBucket	
s3:PutReplicationConfiguration	PutBucketReplicação	Sim, permissões separadas para PUT e DELETE

Permissões que se aplicam a objetos

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:AbortarUploadMultipart	- AbortarMultipartUpload - RestaurarObjeto	
s3:Ignorar Governança Retenção	- ExcluirObjeto - ExcluirObjetos - ColocarRetençãoDeObjeto	
s3:ExcluirObjeto	- ExcluirObjeto - ExcluirObjetos - RestaurarObjeto	
s3:ExcluirMarcaçãoDeObjeto	ExcluirMarcaçãoDeObjeto	
s3:ExcluirMarcaçãoDeVersãoDoObjeto	DeleteObjectTagging (uma versão específica do objeto)	
s3:ExcluirVersãoDoObjeto	DeleteObject (uma versão específica do objeto)	
s3:ObterObjeto	- ObterObjeto - CabeçaObjeto - RestaurarObjeto - SelecionarObjetoConteúdo	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:ObterAclDeObjeto	ObterAclObjeto	
s3:ObterObjetoLegalHold	ObterObjetoLegalHold	
s3:ObterRetençãoDeObjeto	ObterRetençãoDeObjeto	
s3:ObterMarcaçãoDeObjeto	Obter marcação de objeto	
s3:ObterTag deVersão do Objeto	GetObjectTagging (uma versão específica do objeto)	
s3:ObterVersãoDoObjeto	GetObject (uma versão específica do objeto)	
s3:ListMultipartUploadParts	ListParts, RestaurarObjeto	
s3:ColocarObjeto	• ColocarObjeto • CopiarObjeto • RestaurarObjeto • CriarMultipartUpload • Upload completo de várias partes • UploadPart • UploadPartCopy	
s3:ColocarObjetoLegalHold	ColocarObjetoLegalHold	
s3:PutObjectRetention	ColocarRetençãoDeObjeto	
s3:PutObjectTagging	Colocar marcação de objeto	
s3:PutObjectVersionTagging	PutObjectTagging (uma versão específica do objeto)	
s3:ColocarObjetoSobrescrito	• ColocarObjeto • CopiarObjeto • Colocar marcação de objeto • ExcluirMarcaçãoDeObjeto • Upload completo de várias partes	Sim
s3:RestaurarObjeto	RestaurarObjeto	

Usar permissão PutOverwriteObject

A permissão s3:PutOverwriteObject é uma permissão personalizada do StorageGRID que se aplica a operações que criam ou atualizam objetos. A configuração dessa permissão determina se o cliente pode substituir os dados de um objeto, metadados definidos pelo usuário ou marcação de objetos do S3.

As configurações possíveis para essa permissão incluem:

- **Permitir:** O cliente pode substituir um objeto. Esta é a configuração padrão.
- **Negar:** O cliente não pode substituir um objeto. Quando definida como Negar, a permissão PutOverwriteObject funciona da seguinte maneira:
 - Se um objeto existente for encontrado no mesmo caminho:
 - Os dados do objeto, os metadados definidos pelo usuário ou a marcação de objetos S3 não podem ser substituídos.
 - Todas as operações de ingestão em andamento são canceladas e um erro é retornado.
 - Se o controle de versão do S3 estiver habilitado, a configuração Negar impedirá que as operações PutObjectTagging ou DeleteObjectTagging modifiquem o TagSet de um objeto e suas versões não atuais.
 - Se um objeto existente não for encontrado, esta permissão não terá efeito.
- Quando essa permissão não está presente, o efeito é o mesmo que se Permitir estivesse definido.



Se a política atual do S3 permitir a substituição e a permissão PutOverwriteObject estiver definida como Negar, o cliente não poderá substituir os dados de um objeto, os metadados definidos pelo usuário ou a marcação de objetos. Além disso, se a caixa de seleção **Impedir modificação do cliente** estiver marcada (**CONFIGURAÇÃO > Configurações de segurança > Rede e objetos**), essa configuração substituirá a configuração da permissão PutOverwriteObject.

Especificar condições em uma política

As condições definem quando uma política estará em vigor. As condições consistem em operadores e pares chave-valor.

As condições usam pares chave-valor para avaliação. Um elemento Condition pode conter várias condições, e cada condição pode conter vários pares chave-valor. O bloco de condição usa o seguinte formato:

```
Condition: {  
  condition_type: {  
    condition_key: condition_values
```

No exemplo a seguir, a condição IpAddress usa a chave de condição Sourcelp.

```

"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
}

```

Operadores de condição suportados

Os operadores de condição são categorizados da seguinte forma:

- Corda
- Numérico
- Booleano
- Endereço IP
- Verificação nula

Operadores de condição	Descrição
StringEquals	Compara uma chave a um valor de string com base na correspondência exata (diferencia maiúsculas de minúsculas).
StringNotEquals	Compara uma chave a um valor de string com base na correspondência negada (diferencia maiúsculas de minúsculas).
StringEqualsIgnoreCase	Compara uma chave a um valor de string com base na correspondência exata (ignora maiúsculas e minúsculas).
StringNotEqualsIgnoreCase	Compara uma chave a um valor de string com base na correspondência negada (ignora maiúsculas e minúsculas).
StringLike	Compara uma chave a um valor de string com base na correspondência exata (diferencia maiúsculas de minúsculas). Pode incluir caracteres curinga * e ?.
StringNotLike	Compara uma chave a um valor de string com base na correspondência negada (diferencia maiúsculas de minúsculas). Pode incluir caracteres curinga * e ?.
NumericEquals	Compara uma chave a um valor numérico com base na correspondência exata.
NuméricoNãoIgual	Compara uma chave a um valor numérico com base na correspondência negada.

Operadores de condição	Descrição
NuméricoMaiorQue	Compara uma chave a um valor numérico com base na correspondência "maior que".
NuméricoMaiorQueIgual	Compara uma chave a um valor numérico com base na correspondência "maior ou igual a".
NuméricoMenorQue	Compara uma chave a um valor numérico com base na correspondência "menor que".
NuméricoMenorQueIgual	Compara uma chave a um valor numérico com base na correspondência "menor ou igual a".
Bool	Compara uma chave a um valor booleano com base na correspondência "verdadeiro ou falso".
Endereço IP	Compara uma chave a um endereço IP ou intervalo de endereços IP.
Não Endereço IP	Compara uma chave a um endereço IP ou intervalo de endereços IP com base na correspondência negada.
Nulo	Verifica se uma chave de condição está presente no contexto de solicitação atual.

Chaves de condição suportadas

Chaves de condição	Ações	Descrição
aws:SourceIp	Operadores de IP	Será comparado ao endereço IP de onde a solicitação foi enviada. Pode ser usado para operações de bucket ou objeto. Observação: Se a solicitação S3 foi enviada por meio do serviço Load Balancer nos nós de administração e nos nós de gateway, isso será comparado ao endereço IP upstream do serviço Load Balancer. Observação: se um balanceador de carga de terceiros não transparente for usado, isso será comparado ao endereço IP desse balanceador de carga. Qualquer X-Forwarded-For O cabeçalho será ignorado porque sua validade não pode ser verificada.
aws:username	Recurso/Identidade	Será comparado ao nome de usuário do remetente de onde a solicitação foi enviada. Pode ser usado para operações de bucket ou objeto.

Chaves de condição	Ações	Descrição
s3:delimiter	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro delimitador especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:ExistingObjectTag/<chave-tag>	s3:ExcluirMarcaçãoDeObjeto s3:ExcluirMarcaçãoDeVersãoDoObjeto s3:ObterObjeto s3:ObterAclDeObjeto 3: Obter marcação de objeto s3:ObterVersãoDoObjeto s3:ObterVersãoDoObjetoAcl s3:ObterTag deVersão do Objeto s3:ColocarObjetoAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Exigirá que o objeto existente tenha a chave e o valor de tag específicos.
s3:max-chaves	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro max-keys especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:object-lock-remaining-retention-days	s3:ColocarObjeto	Compara com a data de retenção especificada no x-amz-object-lock-retain-until-date cabeçalho de solicitação ou calculado a partir do período de retenção padrão do bucket para garantir que esses valores estejam dentro do intervalo permitido para as seguintes solicitações: • ColocarObjeto • CopiarObjeto • CriarMultipartUpload

Chaves de condição	Ações	Descrição
s3:object-lock-remaining-retention-days	s3:PutObjectRetention	Compara com a data de retenção especificada na solicitação PutObjectRetention para garantir que esteja dentro do intervalo permitido.
s3:prefix	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro de prefixo especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:RequestObjectTag/<ch ave-tag>	s3:ColocarObjeto s3:PutObjectTagging s3:PutObjectVersionTaggi ng	Exigirá uma chave de tag e um valor específicos quando a solicitação de objeto incluir marcação.

Especificar variáveis em uma política

Você pode usar variáveis em políticas para preencher informações de políticas quando elas estiverem disponíveis. Você pode usar variáveis de política no `Resource` elemento e em comparações de strings no `Condition` elemento.

Neste exemplo, a variável `${aws:username}` faz parte do elemento `Recurso`:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

Neste exemplo, a variável `${aws:username}` faz parte do valor da condição no bloco de condição:

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

Variável	Descrição
<code>\${aws:SourceIp}</code>	Usa a chave <code>SourceIp</code> como a variável fornecida.
<code>\${aws:username}</code>	Usa a chave de nome de usuário como a variável fornecida.
<code>\${s3:prefix}</code>	Usa a chave de prefixo específica do serviço como a variável fornecida.

Variável	Descrição
<code>\$ { s3 : max - keys }</code>	Usa a chave max-keys específica do serviço como a variável fornecida.
<code>\$ { * }</code>	Caractere especial. Usa o caractere como um caractere * literal.
<code>\$ { ? }</code>	Caractere especial. Usa o caractere como um caractere literal ?.
<code>\$ { \$ }</code>	Caractere especial. Usa o caractere como um caractere \$ literal.

Crie políticas que exijam tratamento especial

Às vezes, uma política pode conceder permissões que são perigosas para a segurança ou perigosas para operações contínuas, como bloquear o usuário root da conta. A implementação da API REST do StorageGRID S3 é menos restritiva durante a validação de políticas do que a Amazon, mas igualmente rigorosa durante a avaliação de políticas.

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento do StorageGRID
Negar a si mesmo quaisquer permissões para a conta root	Balde	Válido e aplicado, mas a conta do usuário root mantém a permissão para todas as operações de política do bucket S3	Mesmo
Negar a si mesmo quaisquer permissões para usuário/grupo	Grupo	Válido e aplicado	Mesmo
Permitir qualquer permissão a um grupo de contas estrangeiras	Balde	Principal inválido	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro 405 Método Não Permitido quando permitidas por uma política
Permitir que uma conta estrangeira root ou usuário tenha qualquer permissão	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro 405 Método Não Permitido quando permitidas por uma política	Mesmo

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento do StorageGRID
Permitir que todos tenham permissão para todas as ações	Balde	Válido, mas as permissões para todas as operações de política do bucket S3 retornam um erro 405 Método Não Permitido para a raiz da conta estrangeira e usuários	Mesmo
Negar a todos permissões para todas as ações	Balde	Válido e aplicado, mas a conta do usuário root mantém a permissão para todas as operações de política do bucket S3	Mesmo
Principal é um usuário ou grupo inexistente	Balde	Principal inválido	Válido
O recurso é um bucket S3 inexistente	Grupo	Válido	Mesmo
Principal é um grupo local	Balde	Principal inválido	Válido
A política concede a uma conta não proprietária (incluindo contas anônimas) permissões para colocar objetos.	Balde	Válido. Os objetos são de propriedade da conta do criador e a política de bucket não se aplica. A conta do criador deve conceder permissões de acesso ao objeto usando ACLs de objeto.	Válido. Os objetos são de propriedade da conta do proprietário do bucket. Aplica-se a política de balde.

Proteção WORM (gravação única e leitura múltipla)

Você pode criar buckets WORM (write-once-read-many) para proteger dados, metadados de objetos definidos pelo usuário e marcação de objetos do S3. Configure os buckets WORM para permitir a criação de novos objetos e evitar substituições ou exclusões de conteúdo existente. Use uma das abordagens descritas aqui.

Para garantir que as substituições sejam sempre negadas, você pode:

- No Grid Manager, vá para **CONFIGURAÇÃO > Segurança > Configurações de segurança > Rede e objetos** e marque a caixa de seleção **Impedir modificação do cliente**.
- Aplique as seguintes regras e políticas do S3:
 - Adicione uma operação PutOverwriteObject DENY à política S3.
 - Adicione uma operação DeleteObject DENY à política S3.
 - Adicione uma operação PutObject ALLOW à política S3.



Definir DeleteObject como DENY em uma política do S3 não impede que o ILM exclua objetos quando existe uma regra como "zero cópias após 30 dias".



Mesmo quando todas essas regras e políticas são aplicadas, elas não protegem contra gravações simultâneas (veja Situação A). Eles protegem contra sobrescritas sequenciais concluídas (veja Situação B).

Situação A: Gravações simultâneas (não protegidas)

```
/mybucket/important.doc  
PUT#1 ---> OK  
PUT#2 -----> OK
```

Situação B: Substituições sequenciais concluídas (protegidas contra)

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

Informações relacionadas

- ["Como as regras do StorageGRID ILM gerenciam objetos"](#)
- ["Exemplos de políticas de bucket"](#)
- ["Exemplo de políticas de grupo"](#)
- ["Gerenciar objetos com ILM"](#)
- ["Use uma conta de inquilino"](#)

Exemplos de políticas de bucket

Use os exemplos nesta seção para criar políticas de acesso do StorageGRID para buckets.

As políticas de bucket especificam as permissões de acesso para o bucket ao qual a política está anexada. Você configura uma política de bucket usando a API PutBucketPolicy do S3 por meio de uma destas ferramentas:

- ["Gerente de inquilinos"](#) .
- AWS CLI usando este comando (consulte ["Operações em baldes"](#)):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy  
file://policy.json
```

Exemplo: permitir que todos tenham acesso somente leitura a um bucket

Neste exemplo, todos, incluindo anônimos, têm permissão para listar objetos no bucket e executar operações GetObject em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que esta

política pode não ser particularmente útil porque ninguém, exceto o root da conta, tem permissão para gravar no bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ]
    }
  ]
}
```

Exemplo: permitir que todos em uma conta tenham acesso total e todos em outra conta tenham acesso somente leitura a um bucket

Neste exemplo, todos em uma conta especificada têm permissão para acesso total a um bucket, enquanto todos em outra conta especificada têm permissão apenas para listar o bucket e executar operações GetObject em objetos no bucket começando com o `shared/` prefixo de chave de objeto.



No StorageGRID, os objetos criados por uma conta não proprietária (incluindo contas anônimas) são de propriedade da conta do proprietário do bucket. A política de bucket se aplica a esses objetos.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}

```

Exemplo: permitir que todos tenham acesso somente leitura a um bucket e acesso total ao grupo especificado

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar operações GetObject em todos os objetos no bucket, enquanto apenas os usuários pertencentes ao grupo Marketing na conta especificada têm acesso total.


```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Exemplo: permitir que todos tenham acesso de leitura e gravação a um bucket se o cliente estiver no intervalo de IP

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar quaisquer operações de objeto em todos os objetos no bucket, desde que as solicitações venham de um intervalo de IP especificado (54.240.143.0 a 54.240.143.255, exceto 54.240.143.188). Todas as outras operações serão negadas, e todas as solicitações fora do intervalo de IP serão negadas.

```

{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ],
      "Condition": {
        "IpAddress": { "aws:SourceIp": "54.240.143.0/24" },
        "NotIpAddress": { "aws:SourceIp": "54.240.143.188" }
      }
    }
  ]
}

```

Exemplo: permitir acesso total a um bucket exclusivamente por um usuário federado especificado

Neste exemplo, o usuário federado Alex tem acesso total ao `examplebucket` balde e seus objetos. Todos os outros usuários, incluindo `root`, têm todas as operações explicitamente negadas. Observe, no entanto, que `root` nunca tem permissões negadas para `Put/Get/DeleteBucketPolicy`.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Exemplo: permissão PutOverwriteObject

Neste exemplo, o `Deny` O efeito para `PutOverwriteObject` e `DeleteObject` garante que ninguém possa substituir ou excluir os dados do objeto, os metadados definidos pelo usuário e a marcação de objetos do S3.

```

{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}

```

Exemplo de políticas de grupo

Use os exemplos nesta seção para criar políticas de acesso do StorageGRID para grupos.

As políticas de grupo especificam as permissões de acesso para o grupo ao qual a política está anexada. Não há `Principal` elemento na política porque está implícito. As políticas de grupo são configuradas usando o Gerenciador de Tenants ou a API.

Exemplo: definir política de grupo usando o Gerenciador de Tenants

Ao adicionar ou editar um grupo no Gerenciador de Tenants, você pode selecionar uma política de grupo para determinar quais permissões de acesso ao S3 os membros desse grupo terão. Ver ["Criar grupos para um locatário S3"](#).

- **Sem acesso S3:** opção padrão. Os usuários neste grupo não têm acesso aos recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar esta opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
- **Acesso somente leitura:** os usuários neste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários neste grupo podem listar objetos e ler dados de objetos, metadados e tags. Quando você seleciona esta opção, a string JSON para uma política de grupo somente leitura aparece na caixa de texto. Você não pode editar esta sequência.
- **Acesso total:** os usuários neste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona esta opção, a string JSON para uma política de grupo de acesso total aparece na caixa de texto. Você não pode editar esta sequência.
- **Mitigação de ransomware:** esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários neste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que tenham o controle de versão de objetos habilitado.

Usuários do Tenant Manager que têm a permissão Gerenciar todos os buckets podem substituir esta política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação Multifator (MFA) quando disponível.

- **Personalizado:** Os usuários do grupo recebem as permissões que você especifica na caixa de texto.

Exemplo: permitir acesso total do grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm permissão de acesso total a todos os buckets de propriedade da conta do locatário, a menos que seja explicitamente negado pela política de bucket.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemplo: permitir acesso somente leitura do grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm acesso somente leitura aos recursos do S3, a menos que explicitamente negado pela política de bucket. Por exemplo, os usuários neste grupo podem listar objetos e ler dados de objetos, metadados e tags.

```

{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}

```

Exemplo: permitir que os membros do grupo tenham acesso total apenas à sua "pasta" em um bucket

Neste exemplo, os membros do grupo só têm permissão para listar e acessar sua pasta específica (prefixo de chave) no bucket especificado. Observe que as permissões de acesso de outras políticas de grupo e da política de bucket devem ser consideradas ao determinar a privacidade dessas pastas.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Operações S3 rastreadas nos logs de auditoria

As mensagens de auditoria são geradas pelos serviços do StorageGRID e armazenadas em arquivos de log de texto. Você pode revisar as mensagens de auditoria específicas do S3 no log de auditoria para obter detalhes sobre as operações de bucket e objeto.

Operações de bucket rastreadas nos logs de auditoria

- CriarBucket
- ExcluirBucket
- ExcluirBucketTagging
- ExcluirObjetos
- Obter marcação de balde
- Balde de cabeça
- Objetos de Lista
- Versões do objeto de lista
- Conformidade do PUT Bucket
- Colocar marcação de balde
- Versão PutBucket

Operações de objetos rastreadas nos logs de auditoria

- Upload completo de várias partes
- CopiarObjeto
- ExcluirObjeto
- ObterObjeto
- CabeçaObjeto
- ColocarObjeto
- RestaurarObjeto
- SelecionarObjeto
- UploadPart (quando uma regra ILM usa ingestão balanceada ou restrita)
- UploadPartCopy (quando uma regra ILM usa ingestão balanceada ou estrita)

Informações relacionadas

- ["Arquivo de log de auditoria de acesso"](#)
- ["O cliente escreve mensagens de auditoria"](#)
- ["O cliente leu mensagens de auditoria"](#)

Use a API REST do Swift (fim da vida útil)

Usar a API REST do Swift

O suporte para a API Swift chegou ao fim e será removido em uma versão futura.



Os detalhes do Swift foram removidos desta versão do site de documentação. Ver ["StorageGRID 11.8: Use a API REST do Swift"](#).

Monitorar e solucionar problemas de um sistema StorageGRID

Monitorar o sistema StorageGRID

Monitorar um sistema StorageGRID

Monitore seu sistema StorageGRID regularmente para garantir que ele esteja funcionando conforme o esperado.

Antes de começar

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



Para alterar as unidades dos valores de armazenamento exibidos no Grid Manager, selecione o menu suspenso do usuário no canto superior direito do Grid Manager e selecione **Preferências do usuário**.

Sobre esta tarefa

Estas instruções descrevem como:

- ["Visualizar e gerenciar o painel"](#)
- ["Ver a página de nós"](#)
- ["Monitore estes aspectos do sistema regularmente:"](#)
 - ["Saúde do sistema"](#)
 - ["Capacidade de armazenamento"](#)
 - ["Gestão do ciclo de vida da informação"](#)
 - ["Recursos de rede e sistema"](#)
 - ["Atividade do inquilino"](#)
 - ["Operações de balanceamento de carga"](#)
 - ["Conexões de federação de rede"](#)
- ["Gerenciar alertas"](#)
- ["Ver arquivos de log"](#)
- ["Configurar mensagens de auditoria e destinos de log"](#)
- ["Use um servidor syslog externo"](#) para coletar informações de auditoria
- ["Use SNMP para monitoramento"](#)
- ["Obter dados adicionais do StorageGRID"](#), incluindo métricas e diagnósticos

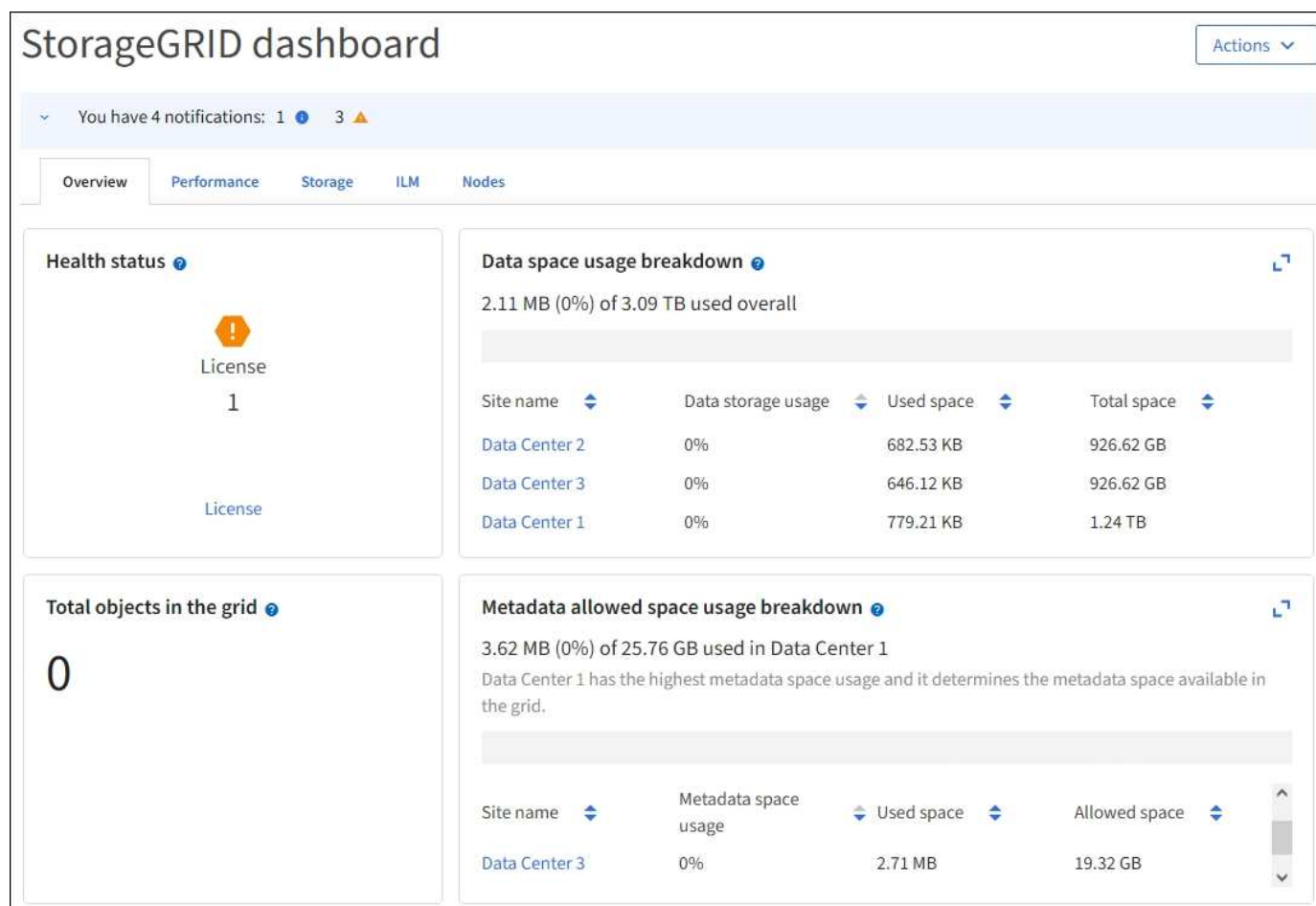
Visualizar e gerenciar o painel

Você pode usar o painel para monitorar as atividades do sistema rapidamente. Você pode criar painéis personalizados para monitorar sua implementação do StorageGRID.



Para alterar as unidades dos valores de armazenamento exibidos no Grid Manager, selecione o menu suspenso do usuário no canto superior direito do Grid Manager e selecione **Preferências do usuário**.

Seu painel pode ser diferente dependendo da configuração do sistema.



Ver o painel

O painel consiste em guias que contêm informações específicas sobre o sistema StorageGRID . Cada aba contém categorias de informações exibidas nos cartões.

Você pode usar o painel fornecido pelo sistema como está. Além disso, você pode criar painéis personalizados que contenham apenas as guias e os cartões relevantes para monitorar sua implementação do StorageGRID.

As guias do painel fornecidas pelo sistema contêm cartões com os seguintes tipos de informações:

Guia no painel fornecido pelo sistema	Contém
Visão geral	Informações gerais sobre a grade, como alertas ativos, uso de espaço e total de objetos na grade.

Guia no painel fornecido pelo sistema	Contém
Desempenho	Uso de espaço, armazenamento usado ao longo do tempo, operações S3, duração da solicitação, taxa de erro.
Armazenar	Uso de cota de locatário e uso de espaço lógico. Previsões de uso do espaço para dados e metadados do usuário.
ILM	Fila de gerenciamento do ciclo de vida da informação e taxa de avaliação.
Nós	Uso de CPU, dados e memória por nó. Operações S3 por nó. Distribuição de nó para site.

Alguns cartões podem ser maximizados para facilitar a visualização. Selecione o ícone maximizar  no canto superior direito do cartão. Para fechar um cartão maximizado, selecione o ícone de minimizar  ou selecione **Fechar**.

Gerenciar painéis

Se você tiver acesso Root (veja "[Permissões do grupo de administração](#)"), você pode executar as seguintes tarefas de gerenciamento para painéis:

- Crie um painel personalizado do zero. Você pode usar painéis personalizados para controlar quais informações do StorageGRID são exibidas e como essas informações são organizadas.
- Clone um painel para criar painéis personalizados.
- Defina um painel ativo para um usuário. O painel ativo pode ser o painel fornecido pelo sistema ou um painel personalizado.
- Defina um painel padrão, que é o que todos os usuários veem, a menos que ativem seu próprio painel.
- Editar um nome de painel.
- Edite um painel para adicionar ou remover guias e cartões. Você pode ter no mínimo 1 e no máximo 20 abas.
- Remover um painel.



Se você tiver qualquer outra permissão além do acesso Root, você só poderá definir um painel ativo.

Para gerenciar painéis, selecione **Ações > Gerenciar painéis**.



Configurar painéis

Para criar um novo painel clonando o painel ativo, selecione **Ações > Clonar painel ativo**.

Para editar ou clonar um painel existente, selecione **Ações > Gerenciar painéis**.



O painel fornecido pelo sistema não pode ser editado ou removido.

Ao configurar um painel, você pode:

- Adicionar ou remover guias
- Renomeie as guias e dê nomes exclusivos às novas guias
- Adicionar, remover ou reorganizar (arrastar) cartões para cada guia
- Selecione o tamanho dos cartões individuais selecionando **P**, **M**, **G** ou **GG** na parte superior do cartão

Site name	Data storage usage	Used space	Total space
Data Center 1	0%	1.79 MB	1.24 TB
Data Center 2	0%	921.11 KB	926.62 GB
Data Center 3	0%	790.21 KB	926.62 GB

Ver a página de nós

Ver a página de nós

Quando precisar de informações mais detalhadas sobre seu sistema StorageGRID do que o painel fornece, você pode usar a página Nós para visualizar métricas para toda a grade, cada site na grade e cada nó em um site.

A tabela Nós lista informações resumidas para toda a grade, cada site e cada nó. Se um nó estiver desconectado ou tiver um alerta ativo, um ícone aparecerá ao lado do nome do nó. Se o nó estiver conectado e não tiver alertas ativos, nenhum ícone será exibido.



Quando um nó não está conectado à rede, como durante uma atualização ou em um estado desconectado, certas métricas podem estar indisponíveis ou excluídas dos totais do site e da rede. Depois que um nó se reconectar à rede, aguarde alguns minutos para que os valores se estabilizem.



Para alterar as unidades dos valores de armazenamento exibidos no Grid Manager, selecione o menu suspenso do usuário no canto superior direito do Grid Manager e selecione **Preferências do usuário**.



As capturas de tela mostradas são exemplos. Seus resultados podem variar dependendo da versão do StorageGRID .

Nodes

View the list and status of sites and grid nodes.

Total node count: 12

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Webscale Deployment	Grid	0%	0%	—
^ DC1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	6%
DC1-ARC1	Archive Node	—	—	1%
DC1-G1	Gateway Node	—	—	3%
DC1-S1	Storage Node	0%	0%	6%
DC1-S2	Storage Node	0%	0%	8%
DC1-S3	Storage Node	0%	0%	4%

Ícones de estado de conexão

Se um nó for desconectado da grade, um dos seguintes ícones aparecerá ao lado do nome do nó.

Ícone	Descrição	Ação necessária
	Não conectado - Desconhecido Por um motivo desconhecido, um nó é desconectado ou os serviços no nó ficam inesperadamente inativos. Por exemplo, um serviço no nó pode ser interrompido, ou o nó pode ter perdido sua conexão de rede devido a uma falha de energia ou interrupção inesperada. O alerta Não foi possível comunicar com o nó também pode ser acionado. Outros alertas também podem estar ativos.	Requer atenção imediata. "Selecione cada alerta" e siga as ações recomendadas. Por exemplo, talvez seja necessário reiniciar um serviço que foi interrompido ou reiniciar o host do nó. Observação: Um nó pode aparecer como Desconhecido durante operações de desligamento gerenciado. Você pode ignorar o estado Desconhecido nesses casos.
	Não conectado - Inativo administrativamente Por um motivo esperado, o nó não está conectado à rede. Por exemplo, o nó, ou os serviços no nó, foram desligados corretamente, o nó está sendo reinicializado ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos. Com base no problema subjacente, esses nós geralmente voltam a ficar online sem intervenção.	Determine se algum alerta está afetando este nó. Se um ou mais alertas estiverem ativos, "Selecione cada alerta" e siga as ações recomendadas.

Se um nó estiver desconectado da rede, poderá haver um alerta subjacente, mas somente o ícone "Não conectado" aparecerá. Para ver os alertas ativos de um nó, selecione o nó.

Ícones de alerta

Se houver um alerta ativo para um nó, um dos seguintes ícones aparecerá ao lado do nome do nó:

 **Crítico:** Existe uma condição anormal que interrompeu as operações normais de um nó ou serviço do StorageGRID . Você deve resolver o problema subjacente imediatamente. Pode haver interrupção do serviço e perda de dados se o problema não for resolvido.

 **Principal:** Existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não interrompa a operação normal de um nó ou serviço do StorageGRID .

 **Menor:** O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se continuar. Você deve monitorar e resolver alertas menores que não desaparecem sozinhos para garantir que eles não resultem em um problema mais sério.

Exibir detalhes de um sistema, site ou nó

Para filtrar as informações mostradas na tabela Nós, insira uma sequência de pesquisa no campo **Pesquisar**. Você pode pesquisar por nome do sistema, nome de exibição ou tipo (por exemplo, digite **gat** para localizar rapidamente todos os nós de gateway).

Para visualizar as informações da grade, site ou nó:

- Selecione o nome da grade para ver um resumo agregado das estatísticas de todo o seu sistema StorageGRID .
- Selecione um site de data center específico para ver um resumo agregado das estatísticas de todos os nós naquele site.
- Selecione um nó específico para visualizar informações detalhadas sobre ele.

Exibir a guia Visão geral

A guia Visão geral fornece informações básicas sobre cada nó. Ele também mostra todos os alertas que estão afetando o nó no momento.

A guia Visão geral é exibida para todos os nós.

Informações do nó

A seção Informações do nó da guia Visão geral lista informações básicas sobre o nó.

NYC-ADM1 (Primary Admin Node) [↗](#)

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Load balancer](#) [Tasks](#)

Node information [?](#)

Display name:	NYC-ADM1
System name:	DC1-ADM1
Type:	Primary Admin Node
ID:	3adb1aa8-9c7a-4901-8074-47054aa06ae6
Connection state:	✔ Connected
Software version:	11.7.0
IP addresses:	10.96.105.85 - eth0 (Grid Network)

[Show additional IP addresses](#) [▼](#)

As informações gerais de um nó incluem o seguinte:

- **Nome de exibição** (mostrado somente se o nó tiver sido renomeado): O nome de exibição atual do nó. Use o "[Renomear grade, sites e nós](#)" procedimento para atualizar este valor.
- **Nome do sistema**: O nome que você inseriu para o nó durante a instalação. Os nomes do sistema são usados para operações internas do StorageGRID e não podem ser alterados.
- **Tipo**: O tipo de nó — Nó de administração, Nó de administração primário, Nó de armazenamento ou Nó de gateway.
- **ID**: O identificador exclusivo do nó, também conhecido como UUID.
- **Estado da conexão**: Um dos três estados. O ícone para o estado mais grave é mostrado.

- **Desconhecido***  : Por um motivo desconhecido, o nó não está conectado à rede ou um ou mais serviços estão inesperadamente inativos. Por exemplo, a conexão de rede entre os nós foi perdida, a energia caiu ou um serviço caiu. O alerta ***Não foi possível comunicar com o nó** também pode ser acionado. Outros alertas também podem estar ativos. Esta situação requer atenção imediata.



Um nó pode aparecer como Desconhecido durante operações de desligamento gerenciado. Você pode ignorar o estado Desconhecido nesses casos.

- ***Administrativamente inativo***  : O nó não está conectado à rede por um motivo esperado. Por exemplo, o nó, ou os serviços no nó, foram desligados corretamente, o nó está sendo reinicializado ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos.

- ***Conectado***  : O nó está conectado à rede.

- **Armazenamento usado**: somente para nós de armazenamento.
 - **Dados do objeto**: A porcentagem do espaço total utilizável para dados do objeto que foi usada no nó de armazenamento.
 - **Metadados do objeto**: A porcentagem do espaço total permitido para metadados do objeto que foi usada no nó de armazenamento.
- **Versão do software**: A versão do StorageGRID que está instalada no nó.
- **Grupos HA**: somente para nós de administração e nós de gateway. Mostrado se uma interface de rede no nó está incluída em um grupo de alta disponibilidade e se essa interface é a interface primária.
- **Endereços IP**: Endereços IP do nó. Clique em **Mostrar endereços IP adicionais** para visualizar os endereços IPv4 e IPv6 do nó e os mapeamentos de interface.

Alertas

A seção Alertas da guia Visão geral lista qualquer ["alertas que atualmente afetam este nó e que não foram silenciados"](#) . Selecione o nome do alerta para ver detalhes adicionais e ações recomendadas.

Alerts			
Alert name 	Severity 	Time triggered 	Current values
Low installed node memory  The amount of installed memory on a node is low.	 Critical	11 hours ago 	Total RAM size: 8.37 GB

Alertas também estão incluídos para "estados de conexão do nó" .

Ver a aba Hardware

A guia Hardware exibe a utilização da CPU e da memória para cada nó, além de informações adicionais de hardware sobre os dispositivos.



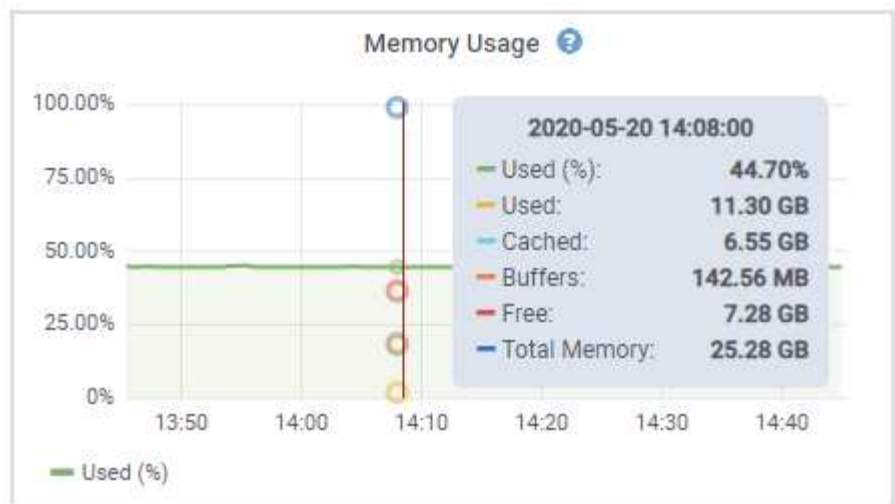
O Grid Manager é atualizado a cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

A guia Hardware é exibida para todos os nós.



Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.

Para ver detalhes sobre a utilização da CPU e da memória, posicione o cursor sobre cada gráfico.



Se o nó for um nó de dispositivo, esta guia também incluirá uma seção com mais informações sobre o hardware do dispositivo.

Exibir informações sobre nós de armazenamento do dispositivo

A página Nós lista informações sobre a integridade do serviço e todos os recursos computacionais, de dispositivo de disco e de rede para cada nó de armazenamento do dispositivo. Você também pode ver memória, hardware de armazenamento, versão de firmware do controlador, recursos de rede, interfaces de rede, endereços de rede e receber e transmitir dados.

Passos

1. Na página Nós, selecione um Nó de Armazenamento do dispositivo.
2. Selecione **Visão geral**.

A seção Informações do nó da guia Visão geral exibe informações resumidas do nó, como nome, tipo, ID e estado da conexão. A lista de endereços IP inclui o nome da interface para cada endereço, da seguinte forma:

- **eth**: Rede Grid, Rede Admin ou Rede Cliente.
- **soluço**: Uma das portas físicas de 10, 25 ou 100 GbE no dispositivo. Essas portas podem ser vinculadas e conectadas à StorageGRID Grid Network (eth0) e à Client Network (eth2).
- **mtc**: Uma das portas físicas de 1 GbE no dispositivo. Uma ou mais interfaces mtc são vinculadas para formar a interface de rede de administração do StorageGRID (eth1). Você pode deixar outras interfaces mtc disponíveis para conectividade local temporária para um técnico no data center.

DC2-SGA-010-096-106-021 (Storage Node) [↗](#)



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

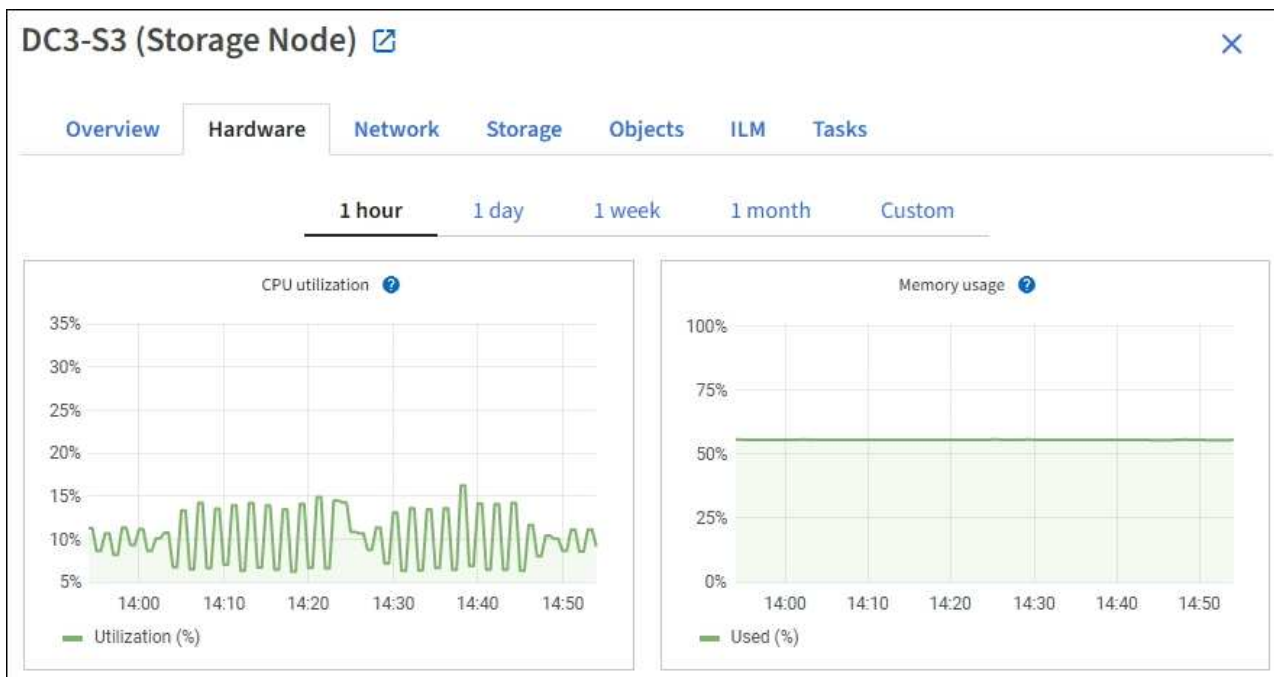
Alerts

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.			

A seção Alertas da guia Visão geral exibe todos os alertas ativos para o nó.

3. Selecione **Hardware** para ver mais informações sobre o aparelho.

- Visualize os gráficos de Utilização da CPU e Memória para determinar as porcentagens de uso da CPU e da memória ao longo do tempo. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.



- b. Role para baixo para ver a tabela de componentes do aparelho. Esta tabela contém informações como o nome do modelo do dispositivo; nomes dos controladores, números de série e endereços IP; e o status de cada componente.



Alguns campos, como IP do BMC do controlador de computação e Hardware de computação, aparecem somente para dispositivos com esse recurso.

Os componentes das prateleiras de armazenamento e das prateleiras de expansão, se fizerem parte da instalação, aparecem em uma tabela separada abaixo da tabela do aparelho.

StorageGRID Appliance

Appliance model:	SG6060	
Storage controller name:	StorageGRID-Lab79-SG6060-7-134	
Storage controller A management IP:	10.2	
Storage controller B management IP:	10.2	
Storage controller WWID:	6d039ea0000173e50000000065b7b761	
Storage appliance chassis serial number:	721924500068	
Storage controller firmware version:	08.53.00.09	
Storage controller SANtricity OS version:	11.50.3R2	
Storage controller NVSRAM version:	N280X-853834-DG1	
Storage hardware:	Nominal	
Storage controller failed drive count:	0	
Storage controller A:	Nominal	
Storage controller B:	Nominal	
Storage controller power supply A:	Nominal	
Storage controller power supply B:	Nominal	
Storage data drive type:	NL-SAS HDD	
Storage data drive size:	4.00 TB	
Storage RAID mode:	DDP16	
Storage connectivity:	Nominal	
Overall power supply:	Degraded	
Compute controller BMC IP:	10.2	
Compute controller serial number:	721917500060	
Compute hardware:	Needs Attention	
Compute controller CPU temperature:	Nominal	
Compute controller chassis temperature:	Nominal	
Compute controller power supply A:	Failed	
Compute controller power supply B:	Nominal	

Storage shelves

Shelf chassis serial number	Shelf ID	Shelf status	IOM status	Power supply status	Drawer status	Fan status
721924500068	99	Nominal	N/A	Nominal	Nominal	Nominal

Campo na tabela Appliance	Descrição
Modelo do aparelho	O número do modelo deste dispositivo StorageGRID mostrado no SANtricity OS.
Nome do controlador de armazenamento	O nome deste dispositivo StorageGRID mostrado no SANtricity OS.
Controlador de armazenamento Um IP de gerenciamento	Endereço IP para a porta de gerenciamento 1 no controlador de armazenamento A. Use esse IP para acessar o SANtricity OS para solucionar problemas de armazenamento.
IP de gerenciamento do controlador de armazenamento B	Endereço IP para a porta de gerenciamento 1 no controlador de armazenamento B. Use esse IP para acessar o SANtricity OS para solucionar problemas de armazenamento. Alguns modelos de aparelhos não possuem um controlador de armazenamento B.

Campo na tabela Appliance	Descrição
Controlador de armazenamento WWID	O identificador mundial do controlador de armazenamento mostrado no SANtricity OS.
Número de série do chassi do dispositivo de armazenamento	O número de série do chassi do aparelho.
Versão do firmware do controlador de armazenamento	A versão do firmware no controlador de armazenamento para este dispositivo.
Controlador de armazenamento SANtricity versão do sistema operacional	A versão do controlador de armazenamento A do SANtricity OS.
Versão NVSRAM do controlador de armazenamento	Versão NVSRAM do controlador de armazenamento, conforme relatado pelo SANtricity System Manager. Para o SG6060 e o SG6160, se houver uma incompatibilidade de versão NVSRAM entre os dois controladores, a versão do controlador A será exibida. Se o controlador A não estiver instalado ou operacional, a versão do controlador B será exibida.
Hardware de armazenamento	O status geral do hardware do controlador de armazenamento. Se o SANtricity System Manager relatar um status de Necessita de Atenção para o hardware de armazenamento, o sistema StorageGRID também relatará esse valor. Se o status for "precisa de atenção", primeiro verifique o controlador de armazenamento usando o SANtricity OS. Em seguida, certifique-se de que não haja outros alertas aplicáveis ao controlador de computação.
Contagem de unidades com falha no controlador de armazenamento	O número de unidades que não são ideais.
Controlador de armazenamento A	O status do controlador de armazenamento A.
Controlador de armazenamento B	O status do controlador de armazenamento B. Alguns modelos de dispositivos não têm um controlador de armazenamento B.
Fonte de alimentação do controlador de armazenamento A	O status da fonte de alimentação A para o controlador de armazenamento.
Fonte de alimentação do controlador de armazenamento B	O status da fonte de alimentação B para o controlador de armazenamento.

Campo na tabela Appliance	Descrição
Tipo de unidade de armazenamento de dados	O tipo de unidades no dispositivo, como HDD (disco rígido) ou SSD (unidade de estado sólido).
Tamanho da unidade de armazenamento de dados	O tamanho efetivo de uma unidade de dados. No SG6160, o tamanho da unidade de cache também é exibido. Observação: Para nós com prateleiras de expansão, use o Tamanho da unidade de dados para cada prateleira em vez de. O tamanho efetivo da unidade pode variar de acordo com a prateleira.
Modo RAID de armazenamento	O modo RAID configurado para o dispositivo.
Conectividade de armazenamento	O estado de conectividade de armazenamento.
Fonte de alimentação geral	O status de todas as fontes de alimentação do aparelho.
Controlador de computação BMC IP	O endereço IP da porta do controlador de gerenciamento da placa base (BMC) no controlador de computação. Use esse IP para se conectar à interface BMC para monitorar e diagnosticar o hardware do dispositivo. Este campo não é exibido para modelos de aparelhos que não contêm um BMC.
Calcular o número de série do controlador	O número de série do controlador de computação.
Hardware de computação	O status do hardware do controlador de computação. Este campo não é exibido para modelos de dispositivos que não têm hardware de computação e hardware de armazenamento separados.
Controlador de computação de temperatura da CPU	O status da temperatura da CPU do controlador de computação.
Calcular a temperatura do chassi do controlador	O status da temperatura do controlador de computação.

+

Coluna na mesa de prateleiras de armazenamento	Descrição
Número de série do chassi da prateleira	O número de série do chassi da prateleira de armazenamento.

Coluna na mesa de prateleiras de armazenamento	Descrição
ID da prateleira	O identificador numérico da prateleira de armazenamento. • 99: Prateleira do controlador de armazenamento • 0: Primeira prateleira de expansão • 1: Segunda prateleira de expansão Observação: Prateleiras de expansão se aplicam somente ao SG6060 e SG6160.
Status da prateleira	O status geral da prateleira de armazenamento.
Status da OIM	O status dos módulos de entrada/saída (IOMs) em quaisquer prateleiras de expansão. N/A se esta não for uma prateleira de expansão.
Status da fonte de alimentação	Status geral das fontes de alimentação da prateleira de armazenamento.
Status da gaveta	O status das gavetas na prateleira de armazenamento. N/A se a prateleira não contiver gavetas.
Status do fã	O status geral dos ventiladores de resfriamento na prateleira de armazenamento.
Slots de unidade	O número total de slots de unidade na prateleira de armazenamento.
Unidades de dados	O número de unidades na prateleira de armazenamento que são usadas para armazenamento de dados.
Tamanho da unidade de dados	O tamanho efetivo de uma unidade de dados na prateleira de armazenamento.
Unidades de cache	O número de unidades na prateleira de armazenamento que são usadas como cache.
Tamanho da unidade de cache	O tamanho da menor unidade de cache na prateleira de armazenamento. Normalmente, todas as unidades de cache têm o mesmo tamanho.
Status da configuração	O status de configuração da prateleira de armazenamento.

a. Confirme se todos os status são "Nominais".

Se um status não for "Nominal", revise todos os alertas atuais. Você também pode usar o SANtricity System Manager para saber mais sobre alguns desses valores de hardware. Consulte as instruções

de instalação e manutenção do seu aparelho.

4. Selecione **Rede** para visualizar informações de cada rede.

O gráfico Tráfego de rede fornece um resumo do tráfego geral da rede.



- a. Revise a seção Interfaces de rede.

Network interfaces					
Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

Use a tabela a seguir com os valores na coluna **Velocidade** na tabela Interfaces de rede para determinar se as portas de rede 10/25 GbE no dispositivo foram configuradas para usar o modo ativo/de backup ou o modo LACP.



Os valores mostrados na tabela pressupõem que todos os quatro links sejam usados.

Modo de link	Modo de ligação	Velocidade de link HIC individual (hic1, hic2, hic3, hic4)	Velocidade esperada da rede de grade/cliente (eth0,eth2)
Agregar	LACP	25	100
Fixo	LACP	25	50
Fixo	Ativo/Backup	25	25
Agregar	LACP	10	40
Fixo	LACP	10	20

Modo de link	Modo de ligação	Velocidade de link HIC individual (hic1, hic2, hic3, hic4)	Velocidade esperada da rede de grade/cliente (eth0,eth2)
Fixo	Ativo/Backup	10	10

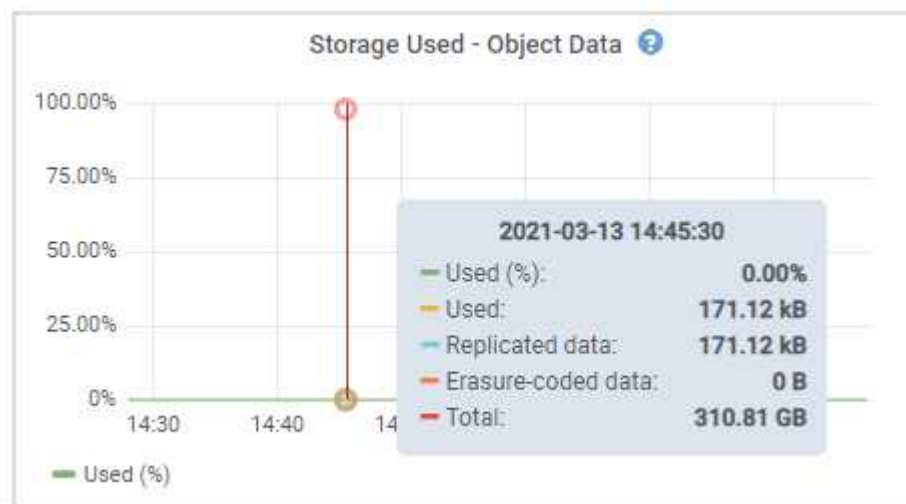
Ver "[Configurar links de rede](#)" para obter mais informações sobre como configurar as portas 10/25-GbE.

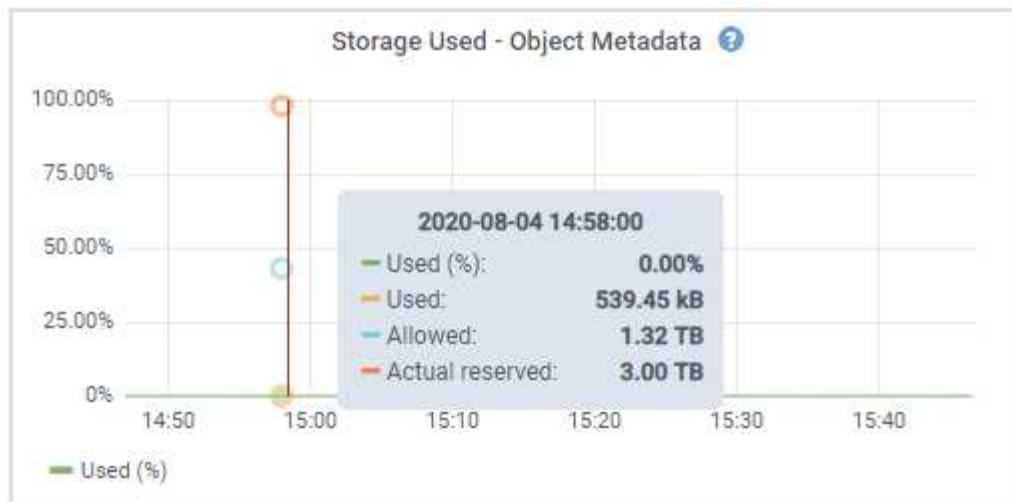
b. Revise a seção Comunicação de rede.

As tabelas de recebimento e transmissão mostram quantos bytes e pacotes foram recebidos e enviados por cada rede, bem como outras métricas de recebimento e transmissão.

Network communication						
Receive						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Frame overruns ?	Frames ?
eth0	2.89 GB	19,421,503	0	24,032	0	0
Transmit						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Collisions ?	Carrier ?
eth0	3.64 GB	18,494,381	0	0	0	0

5. Selecione **Armazenamento** para visualizar gráficos que mostram as porcentagens de armazenamento usadas ao longo do tempo para dados de objetos e metadados de objetos, bem como informações sobre dispositivos de disco, volumes e armazenamentos de objetos.





- a. Role para baixo para ver as quantidades de armazenamento disponíveis para cada volume e armazenamento de objetos.

O Nome Mundial de cada disco corresponde ao identificador mundial do volume (WWID) que aparece quando você visualiza as propriedades de volume padrão no SANtricity OS (o software de gerenciamento conectado ao controlador de armazenamento do dispositivo).

Para ajudar você a interpretar estatísticas de leitura e gravação de disco relacionadas aos pontos de montagem de volume, a primeira parte do nome mostrada na coluna **Nome** da tabela Dispositivos de disco (ou seja, *sdc*, *sdd*, *sde* e assim por diante) corresponde ao valor mostrado na coluna **Dispositivo** da tabela Volumes.

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.75 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB 	Enabled

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB 	124.60 KB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

Exibir informações sobre nós de administração e nós de gateway do dispositivo

A página Nós lista informações sobre a integridade do serviço e todos os recursos computacionais, de dispositivo de disco e de rede para cada dispositivo de serviço usado como um Nó de administração ou um Nó de gateway. Você também pode ver memória, hardware de armazenamento, recursos de rede, interfaces de rede, endereços de rede e receber e transmitir dados.

Passos

1. Na página Nós, selecione um Nó de administração do dispositivo ou um Nó de gateway do dispositivo.
2. Selecione **Visão geral**.

A seção Informações do nó da guia Visão geral exibe informações resumidas do nó, como nome, tipo, ID e estado da conexão. A lista de endereços IP inclui o nome da interface para cada endereço, da seguinte

forma:

- **adllb** e **adlli**: Mostrados se a vinculação ativa/de backup for usada para a interface de rede de administração
- **eth**: Rede Grid, Rede Admin ou Rede Cliente.
- **solução**: Uma das portas físicas de 10, 25 ou 100 GbE no dispositivo. Essas portas podem ser vinculadas e conectadas à StorageGRID Grid Network (eth0) e à Client Network (eth2).
- **mtc**: Uma das portas físicas de 1 GbE no dispositivo. Uma ou mais interfaces mtc são vinculadas para formar a interface de rede de administração (eth1). Você pode deixar outras interfaces mtc disponíveis para conectividade local temporária para um técnico no data center.

10-224-6-199-ADM1 (Primary Admin Node) [🔗](#)

Overview

Hardware

Network

Storage

Load balancer

Tasks

SANtricity System Manager

Node information [?](#)

Name:

10-224-6-199-ADM1

Type:

Primary Admin Node

ID:

6fdc1890-ca0a-4493-acdd-72ed317d95fb

Connection state:

🟢

Connected

Software version:

11.6.0 (build 20210928.1321.6687ee3)

IP addresses:

172.16.6.199 - eth0 (Grid Network)

10.224.6.199 - eth1 (Admin Network)

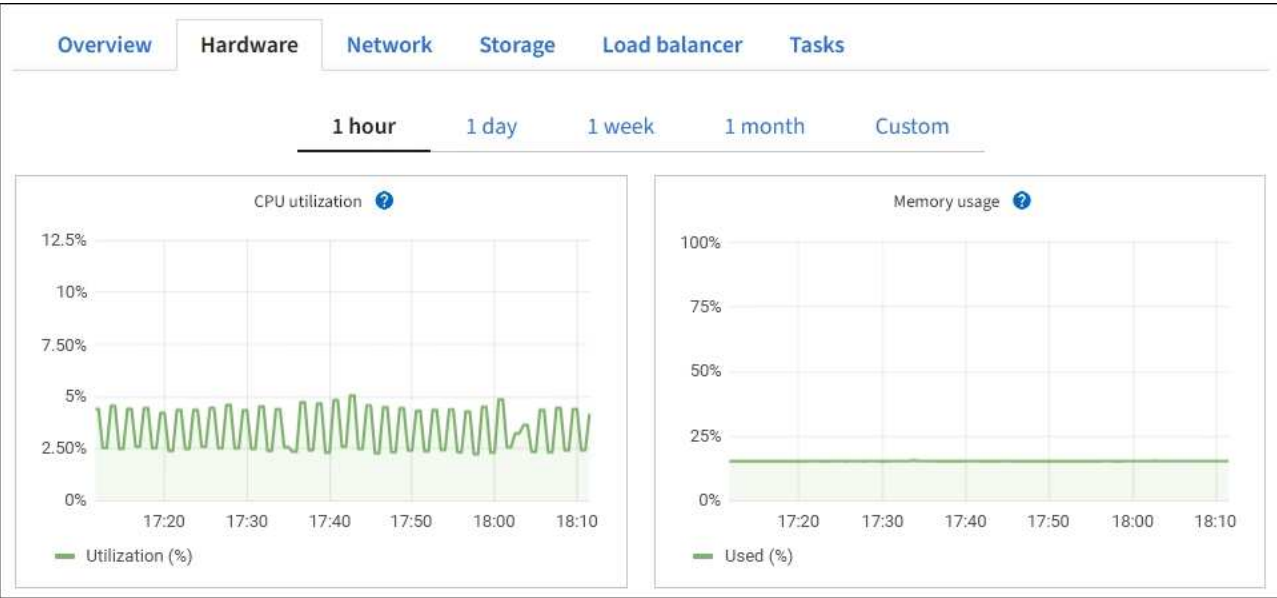
47.47.7.241 - eth2 (Client Network)

[Hide additional IP addresses ^](#)

Interface ↕	IP address ↕
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

A seção Alertas da guia Visão geral exibe todos os alertas ativos para o nó.

3. Selecione **Hardware** para ver mais informações sobre o aparelho.
 - a. Visualize os gráficos de Utilização da CPU e Memória para determinar as porcentagens de uso da CPU e da memória ao longo do tempo. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.



b. Role para baixo para ver a tabela de componentes do aparelho. Esta tabela contém informações como nome do modelo, número de série, versão do firmware do controlador e o status de cada componente.

StorageGRID Appliance		
Appliance model: ?	SG100	
Storage controller failed drive count: ?	0	
Storage data drive type: ?	SSD	
Storage data drive size: ?	960.20 GB	
Storage RAID mode: ?	RAID1 [healthy]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller BMC IP: ?	10.60.8.38	
Compute controller serial number: ?	372038000093	
Compute hardware: ?	Nominal	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Nominal	
Compute controller power supply B: ?	Nominal	

Campo na tabela Appliance	Descrição
Modelo do aparelho	O número do modelo deste dispositivo StorageGRID .

Campo na tabela Appliance	Descrição
Contagem de unidades com falha no controlador de armazenamento	O número de unidades que não são ideais.
Tipo de unidade de armazenamento de dados	O tipo de unidades no dispositivo, como HDD (disco rígido) ou SSD (unidade de estado sólido).
Tamanho da unidade de armazenamento de dados	O tamanho efetivo de uma unidade de dados.
Modo RAID de armazenamento	O modo RAID do dispositivo.
Fonte de alimentação geral	O status de todas as fontes de alimentação do aparelho.
Controlador de computação BMC IP	O endereço IP da porta do controlador de gerenciamento da placa base (BMC) no controlador de computação. Você pode usar esse IP para se conectar à interface BMC para monitorar e diagnosticar o hardware do dispositivo. Este campo não é exibido para modelos de aparelhos que não contêm um BMC.
Calcular o número de série do controlador	O número de série do controlador de computação.
Hardware de computação	O status do hardware do controlador de computação.
Controlador de computação de temperatura da CPU	O status da temperatura da CPU do controlador de computação.
Calcular a temperatura do chassi do controlador	O status da temperatura do controlador de computação.

a. Confirme se todos os status são "Nominais".

Se um status não for "Nominal", revise todos os alertas atuais.

4. Selecione **Rede** para visualizar informações de cada rede.

O gráfico Tráfego de rede fornece um resumo do tráfego geral da rede.



a. Revise a seção Interfaces de rede.

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
eth1	B4:A9:FC:71:68:36	Gigabit	Full	Off	Up
eth2	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
hic1	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic2	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic3	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic4	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
mtc1	B4:A9:FC:71:68:36	Gigabit	Full	On	Up
mtc2	B4:A9:FC:71:68:35	Gigabit	Full	On	Up

Use a tabela a seguir com os valores na coluna **Velocidade** na tabela Interfaces de rede para determinar se as quatro portas de rede 40/100 GbE no dispositivo foram configuradas para usar o modo ativo/de backup ou o modo LACP.



Os valores mostrados na tabela pressupõem que todos os quatro links sejam usados.

Modo de link	Modo de ligação	Velocidade de link HIC individual (hic1, hic2, hic3, hic4)	Velocidade esperada da rede de grade/cliente (eth0, eth2)
Agregar	LACP	100	400
Fixo	LACP	100	200
Fixo	Ativo/Backup	100	100
Agregar	LACP	40	160
Fixo	LACP	40	80
Fixo	Ativo/Backup	40	40

b. Revise a seção Comunicação de rede.

As tabelas de recebimento e transmissão mostram quantos bytes e pacotes foram recebidos e enviados por cada rede, bem como outras métricas de recebimento e transmissão.

Network communication

Receive

Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Frame overruns ?	Frames ?
eth0	2.89 GB	19,421,503	0	24,032	0	0

Transmit

Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Collisions ?	Carrier ?
eth0	3.64 GB	18,494,381	0	0	0	0

5. Selecione **Armazenamento** para visualizar informações sobre os dispositivos de disco e volumes no dispositivo de serviços.

Disk devices

Name ? ↕	World Wide Name ? ↕	I/O load ? ↕	Read rate ? ↕	Write rate ? ↕
croot(8:1,sda1)	N/A	0.02%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.03%	0 bytes/s	6 KB/s

Volumes

Mount point ? ↕	Device ? ↕	Status ? ↕	Size ? ↕	Available ? ↕	Write cache status ? ↕
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	84.63 GB 	Unknown

Ver a aba Rede

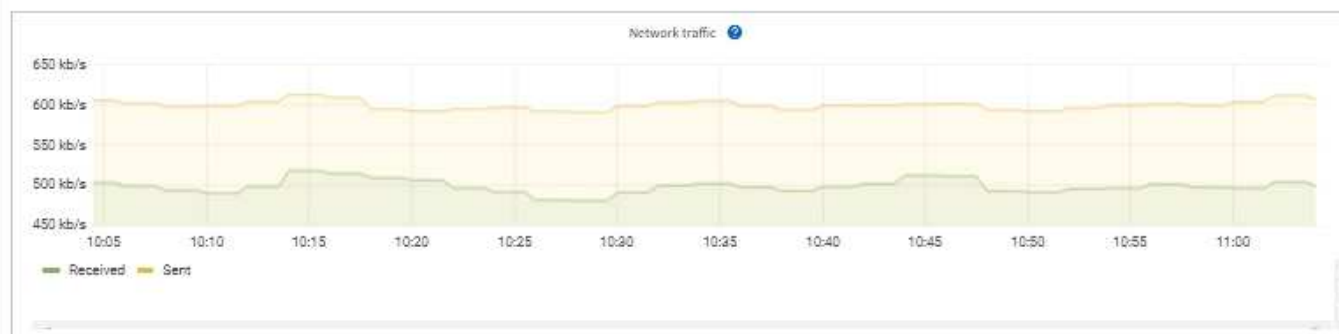
A guia Rede exibe um gráfico mostrando o tráfego de rede recebido e enviado por todas as interfaces de rede no nó, site ou grade.

A guia Rede é exibida para todos os nós, cada site e toda a grade.

Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.

Para nós, a tabela Interfaces de rede fornece informações sobre as portas de rede física de cada nó. A tabela de comunicações de rede fornece detalhes sobre as operações de recepção e transmissão de cada nó e quaisquer contadores de falhas relatados pelo driver.

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

Informações relacionadas

["Monitore as conexões e o desempenho da rede"](#)

Ver a aba Armazenamento

A guia Armazenamento resume a disponibilidade de armazenamento e outras métricas de armazenamento.

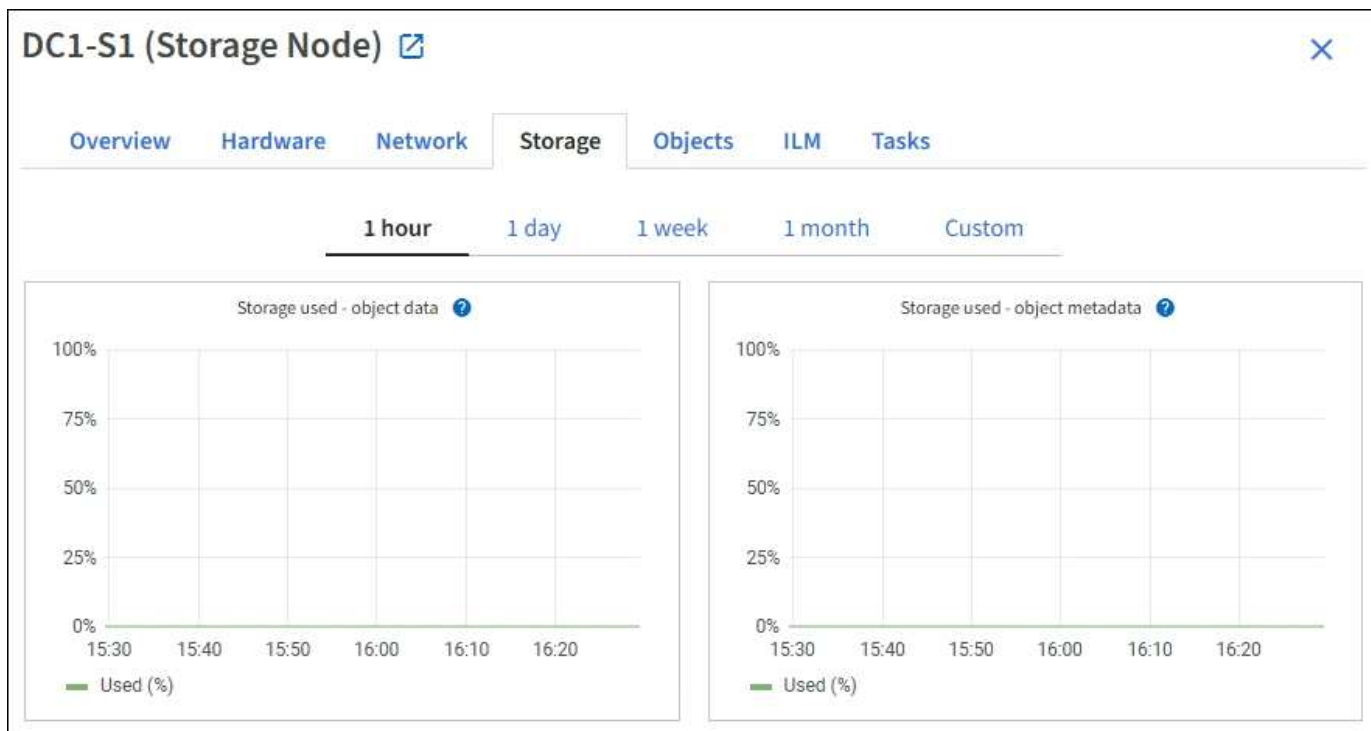
A guia Armazenamento é exibida para todos os nós, cada site e toda a grade.

Gráficos de armazenamento usados

Para nós de armazenamento, cada site e toda a grade, a guia Armazenamento inclui gráficos que mostram quanto armazenamento foi usado por dados de objeto e metadados de objeto ao longo do tempo.



Quando um nó não está conectado à rede, como durante uma atualização ou em um estado desconectado, certas métricas podem estar indisponíveis ou excluídas dos totais do site e da rede. Depois que um nó se reconectar à rede, aguarde alguns minutos para que os valores se estabilizem.



Dispositivos de disco, volumes e tabelas de armazenamento de objetos

Para todos os nós, a guia Armazenamento contém detalhes dos dispositivos de disco e volumes no nó. Para nós de armazenamento, a tabela Object Stores fornece informações sobre cada volume de armazenamento.

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.75 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB 	Enabled

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB 	124.60 KB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

Informações relacionadas

["Monitorar capacidade de armazenamento"](#)

Ver a aba Objetos

A guia Objetos fornece informações sobre ["Taxas de ingestão e recuperação do S3"](#) .

A guia Objetos é exibida para cada nó de armazenamento, cada site e toda a grade. Para nós de armazenamento, a guia Objetos também fornece contagens de objetos e informações sobre consultas de metadados e verificação de antecedentes.

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Object counts

Total objects: ? 1,295

Lost objects: ? 0

S3 buckets and Swift containers: ? 161

Metadata store queries

Average latency: ? 10.00 milliseconds

Queries - successful: ? 14,587

Queries - failed (timed out): ? 0

Queries - failed (consistency level unmet): ? 0

Verification

Status: ? No errors

Percent complete: ? 47.14%

Average stat time: ? 0.00 microseconds

Objects verified: ? 0

Object verification rate: ? 0.00 objects / second

Data verified: ? 0 bytes

Data verification rate: ? 0.00 bytes / second

Missing objects: ? 0

Corrupt objects: ? 0

Corrupt objects unidentified: ? 0

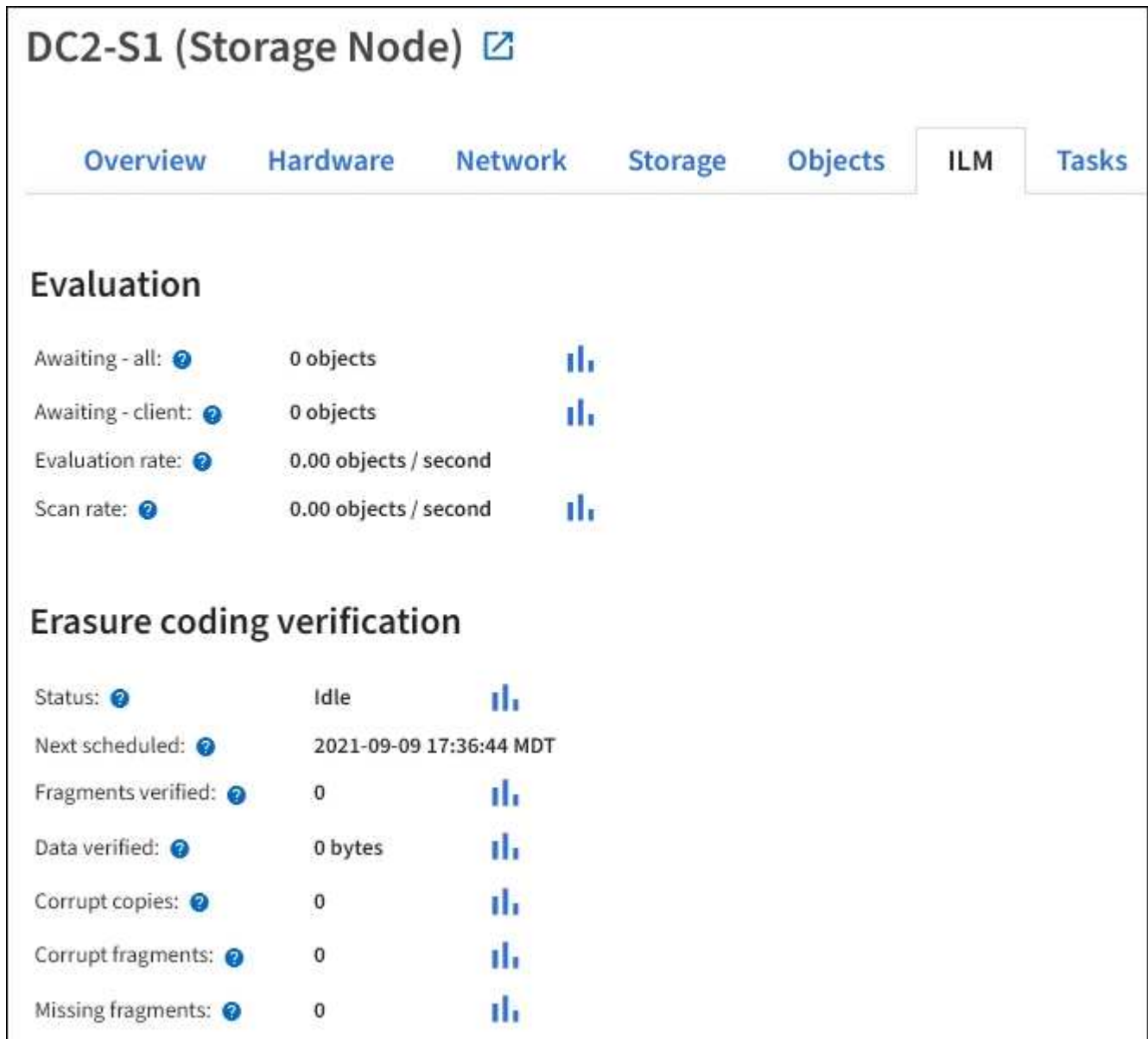
Quarantined objects: ? 0

Ver a aba ILM

A guia ILM fornece informações sobre operações de gerenciamento do ciclo de vida das informações (ILM).

A guia ILM é exibida para cada nó de armazenamento, cada site e toda a grade. Para cada site e grade, a guia ILM mostra um gráfico da fila do ILM ao longo do tempo. Para a grade, esta guia também fornece o tempo estimado para concluir uma varredura ILM completa de todos os objetos.

Para nós de armazenamento, a guia ILM fornece detalhes sobre a avaliação do ILM e a verificação em segundo plano para objetos codificados para eliminação.



Informações relacionadas

- ["Monitorar o gerenciamento do ciclo de vida das informações"](#)
- ["Administrar StorageGRID"](#)

Use a aba Tarefas

A guia Tarefas é exibida para todos os nós. Você pode usar esta guia para renomear ou reinicializar um nó ou colocar um nó do dispositivo no modo de manutenção.

Para obter os requisitos e instruções completos para cada opção nesta guia, consulte o seguinte:

- ["Renomear grade, sites e nós"](#)
- ["Reinicializar nó de grade"](#)
- ["Coloque o aparelho em modo de manutenção"](#)

Exibir a guia Balanceador de carga

A guia Balanceador de Carga inclui gráficos de desempenho e diagnóstico relacionados à operação do serviço Balanceador de Carga.

A guia Balanceador de Carga é exibida para Nós de Administração e Nós de Gateway, cada site e toda a grade. Para cada site, a guia Balanceador de Carga fornece um resumo agregado das estatísticas de todos os nós naquele site. Para toda a grade, a guia Balanceador de Carga fornece um resumo agregado das estatísticas de todos os sites.

Se não houver E/S sendo executada pelo serviço Load Balancer, ou se não houver nenhum balanceador de carga configurado, os gráficos exibirão "Nenhum dado".



Solicitar tráfego

Este gráfico fornece uma média móvel de 3 minutos da taxa de transferência de dados transmitidos entre os pontos de extremidade do balanceador de carga e os clientes que fazem as solicitações, em bits por segundo.



Este valor é atualizado na conclusão de cada solicitação. Como resultado, esse valor pode ser diferente da taxa de transferência em tempo real em taxas de solicitação baixas ou para solicitações de duração muito longa. Você pode consultar a aba Rede para ter uma visão mais realista do comportamento atual da rede.

Taxa de solicitação de entrada

Este gráfico fornece uma média móvel de 3 minutos do número de novas solicitações por segundo, divididas por tipo de solicitação (GET, PUT, HEAD e DELETE). Este valor é atualizado quando os cabeçalhos de uma nova solicitação são validados.

Duração média da solicitação (sem erro)

Este gráfico fornece uma média móvel de 3 minutos de durações de solicitações, divididas por tipo de solicitação (GET, PUT, HEAD e DELETE). Cada duração de solicitação começa quando um cabeçalho de solicitação é analisado pelo serviço Load Balancer e termina quando o corpo de resposta completo é

retornado ao cliente.

Taxa de resposta de erro

Este gráfico fornece uma média móvel de 3 minutos do número de respostas de erro retornadas aos clientes por segundo, divididas pelo código de resposta de erro.

Informações relacionadas

- ["Monitorar operações de balanceamento de carga"](#)
- ["Administrar StorageGRID"](#)

Ver a aba Serviços da plataforma

A guia Serviços da plataforma fornece informações sobre quaisquer operações de serviço da plataforma S3 em um site.

A aba Serviços da plataforma é exibida para cada site. Esta guia fornece informações sobre os serviços da plataforma S3, como a replicação do CloudMirror e o serviço de integração de pesquisa. Os gráficos nesta guia exibem métricas como o número de solicitações pendentes, a taxa de conclusão da solicitação e a taxa de falha da solicitação.

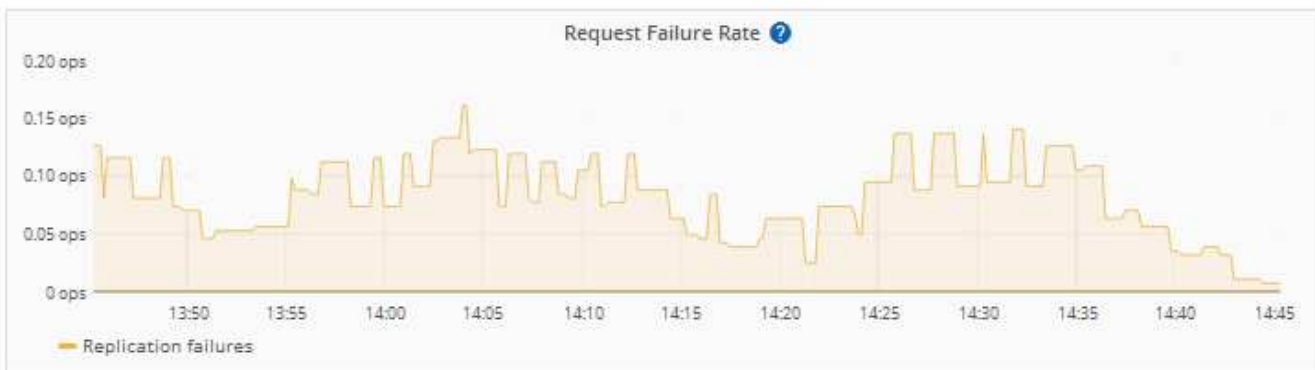
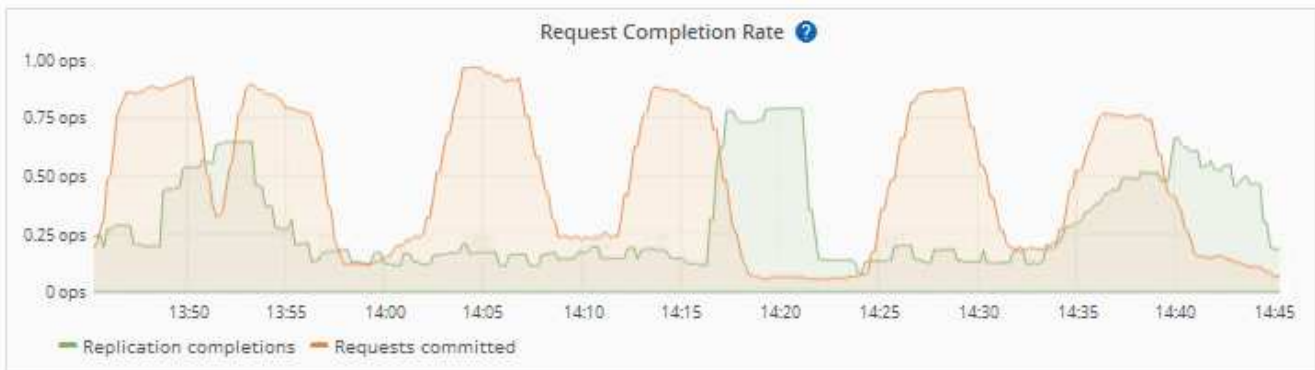
1 hour

1 day

1 week

1 month

Custom



Para obter mais informações sobre os serviços da plataforma S3, incluindo detalhes de solução de problemas, consulte o ["instruções para administrar o StorageGRID"](#).

Exibir a guia Gerenciar unidades

A guia Gerenciar unidades permite que você acesse detalhes e execute tarefas de solução de problemas e manutenção em unidades nos dispositivos que oferecem suporte a esse recurso.

Usando a guia Gerenciar unidades, você pode fazer o seguinte:

- Visualize um layout das unidades de armazenamento de dados no dispositivo
- Veja uma tabela que lista cada local da unidade, tipo, status, versão do firmware e número de série
- Executar funções de solução de problemas e manutenção em cada unidade

Para acessar a aba Gerenciar unidades, você deve ter o ["Permissão de acesso root ou de administrador do dispositivo de armazenamento"](#) .

Para obter informações sobre como usar a guia Gerenciar unidades, consulte ["Use a guia Gerenciar unidades"](#) .

Exibir a guia SANtricity System Manager (somente Série E)

A guia SANtricity System Manager permite que você acesse o SANtricity System Manager sem precisar configurar ou conectar a porta de gerenciamento do dispositivo de armazenamento. Você pode usar esta guia para revisar diagnósticos de hardware e informações ambientais, bem como problemas relacionados às unidades.



O acesso ao SANtricity System Manager a partir do Grid Manager geralmente serve apenas para monitorar o hardware do dispositivo e configurar o E-Series AutoSupport. Muitos recursos e operações do SANtricity System Manager, como atualização de firmware, não se aplicam ao monitoramento do seu dispositivo StorageGRID . Para evitar problemas, siga sempre as instruções de manutenção de hardware do seu aparelho. Para atualizar o firmware do SANtricity , consulte o ["Procedimentos de configuração de manutenção"](#) para seu dispositivo de armazenamento.



A guia SANtricity System Manager é exibida somente para nós de dispositivos de armazenamento que usam hardware da Série E.

Usando o SANtricity System Manager, você pode fazer o seguinte:

- Visualize dados de desempenho, como desempenho em nível de matriz de armazenamento, latência de E/S, utilização de CPU do controlador de armazenamento e taxa de transferência.
- Verifique o status do componente de hardware.
- Execute funções de suporte, incluindo visualização de dados de diagnóstico e configuração do E-Series AutoSupport.



Para usar o SANtricity System Manager para configurar um proxy para o E-Series AutoSupport, consulte ["Enviar pacotes E-Series AutoSupport por meio do StorageGRID"](#) .

Para acessar o SANtricity System Manager por meio do Grid Manager, você deve ter o ["Permissão de acesso root ou de administrador do dispositivo de armazenamento"](#) .



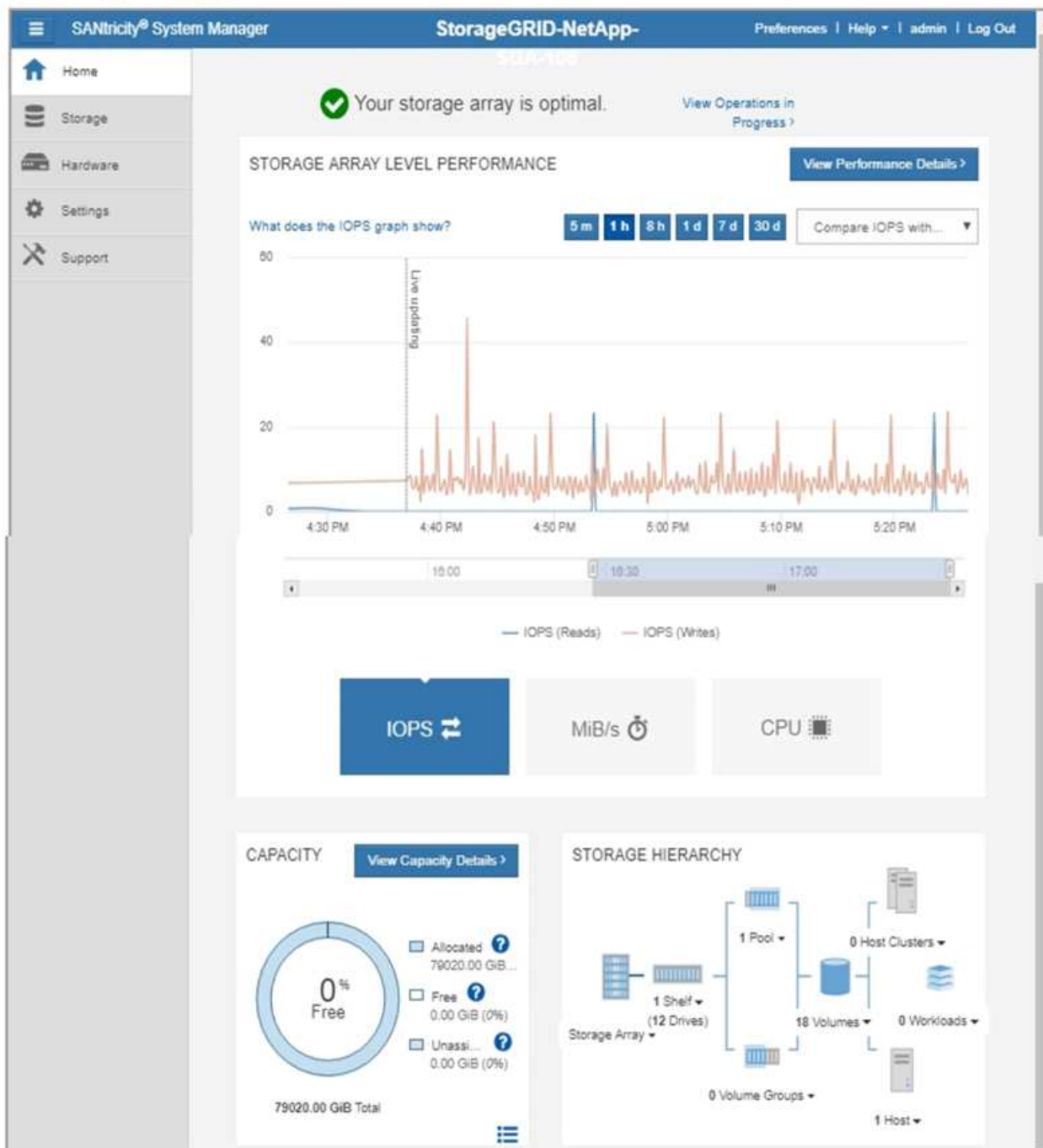
Você deve ter o firmware SANtricity 8.70 ou superior para acessar o SANtricity System Manager usando o Grid Manager.

A guia exibe a página inicial do SANtricity System Manager.

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

Note: Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open [SANtricity System Manager](#) in a new browser tab.



Você pode usar o link do SANtricity System Manager para abrir o SANtricity System Manager em uma nova janela do navegador para facilitar a visualização.

Para ver detalhes sobre o desempenho do nível de matriz de armazenamento e o uso da capacidade,

posicione o cursor sobre cada gráfico.

Para obter mais detalhes sobre como visualizar as informações acessíveis na guia SANtricity System Manager, consulte ["Documentação do NetApp E-Series e SANtricity"](#).

Informações para monitorar regularmente

O que e quando monitorar

Mesmo que o sistema StorageGRID possa continuar a operar quando ocorrerem erros ou partes da rede estiverem indisponíveis, você deve monitorar e resolver possíveis problemas antes que eles afetem a eficiência ou a disponibilidade da rede.

Antes de começar

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

Sobre tarefas de monitoramento

Um sistema ocupado gera grandes quantidades de informações. A lista a seguir fornece orientação sobre as informações mais importantes a serem monitoradas continuamente.

O que monitorar	Frequência
"Status de saúde do sistema"	Diário
Taxa na qual "Capacidade de objetos e metadados do nó de armazenamento" está sendo consumido	Semanalmente
"Operações de gerenciamento do ciclo de vida da informação"	Semanalmente
"Recursos de rede e sistema"	Semanalmente
"Atividade do inquilino"	Semanalmente
"Operações do cliente S3"	Semanalmente
"Operações de balanceamento de carga"	Após a configuração inicial e após quaisquer alterações de configuração
"Conexões de federação de rede"	Semanalmente

Monitorar a saúde do sistema

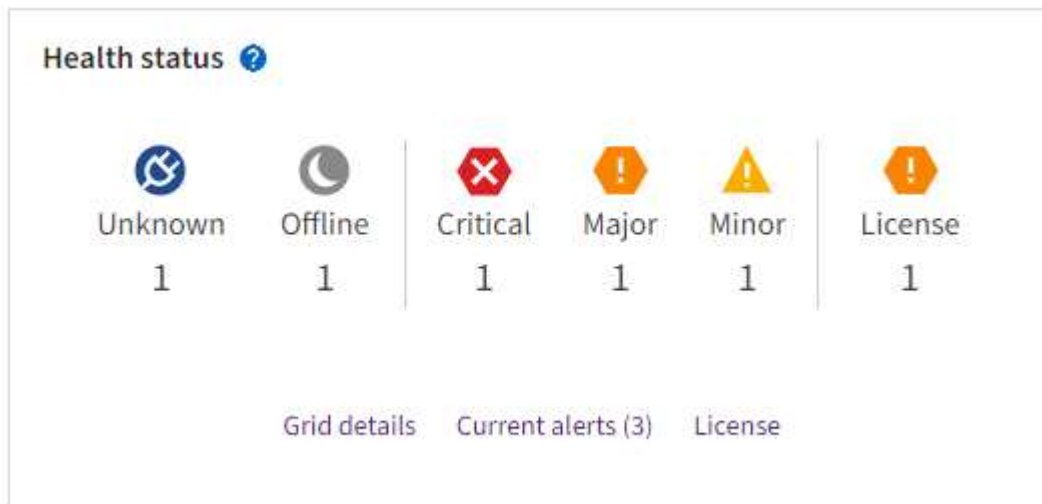
Monitore a saúde geral do seu sistema StorageGRID diariamente.

Sobre esta tarefa

O sistema StorageGRID pode continuar a operar quando partes da rede não estiverem disponíveis. Possíveis problemas indicados por alertas não são necessariamente problemas com operações do sistema. Investigue

os problemas resumidos no cartão de status de integridade do painel do Grid Manager.

Para ser notificado sobre alertas assim que eles forem acionados, você pode ["configurar notificações por e-mail para alertas"](#) ou ["configurar armadilhas SNMP"](#) .



Quando há problemas, aparecem links que permitem visualizar detalhes adicionais:

Link	Aparece quando...
Detalhes da grade	Todos os nós estão desconectados (estado de conexão Desconhecido ou Administrativamente Inativo).
Alertas atuais (crítico, grave, secundário)	Os alertas são atualmente ativo .
Alertas resolvidos recentemente	Alertas acionados na semana passada agora estão resolvidos .
Licença	Há um problema com a licença de software para este sistema StorageGRID . Você pode "atualizar informações de licença conforme necessário" .

Monitorar estados de conexão de nós

Se um ou mais nós forem desconectados da grade, operações críticas do StorageGRID poderão ser afetadas. Monitore os estados de conexão dos nós e resolva quaisquer problemas imediatamente.

Ícone	Descrição	Ação necessária
	Não conectado - Desconhecido Por um motivo desconhecido, um nó é desconectado ou os serviços no nó ficam inesperadamente inativos. Por exemplo, um serviço no nó pode ser interrompido, ou o nó pode ter perdido sua conexão de rede devido a uma falha de energia ou interrupção inesperada. O alerta Não foi possível comunicar com o nó também pode ser acionado. Outros alertas também podem estar ativos.	Requer atenção imediata. Selecione cada alerta e siga as ações recomendadas. Por exemplo, talvez seja necessário reiniciar um serviço que foi interrompido ou reiniciar o host do nó. Observação: Um nó pode aparecer como Desconhecido durante operações de desligamento gerenciado. Você pode ignorar o estado Desconhecido nesses casos.
	Não conectado - Inativo administrativamente Por um motivo esperado, o nó não está conectado à rede. Por exemplo, o nó, ou os serviços no nó, foram desligados corretamente, o nó está sendo reinicializado ou o software está sendo atualizado. Um ou mais alertas também podem estar ativos. Com base no problema subjacente, esses nós geralmente voltam a ficar online sem intervenção.	Determine se algum alerta está afetando este nó. Se um ou mais alertas estiverem ativos, selecione cada alerta e siga as ações recomendadas.
	Conectado O nó está conectado à rede.	Nenhuma ação necessária.

Ver alertas atuais e resolvidos

Alertas atuais: Quando um alerta é acionado, um ícone de alerta é exibido no painel. Um ícone de alerta também é exibido para o nó na página Nós. Se "[notificações de alerta por e-mail são configuradas](#)", uma notificação por e-mail também será enviada, a menos que o alerta tenha sido silenciado.

Alertas resolvidos: Você pode pesquisar e visualizar um histórico de alertas que foram resolvidos.

Opcionalmente, você assistiu ao vídeo: "[Vídeo: Visão geral dos alertas](#)"



A tabela a seguir descreve as informações mostradas no Grid Manager para alertas atuais e resolvidos.

Cabeçalho da coluna	Descrição
Nome ou título	O nome do alerta e sua descrição.
Gravidade	A gravidade do alerta. Para alertas atuais, se vários alertas forem agrupados, a linha de título mostrará quantas instâncias desse alerta estão ocorrendo em cada gravidade.  Crítico: Existe uma condição anormal que interrompeu as operações normais de um nó ou serviço do StorageGRID . Você deve resolver o problema subjacente imediatamente. Pode haver interrupção do serviço e perda de dados se o problema não for resolvido.  Principal: Existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não interrompa a operação normal de um nó ou serviço do StorageGRID .  Menor: O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se continuar. Você deve monitorar e resolver alertas menores que não desaparecem sozinhos para garantir que eles não resultem em um problema mais sério.
Tempo acionado	Alertas atuais: A data e a hora em que o alerta foi disparado no seu horário local e em UTC. Se vários alertas forem agrupados, a linha de título mostrará os horários da instância mais recente do alerta (<i>newest</i>) e da instância mais antiga do alerta (<i>oldest</i>). Alertas resolvidos: Há quanto tempo o alerta foi disparado.
Site/Nó	O nome do site e do nó onde o alerta está ocorrendo ou ocorreu.
Status	Se o alerta está ativo, silenciado ou resolvido. Se vários alertas forem agrupados e Todos os alertas for selecionado no menu suspenso, a linha de título mostrará quantas instâncias desse alerta estão ativas e quantas instâncias foram silenciadas.

Cabeçalho da coluna	Descrição
Tempo resolvido (somente alertas resolvidos)	Há quanto tempo o alerta foi resolvido.
Valores atuais ou <i>valores de dados</i>	O valor da métrica que fez com que o alerta fosse acionado. Para alguns alertas, valores adicionais são mostrados para ajudar você a entender e investigar o alerta. Por exemplo, os valores mostrados para um alerta de Armazenamento de dados de objeto baixo incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado. Observação: Se vários alertas atuais forem agrupados, os valores atuais não serão exibidos na linha de título.
Valores acionados (somente alertas resolvidos)	O valor da métrica que fez com que o alerta fosse acionado. Para alguns alertas, valores adicionais são mostrados para ajudar você a entender e investigar o alerta. Por exemplo, os valores mostrados para um alerta de Armazenamento de dados de objeto baixo incluem a porcentagem de espaço em disco usado, a quantidade total de espaço em disco e a quantidade de espaço em disco usado.

Passos

1. Selecione o link **Alertas atuais** ou **Alertas resolvidos** para visualizar uma lista de alertas nessas categorias. Você também pode visualizar os detalhes de um alerta selecionando **Nós > nó > Visão geral** e, em seguida, selecionando o alerta na tabela Alertas.

Por padrão, os alertas atuais são mostrados da seguinte forma:

- Os alertas disparados mais recentemente são mostrados primeiro.
- Vários alertas do mesmo tipo são exibidos como um grupo.
- Alertas que foram silenciados não são exibidos.
- Para um alerta específico em um nó específico, se os limites forem atingidos para mais de uma gravidade, somente o alerta mais grave será mostrado. Ou seja, se os limites de alerta forem atingidos para as gravidades menor, maior e crítica, somente o alerta crítico será exibido.

A página Alertas atuais é atualizada a cada dois minutos.

2. Para expandir grupos de alertas, selecione o cursor para baixo ▼ . Para recolher alertas individuais em um grupo, selecione o cursor para cima ▲ , ou selecione o nome do grupo.
3. Para exibir alertas individuais em vez de grupos de alertas, desmarque a caixa de seleção **Alertas de grupo**.
4. Para classificar alertas atuais ou grupos de alertas, selecione as setas para cima/baixo ⬆️ em cada cabeçalho de coluna.
 - Quando **Alertas de grupo** é selecionado, tanto os grupos de alertas quanto os alertas individuais dentro de cada grupo são classificados. Por exemplo, você pode querer classificar os alertas em um grupo por **Tempo de acionamento** para encontrar a instância mais recente de um alerta específico.
 - Quando **Alertas de grupo** é limpo, toda a lista de alertas é classificada. Por exemplo, você pode querer classificar todos os alertas por **Nó/Site** para ver todos os alertas que afetam um nó específico.
5. Para filtrar alertas atuais por status (**Todos os alertas**, **Ativos** ou **Silenciados**, use o menu suspenso na

parte superior da tabela.

Ver ["Silenciar notificações de alerta"](#) .

6. Para classificar alertas resolvidos:

- Selecione um período de tempo no menu suspenso **Quando acionado**.
- Selecione uma ou mais gravidades no menu suspenso **Gravidade**.
- Selecione uma ou mais regras de alerta padrão ou personalizadas no menu suspenso **Regra de alerta** para filtrar alertas resolvidos relacionados a uma regra de alerta específica.
- Selecione um ou mais nós no menu suspenso **Nó** para filtrar alertas resolvidos relacionados a um nó específico.

7. Para visualizar detalhes de um alerta específico, selecione o alerta. Uma caixa de diálogo fornece detalhes e ações recomendadas para o alerta selecionado.

8. (Opcional) Para um alerta específico, selecione silenciar este alerta para silenciar a regra de alerta que causou o disparo deste alerta.

Você deve ter o ["Gerenciar alertas ou permissão de acesso root"](#) para silenciar uma regra de alerta.



Tenha cuidado ao decidir silenciar uma regra de alerta. Se uma regra de alerta for silenciada, você poderá não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

9. Para visualizar as condições atuais da regra de alerta:

- a. Nos detalhes do alerta, selecione **Exibir condições**.

Um pop-up aparece, listando a expressão do Prometheus para cada gravidade definida.

- b. Para fechar o pop-up, clique em qualquer lugar fora dele.

10. Opcionalmente, selecione **Editar regra** para editar a regra de alerta que causou o disparo deste alerta.

Você deve ter o ["Gerenciar alertas ou permissão de acesso root"](#) para editar uma regra de alerta.



Tenha cuidado ao decidir editar uma regra de alerta. Se você alterar os valores do gatilho, talvez não seja possível detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

11. Para fechar os detalhes do alerta, selecione **Fechar**.

Monitorar capacidade de armazenamento

Monitore o espaço total utilizável disponível para garantir que o sistema StorageGRID não fique sem espaço de armazenamento para objetos ou para metadados de objetos.

O StorageGRID armazena dados de objetos e metadados de objetos separadamente e reserva uma quantidade específica de espaço para um banco de dados Cassandra distribuído que contém metadados de objetos. Monitore a quantidade total de espaço consumido por objetos e metadados de objetos, bem como tendências na quantidade de espaço consumido por cada um. Isso permitirá que você planeje com antecedência a adição de nós e evite interrupções de serviço.

Você pode ["ver informações sobre capacidade de armazenamento"](#) para toda a grade, para cada site e para

cada nó de armazenamento no seu sistema StorageGRID .

Monitorar a capacidade de armazenamento de toda a rede

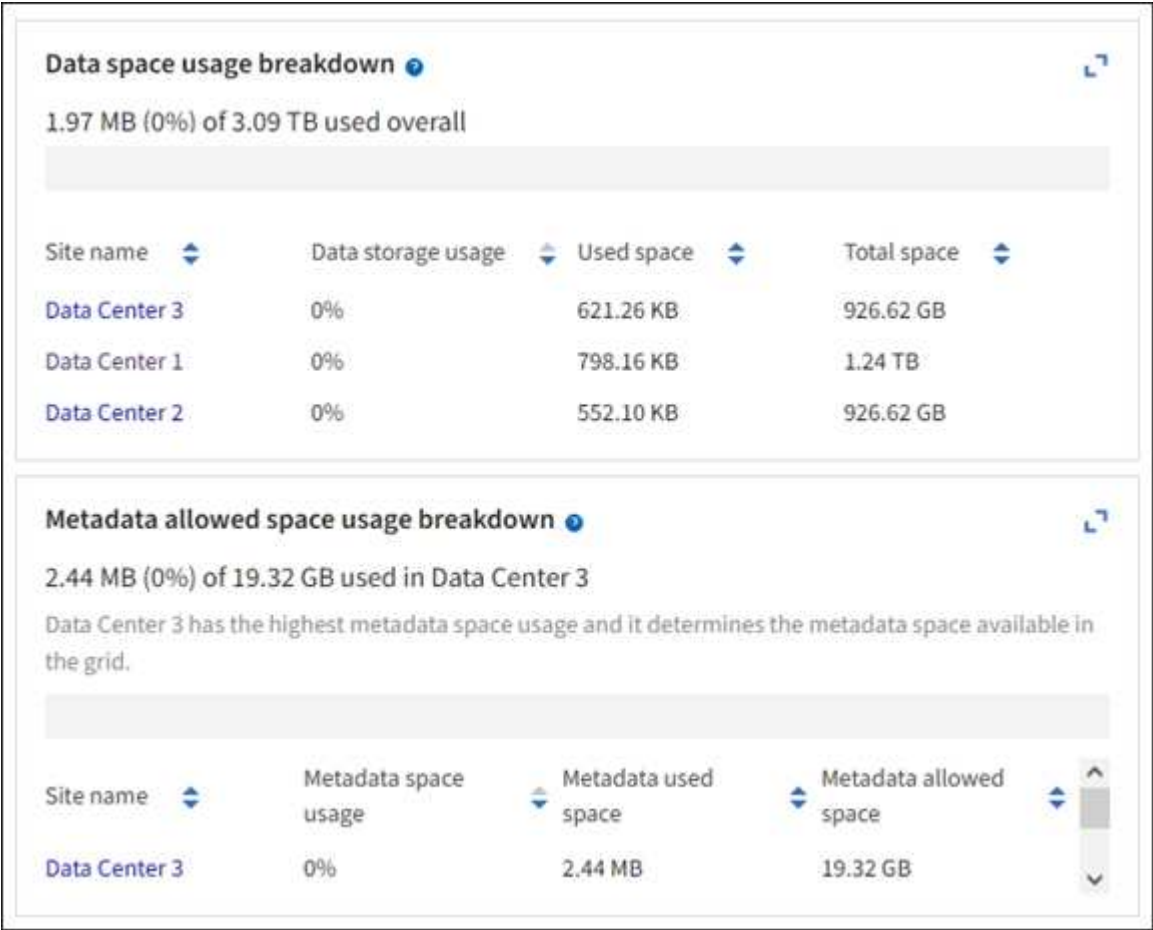
Monitore a capacidade geral de armazenamento da sua grade para garantir que haja espaço livre adequado para dados e metadados de objetos. Entender como a capacidade de armazenamento muda ao longo do tempo pode ajudar você a planejar a adição de nós de armazenamento ou volumes de armazenamento antes que a capacidade de armazenamento utilizável da grade seja consumida.

O painel do Grid Manager permite que você avalie rapidamente quanto armazenamento está disponível para toda a grade e para cada data center. A página Nós fornece valores mais detalhados para dados de objetos e metadados de objetos.

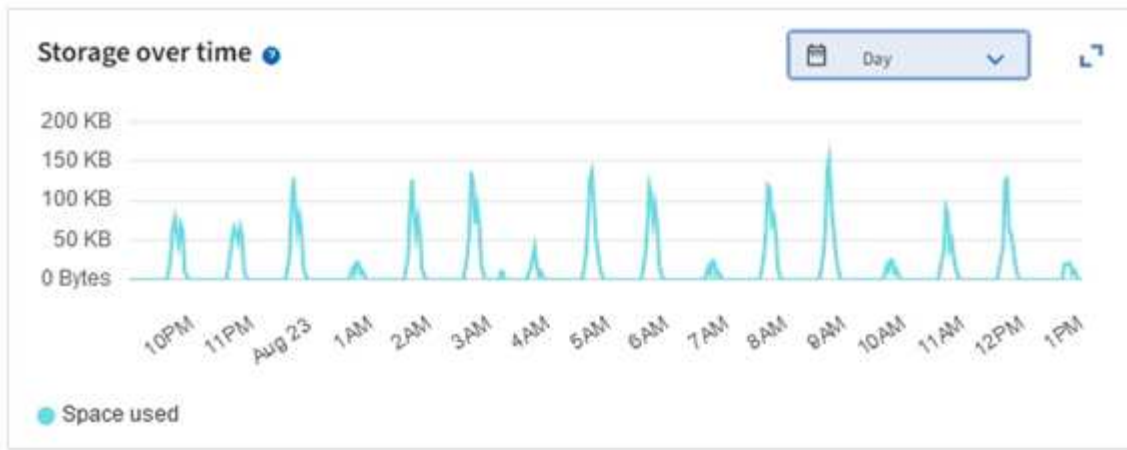
Passos

- 1. Avalie quanto armazenamento está disponível para toda a grade e para cada data center.
 - a. Selecione **Painel > Visão geral**.
 - b. Observe os valores nos cartões Detalhamento do uso do espaço de dados e Detalhamento do uso do espaço permitido de metadados. Cada cartão lista uma porcentagem de uso de armazenamento, a capacidade de espaço usado e o espaço total disponível ou permitido pelo site.

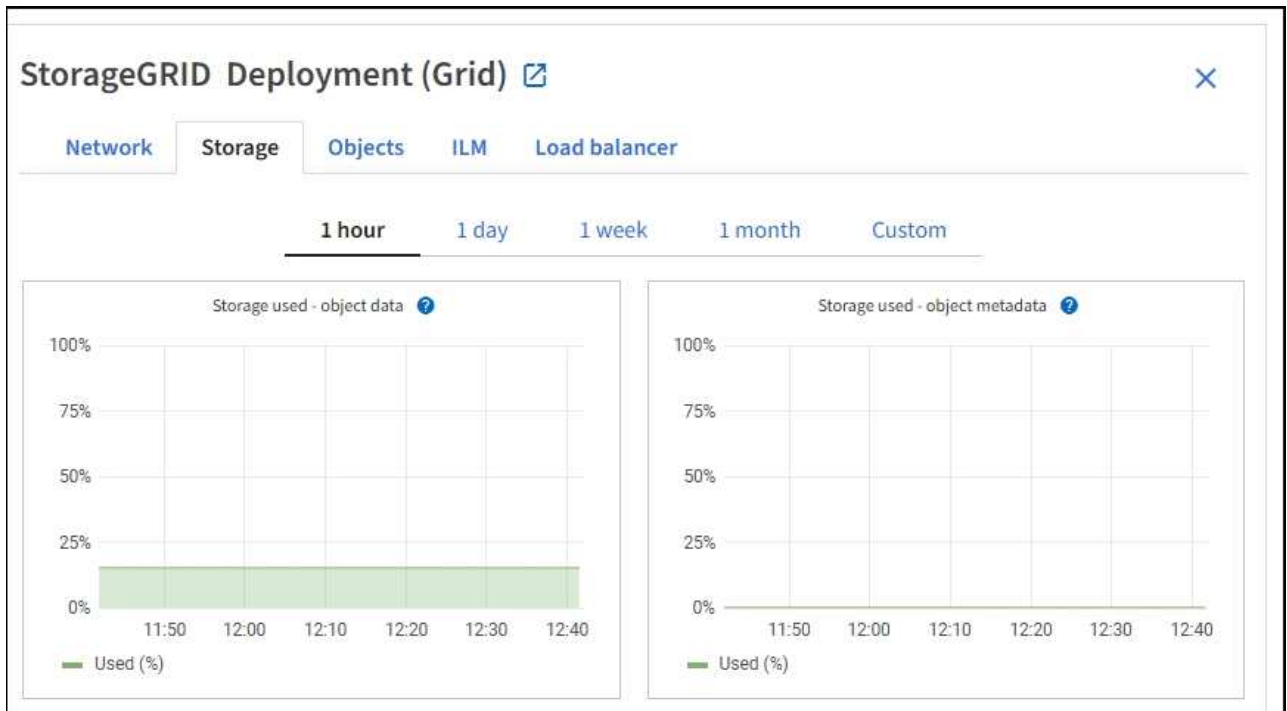
 O resumo não inclui média de arquivo.



- a. Observe o gráfico no cartão Armazenamento ao longo do tempo. Use o menu suspenso de período de tempo para ajudar a determinar a rapidez com que o armazenamento é consumido.



2. Use a página Nós para obter detalhes adicionais sobre quanto armazenamento foi usado e quanto armazenamento permanece disponível na grade para dados de objetos e metadados de objetos.
 - a. Selecione **NODES**.
 - b. Selecione **grid > Armazenamento**.



- c. Posicione o cursor sobre os gráficos **Armazenamento usado - dados do objeto** e **Armazenamento usado - metadados do objeto** para ver quanto armazenamento de objeto e armazenamento de metadados do objeto está disponível para toda a grade e quanto foi usado ao longo do tempo.



Os valores totais de um site ou da grade não incluem nós que não relataram métricas por pelo menos cinco minutos, como nós offline.

3. Planeje executar uma expansão para adicionar nós de armazenamento ou volumes de armazenamento antes que a capacidade de armazenamento utilizável da grade seja consumida.

Ao planejar o momento de uma expansão, considere quanto tempo levará para adquirir e instalar armazenamento adicional.



Se sua política de ILM usar codificação de eliminação, talvez você prefira expandir quando os nós de armazenamento existentes estiverem aproximadamente 70% cheios para reduzir o número de nós que devem ser adicionados.

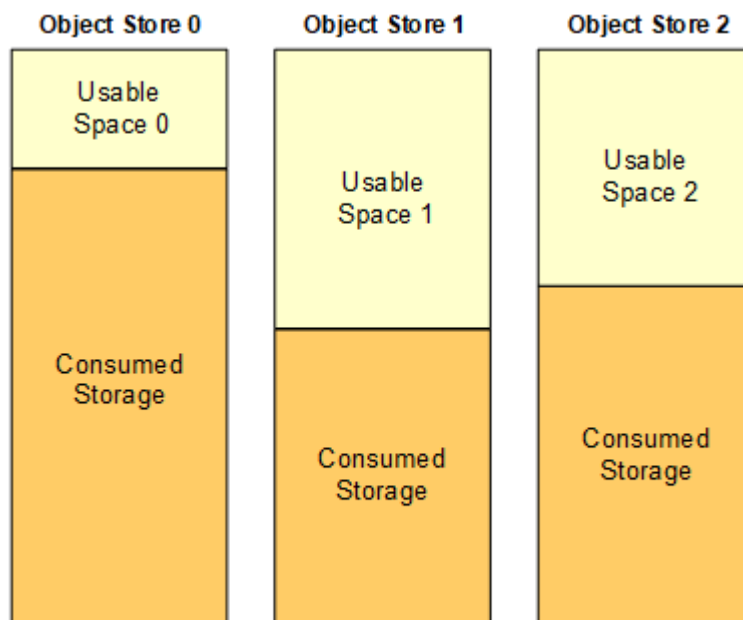
Para obter mais informações sobre o planejamento de uma expansão de armazenamento, consulte o ["instruções para expandir o StorageGRID"](#).

Monitore a capacidade de armazenamento de cada nó de armazenamento

Monitore o espaço total utilizável de cada nó de armazenamento para garantir que o nó tenha espaço suficiente para novos dados de objeto.

Sobre esta tarefa

Espaço utilizável é a quantidade de espaço de armazenamento disponível para armazenar objetos. O espaço total utilizável para um nó de armazenamento é calculado somando o espaço disponível em todos os armazenamentos de objetos dentro do nó.



$$\text{Total Usable Space} = \text{Usable Space 0} + \text{Usable Space 1} + \text{Usable Space 2}$$

Passos

1. Selecione **NÓS > Nó de armazenamento > Armazenamento**.

Os gráficos e tabelas do nó aparecem.

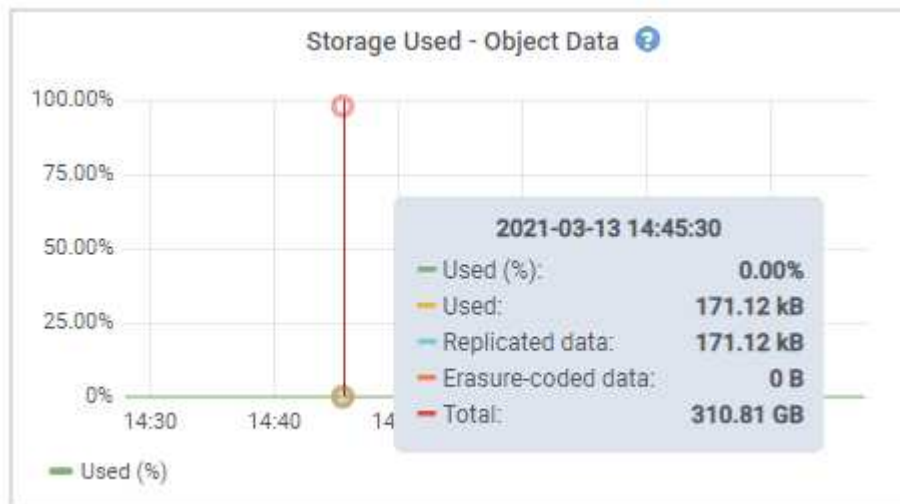
2. Posicione o cursor sobre o gráfico Armazenamento usado - dados do objeto.

Os seguintes valores são mostrados:

- **Usado (%)**: A porcentagem do espaço total utilizável que foi usada para dados do objeto.
- **Usado**: A quantidade de espaço total utilizável que foi usada para dados do objeto.
- **Dados replicados**: Uma estimativa da quantidade de dados de objetos replicados neste nó, site ou grade.
- **Dados codificados por eliminação**: Uma estimativa da quantidade de dados de objetos codificados

por eliminação neste nó, site ou grade.

- **Total:** A quantidade total de espaço utilizável neste nó, site ou grade. O valor usado é o `storagegrid_storage_utilization_data_bytes` métrica.



3. Revise os valores disponíveis nas tabelas Volumes e Armazenamentos de objetos, abaixo dos gráficos.



Para visualizar gráficos desses valores, clique nos ícones do gráfico  nas colunas Disponíveis.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

- Monitore os valores ao longo do tempo para estimar a taxa em que o espaço de armazenamento utilizável está sendo consumido.
- Para manter as operações normais do sistema, adicione nós de armazenamento, adicione volumes de armazenamento ou archive dados de objetos antes que o espaço utilizável seja consumido.

Ao planejar o momento de uma expansão, considere quanto tempo levará para adquirir e instalar armazenamento adicional.



Se sua política de ILM usar codificação de eliminação, talvez você prefira expandir quando os nós de armazenamento existentes estiverem aproximadamente 70% cheios para reduzir o número de nós que devem ser adicionados.

Para obter mais informações sobre o planejamento de uma expansão de armazenamento, consulte

o"instruções para expandir o StorageGRID" .

O"Armazenamento de dados de objetos baixos" O alerta é acionado quando não há espaço suficiente para armazenar dados de objetos em um nó de armazenamento.

Monitorar a capacidade de metadados do objeto para cada nó de armazenamento

Monitore o uso de metadados para cada nó de armazenamento para garantir que haja espaço adequado disponível para operações essenciais do banco de dados. Você deve adicionar novos nós de armazenamento em cada site antes que os metadados do objeto excedam 100% do espaço de metadados permitido.

Sobre esta tarefa

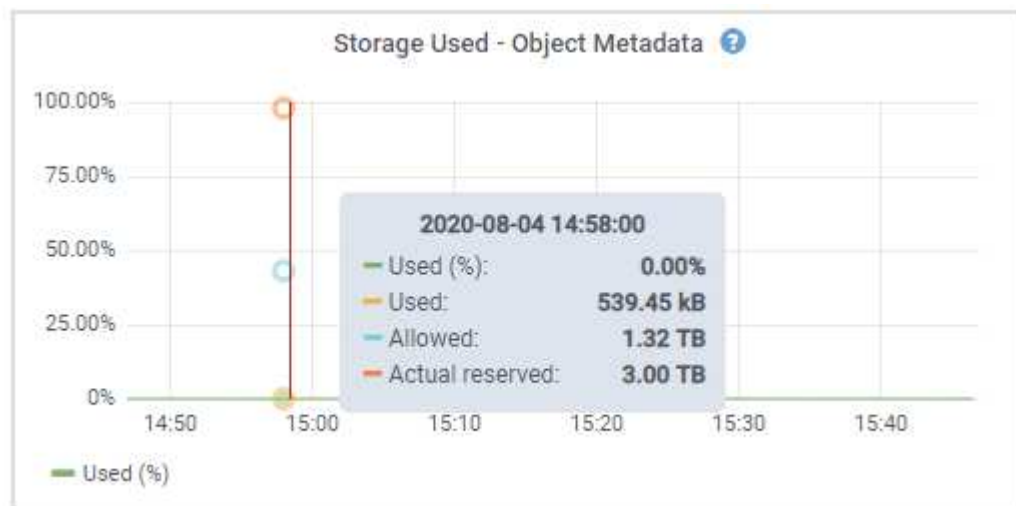
O StorageGRID mantém três cópias de metadados de objetos em cada site para fornecer redundância e proteger os metadados de objetos contra perdas. As três cópias são distribuídas uniformemente entre todos os nós de armazenamento em cada site, usando o espaço reservado para metadados no volume de armazenamento 0 de cada nó de armazenamento.

Em alguns casos, a capacidade de metadados de objetos da grade pode ser consumida mais rapidamente do que sua capacidade de armazenamento de objetos. Por exemplo, se você normalmente ingere grandes quantidades de objetos pequenos, pode ser necessário adicionar nós de armazenamento para aumentar a capacidade de metadados, mesmo que ainda haja capacidade de armazenamento de objetos suficiente.

Alguns dos fatores que podem aumentar o uso de metadados incluem o tamanho e a quantidade de metadados e tags do usuário, o número total de partes em um upload multiparte e a frequência de alterações nos locais de armazenamento do ILM.

Passos

1. Selecione **NÓS > Nó de armazenamento > Armazenamento**.
2. Posicione o cursor sobre o gráfico Armazenamento usado - metadados do objeto para ver os valores de um período específico.



Usado (%)

A porcentagem do espaço de metadados permitido que foi usado neste nó de armazenamento.

Métricas do Prometheus: `storagegrid_storage_utilization_metadata_bytes` e `storagegrid_storage_utilization_metadata_allowed_bytes`

Usado

Os bytes do espaço de metadados permitido que foram usados neste nó de armazenamento.

Métrica do Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Permitido

O espaço permitido para metadados de objetos neste nó de armazenamento. Para saber como esse valor é determinado para cada nó de armazenamento, consulte o ["descrição completa do espaço de metadados permitido"](#).

Métrica do Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Reservado atualmente

O espaço real reservado para metadados neste nó de armazenamento. Inclui o espaço permitido e o espaço necessário para operações essenciais de metadados. Para saber como esse valor é calculado para cada nó de armazenamento, consulte o ["descrição completa do espaço reservado real para metadados"](#).

A métrica Prometheus será adicionada em uma versão futura.



Os valores totais de um site ou da grade não incluem nós que não relataram métricas por pelo menos cinco minutos, como nós offline.

- Se o valor **Usado (%)** for 70% ou superior, expanda seu sistema StorageGRID adicionando nós de armazenamento a cada site.



O alerta **Baixo armazenamento de metadados** é acionado quando o valor **Usado (%)** atinge determinados limites. Resultados indesejados podem ocorrer se os metadados do objeto usarem mais de 100% do espaço permitido.

Quando você adiciona novos nós, o sistema reequilibra automaticamente os metadados do objeto em todos os nós de armazenamento do site. Veja o ["instruções para expandir um sistema StorageGRID"](#).

Monitorar previsões de uso do espaço

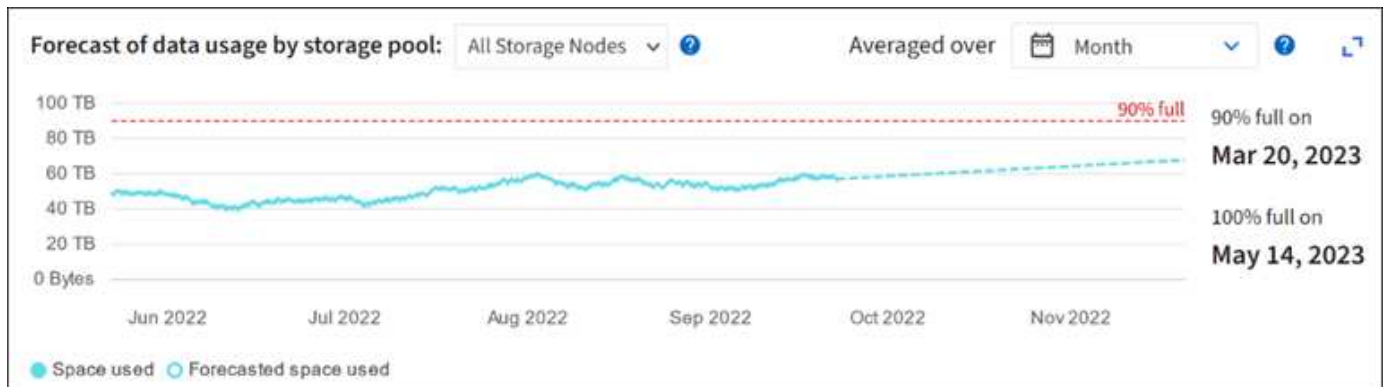
Monitore as previsões de uso do espaço para dados e metadados do usuário para estimar quando você precisará ["expandir uma grade"](#).

Se você notar que a taxa de consumo muda ao longo do tempo, selecione um intervalo menor no menu suspenso **Média sobre** para refletir apenas os padrões de ingestão mais recentes. Se você notar padrões sazonais, selecione um intervalo maior.

Se você tiver uma nova instalação do StorageGRID, permita que dados e metadados se acumulem antes de avaliar as previsões de uso do espaço.

Passos

- No painel, selecione **Armazenamento**.
- Visualize os cartões do painel, Previsão de uso de dados por pool de armazenamento e Previsão de uso de metadados por site.
- Use esses valores para estimar quando você precisará adicionar novos nós de armazenamento para armazenamento de dados e metadados.



Monitorar o gerenciamento do ciclo de vida das informações

O sistema de gerenciamento do ciclo de vida da informação (ILM) fornece gerenciamento de dados para todos os objetos armazenados na grade. Você deve monitorar as operações do ILM para entender se a rede pode lidar com a carga atual ou se mais recursos são necessários.

Sobre esta tarefa

O sistema StorageGRID gerencia objetos aplicando as políticas de ILM ativas. As políticas do ILM e as regras associadas do ILM determinam quantas cópias são feitas, o tipo de cópias que são criadas, onde as cópias são colocadas e por quanto tempo cada cópia é retida.

A ingestão de objetos e outras atividades relacionadas a objetos podem exceder a taxa na qual o StorageGRID pode avaliar o ILM, fazendo com que o sistema enfileire objetos cujas instruções de posicionamento do ILM não podem ser atendidas quase em tempo real. Você deve monitorar se o StorageGRID está acompanhando as ações do cliente.

Use a guia do painel do Grid Manager

Passos

Use a guia ILM no painel do Grid Manager para monitorar as operações do ILM:

1. Sign in no Grid Manager.
2. No painel, selecione a guia ILM e anote os valores no cartão Fila ILM (Objetos) e no cartão Taxa de avaliação ILM.

Picos temporários no cartão da fila ILM (Objetos) no painel são esperados. Mas se a fila continuar a aumentar e nunca diminuir, a grade precisará de mais recursos para operar com eficiência: mais nós de armazenamento ou, se a política de ILM colocar objetos em locais remotos, mais largura de banda de rede.

Use a página NODES

Passos

Além disso, investigue as filas do ILM usando a página **NODES**:



Os gráficos na página **NODES** serão substituídos pelos cartões do painel correspondentes em uma versão futura do StorageGRID.

1. Selecione **NODES**.
2. Selecione **nome da grade > ILM**.
3. Posicione o cursor sobre o gráfico de fila do ILM para ver o valor dos seguintes atributos em um determinado momento:
 - **Objetos na fila (de operações do cliente)**: O número total de objetos aguardando avaliação do ILM devido a operações do cliente (por exemplo, ingestão).
 - **Objetos na fila (de todas as operações)**: O número total de objetos aguardando avaliação do ILM.
 - **Taxa de varredura (objetos/seg)**: A taxa na qual os objetos na grade são varridos e colocados na fila para ILM.
 - **Taxa de avaliação (objetos/seg)**: A taxa atual na qual os objetos estão sendo avaliados em relação à política de ILM na grade.
4. Na seção Fila do ILM, observe os seguintes atributos.



A seção da fila ILM está incluída somente para a grade. Essas informações não são mostradas na guia ILM de um site ou nó de armazenamento.

- **Período de verificação - estimado**: Tempo estimado para concluir uma verificação ILM completa de todos os objetos.



Uma verificação completa não garante que o ILM foi aplicado a todos os objetos.

- **Reparos tentados**: O número total de operações de reparo de objetos para dados replicados que foram tentadas. Essa contagem aumenta cada vez que um nó de armazenamento tenta reparar um objeto de alto risco. Reparos de ILM de alto risco são priorizados se a rede ficar ocupada.



O mesmo reparo de objeto pode ser incrementado novamente se a replicação falhar após o reparo.

Esses atributos podem ser úteis ao monitorar o progresso da recuperação do volume do nó de armazenamento. Se o número de reparos tentados parou de aumentar e uma verificação completa foi concluída, o reparo provavelmente foi concluído.

Monitorar recursos de rede e sistema

A integridade e a largura de banda da rede entre nós e sites, bem como o uso de recursos por nós de grade individuais, são essenciais para operações eficientes.

Monitore as conexões e o desempenho da rede

A conectividade de rede e a largura de banda são especialmente importantes se sua política de gerenciamento do ciclo de vida das informações (ILM) copiar objetos replicados entre sites ou armazenar objetos codificados para eliminação usando um esquema que forneça proteção contra perda de site. Se a rede entre os sites não estiver disponível, a latência da rede for muito alta ou a largura de banda da rede for insuficiente, algumas regras de ILM podem não conseguir colocar objetos onde esperado. Isso pode levar a falhas de ingestão (quando a opção Ingestão estrita é selecionada para regras de ILM) ou a baixo desempenho de ingestão e pendências de ILM.

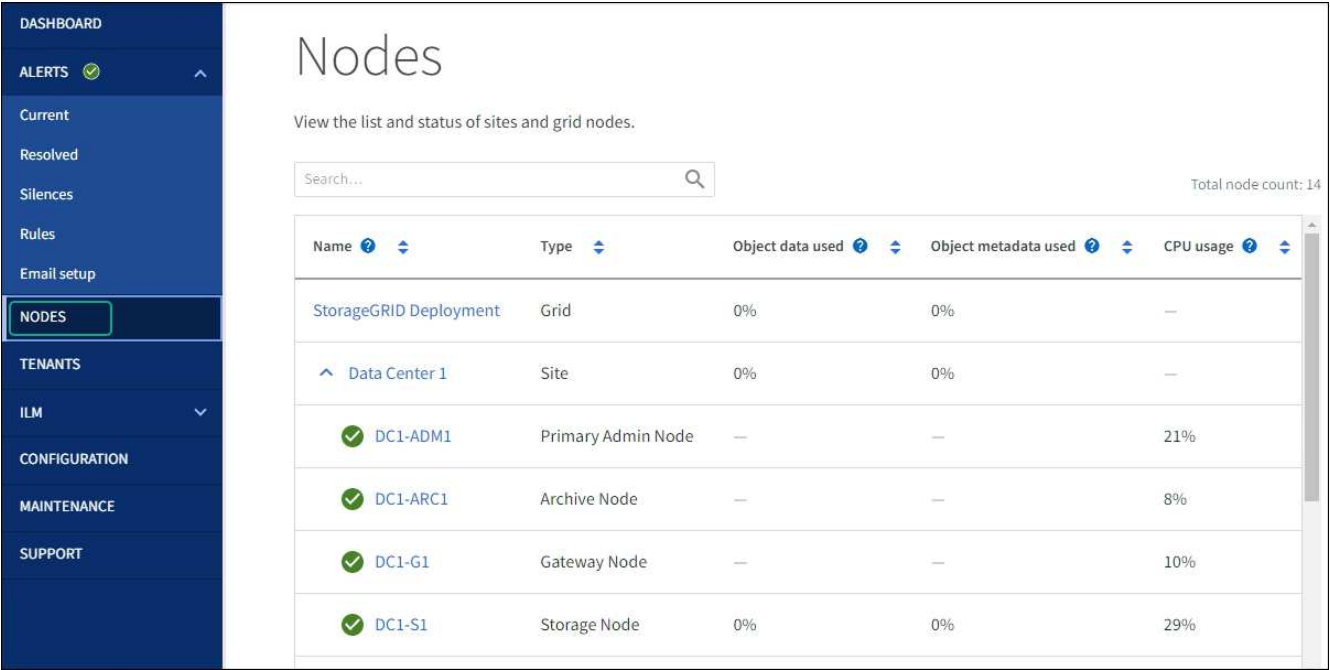
Use o Grid Manager para monitorar a conectividade e o desempenho da rede para que você possa resolver quaisquer problemas imediatamente.

Além disso, considere "[criando políticas de classificação de tráfego de rede](#)" para que você possa monitorar o tráfego relacionado a locatários, buckets, sub-redes ou endpoints de balanceador de carga específicos. Você pode definir políticas de limitação de tráfego conforme necessário.

Passos

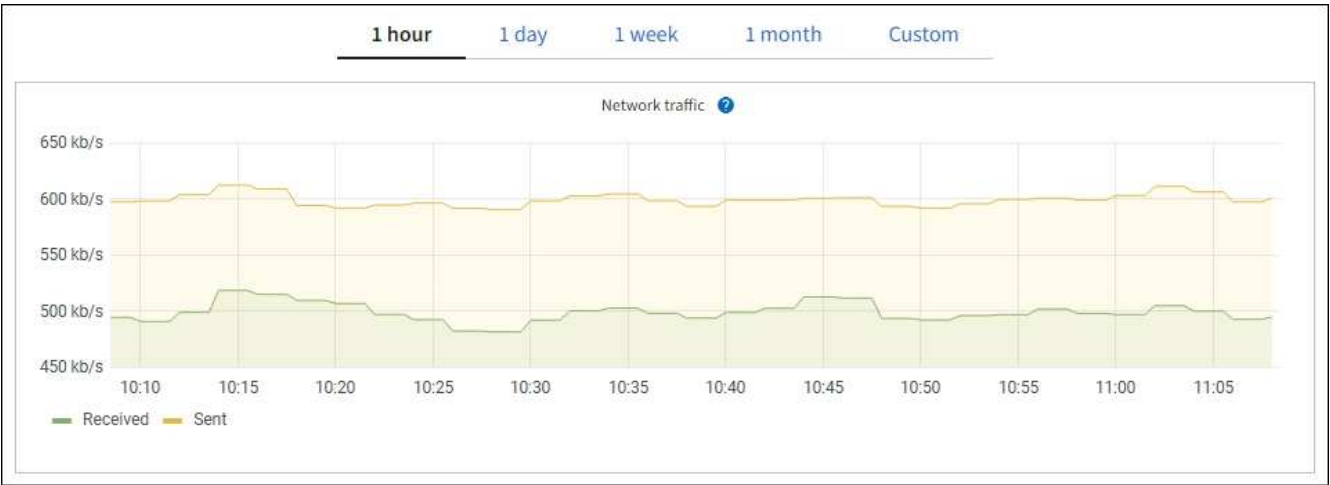
- 1. Selecione **NODES**.

A página Nós é exibida. Cada nó na grade é listado em formato de tabela.



- 2. Selecione o nome da grade, um site de data center específico ou um nó da grade e, em seguida, selecione a guia **Rede**.

O gráfico de tráfego de rede fornece um resumo do tráfego geral de rede para a grade como um todo, para o site do data center ou para o nó.



- a. Se você selecionou um nó de grade, role para baixo para revisar a seção **Interfaces de rede** da página.

Network interfaces					
Name ?	Hardware address ?	Speed ?	Duplex ?	Auto-negotiation ?	Link status ?
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

b. Para nós de grade, role para baixo para revisar a seção **Comunicação de rede** da página.

As tabelas de recebimento e transmissão mostram quantos bytes e pacotes foram recebidos e enviados por cada rede, bem como outras métricas de recebimento e transmissão.

Network communication						
Receive						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Frame overruns ?	Frames ?
eth0	2.89 GB	19,421,503	0	24,032	0	0
Transmit						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Collisions ?	Carrier ?
eth0	3.64 GB	18,494,381	0	0	0	0

3. Use as métricas associadas às suas políticas de classificação de tráfego para monitorar o tráfego de rede.

a. Selecione **CONFIGURAÇÃO > Rede > Classificação de tráfego**.

A página Políticas de Classificação de Tráfego é exibida e as políticas existentes são listadas na tabela.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create Edit ✕ Remove Metrics		
Name	Description	ID
☐ ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
☒ Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b
Displaying 2 traffic classification policies.		

a. Para visualizar gráficos que mostram as métricas de rede associadas a uma política, selecione o botão de opção à esquerda da política e clique em **Métricas**.

b. Revise os gráficos para entender o tráfego de rede associado à política.

Se uma política de classificação de tráfego for projetada para limitar o tráfego de rede, analise com que frequência o tráfego é limitado e decida se a política continua atendendo às suas necessidades.

De tempos em tempos, ["ajuste cada política de classificação de tráfego conforme necessário"](#) .

Informações relacionadas

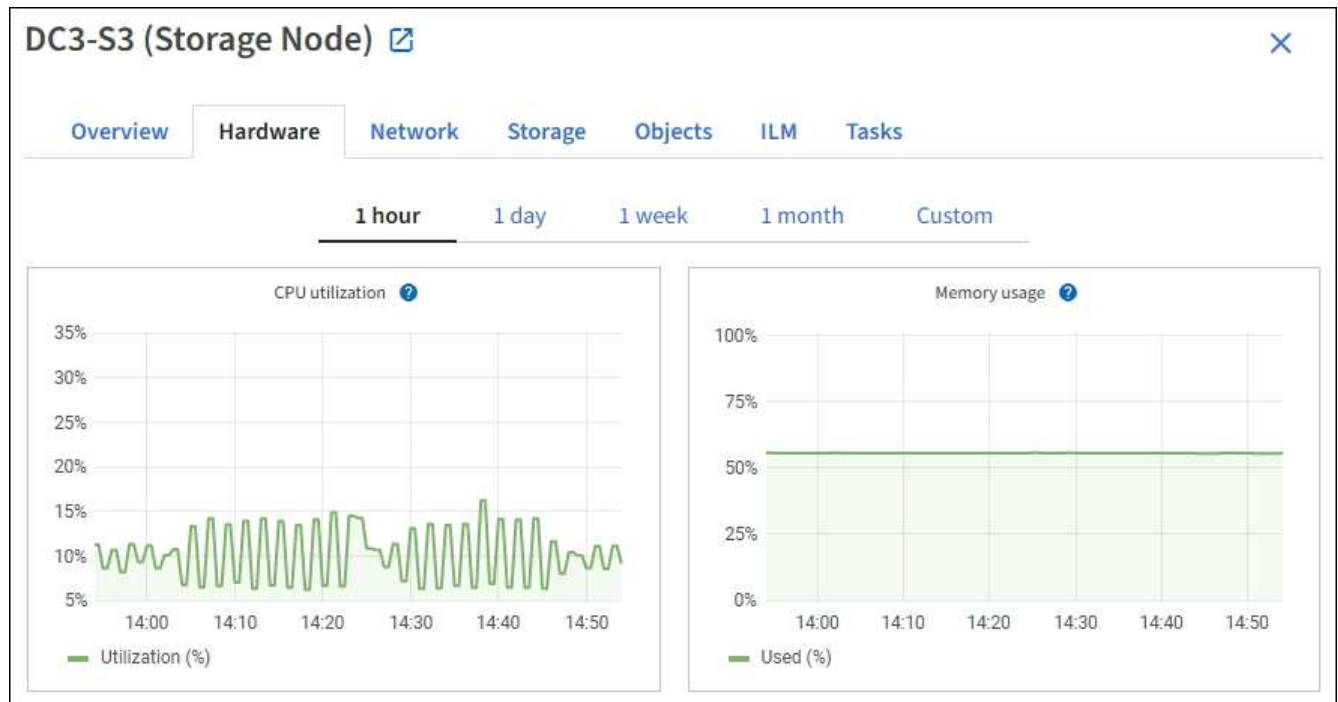
- ["Ver a aba Rede"](#)
- ["Monitorar estados de conexão de nós"](#)

Monitorar recursos em nível de nó

Monitore nós de grade individuais para verificar seus níveis de uso de recursos. Se os nós estiverem constantemente sobrecarregados, mais nós poderão ser necessários para operações eficientes.

Passos

1. Na página **NÓS**, selecione o nó.
2. Selecione a aba **Hardware** para exibir gráficos de Utilização da CPU e Uso da Memória.



3. Para exibir um intervalo de tempo diferente, selecione um dos controles acima do gráfico. Você pode exibir as informações disponíveis para intervalos de 1 hora, 1 dia, 1 semana ou 1 mês. Você também pode definir um intervalo personalizado, que permite especificar intervalos de data e hora.
4. Se o nó estiver hospedado em um dispositivo de armazenamento ou de serviços, role para baixo para visualizar as tabelas de componentes. O status de todos os componentes deve ser "Nominal". Investigue componentes que tenham qualquer outro status.

Informações relacionadas

- ["Exibir informações sobre nós de armazenamento do dispositivo"](#)
- ["Exibir informações sobre nós de administração e nós de gateway do dispositivo"](#)

Monitorar a atividade do inquilino

Todas as atividades do cliente S3 estão associadas às contas de locatário do StorageGRID . Você pode usar o Grid Manager para monitorar o uso de armazenamento

ou o tráfego de rede para todos os locatários ou um locatário específico. Você pode usar o log de auditoria ou os painéis do Grafana para coletar informações mais detalhadas sobre como os locatários estão usando o StorageGRID.

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" .

Ver todos os inquilinos

A página Inquilinos mostra informações básicas para todas as contas de inquilinos atuais.

Passos

1. Selecione **LOCATÁRIOS**.
2. Revise as informações mostradas nas páginas do Locatário.

O espaço lógico usado, o uso da cota, a cota e a contagem de objetos são listados para cada locatário. Se uma cota não for definida para um locatário, os campos Uso de cota e Cota conterão um hífen (—).



Os valores de espaço utilizado são estimativas. Essas estimativas são afetadas pelo tempo de ingestão, pela conectividade de rede e pelo status do nó.

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.

CreateExport to CSVActions

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	→ 📄

3. Opcionalmente, faça login em uma conta de locatário selecionando o link de login→ na coluna * Sign in/Copiar URL*.
4. Opcionalmente, copie o URL da página de login de um locatário selecionando o link copiar URL📄 na coluna * Sign in/Copiar URL*.
5. Opcionalmente, selecione **Exportar para CSV** para visualizar e exportar um .csv arquivo contendo os valores de uso para todos os locatários.

Você será solicitado a abrir ou salvar o .csv arquivo.

O conteúdo do .csv arquivo se parece com o exemplo a seguir:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	1100000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	47500000000	95	1400000000	50000	S3
36521587546689565123	Tenant 05	50000000000	Infinity		500	S3

Você pode abrir o .csv arquivar em um aplicativo de planilha ou usá-lo em automação.

6. Se nenhum objeto estiver listado, opcionalmente, selecione **Ações > Excluir** para remover um ou mais inquilinos. Ver "[Excluir conta de inquilino](#)".

Não é possível remover uma conta de locatário se ela incluir buckets ou contêineres.

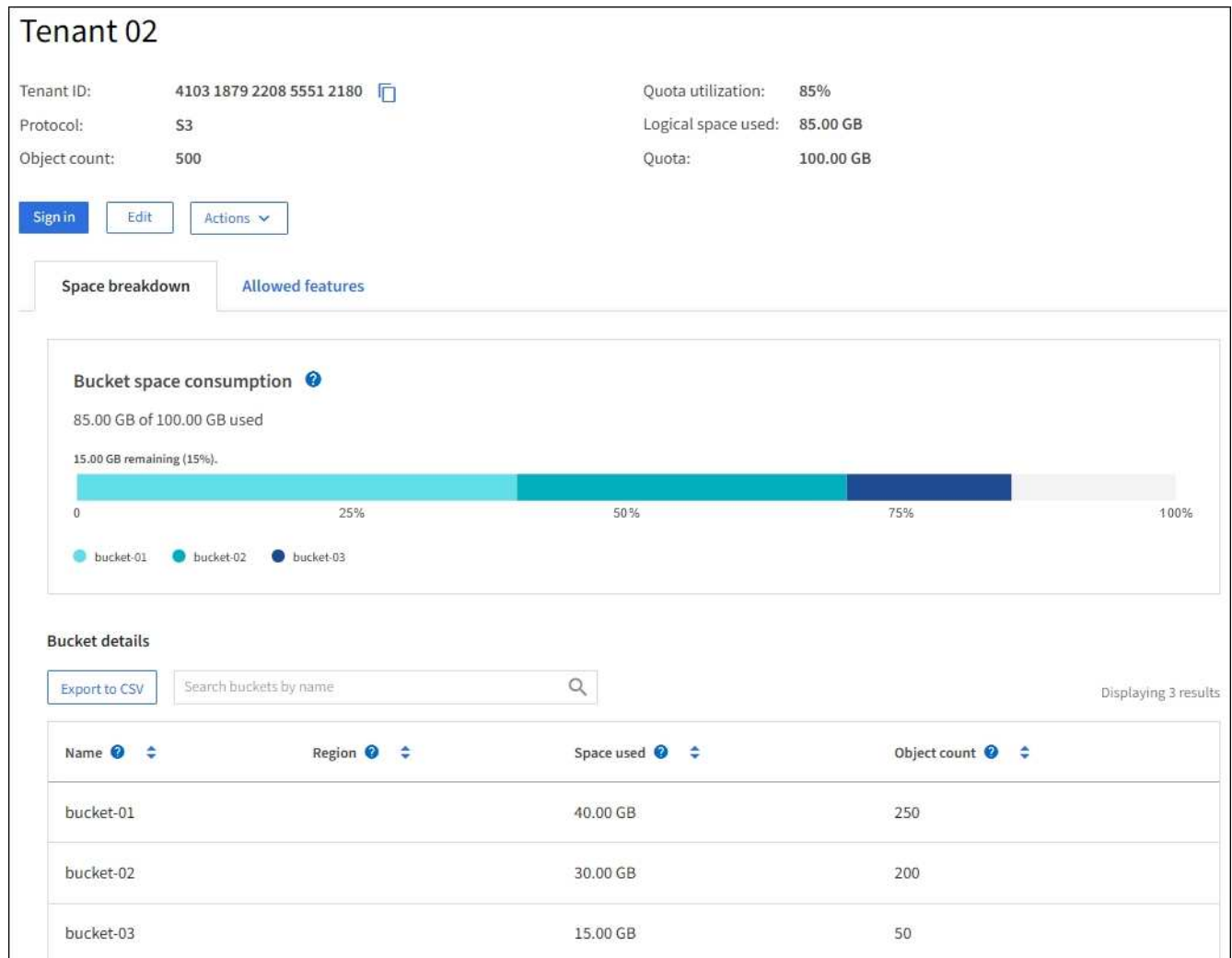
Ver um inquilino específico

Você pode visualizar detalhes de um inquilino específico.

Passos

1. Selecione o nome do inquilino na página Inquilinos.

A página de detalhes do inquilino é exibida.



2. Revise a visão geral do inquilino no topo da página.

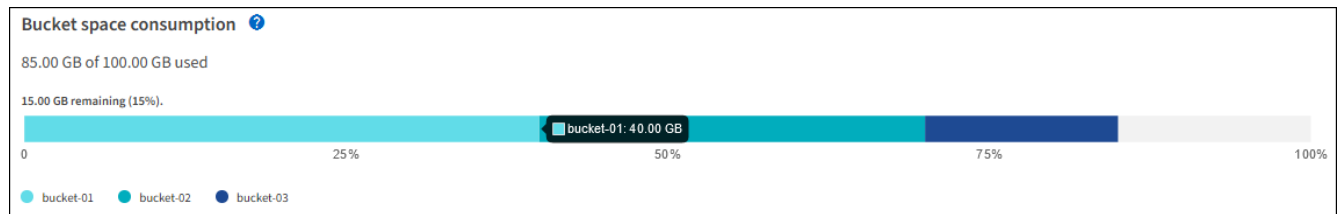
Esta seção da página de detalhes fornece informações resumidas sobre o locatário, incluindo a contagem de objetos do locatário, o uso da cota, o espaço lógico usado e a configuração da cota.

3. Na aba **Detalhamento de espaço**, revise o gráfico **Consumo de espaço**.

Este gráfico mostra o consumo total de espaço para todos os buckets S3 do locatário.

Se uma cota foi definida para este locatário, a quantidade de cota usada e restante será exibida em texto (por exemplo, 85.00 GB of 100 GB used). Se nenhuma cota foi definida, o locatário tem uma cota ilimitada e o texto inclui apenas uma quantidade de espaço usado (por exemplo, 85.00 GB used). O gráfico de barras mostra a porcentagem de cota em cada balde ou contêiner. Se o locatário tiver excedido a cota de armazenamento em mais de 1% e em pelo menos 1 GB, o gráfico mostrará a cota total e o valor excedente.

Você pode colocar o cursor sobre o gráfico de barras para ver o armazenamento usado por cada bucket ou contêiner. Você pode colocar o cursor sobre o segmento de espaço livre para ver a quantidade de cota de armazenamento restante.



O uso da cota é baseado em estimativas internas e pode ser excedido em alguns casos. Por exemplo, o StorageGRID verifica a cota quando um locatário começa a carregar objetos e rejeita novas ingestões se o locatário tiver excedido a cota. No entanto, o StorageGRID não leva em consideração o tamanho do upload atual ao determinar se a cota foi excedida. Se os objetos forem excluídos, um locatário poderá ser temporariamente impedido de carregar novos objetos até que o uso da cota seja recalculado. Os cálculos de uso de cota podem levar 10 minutos ou mais.



O uso de cota de um locatário indica a quantidade total de dados de objeto que o locatário carregou no StorageGRID (tamanho lógico). O uso da cota não representa o espaço usado para armazenar cópias desses objetos e seus metadados (tamanho físico).



Você pode habilitar a regra de alerta **Uso alto de cota de locatário** para determinar se os locatários estão consumindo suas cotas. Se habilitado, esse alerta será acionado quando um locatário tiver usado 90% de sua cota. Para obter instruções, consulte ["Editar regras de alerta"](#).

4. Na aba **Detalhamento do espaço**, revise os **Detalhes do bucket**.

Esta tabela lista os buckets do S3 para o locatário. O espaço usado é a quantidade total de dados de objeto no bucket ou contêiner. Este valor não representa o espaço de armazenamento necessário para cópias do ILM e metadados de objetos.

5. Opcionalmente, selecione **Exportar para CSV** para visualizar e exportar um arquivo .csv contendo os valores de uso para cada bucket ou contêiner.

O conteúdo de um locatário S3 individual .csv arquivo se parece com o exemplo a seguir:

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

Você pode abrir o .csv arquivar em um aplicativo de planilha ou usá-lo em automação.

- Opcionalmente, selecione a aba **Recursos permitidos** para ver uma lista de permissões e recursos habilitados para o locatário. Ver ["Editar conta de inquilino"](#) se você precisar alterar qualquer uma dessas configurações.
- Se o locatário tiver a permissão **Usar conexão de federação de grade**, selecione opcionalmente a guia **Federação de grade** para saber mais sobre a conexão.

Ver ["O que é federação de grade?"](#) e ["Gerenciar os inquilinos permitidos para federação de rede"](#).

Exibir tráfego de rede

Se houver políticas de classificação de tráfego em vigor para um locatário, revise o tráfego de rede desse locatário.

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. Revise a lista de políticas para identificar aquelas que se aplicam a um inquilino específico.
3. Para visualizar métricas associadas a uma política, selecione o botão de opção à esquerda da política e selecione **Métricas**.
4. Analise os gráficos para determinar com que frequência a política está limitando o tráfego e se você precisa ajustá-la.

Ver ["Gerenciar políticas de classificação de tráfego"](#) para maiores informações.

Use o log de auditoria

Opcionalmente, você pode usar o log de auditoria para um monitoramento mais granular das atividades de um locatário.

Por exemplo, você pode monitorar os seguintes tipos de informações:

- Operações específicas do cliente, como PUT, GET ou DELETE
- Tamanhos de objetos
- A regra ILM aplicada a objetos
- O IP de origem das solicitações do cliente

Os logs de auditoria são gravados em arquivos de texto que você pode analisar usando a ferramenta de análise de logs de sua escolha. Isso permite que você entenda melhor as atividades do cliente ou implemente modelos sofisticados de cobrança e estorno.

Ver ["Revisar logs de auditoria"](#) para maiores informações.

Use métricas do Prometheus

Opcionalmente, use as métricas do Prometheus para relatar a atividade do locatário.

- No Grid Manager, selecione **SUORTE > Ferramentas > Métricas**. Você pode usar painéis existentes, como o S3 Overview, para revisar as atividades do cliente.



As ferramentas disponíveis na página Métricas destinam-se principalmente ao uso do suporte técnico. Alguns recursos e itens de menu nessas ferramentas são intencionalmente não funcionais.

- Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API**. Você pode usar as métricas na seção Métricas da API de gerenciamento de grade para criar regras de alerta e painéis personalizados para a atividade do locatário.

Ver ["Revisar métricas de suporte"](#) para maiores informações.

Monitorar operações do cliente S3

Você pode monitorar as taxas de ingestão e recuperação de objetos, bem como métricas para contagens, consultas e verificação de objetos. Você pode visualizar o número de tentativas bem-sucedidas e malsucedidas de aplicativos clientes para ler, gravar e modificar objetos no sistema StorageGRID .

Antes de começar

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

Passos

1. No painel, selecione a aba **Desempenho**.
2. Consulte os gráficos do S3, que resumem o número de operações de cliente executadas pelos nós de armazenamento e o número de solicitações de API recebidas pelos nós de armazenamento durante o período selecionado.
3. Selecione **NÓS** para acessar a página Nós.
4. Na página inicial dos Nós (nível de grade), selecione a aba **Objetos**.

O gráfico mostra as taxas de ingestão e recuperação do S3 para todo o seu sistema StorageGRID em bytes por segundo e a quantidade de dados ingeridos ou recuperados. Você pode selecionar um intervalo de tempo ou aplicar um intervalo personalizado.

5. Para ver informações de um nó de armazenamento específico, selecione o nó na lista à esquerda e selecione a guia **Objetos**.

O gráfico mostra as taxas de ingestão e recuperação do nó. A guia também inclui métricas para contagens de objetos, consultas de metadados e operações de verificação.



Monitorar operações de balanceamento de carga

Se estiver usando um balanceador de carga para gerenciar conexões de clientes com o StorageGRID, você deverá monitorar as operações de balanceamento de carga depois de configurar o sistema inicialmente e depois de fazer qualquer alteração de configuração ou executar uma expansão.

Sobre esta tarefa

Você pode usar o serviço Load Balancer em nós de administração ou nós de gateway ou um balanceador de carga externo de terceiros para distribuir solicitações de clientes entre vários nós de armazenamento.

Após configurar o balanceamento de carga, você deve confirmar se as operações de ingestão e recuperação de objetos estão sendo distribuídas uniformemente entre os nós de armazenamento. Solicitações distribuídas uniformemente garantem que o StorageGRID permaneça responsivo às solicitações do cliente sob carga e podem ajudar a manter o desempenho do cliente.

Se você configurou um grupo de alta disponibilidade (HA) de nós de gateway ou nós de administração no modo de backup ativo, somente um nó no grupo distribui ativamente as solicitações do cliente.

Para obter mais informações, consulte ["Configurar conexões do cliente S3"](#).

Passos

1. Se os clientes S3 se conectarem usando o serviço Load Balancer, verifique se os nós de administração ou os nós de gateway estão distribuindo ativamente o tráfego conforme o esperado:

- a. Selecione **NODES**.
- b. Selecione um nó de gateway ou um nó de administração.
- c. Na guia **Visão geral**, verifique se uma interface de nó está em um grupo de HA e se a interface de nó tem a função de Primária.

Nós com a função Primário e nós que não estão em um grupo HA devem distribuir ativamente solicitações aos clientes.

- d. Para cada nó que deve distribuir ativamente solicitações de clientes, selecione o ["Guia Balanceador de Carga"](#).
- e. Revise o gráfico de tráfego de solicitações do balanceador de carga da última semana para garantir que o nó esteja distribuindo solicitações ativamente.

Os nós em um grupo de HA de backup ativo podem assumir a função de Backup de tempos em tempos. Durante esse tempo, os nós não distribuem solicitações de clientes.

- f. Revise o gráfico da Taxa de Solicitações de Entrada do Balanceador de Carga da última semana para analisar a taxa de transferência de objetos do nó.
- g. Repita essas etapas para cada nó de administração ou nó de gateway no sistema StorageGRID.
- h. Opcionalmente, use políticas de classificação de tráfego para visualizar uma análise mais detalhada do tráfego atendido pelo serviço Load Balancer.

2. Verifique se essas solicitações estão sendo distribuídas uniformemente aos nós de armazenamento.

- a. Selecione **Nó de armazenamento > LDR > HTTP**.
- b. Revise o número de **Sessões de entrada atualmente estabelecidas**.
- c. Repita para cada nó de armazenamento na grade.

O número de sessões deve ser aproximadamente igual em todos os nós de armazenamento.

Monitorar conexões de federação de rede

Você pode monitorar informações básicas sobre todos ["conexões de federação de rede"](#), informações detalhadas sobre uma conexão específica ou métricas do Prometheus sobre operações de replicação entre redes. Você pode monitorar uma conexão de qualquer uma das redes.

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.

Ver todas as conexões

A página Federação de grade mostra informações básicas sobre todas as conexões de federação de grade e sobre todas as contas de locatário que têm permissão para usar conexões de federação de grade.

Passos

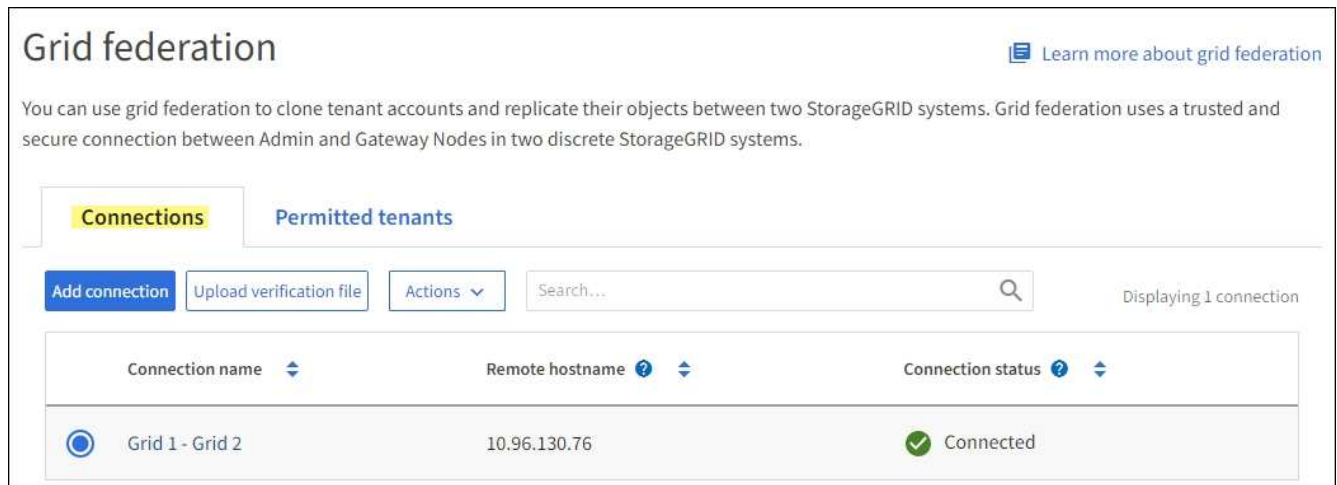
1. Selecione **CONFIGURAÇÃO > Sistema > Federação de grade**.

A página da federação Grid é exibida.

2. Para ver informações básicas de todas as conexões nesta grade, selecione a aba **Conexões**.

Nesta aba, você pode:

- ["Criar uma nova conexão"](#) .
- Selecione uma conexão existente para ["editar ou testar"](#) .



The screenshot shows the 'Grid federation' page. At the top, there's a title 'Grid federation' and a link 'Learn more about grid federation'. Below this is a descriptive paragraph: 'You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.' There are two tabs: 'Connections' (active) and 'Permitted tenants'. Under the 'Connections' tab, there are buttons for 'Add connection', 'Upload verification file', and 'Actions'. A search bar is also present. Below these is a table with columns: 'Connection name', 'Remote hostname', and 'Connection status'. The table displays one connection: 'Grid 1 - Grid 2' with remote hostname '10.96.130.76' and status 'Connected' (indicated by a green checkmark). The text 'Displaying 1 connection' is shown on the right.

Connection name	Remote hostname	Connection status
Grid 1 - Grid 2	10.96.130.76	Connected

3. Para ver informações básicas de todas as contas de locatários nesta grade que têm a permissão **Usar conexão de federação de grade**, selecione a guia **Locatários permitidos**.

Nesta aba, você pode:

- ["Veja a página de detalhes de cada inquilino permitido"](#) .
- Veja a página de detalhes de cada conexão. Ver [Ver uma conexão específica](#) .
- Selecione um inquilino permitido e ["remover a permissão"](#) .
- Verifique se há erros de replicação entre grades e limpe o último erro, se houver. Ver ["Solucionar erros de federação de grade"](#) .

Grid federation [Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

[Connections](#)
[Permitted tenants](#)

[Remove permission](#)
[Clear error](#)

Displaying one result

Tenant name	Connection name	Connection status	Remote grid hostname	Last error
Tenant A	Grid 1 - Grid 2	Connected	10.96.130.76	Check for errors

Ver uma conexão específica

Você pode visualizar detalhes de uma conexão de federação de grade específica.

Passos

1. Selecione qualquer uma das guias na página Federação da grade e, em seguida, selecione o nome da conexão na tabela.

Na página de detalhes da conexão, você pode:

- Veja informações básicas de status sobre a conexão, incluindo nomes de host locais e remotos, porta e status da conexão.
- Selecione uma conexão para ["editar, testar ou remover"](#) .

2. Ao visualizar uma conexão específica, selecione a aba **Inquilinos permitidos** para ver detalhes sobre os inquilinos permitidos para a conexão.

Nesta aba, você pode:

- ["Veja a página de detalhes de cada inquilino permitido"](#) .
- ["Remover a permissão de um inquilino"](#) para usar a conexão.
- Verifique se há erros de replicação entre grades e limpe o último erro. Ver ["Solucionar erros de federação de grade"](#) .

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	Check for errors

3. Ao visualizar uma conexão específica, selecione a guia **Certificados** para visualizar os certificados de servidor e cliente gerados pelo sistema para esta conexão.

Nesta aba, você pode:

- ["Girar certificados de conexão"](#) .
- Selecione **Servidor** ou **Cliente** para visualizar ou baixar o certificado associado ou copiar o certificado PEM.

Grid A-Grid B

Local hostname (this grid):
Port:
Remote hostname (other grid):
Connection status:

10.96.106.230
23000
10.96.104.230

Connected

EditDownload fileTest connectionRemove

Permitted tenantsCertificates

Rotate certificates

ServerClient

Download certificateCopy certificate PEM

Metadata ?

Subject DN:
Serial number:
Issuer DN:
Issued on:
Expires on:
SHA-1 fingerprint:
SHA-256 fingerprint:
Alternative names:

/C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230
30:81:B8:DD:AE:B2:86:0A
/C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT
2022-10-04T02:21:18.000Z
2024-10-03T19:05:13.000Z
92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DF
54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60
IP Address:10.96.106.230

Certificate PEM ?

-----BEGIN CERTIFICATE-----
MIIGdTCCBF2gAwIBAgIIHIG43a6yhgowDQYJKoZIhvcNAQENBQAwdzELMAkGA1UE
BhIMCVVMwEezARBGNVBAGlMcKnhbG1mb3JualWExejAQBgNVBAcMCVN1bm55dmFsZTEU
MBITGCBlhSCouhVDBQwEgYDVChAZBbnVBAzMFEjDEFrCBZdG9uXWd1R2IjIj

Revisar métricas de replicação entre grades

Você pode usar o painel de replicação entre grades no Grafana para visualizar métricas do Prometheus sobre operações de replicação entre grades na sua grade.

Passos

1. No Grid Manager, seleccione **SUPOORTE** > **Ferramentas** > **Métricas**.



As ferramentas disponíveis na página Métricas são destinadas ao uso do suporte técnico. Alguns recursos e itens de menu dessas ferramentas são intencionalmente não funcionais e estão sujeitos a alterações. Veja a lista de ["métricas Prometheus comumente usadas"](#).

2. Na seção Grafana da página, selecione **Cross Grid Replication**.

Para obter instruções detalhadas, consulte "[Revisar métricas de suporte](#)".

3. Para tentar replicar novamente objetos que falharam na replicação, consulte ["Identificar e tentar novamente operações de replicação com falha"](#) .

Gerenciar alertas

Gerenciar alertas

O sistema de alerta fornece uma interface fácil de usar para detectar, avaliar e resolver problemas que podem ocorrer durante a operação do StorageGRID .

Os alertas são acionados em níveis de gravidade específicos quando as condições da regra de alerta são avaliadas como verdadeiras. Quando um alerta é disparado, as seguintes ações ocorrem:

- Um ícone de gravidade de alerta é exibido no painel do Grid Manager, e a contagem de Alertas Atuais é incrementada.
- O alerta é exibido na página de resumo **NODES** e na guia **NODES > node > Overview**.
- Uma notificação por e-mail é enviada, supondo que você tenha configurado um servidor SMTP e fornecido endereços de e-mail para os destinatários.
- Uma notificação do Protocolo Simples de Gerenciamento de Rede (SNMP) é enviada, supondo que você tenha configurado o agente SNMP do StorageGRID .

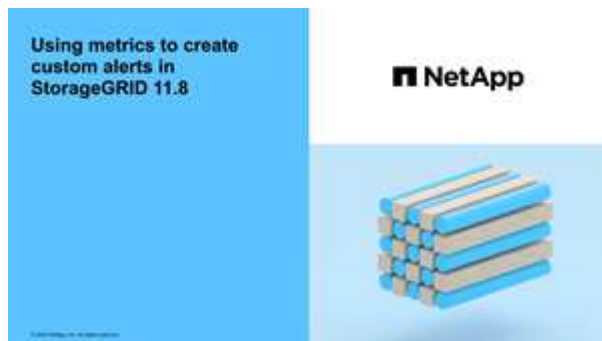
Você pode criar alertas personalizados, editar ou desabilitar alertas e gerenciar notificações de alertas.

Para saber mais:

- Reveja o vídeo: ["Vídeo: Visão geral dos alertas"](#)



- Reveja o vídeo: ["Vídeo: Alertas personalizados"](#)



- Veja o ["Referência de alertas"](#) .

Ver regras de alerta

As regras de alerta definem as condições que desencadeiam "alertas específicos" . O StorageGRID inclui um conjunto de regras de alerta padrão, que você pode usar como estão ou modificar, ou pode criar regras de alerta personalizadas.

Você pode visualizar a lista de todas as regras de alerta padrão e personalizadas para saber quais condições acionarão cada alerta e para ver se algum alerta está desabilitado.

Antes de começar

- Você está conectado ao Grid Manager usando um "navegador da web compatível" .
- Você tem o "Gerenciar alertas ou permissão de acesso root" .
- Opcionalmente, você assistiu ao vídeo: "Vídeo: Visão geral dos alertas"



Passos

1. Selecione **ALERTAS > Regras**.

A página Regras de alerta é exibida.

Alert Rules [Learn more](#)

Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

+ Create custom rule Edit rule Remove custom rule

Name	Conditions	Type	Status
☐ Appliance battery expired The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") Major > 0	Default	Enabled
☐ Appliance battery failed The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") Major > 0	Default	Enabled
☐ Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") Major > 0	Default	Enabled
☐ Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") Major > 0	Default	Enabled
☐ Appliance battery removed The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") Major > 0	Default	Enabled
☐ Appliance battery too hot The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") Major > 0	Default	Enabled
☐ Appliance cache backup device failed A persistent cache backup device has failed.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") Major > 0	Default	Enabled
☐ Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") Major > 0	Default	Enabled
☐ Appliance cache backup device write-protected A cache backup device is write-protected.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") Major > 0	Default	Enabled
☐ Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") Major > 0	Default	Enabled

Displaying 62 alert rules.

2. Revise as informações na tabela de regras de alerta:

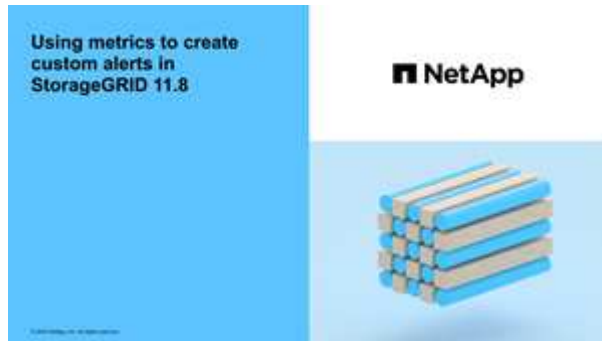
Cabeçalho da coluna	Descrição
Nome	O nome exclusivo e a descrição da regra de alerta. As regras de alerta personalizadas são listadas primeiro, seguidas pelas regras de alerta padrão. O nome da regra de alerta é o assunto das notificações por e-mail.
Condições	As expressões do Prometheus que determinam quando esse alerta é acionado. Um alerta pode ser disparado em um ou mais dos seguintes níveis de gravidade, mas não é necessária uma condição para cada gravidade. • *Crítico*  : Existe uma condição anormal que interrompeu as operações normais de um nó ou serviço do StorageGRID . Você deve resolver o problema subjacente imediatamente. Pode haver interrupção do serviço e perda de dados se o problema não for resolvido. • *Principal*  : Existe uma condição anormal que está afetando as operações atuais ou se aproximando do limite para um alerta crítico. Você deve investigar os principais alertas e resolver quaisquer problemas subjacentes para garantir que a condição anormal não interrompa a operação normal de um nó ou serviço do StorageGRID . • *Menor*  : O sistema está operando normalmente, mas existe uma condição anormal que pode afetar a capacidade do sistema de operar se continuar. Você deve monitorar e resolver alertas menores que não desaparecem sozinhos para garantir que eles não resultem em um problema mais sério.
Tipo	O tipo de regra de alerta: • Padrão: Uma regra de alerta fornecida com o sistema. Você pode desabilitar uma regra de alerta padrão ou editar as condições e a duração de uma regra de alerta padrão. Você não pode remover uma regra de alerta padrão. • Padrão*: Uma regra de alerta padrão que inclui uma condição ou duração editada. Conforme necessário, você pode facilmente reverter uma condição modificada para o padrão original. • Personalizado: Uma regra de alerta que você criou. Você pode desabilitar, editar e remover regras de alerta personalizadas.
Status	Se esta regra de alerta está habilitada ou desabilitada no momento. As condições para regras de alerta desabilitadas não são avaliadas, portanto, nenhum alerta é acionado.

Crie regras de alerta personalizadas

Você pode criar regras de alerta personalizadas para definir suas próprias condições para acionar alertas.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Gerenciar alertas ou permissão de acesso root"](#) .
- Você está familiarizado com o ["métricas Prometheus comumente usadas"](#) .
- Você entende o ["sintaxe das consultas do Prometheus"](#) .
- Opcionalmente, você assistiu ao vídeo: ["Vídeo: Alertas personalizados"](#) .



Sobre esta tarefa

O StorageGRID não valida alertas personalizados. Se você decidir criar regras de alerta personalizadas, siga estas diretrizes gerais:

- Veja as condições das regras de alerta padrão e use-as como exemplos para suas regras de alerta personalizadas.
- Se você definir mais de uma condição para uma regra de alerta, use a mesma expressão para todas as condições. Em seguida, altere o valor limite para cada condição.
- Verifique cuidadosamente cada condição em busca de erros de digitação e de lógica.
- Use apenas as métricas listadas na API de gerenciamento de grade.
- Ao testar uma expressão usando a API de gerenciamento de grade, esteja ciente de que uma resposta "bem-sucedida" pode ser um corpo de resposta vazio (nenhum alerta acionado). Para ver se o alerta realmente foi acionado, você pode definir temporariamente um limite para um valor que você espera que seja verdadeiro no momento.

Por exemplo, para testar a expressão `node_memory_MemTotal_bytes < 24000000000` , primeiro execute `node_memory_MemTotal_bytes >= 0` e garantir que você obtenha os resultados esperados (todos os nós retornam um valor). Em seguida, altere o operador e o limite de volta para os valores pretendidos e execute novamente. Nenhum resultado indica que não há alertas atuais para esta expressão.

- Não presuma que um alerta personalizado está funcionando a menos que você tenha validado que o alerta foi disparado quando esperado.

Passos

1. Selecione **ALERTAS > Regras**.

A página Regras de alerta é exibida.

2. Selecione **Criar regra personalizada**.

A caixa de diálogo Criar regra personalizada é exibida.

Create Custom Rule

Enabled ☒

Unique Name

Description

Recommended Actions
(optional)

Conditions

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

5

minutes

Cancel

Save

3. Marque ou desmarque a caixa de seleção **Ativado** para determinar se esta regra de alerta está ativada no momento.

Se uma regra de alerta estiver desabilitada, suas expressões não serão avaliadas e nenhum alerta será acionado.

4. Insira as seguintes informações:

Campo	Descrição
Nome Único	Um nome exclusivo para esta regra. O nome da regra de alerta é exibido na página Alertas e também é o assunto das notificações por e-mail. Os nomes das regras de alerta podem ter entre 1 e 64 caracteres.

Campo	Descrição
Descrição	Uma descrição do problema que está ocorrendo. A descrição é a mensagem de alerta exibida na página Alertas e nas notificações por e-mail. As descrições das regras de alerta podem ter entre 1 e 128 caracteres.
Ações recomendadas	Opcionalmente, as ações recomendadas a serem tomadas quando este alerta for acionado. Insira as ações recomendadas como texto simples (sem códigos de formatação). As ações recomendadas para regras de alerta podem ter entre 0 e 1.024 caracteres.

- Na seção Condições, insira uma expressão do Prometheus para um ou mais níveis de gravidade do alerta.

Uma expressão básica geralmente tem a forma:

```
[metric] [operator] [value]
```

As expressões podem ter qualquer comprimento, mas aparecem em uma única linha na interface do usuário. Pelo menos uma expressão é necessária.

Esta expressão faz com que um alerta seja disparado se a quantidade de RAM instalada para um nó for menor que 24.000.000.000 bytes (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

Para ver as métricas disponíveis e testar as expressões do Prometheus, selecione o ícone de ajuda  e siga o link para a seção Métricas da API de gerenciamento de grade.

- No campo **Duração**, insira o tempo que uma condição deve permanecer continuamente em vigor antes que o alerta seja acionado e selecione uma unidade de tempo.

Para acionar um alerta imediatamente quando uma condição se tornar verdadeira, digite **0**. Aumente esse valor para evitar que condições temporárias acionem alertas.

O padrão é 5 minutos.

- Selecione **Salvar**.

A caixa de diálogo é fechada e a nova regra de alerta personalizada aparece na tabela Regras de alerta.

Editar regras de alerta

Você pode editar uma regra de alerta para alterar as condições de acionamento. Para uma regra de alerta personalizada, você também pode atualizar o nome da regra, a descrição e as ações recomendadas.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem o ["Gerenciar alertas ou permissão de acesso root"](#).

Sobre esta tarefa

Ao editar uma regra de alerta padrão, você pode alterar as condições para alertas secundários, principais e críticos; e a duração. Ao editar uma regra de alerta personalizada, você também pode editar o nome, a descrição e as ações recomendadas da regra.



Tenha cuidado ao decidir editar uma regra de alerta. Se você alterar os valores do gatilho, talvez não seja possível detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

Passos

1. Selecione **ALERTAS > Regras**.

A página Regras de alerta é exibida.

2. Selecione o botão de opção da regra de alerta que você deseja editar.
3. Selecione **Editar regra**.

A caixa de diálogo Editar regra é exibida. Este exemplo mostra uma regra de alerta padrão: os campos Nome exclusivo, Descrição e Ações recomendadas estão desabilitados e não podem ser editados.

Edit Rule - Low installed node memory

Enabled

☒

Unique Name

Low installed node memory

Description

The amount of installed memory on a node is low.

Recommended Actions (optional)

Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node.

See the instructions for your platform:

- [VMware installation](#)
- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)

Conditions

Minor

Major

node_memory_MemTotal_bytes < 24000000000

Critical

node_memory_MemTotal_bytes <= 12000000000

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

2

minutes

Cancel

Save

4. Marque ou desmarque a caixa de seleção **Ativado** para determinar se esta regra de alerta está ativada no

momento.

Se uma regra de alerta estiver desabilitada, suas expressões não serão avaliadas e nenhum alerta será acionado.



Se você desabilitar a regra de alerta para um alerta atual, deverá aguardar alguns minutos para que o alerta não apareça mais como um alerta ativo.



Em geral, não é recomendado desabilitar uma regra de alerta padrão. Se uma regra de alerta estiver desabilitada, você poderá não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

5. Para regras de alerta personalizadas, atualize as seguintes informações conforme necessário.



Você não pode editar essas informações para regras de alerta padrão.

Campo	Descrição
Nome Único	Um nome exclusivo para esta regra. O nome da regra de alerta é exibido na página Alertas e também é o assunto das notificações por e-mail. Os nomes das regras de alerta podem ter entre 1 e 64 caracteres.
Descrição	Uma descrição do problema que está ocorrendo. A descrição é a mensagem de alerta exibida na página Alertas e nas notificações por e-mail. As descrições das regras de alerta podem ter entre 1 e 128 caracteres.
Ações recomendadas	Opcionalmente, as ações recomendadas a serem tomadas quando este alerta for acionado. Insira as ações recomendadas como texto simples (sem códigos de formatação). As ações recomendadas para regras de alerta podem ter entre 0 e 1.024 caracteres.

6. Na seção Condições, insira ou atualize a expressão do Prometheus para um ou mais níveis de gravidade do alerta.



Se você quiser restaurar uma condição de uma regra de alerta padrão editada ao seu valor original, selecione os três pontos à direita da condição modificada.

Conditions ⓘ

Minor	
Major	node_memory_MemTotal_bytes < 2400000000
Critical	node_memory_MemTotal_bytes <= 1400000000





Se você atualizar as condições de um alerta atual, suas alterações poderão não ser implementadas até que a condição anterior seja resolvida. Na próxima vez que uma das condições da regra for atendida, o alerta refletirá os valores atualizados.

Uma expressão básica geralmente tem a forma:

```
[metric] [operator] [value]
```

As expressões podem ter qualquer comprimento, mas aparecem em uma única linha na interface do usuário. Pelo menos uma expressão é necessária.

Esta expressão faz com que um alerta seja disparado se a quantidade de RAM instalada para um nó for menor que 24.000.000.000 bytes (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

7. No campo **Duração**, insira o tempo que uma condição deve permanecer continuamente em vigor antes que o alerta seja acionado e selecione a unidade de tempo.

Para acionar um alerta imediatamente quando uma condição se tornar verdadeira, digite **0**. Aumente esse valor para evitar que condições temporárias acionem alertas.

O padrão é 5 minutos.

8. Selecione **Salvar**.

Se você editou uma regra de alerta padrão, **Padrão*** aparecerá na coluna Tipo. Se você desabilitou uma regra de alerta padrão ou personalizada, **Desabilitado** aparecerá na coluna **Status**.

Desativar regras de alerta

Você pode alterar o estado ativado/desativado de uma regra de alerta padrão ou personalizada.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem o ["Gerenciar alertas ou permissão de acesso root"](#).

Sobre esta tarefa

Quando uma regra de alerta é desabilitada, suas expressões não são avaliadas e nenhum alerta é acionado.



Em geral, não é recomendado desabilitar uma regra de alerta padrão. Se uma regra de alerta estiver desabilitada, você poderá não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

Passos

1. Selecione **ALERTAS > Regras**.

A página Regras de alerta é exibida.

2. Selecione o botão de opção da regra de alerta que você deseja desabilitar ou habilitar.

3. Selecione **Editar regra**.

A caixa de diálogo Editar regra é exibida.

4. Marque ou desmarque a caixa de seleção **Ativado** para determinar se esta regra de alerta está ativada no momento.

Se uma regra de alerta estiver desabilitada, suas expressões não serão avaliadas e nenhum alerta será acionado.



Se você desabilitar a regra de alerta para um alerta atual, deverá aguardar alguns minutos para que o alerta não seja mais exibido como um alerta ativo.

5. Selecione **Salvar**.

Desativado aparece na coluna **Status**.

Remover regras de alerta personalizadas

Você pode remover uma regra de alerta personalizada se não quiser mais usá-la.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem o ["Gerenciar alertas ou permissão de acesso root"](#).

Passos

1. Selecione **ALERTAS > Regras**.

A página Regras de alerta é exibida.

2. Selecione o botão de opção da regra de alerta personalizada que você deseja remover.

Você não pode remover uma regra de alerta padrão.

3. Selecione **Remover regra personalizada**.

Uma caixa de diálogo de confirmação é exibida.

4. Selecione **OK** para remover a regra de alerta.

Quaisquer instâncias ativas do alerta serão resolvidas em 10 minutos.

Gerenciar notificações de alerta

Configurar notificações SNMP para alertas

Se quiser que o StorageGRID envie notificações SNMP quando ocorrerem alertas, você deve habilitar o agente SNMP do StorageGRID e configurar um ou mais destinos de interceptação.

Você pode usar a opção **CONFIGURAÇÃO > Monitoramento > Agente SNMP** no Grid Manager ou os pontos de extremidade SNMP da Grid Management API para habilitar e configurar o agente SNMP do

StorageGRID . O agente SNMP suporta todas as três versões do protocolo SNMP.

Para aprender a configurar o agente SNMP, consulte "[Usar monitoramento SNMP](#)".

Depois de configurar o agente SNMP do StorageGRID , dois tipos de notificações orientadas a eventos podem ser enviadas:

- Armadilhas são notificações enviadas pelo agente SNMP que não exigem confirmação pelo sistema de gerenciamento. As armadilhas servem para notificar o sistema de gerenciamento de que algo aconteceu no StorageGRID, como um alerta sendo disparado. As armadilhas são suportadas em todas as três versões do SNMP.
- As informações são semelhantes às armadilhas, mas exigem reconhecimento pelo sistema de gerenciamento. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenviará a informação até que uma confirmação seja recebida ou o valor máximo de novas tentativas seja atingido. As informações são suportadas em SNMPv2c e SNMPv3.

Notificações de captura e informação são enviadas quando um alerta padrão ou personalizado é acionado em qualquer nível de gravidade. Para suprimir notificações SNMP de um alerta, você deve configurar um silêncio para o alerta. Ver "[Silenciar notificações de alerta](#)".

Se sua implantação do StorageGRID incluir vários nós de administração, o nó de administração principal será o remetente preferencial para notificações de alerta, pacotes de AutoSupport e traps e informações SNMP. Se o nó administrativo principal ficar indisponível, as notificações serão enviadas temporariamente por outros nós administrativos. Ver "[O que é um nó de administração?](#)".

Configurar notificações por e-mail para alertas

Se quiser que notificações por e-mail sejam enviadas quando ocorrerem alertas, você deve fornecer informações sobre seu servidor SMTP. Você também deve inserir os endereços de e-mail dos destinatários das notificações de alerta.

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você tem o "[Gerenciar alertas ou permissão de acesso root](#)".

Sobre esta tarefa

A configuração de e-mail usada para notificações de alerta não é usada para pacotes AutoSupport . No entanto, você pode usar o mesmo servidor de e-mail para todas as notificações.

Se sua implantação do StorageGRID incluir vários nós de administração, o nó de administração principal será o remetente preferencial para notificações de alerta, pacotes de AutoSupport e traps e informações SNMP. Se o nó administrativo principal ficar indisponível, as notificações serão enviadas temporariamente por outros nós administrativos. Ver "[O que é um nó de administração?](#)".

Passos

1. Selecione **ALERTAS > Configuração de e-mail**.

A página Configuração de e-mail é exibida.

2. Marque a caixa de seleção **Ativar notificações por e-mail** para indicar que você deseja que e-mails de notificação sejam enviados quando os alertas atingirem os limites configurados.

As seções Servidor de e-mail (SMTP), Segurança da camada de transporte (TLS), Endereços de e-mail e

Filtros são exibidas.

3. Na seção Servidor de e-mail (SMTP), insira as informações que o StorageGRID precisa para acessar seu servidor SMTP.

Se o seu servidor SMTP exigir autenticação, você deverá fornecer um nome de usuário e uma senha.

Campo	Digitar
Servidor de e-mail	O nome de domínio totalmente qualificado (FQDN) ou endereço IP do servidor SMTP.
Porta	A porta usada para acessar o servidor SMTP. Deve estar entre 1 e 65535.
Nome de usuário (opcional)	Se o seu servidor SMTP exigir autenticação, insira o nome de usuário para autenticação.
Senha (opcional)	Se o seu servidor SMTP exigir autenticação, digite a senha para autenticação.

4. Na seção Endereços de e-mail, insira os endereços de e-mail do remetente e de cada destinatário.
 - a. Para o **Endereço de e-mail do remetente**, especifique um endereço de e-mail válido para usar como endereço De para notificações de alerta.

Por exemplo: `storagegrid-alerts@example.com`

- b. Na seção Destinatários, insira um endereço de e-mail para cada lista de e-mail ou pessoa que deve receber um e-mail quando ocorrer um alerta.

Selecione o ícone de mais  para adicionar destinatários.

5. Se a Segurança da Camada de Transporte (TLS) for necessária para comunicações com o servidor SMTP, selecione **Exigir TLS** na seção Segurança da Camada de Transporte (TLS).

- a. No campo **Certificado CA**, forneça o certificado CA que será usado para verificar a identidade do servidor SMTP.

Você pode copiar e colar o conteúdo neste campo ou selecionar **Procurar** e selecionar o arquivo.

Você deve fornecer um único arquivo que contenha os certificados de cada autoridade certificadora (CA) emissora intermediária. O arquivo deve conter cada um dos arquivos de certificado CA codificados em PEM, concatenados na ordem da cadeia de certificados.

- b. Marque a caixa de seleção **Enviar certificado de cliente** se o seu servidor de e-mail SMTP exigir que os remetentes de e-mail forneçam certificados de cliente para autenticação.
 - c. No campo **Certificado do cliente**, forneça o certificado do cliente codificado em PEM para enviar ao servidor SMTP.

Você pode copiar e colar o conteúdo neste campo ou selecionar **Procurar** e selecionar o arquivo.

- d. No campo **Chave Privada**, insira a chave privada do certificado do cliente na codificação PEM não

criptografada.

Você pode copiar e colar o conteúdo neste campo ou selecionar **Procurar** e selecionar o arquivo.



Se precisar editar a configuração do e-mail, selecione o ícone de lápis para atualizar este campo.

6. Na seção Filtros, selecione quais níveis de gravidade de alerta devem resultar em notificações por e-mail, a menos que a regra para um alerta específico tenha sido silenciada.

Gravidade	Descrição
Menor, maior, crítico	Uma notificação por e-mail é enviada quando a condição menor, maior ou crítica de uma regra de alerta é atendida.
Importante, crítico	Uma notificação por e-mail é enviada quando a condição principal ou crítica para uma regra de alerta é atendida. Notificações não são enviadas para alertas menores.
Somente crítico	Uma notificação por e-mail é enviada somente quando a condição crítica para uma regra de alerta é atendida. Notificações não são enviadas para alertas menores ou maiores.

7. Quando estiver pronto para testar suas configurações de e-mail, execute estas etapas:

- a. Selecione **Enviar e-mail de teste**.

Uma mensagem de confirmação é exibida, indicando que um e-mail de teste foi enviado.

- b. Verifique as caixas de entrada de todos os destinatários de e-mail e confirme se um e-mail de teste foi recebido.



Se o e-mail não for recebido em alguns minutos ou se o alerta **Falha na notificação por e-mail** for acionado, verifique suas configurações e tente novamente.

- c. Sign in em qualquer outro nó de administração e envie um e-mail de teste para verificar a conectividade de todos os sites.



Ao testar notificações de alerta, você deve fazer login em cada nó de administração para verificar a conectividade. Isso contrasta com o teste de pacotes do AutoSupport, em que todos os nós administrativos enviam o e-mail de teste.

8. Selecione **Salvar**.

O envio de um e-mail de teste não salva suas configurações. Você deve selecionar **Salvar**.

As configurações de e-mail são salvas.

Informações incluídas nas notificações de alerta por e-mail

Após configurar o servidor de e-mail SMTP, notificações por e-mail serão enviadas aos destinatários designados quando um alerta for acionado, a menos que a regra de alerta seja suprimida por um silêncio. Ver

"Silenciar notificações de alerta" .

As notificações por e-mail incluem as seguintes informações:

NetApp StorageGRID

Low object data storage (6 alerts) ①

The space available for storing object data is low. ②

Recommended actions ③

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

Node DC1-S1-226 ④
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

DC1-S2-227

Node DC1-S2-227
Site DC1 225-230
Severity Minor
Time triggered Fri Jun 28 14:43:27 UTC 2019
Job storagegrid
Service ldr

Sent from: DC1-ADM1-225 ⑤

Chamar	Descrição
1	O nome do alerta, seguido pelo número de instâncias ativas deste alerta.
2	A descrição do alerta.
3	Quaisquer ações recomendadas para o alerta.
4	Detalhes sobre cada instância ativa do alerta, incluindo o nó e o site afetados, a gravidade do alerta, o horário UTC em que a regra de alerta foi acionada e o nome do trabalho e serviço afetados.
5	O nome do host do nó de administração que enviou a notificação.

Como os alertas são agrupados

Para evitar que um número excessivo de notificações por e-mail seja enviado quando os alertas são acionados, o StorageGRID tenta agrupar vários alertas na mesma notificação.

Consulte a tabela a seguir para obter exemplos de como o StorageGRID agrupa vários alertas em notificações por e-mail.

Comportamento	Exemplo
Cada notificação de alerta se aplica somente a alertas que tenham o mesmo nome. Se dois alertas com nomes diferentes forem disparados ao mesmo tempo, duas notificações por e-mail serão enviadas.	• O alerta A é acionado em dois nós ao mesmo tempo. Apenas uma notificação é enviada. • O alerta A é acionado no nó 1 e o alerta B é acionado no nó 2 ao mesmo tempo. Duas notificações são enviadas — uma para cada alerta.
Para um alerta específico em um nó específico, se os limites forem atingidos para mais de uma gravidade, uma notificação será enviada apenas para o alerta mais grave.	• O alerta A é acionado e os limites de alerta menor, maior e crítico são atingidos. Uma notificação é enviada para o alerta crítico.
Na primeira vez que um alerta é disparado, o StorageGRID aguarda 2 minutos antes de enviar uma notificação. Se outros alertas com o mesmo nome forem acionados durante esse período, o StorageGRID agrupará todos os alertas na notificação inicial.	1. O alerta A é acionado no nó 1 às 08:00. Nenhuma notificação é enviada. 2. O alerta A é acionado no nó 2 às 08:01. Nenhuma notificação é enviada. 3. Às 08:02, uma notificação é enviada para relatar ambas as instâncias do alerta.
Se outro alerta com o mesmo nome for acionado, o StorageGRID aguardará 10 minutos antes de enviar uma nova notificação. A nova notificação relata todos os alertas ativos (alertas atuais que não foram silenciados), mesmo que tenham sido relatados anteriormente.	1. O alerta A é acionado no nó 1 às 08:00. Uma notificação é enviada às 08:02. 2. O alerta A é acionado no nó 2 às 08:05. Uma segunda notificação é enviada às 08:15 (10 minutos depois). Ambos os nós são relatados.
Se houver vários alertas atuais com o mesmo nome e um deles for resolvido, uma nova notificação não será enviada se o alerta ocorrer novamente no nó para o qual o alerta foi resolvido.	1. O alerta A é acionado para o nó 1. Uma notificação é enviada. 2. O alerta A é acionado para o nó 2. Uma segunda notificação é enviada. 3. O alerta A é resolvido para o nó 2, mas permanece ativo para o nó 1. 4. O alerta A é acionado novamente para o nó 2. Nenhuma nova notificação é enviada porque o alerta ainda está ativo para o nó 1.
O StorageGRID continua enviando notificações por e-mail uma vez a cada 7 dias até que todas as instâncias do alerta sejam resolvidas ou a regra de alerta seja silenciada.	1. O alerta A é acionado para o nó 1 em 8 de março. Uma notificação é enviada. 2. O alerta A não foi resolvido nem silenciado. Notificações adicionais são enviadas em 15 de março, 22 de março, 29 de março e assim por diante.

Solucionar problemas de notificações de alerta por e-mail

Se o alerta **Falha na notificação por e-mail** for acionado ou você não conseguir receber a notificação por e-mail de alerta de teste, siga estas etapas para resolver o problema.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Gerenciar alertas ou permissão de acesso root"](#) .

Passos

1. Verifique suas configurações.
 - a. Selecione **ALERTAS > Configuração de e-mail**.
 - b. Verifique se as configurações do servidor de e-mail (SMTP) estão corretas.
 - c. Verifique se você especificou endereços de e-mail válidos para os destinatários.
2. Verifique seu filtro de spam e certifique-se de que o e-mail não foi enviado para uma pasta de lixo eletrônico.
3. Peça ao seu administrador de e-mail para confirmar se os e-mails do endereço do remetente não estão sendo bloqueados.
4. Colete um arquivo de log para o nó de administração e entre em contato com o suporte técnico.

O suporte técnico pode usar as informações nos logs para ajudar a determinar o que deu errado. Por exemplo, o arquivo prometheus.log pode mostrar um erro ao conectar-se ao servidor especificado.

Ver ["Coletar arquivos de log e dados do sistema"](#) .

Silenciar notificações de alerta

Opcionalmente, você pode configurar silêncios para suprimir temporariamente notificações de alerta.

Antes de começar

- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#) .
- Você tem o ["Gerenciar alertas ou permissão de acesso root"](#) .

Sobre esta tarefa

Você pode silenciar regras de alerta em toda a grade, em um único site ou em um único nó e para uma ou mais severidades. Cada silêncio suprime todas as notificações para uma única regra de alerta ou para todas as regras de alerta.

Se você tiver habilitado o agente SNMP, os silêncios também suprimem as interceptações e informações SNMP.



Tenha cuidado ao decidir silenciar uma regra de alerta. Se você silenciar um alerta, poderá não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica.

Passos

1. Selecione **ALERTAS > Silêncios**.

A página Silêncios é exibida.

Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

+ Create

Edit

Remove

Alert Rule	Description	Severity	Time Remaining	Nodes
No results found.				

2. Selecione **Criar**.

A caixa de diálogo Criar Silêncio é exibida.

Create Silence

Alert Rule

Description (optional)

Duration

Minutes

Severity

Minor only

Minor, major

Minor, major, critical

Nodes

StorageGRID Deployment

Data Center 1

DC1-ADM1

DC1-G1

DC1-S1

DC1-S2

DC1-S3

Cancel

Save

3. Selecione ou insira as seguintes informações:

Campo	Descrição
Regra de Alerta	O nome da regra de alerta que você deseja silenciar. Você pode selecionar qualquer regra de alerta padrão ou personalizada, mesmo que a regra de alerta esteja desabilitada. Observação: Selecione Todas as regras se quiser silenciar todas as regras de alerta usando os critérios especificados nesta caixa de diálogo.

Campo	Descrição
Descrição	Opcionalmente, uma descrição do silêncio. Por exemplo, descreva o propósito desse silêncio.
Duração	Por quanto tempo você quer que esse silêncio permaneça em vigor, em minutos, horas ou dias. O silêncio pode vigorar de 5 minutos a 1.825 dias (5 anos). Observação: você não deve silenciar uma regra de alerta por um longo período de tempo. Se uma regra de alerta for silenciada, você poderá não detectar um problema subjacente até que ele impeça a conclusão de uma operação crítica. No entanto, pode ser necessário usar um silêncio prolongado se um alerta for disparado por uma configuração específica e intencional, como pode ser o caso dos alertas Link do dispositivo de serviços inativo e Link do dispositivo de armazenamento inativo.
Gravidade	Qual(is) gravidade(s) de alerta deve(m) ser silenciada(s). Se o alerta for disparado em uma das gravidades selecionadas, nenhuma notificação será enviada.
Nós	A qual nó ou nós você deseja que esse silêncio seja aplicado. Você pode suprimir uma regra de alerta ou todas as regras na grade inteira, em um único site ou em um único nó. Se você selecionar a grade inteira, o silêncio será aplicado a todos os sites e todos os nós. Se você selecionar um site, o silêncio se aplicará somente aos nós naquele site. Observação: você não pode selecionar mais de um nó ou mais de um site para cada silêncio. Você deve criar silêncios adicionais se quiser suprimir a mesma regra de alerta em mais de um nó ou mais de um site ao mesmo tempo.

4. Selecione **Salvar**.

5. Se quiser modificar ou encerrar um silêncio antes que ele expire, você pode editá-lo ou removê-lo.

Opção	Descrição
Editar um silêncio	a. Selecione ALERTAS > Silêncios. b. Na tabela, selecione o botão de opção para o silêncio que você deseja editar. c. Selecione Editar. d. Altere a descrição, o tempo restante, as gravidades selecionadas ou o nó afetado. e. Selecione Salvar.

Opção	Descrição
Remover um silêncio	a. Selecione ALERTAS > Silêncios. b. Na tabela, selecione o botão de opção para o silêncio que você deseja remover. c. Selecione Remover. d. Selecione OK para confirmar que deseja remover esse silêncio. Observação: agora as notificações serão enviadas quando este alerta for acionado (a menos que seja suprimido por outro silêncio). Se este alerta estiver acionado no momento, pode levar alguns minutos para que as notificações por e-mail ou SNMP sejam enviadas e para que a página Alertas seja atualizada.

Informações relacionadas

["Configurar o agente SNMP"](#)

Referência de alertas

Esta referência lista os alertas padrão que aparecem no Grid Manager. As ações recomendadas estão na mensagem de alerta que você recebe.

Conforme necessário, você pode criar regras de alerta personalizadas para se adequar à sua abordagem de gerenciamento de sistema.

Alguns dos alertas padrão usam ["Métricas do Prometheus"](#).

Alertas de aparelhos

Nome do alerta	Descrição
Bateria do aparelho vencida	A bateria no controlador de armazenamento do aparelho expirou.
A bateria do aparelho falhou	A bateria no controlador de armazenamento do aparelho falhou.
A bateria do aparelho tem capacidade de aprendizagem insuficiente	A bateria no controlador de armazenamento do aparelho não tem capacidade de aprendizagem suficiente.
Bateria do aparelho próxima da validade	A bateria no controlador de armazenamento do aparelho está quase acabando.
Bateria do aparelho removida	A bateria no controlador de armazenamento do aparelho está faltando.
Bateria do aparelho muito quente	A bateria no controlador de armazenamento do aparelho está superaquecida.

Nome do alerta	Descrição
Erro de comunicação BMC do aparelho	A comunicação com o controlador de gerenciamento da placa de base (BMC) foi perdida.
Falha detectada no dispositivo de inicialização do aparelho	Foi detectado um problema com o dispositivo de inicialização no dispositivo.
Falha no dispositivo de backup do cache do aparelho	Um dispositivo de backup de cache persistente falhou.
Capacidade insuficiente do dispositivo de backup de cache do aparelho	Não há capacidade suficiente no dispositivo de backup de cache.
Dispositivo de backup de cache do aparelho protegido contra gravação	Um dispositivo de backup de cache é protegido contra gravação.
Incompatibilidade de tamanho de memória cache do dispositivo	Os dois controladores no dispositivo têm tamanhos de cache diferentes.
Falha na bateria do CMOS do aparelho	Foi detectado um problema com a bateria CMOS do aparelho.
Temperatura do chassi do controlador de computação do dispositivo muito alta	A temperatura do controlador de computação em um dispositivo StorageGRID excedeu um limite nominal.
Temperatura da CPU do controlador de computação do dispositivo muito alta	A temperatura da CPU no controlador de computação em um dispositivo StorageGRID excedeu um limite nominal.
O controlador de computação do dispositivo precisa de atenção	Uma falha de hardware foi detectada no controlador de computação de um dispositivo StorageGRID .
A fonte de alimentação do controlador de computação do aparelho A tem um problema	A fonte de alimentação A no controlador de computação tem um problema.
A fonte de alimentação do controlador de computação do aparelho B tem um problema	A fonte de alimentação B no controlador de computação tem um problema.
O serviço de monitoramento de hardware de computação do dispositivo foi interrompido	O serviço que monitora o status do hardware de armazenamento parou.

Nome do alerta	Descrição
Unidade DAS do dispositivo excedendo o limite de dados gravados por dia	Uma quantidade excessiva de dados está sendo gravada em uma unidade todos os dias, o que pode anular sua garantia.
Falha detectada na unidade DAS do aparelho	Um problema foi detectado com uma unidade de armazenamento de conexão direta (DAS) no dispositivo.
Luz localizadora do acionamento DAS do aparelho acesa	A luz do localizador de unidade para uma ou mais unidades de armazenamento de conexão direta (DAS) em um nó de armazenamento do dispositivo está acesa.
Reconstrução da unidade DAS do aparelho	Uma unidade de armazenamento de conexão direta (DAS) está sendo reconstruída. Isso é esperado se ele foi substituído ou removido/reinserida recentemente.
Falha detectada no ventilador do aparelho	Foi detectado um problema com uma unidade de ventilação do aparelho.
Falha de canal de fibra do aparelho detectada	Um problema de link Fibre Channel foi detectado entre o controlador de armazenamento do dispositivo e o controlador de computação
Falha na porta HBA do Fibre Channel do aparelho	Uma porta HBA Fibre Channel está falhando ou falhou.
Unidades de cache flash do dispositivo não são ideais	As unidades usadas para o cache SSD não são ideais.
Interconexão do aparelho/recipiente da bateria removido	O compartimento de interconexão/bateria está faltando.
Porta LACP do aparelho ausente	Uma porta em um dispositivo StorageGRID não está participando do vínculo LACP.
Falha na placa de rede do dispositivo detectada	Foi detectado um problema com uma placa de interface de rede (NIC) no dispositivo.
O fornecimento geral de energia do aparelho está degradado	A alimentação de um dispositivo StorageGRID desviou-se da tensão operacional recomendada.
Aviso crítico de SSD do aparelho	Um SSD de dispositivo está relatando um aviso crítico.
Falha do controlador de armazenamento do dispositivo A	O controlador de armazenamento A em um dispositivo StorageGRID falhou.

Nome do alerta	Descrição
Falha do controlador de armazenamento do aparelho B	O controlador de armazenamento B em um dispositivo StorageGRID falhou.
Falha na unidade do controlador de armazenamento do dispositivo	Uma ou mais unidades em um dispositivo StorageGRID falharam ou não estão ideais.
Problema de hardware do controlador de armazenamento do dispositivo	O software SANtricity está relatando "Precisa de atenção" para um componente em um dispositivo StorageGRID .
Falha na fonte de alimentação A do controlador de armazenamento do aparelho	A fonte de alimentação A em um dispositivo StorageGRID desviou-se da tensão operacional recomendada.
Falha na fonte de alimentação B do controlador de armazenamento do aparelho	A fonte de alimentação B em um dispositivo StorageGRID desviou-se da tensão operacional recomendada.
O serviço de monitoramento de hardware de armazenamento do dispositivo foi interrompido	O serviço que monitora o status do hardware de armazenamento parou.
Prateleiras de armazenamento de eletrodomésticos degradadas	O status de um dos componentes na prateleira de armazenamento de um dispositivo de armazenamento está degradado.
Temperatura do aparelho excedida	A temperatura nominal ou máxima do controlador de armazenamento do aparelho foi excedida.
Sensor de temperatura do aparelho removido	Um sensor de temperatura foi removido.
Erro de inicialização segura UEFI do dispositivo	Um dispositivo não foi inicializado com segurança.
A E/S do disco é muito lenta	E/S de disco muito lentas podem estar afetando o desempenho da grade.
Falha detectada no ventilador do aparelho de armazenamento	Foi detectado um problema com uma unidade de ventilador no controlador de armazenamento de um aparelho.
Conectividade de armazenamento do dispositivo de armazenamento degradada	Há um problema com uma ou mais conexões entre o controlador de computação e o controlador de armazenamento.
Dispositivo de armazenamento inacessível	Não é possível acessar um dispositivo de armazenamento.

Alertas de auditoria e syslog

Nome do alerta	Descrição
Os logs de auditoria estão sendo adicionados à fila na memória	O nó não pode enviar logs para o servidor syslog local e a fila na memória está ficando cheia.
Erro de encaminhamento do servidor syslog externo	O nó não pode encaminhar logs para o servidor syslog externo.
Grande fila de auditoria	A fila de disco para mensagens de auditoria está cheia. Se essa condição não for resolvida, as operações do S3 ou Swift poderão falhar.
Os logs estão sendo adicionados à fila no disco	O nó não pode encaminhar logs para o servidor syslog externo e a fila no disco está ficando cheia.

Alertas de balde

Nome do alerta	Descrição
O bucket FabricPool tem uma configuração de consistência de bucket não suportada	Um bucket FabricPool usa o nível de consistência Available ou Strong-site, que não é suportado.
O bucket FabricPool tem uma configuração de controle de versão não suportada	Um bucket FabricPool tem controle de versão ou bloqueio de objeto S3 habilitado, que não são suportados.

Alertas de Cassandra

Nome do alerta	Descrição
Erro do compactador automático do Cassandra	Ocorreu um erro no compactador automático Cassandra.
Métricas do compactador automático Cassandra desatualizadas	As métricas que descrevem o autocompactador Cassandra estão desatualizadas.
Erro de comunicação do Cassandra	Os nós que executam o serviço Cassandra estão tendo problemas para se comunicar entre si.
Compactações de Cassandra sobrecarregadas	O processo de compactação do Cassandra está sobrecarregado.
Erro de gravação de tamanho excessivo do Cassandra	Um processo interno do StorageGRID enviou uma solicitação de gravação ao Cassandra que era muito grande.

Nome do alerta	Descrição
Métricas de reparo do Cassandra desatualizadas	As métricas que descrevem os trabalhos de reparo do Cassandra estão desatualizadas.
Progresso lento no reparo do Cassandra	O progresso dos reparos do banco de dados Cassandra é lento.
Serviço de reparo Cassandra não disponível	O serviço de reparo do Cassandra não está disponível.
Corrupção da tabela Cassandra	Cassandra detectou corrupção de tabela. O Cassandra reinicia automaticamente se detectar corrupção de tabela.

Alertas do Cloud Storage Pool

Nome do alerta	Descrição
Erro de conectividade do Cloud Storage Pool	A verificação de integridade dos pools de armazenamento em nuvem detectou um ou mais novos erros.
Expiração da certificação de entidade final do IAM Roles Anywhere	O certificado de entidade final do IAM Roles Anywhere está prestes a expirar.

Alertas de replicação entre grades

Nome do alerta	Descrição
Falha permanente na replicação entre redes	Ocorreu um erro de replicação entre grades que requer intervenção do usuário para ser resolvido.
Recursos de replicação entre redes indisponíveis	Solicitações de replicação entre grades estão pendentes porque um recurso não está disponível.

Alertas DHCP

Nome do alerta	Descrição
Concessão de DHCP expirada	O contrato de concessão de DHCP em uma interface de rede expirou.
Concessão de DHCP expirando em breve	O contrato de concessão de DHCP em uma interface de rede expirará em breve.
Servidor DHCP indisponível	O servidor DHCP não está disponível.

Alertas de depuração e rastreamento

Nome do alerta	Descrição
Impacto no desempenho da depuração	Quando o modo de depuração está ativado, o desempenho do sistema pode ser afetado negativamente.
Configuração de rastreamento habilitada	Quando a configuração de rastreamento está ativada, o desempenho do sistema pode ser afetado negativamente.

Alertas de e-mail e AutoSupport

Nome do alerta	Descrição
Falha ao enviar a mensagem do AutoSupport	A mensagem mais recente do AutoSupport falhou ao ser enviada.
Falha na resolução do nome de domínio	O nó StorageGRID não conseguiu resolver nomes de domínio.
Falha na notificação por e-mail	Não foi possível enviar a notificação por e-mail de um alerta.
Erros de informação SNMP	Erros ao enviar notificações de informação SNMP para um destino de interceptação.
Login SSH ou console detectado	Nas últimas 24 horas, um usuário fez login com o Web Console ou SSH.

Alertas de codificação de apagamento (EC)

Nome do alerta	Descrição
Falha de rebalanceamento da CE	O procedimento de rebalanceamento da CE falhou ou foi interrompido.
Falha no reparo da CE	Um trabalho de reparo para dados EC falhou ou foi interrompido.
Reparo da CE paralisado	Um trabalho de reparo de dados da CE foi interrompido.
Erro de verificação de fragmento codificado por apagamento	Fragmentos codificados por apagamento não podem mais ser verificados. Fragmentos corrompidos podem não ser reparados.

Alertas de expiração de certificados

Nome do alerta	Descrição
Expiração do certificado CA do Proxy de Administração	Um ou mais certificados no pacote de CA do servidor proxy de administração estão prestes a expirar.
Expiração do certificado do cliente	Um ou mais certificados de cliente estão prestes a expirar.

Nome do alerta	Descrição
Expiração do certificado global do servidor para S3 e Swift	O certificado do servidor global para S3 e Swift está prestes a expirar.
Expiração do certificado de ponto de extremidade do balanceador de carga	Um ou mais certificados de ponto de extremidade do balanceador de carga estão prestes a expirar.
Expiração do certificado do servidor para interface de gerenciamento	O certificado do servidor usado para a interface de gerenciamento está prestes a expirar.
Expiração do certificado CA do syslog externo	O certificado da autoridade de certificação (CA) usado para assinar o certificado do servidor syslog externo está prestes a expirar.
Expiração do certificado do cliente syslog externo	O certificado do cliente para um servidor syslog externo está prestes a expirar.
Expiração do certificado do servidor syslog externo	O certificado do servidor apresentado pelo servidor syslog externo está prestes a expirar.

Alertas de rede de grade

Nome do alerta	Descrição
Incompatibilidade de MTU da rede de grade	A configuração de MTU para a interface da rede Grid (eth0) difere significativamente entre os nós da grade.

Alertas de federação de rede

Nome do alerta	Descrição
Expiração do certificado de federação de rede	Um ou mais certificados de federação de rede estão prestes a expirar.
Falha na conexão da federação de rede	A conexão da federação de rede entre a rede local e a remota não está funcionando.

Alertas de alto uso ou alta latência

Nome do alerta	Descrição
Alto uso de heap Java	Uma alta porcentagem do espaço de heap do Java está sendo usada.
Alta latência para consultas de metadados	O tempo médio para consultas de metadados do Cassandra é muito longo.

Alertas de federação de identidade

Nome do alerta	Descrição
Falha na sincronização da federação de identidade	Não é possível sincronizar grupos federados e usuários da fonte de identidade.
Falha na sincronização da federação de identidade para um locatário	Não é possível sincronizar grupos federados e usuários da fonte de identidade configurada por um locatário.

Alertas de gerenciamento do ciclo de vida da informação (ILM)

Nome do alerta	Descrição
Posicionamento ILM inatingível	Uma instrução de posicionamento em uma regra ILM não pode ser obtida para determinados objetos.
Taxa de varredura ILM baixa	A taxa de varredura do ILM está definida para menos de 100 objetos/segundo.

Alertas do servidor de gerenciamento de chaves (KMS)

Nome do alerta	Descrição
Expiração do certificado KMS CA	O certificado da autoridade de certificação (CA) usado para assinar o certificado do servidor de gerenciamento de chaves (KMS) está prestes a expirar.
Expiração do certificado do cliente KMS	O certificado do cliente para um servidor de gerenciamento de chaves está prestes a expirar
Falha ao carregar a configuração do KMS	A configuração do servidor de gerenciamento de chaves existe, mas falhou ao carregar.
Erro de conectividade do KMS	Um nó do dispositivo não pôde se conectar ao servidor de gerenciamento de chaves do seu site.
Nome da chave de criptografia KMS não encontrado	O servidor de gerenciamento de chaves configurado não possui uma chave de criptografia que corresponda ao nome fornecido.
Falha na rotação da chave de criptografia do KMS	Todos os volumes do dispositivo foram descriptografados com sucesso, mas um ou mais volumes não puderam ser girados para a chave mais recente.
O KMS não está configurado	Não existe nenhum servidor de gerenciamento de chaves para este site.

Nome do alerta	Descrição
A chave KMS falhou ao descriptografar um volume do dispositivo	Um ou mais volumes em um dispositivo com criptografia de nó habilitada não puderam ser descriptografados com a chave KMS atual.
Expiração do certificado do servidor KMS	O certificado do servidor usado pelo servidor de gerenciamento de chaves (KMS) está prestes a expirar.
Falha de conectividade do servidor KMS	Um nó do dispositivo não pôde se conectar a um ou mais servidores no cluster do servidor de gerenciamento de chaves do seu site.

Alertas do balanceador de carga

Nome do alerta	Descrição
Conexões elevadas do balanceador de carga de solicitação zero	Uma porcentagem elevada de conexões com endpoints do balanceador de carga foram desconectadas sem executar solicitações.

Alertas de deslocamento do relógio local

Nome do alerta	Descrição
Grande deslocamento de tempo do relógio local	O deslocamento entre o relógio local e o horário do Protocolo de Tempo de Rede (NTP) é muito grande.

Alertas de pouca memória ou pouco espaço

Nome do alerta	Descrição
Baixa capacidade do disco de log de auditoria	O espaço disponível para logs de auditoria é baixo. Se essa condição não for resolvida, as operações do S3 ou Swift poderão falhar.
Memória de nó baixa disponível	A quantidade de RAM disponível em um nó é baixa.
Pouco espaço livre para pool de armazenamento	O espaço disponível para armazenar dados de objetos no Nó de Armazenamento é baixo.
Baixa memória de nó instalada	A quantidade de memória instalada em um nó é baixa.
Baixo armazenamento de metadados	O espaço disponível para armazenar metadados de objetos é baixo.
Baixa capacidade de disco de métricas	O espaço disponível para o banco de dados de métricas é baixo.

Nome do alerta	Descrição
Armazenamento de dados de objetos baixos	O espaço disponível para armazenar dados de objetos é baixo.
Substituição de marca d'água somente leitura	A substituição da marca d'água somente leitura do volume de armazenamento é menor que a marca d'água otimizada mínima para um nó de armazenamento.
Baixa capacidade do disco raiz	O espaço disponível no disco raiz é baixo.
Baixa capacidade de dados do sistema	O espaço disponível para /var/local é baixo. Se essa condição não for resolvida, as operações do S3 ou Swift poderão falhar.
Pouco espaço livre no diretório tmp	O espaço disponível no diretório /tmp é baixo.

Alertas de nó ou rede de nó

Nome do alerta	Descrição
Uso de recebimento da rede de administração	O uso de recebimento na Rede de Administração é alto.
Uso de transmissão da rede de administração	O uso de transmissão na rede de administração é alto.
Falha na configuração do firewall	Falha ao aplicar a configuração do firewall.
Pontos de extremidade da interface de gerenciamento em modo de fallback	Todos os pontos de extremidade da interface de gerenciamento estão retornando às portas padrão há muito tempo.
Erro de conectividade de rede do nó	Ocorreram erros durante a transferência de dados entre nós.
Erro de quadro de recepção de rede de nó	Uma alta porcentagem dos quadros de rede recebidos por um nó continham erros.
Nó não sincronizado com o servidor NTP	O nó não está sincronizado com o servidor de protocolo de tempo de rede (NTP).
Nó não bloqueado com servidor NTP	O nó não está bloqueado em um servidor de protocolo de tempo de rede (NTP).
Rede de nós não pertencentes ao dispositivo inoperante	Um ou mais dispositivos de rede estão inativos ou desconectados.

Nome do alerta	Descrição
Link do dispositivo de serviços inativo na rede de administração	A interface do dispositivo para a rede de administração (eth1) está inativa ou desconectada.
O link do dispositivo de serviços está inativo na porta 1 da rede de administração	A porta 1 da rede de administração no dispositivo está inativa ou desconectada.
Link do dispositivo de serviços inativo na rede do cliente	A interface do dispositivo para a rede do cliente (eth2) está inativa ou desconectada.
O link do dispositivo de serviços está inativo na porta de rede 1	A porta de rede 1 no dispositivo está inativa ou desconectada.
Link do dispositivo de serviços inativo na porta de rede 2	A porta de rede 2 do dispositivo está inativa ou desconectada.
Link do dispositivo de serviços inativo na porta de rede 3	A porta de rede 3 do dispositivo está inativa ou desconectada.
Link do dispositivo de serviços inativo na porta de rede 4	A porta de rede 4 do dispositivo está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na rede de administração	A interface do dispositivo para a rede de administração (eth1) está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na porta 1 da rede de administração	A porta 1 da rede de administração no dispositivo está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na rede do cliente	A interface do dispositivo para a rede do cliente (eth2) está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na porta de rede 1	A porta de rede 1 no dispositivo está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na porta de rede 2	A porta de rede 2 do dispositivo está inativa ou desconectada.
Link do dispositivo de armazenamento inativo na porta de rede 3	A porta de rede 3 do dispositivo está inativa ou desconectada.

Nome do alerta	Descrição
Link do dispositivo de armazenamento inativo na porta de rede 4	A porta de rede 4 do dispositivo está inativa ou desconectada.
Nó de armazenamento não está no estado de armazenamento desejado	O serviço LDR em um nó de armazenamento não pode fazer a transição para o estado desejado devido a um erro interno ou problema relacionado ao volume
Uso da conexão TCP	O número de conexões TCP neste nó está se aproximando do número máximo que pode ser rastreado.
Não é possível comunicar com o nó	Um ou mais serviços não respondem ou o nó não pode ser alcançado.
Reinicialização inesperada do nó	Um nó foi reinicializado inesperadamente nas últimas 24 horas.

Alertas de objetos

Nome do alerta	Descrição
Falha na verificação de existência do objeto	A tarefa de verificação da existência do objeto falhou.
Verificação de existência de objeto paralisada	O trabalho de verificação de existência do objeto foi interrompido.
Objetos perdidos	Um ou mais objetos foram perdidos da grade.
Tamanho do objeto S3 PUT muito grande	Um cliente está tentando uma operação PUT Object que excede os limites de tamanho do S3.
Objeto corrompido não identificado detectado	Foi encontrado um arquivo no armazenamento de objetos replicados que não pôde ser identificado como um objeto replicado.

Alertas de serviços de plataforma

Nome do alerta	Descrição
Capacidade de solicitação pendente dos Serviços de Plataforma baixa	O número de solicitações pendentes dos Serviços de Plataforma está se aproximando da capacidade.
Serviços de plataforma indisponíveis	Poucos nós de armazenamento com o serviço RSM estão em execução ou disponíveis em um site.

Alertas de volume de armazenamento

Nome do alerta	Descrição
O volume de armazenamento precisa de atenção	Um volume de armazenamento está offline e precisa de atenção.
O volume de armazenamento precisa ser restaurado	Um volume de armazenamento foi recuperado e precisa ser restaurado.
Volume de armazenamento offline	Um volume de armazenamento ficou offline por mais de 5 minutos.
Tentativa de remontagem do volume de armazenamento	Um volume de armazenamento estava offline e acionou uma remontagem automática. Isso pode indicar um problema na unidade ou erros no sistema de arquivos.
A restauração de volume falhou ao iniciar o reparo de dados replicados	O reparo de dados replicados para um volume reparado não pôde ser iniciado automaticamente.

Alertas de serviços do StorageGRID

Nome do alerta	Descrição
serviço nginx usando configuração de backup	A configuração do serviço nginx é inválida. A configuração anterior agora está sendo usada.
serviço nginx-gw usando configuração de backup	A configuração do serviço nginx-gw é inválida. A configuração anterior agora está sendo usada.
Reinicialização necessária para desabilitar o FIPS	A política de segurança não requer o modo FIPS, mas o Módulo de Segurança Criptográfica NetApp está habilitado.
Reinicialização necessária para habilitar o FIPS	A política de segurança requer o modo FIPS, mas o Módulo de Segurança Criptográfica NetApp está desabilitado.
Serviço SSH usando configuração de backup	A configuração do serviço SSH é inválida. A configuração anterior agora está sendo usada.

Alertas de inquilinos

Nome do alerta	Descrição
Uso de cota de inquilino alto	Uma alta porcentagem do espaço de cota está sendo usada. Esta regra está desabilitada por padrão porque pode causar muitas notificações.

Métricas do Prometheus comumente usadas

Consulte esta lista de métricas do Prometheus comumente usadas para entender melhor as condições nas regras de alerta padrão ou para construir as condições para regras de alerta personalizadas.

Você também pode [obter uma lista completa de todas as métricas](#) .

Para obter detalhes sobre a sintaxe das consultas do Prometheus, consulte "[Consultando Prometeu](#)" .

O que são métricas do Prometheus?

As métricas do Prometheus são medições de séries temporais. O serviço Prometheus nos nós administrativos coleta essas métricas dos serviços em todos os nós. As métricas são armazenadas em cada nó administrativo até que o espaço reservado para dados do Prometheus esteja cheio. Quando o `/var/local/mysql_ibdata/` quando o volume atinge a capacidade, as métricas mais antigas são excluídas primeiro.

Onde as métricas do Prometheus são usadas?

As métricas coletadas pelo Prometheus são usadas em vários lugares no Grid Manager:

- **Página Nós:** Os gráficos e tabelas nas guias disponíveis na página Nós usam a ferramenta de visualização Grafana para exibir as métricas de séries temporais coletadas pelo Prometheus. O Grafana exibe dados de séries temporais em formatos de gráfico e tabela, enquanto o Prometheus serve como fonte de dados de back-end.



- **Alertas:** Os alertas são acionados em níveis de gravidade específicos quando as condições da regra de alerta que usam métricas do Prometheus são avaliadas como verdadeiras.
- **API de gerenciamento de grade:** você pode usar métricas do Prometheus em regras de alerta personalizadas ou com ferramentas de automação externas para monitorar seu sistema StorageGRID . Uma lista completa de métricas do Prometheus está disponível na API de gerenciamento de grade. (Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API > métricas**.) Embora mais de mil métricas estejam disponíveis, apenas um número relativamente pequeno é necessário para monitorar as operações mais críticas do StorageGRID .



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

- A página **SUORTE > Ferramentas > Diagnóstico** e a página **SUORTE > Ferramentas > Métricas**: Essas páginas, que são destinadas principalmente ao uso do suporte técnico, fornecem diversas ferramentas e gráficos que usam os valores das métricas do Prometheus.



Alguns recursos e itens de menu na página Métricas são intencionalmente não funcionais e estão sujeitos a alterações.

Lista das métricas mais comuns

A lista a seguir contém as métricas do Prometheus mais comumente usadas.



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

alertmanager_notifications_failed_total

O número total de notificações de alerta com falha.

bytes disponíveis do sistema de arquivos do nó

A quantidade de espaço do sistema de arquivos disponível para usuários não root em bytes.

node_memory_MemAvailable_bytes

Campo de informações de memória MemAvailable_bytes.

portadora_de_rede_nó

Valor da transportadora de `/sys/class/net/iface` .

total_de_errores_de_recebimento_de_nó_rede

Estatística do dispositivo de rede `receive_errs` .

total_de_errores_de_transmissão_de_nó

Estatística do dispositivo de rede `transmit_errs` .

storagegrid_administrativamente_inativo

O nó não está conectado à rede por um motivo esperado. Por exemplo, o nó, ou os serviços no nó, foram desligados corretamente, o nó está sendo reinicializado ou o software está sendo atualizado.

status_do_hardware_do_controlador_de_computação_do_dispositivo_de_grade_de_armazenamento

O status do hardware do controlador de computação em um dispositivo.

storagegrid_appliance_discos_com_falha

Para o controlador de armazenamento em um dispositivo, o número de unidades que não são ideais.

status do hardware do controlador de armazenamento do dispositivo de grade de armazenamento

O status geral do hardware do controlador de armazenamento em um dispositivo.

balde_e_contêineres_de_conteúdo_da_grade_de_armazenamento

O número total de buckets S3 e contêineres Swift conhecidos por este nó de armazenamento.

objetos_de_conteúdo_da_grade_de_armazenamento

O número total de objetos de dados S3 e Swift conhecidos por este nó de armazenamento. A contagem é

válida somente para objetos de dados criados por aplicativos clientes que fazem interface com o sistema por meio do S3.

objetos_de_conteúdo_da_grade_de_armazenamento_perdidos

O número total de objetos que este serviço detecta como ausentes no sistema StorageGRID . Devem ser tomadas medidas para determinar a causa da perda e se a recuperação é possível.

["Solucionar problemas de dados de objetos perdidos e ausentes"](#)

tentativas_de_entrada_de_sessões_http_da_grade_de_armazenamento

O número total de sessões HTTP que foram tentadas em um nó de armazenamento.

storagegrid_http_sessions_incoming_atualmente_estabelecidas

O número de sessões HTTP que estão atualmente ativas (abertas) no nó de armazenamento.

storagegrid_http_sessions_incoming_failed

O número total de sessões HTTP que não foram concluídas com sucesso, seja devido a uma solicitação HTTP malformada ou a uma falha durante o processamento de uma operação.

storagegrid_http_sessions_incoming_sucesso

O número total de sessões HTTP que foram concluídas com sucesso.

storagegrid_ilm_aguardando_objetos_de_fundo

O número total de objetos neste nó aguardando avaliação do ILM da verificação.

storagegrid_ilm_aguardando_objetos_de_avaliação_do_cliente_por_segundo

A taxa atual na qual os objetos são avaliados em relação à política ILM neste nó.

storagegrid_ilm_aguardando_objetos_do_cliente

O número total de objetos neste nó aguardando avaliação do ILM de operações do cliente (por exemplo, ingestão).

storagegrid_ilm_aguardando_total_objetos

O número total de objetos aguardando avaliação do ILM.

storagegrid_ilm_scan_objetos_por_segundo

A taxa na qual os objetos pertencentes a este nó são verificados e enfileirados para ILM.

período_de_varredura_do_ilm_da_grade_de_armazenamento_minutos_estimados

Tempo estimado para concluir uma varredura ILM completa neste nó.

Observação: uma verificação completa não garante que o ILM foi aplicado a todos os objetos pertencentes a este nó.

tempo_de_expiração_do_certificado_do_endpoint_do_balanceador_de_carga_da_grade_de_armazenamento

O tempo de expiração do certificado do ponto de extremidade do balanceador de carga em segundos desde a época.

consultas_de_metadados_da_grade_de_armazenamento_latência_média_em_milissegundos

O tempo médio necessário para executar uma consulta no repositório de metadados por meio deste serviço.

bytes_recebidos_da_rede_de_grade_de_armazenamento

A quantidade total de dados recebidos desde a instalação.

bytes_transmitidos_da_rede_de_grade_de_armazenamento

A quantidade total de dados enviados desde a instalação.

porcentagem_de_utilização_da_cpu_do_nó_da_grade_de_armazenamento

A porcentagem de tempo de CPU disponível atualmente sendo usada por este serviço. Indica o quão ocupado o serviço está. A quantidade de tempo de CPU disponível depende do número de CPUs do servidor.

storagegrid_ntp_tempo_fonte_escolhido_deslocamento_em_milissegundos

Deslocamento sistemático de tempo fornecido por uma fonte de tempo escolhida. O deslocamento é introduzido quando o atraso para atingir uma fonte de tempo não é igual ao tempo necessário para que a fonte de tempo atinja o cliente NTP.

storagegrid_ntp_bloqueado

O nó não está bloqueado para um servidor NTP (Network Time Protocol).

storagegrid_s3_data_transfers_bytes_ingested

A quantidade total de dados ingeridos de clientes S3 para este nó de armazenamento desde a última redefinição do atributo.

storagegrid_s3_data_transfers_bytes_retrieved

A quantidade total de dados recuperados pelos clientes S3 deste nó de armazenamento desde a última redefinição do atributo.

storagegrid_s3_operations_failed

O número total de operações S3 com falha (códigos de status HTTP 4xx e 5xx), excluindo aquelas causadas por falha de autorização S3.

storagegrid_s3_operations_successful

O número total de operações S3 bem-sucedidas (código de status HTTP 2xx).

storagegrid_s3_operations_unauthorized

O número total de operações S3 com falha que são resultado de uma falha de autorização.

dias_de_expiração_do_certificado_do_servidor_de_grade_de_armazenamento_da_interface_de_gerenciamento_do_certificado

O número de dias antes do certificado da Interface de Gerenciamento expirar.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

O número de dias antes da expiração do certificado da API de armazenamento de objetos.

segundos_da_cpu_do_serviço_da_grade_de_armazenamento

A quantidade cumulativa de tempo que a CPU foi usada por este serviço desde a instalação.

bytes_de_uso_de_memória_do_serviço_de_grade_de_armazenamento

A quantidade de memória (RAM) atualmente em uso por este serviço. Este valor é idêntico ao exibido pelo utilitário Linux top como RES.

bytes_recebidos_da_rede_de_serviço_de_grade_de_armazenamento

A quantidade total de dados recebidos por este serviço desde a instalação.

bytes_transmitidos_pela_rede_de_serviço_de_grade_de_armazenamento

A quantidade total de dados enviados por este serviço.

reinicializações do serviço de storagegrid

O número total de vezes que o serviço foi reiniciado.

segundos_de_tempo_de_execução_do_serviço_de_grade_de_armazenamento

O tempo total em que o serviço está em execução desde a instalação.

segundos_de_tempo_de_atividade_do_serviço_da_grade_de_armazenamento

O tempo total em que o serviço ficou em execução desde que foi reiniciado pela última vez.

estado_de_armazenamento_atual_da_grade_de_armazenamento

O estado atual dos serviços de armazenamento. Os valores dos atributos são:

- 10 = Off-line
- 15 = Manutenção
- 20 = Somente leitura
- 30 = On-line

status_de_armazenamento_da_grade_de_armazenamento

O status atual dos serviços de armazenamento. Os valores dos atributos são:

- 0 = Sem erros
- 10 = Em transição
- 20 = Espaço livre insuficiente
- 30 = Volume(s) indisponíveis
- 40 = Erro

bytes_de_dados_de_utilização_de_armazenamento_da_grade_de_armazenamento

Uma estimativa do tamanho total de dados de objetos replicados e codificados para eliminação no Nó de Armazenamento.

utilização_de_metadados_de_armazenamento_da_grade_de_armazenamento_bytes_permitidos

O espaço total no volume 0 de cada nó de armazenamento permitido para metadados de objeto. Esse valor é sempre menor que o espaço real reservado para metadados em um nó, porque uma parte do espaço reservado é necessária para operações essenciais do banco de dados (como compactação e reparo) e futuras atualizações de hardware e software. O espaço permitido para metadados de objetos controla a capacidade geral do objeto.

bytes_de_metadados_de_utilização_de_armazenamento_da_grade_de_armazenamento

A quantidade de metadados do objeto no volume de armazenamento 0, em bytes.

utilização_de_armazenamento_da_grade_de_armazenamento_total_de_bytes_de_espço

A quantidade total de espaço de armazenamento alocado para todos os armazenamentos de objetos.

utilização_de_armazenamento_da_grade_de_armazenamento_bytes_de_espaco_utilizável

A quantidade total de espaço de armazenamento de objetos restante. Calculado somando a quantidade de espaço disponível para todos os armazenamentos de objetos no Nó de Armazenamento.

storagegrid_swift_data_transfers_bytes_ingestados

A quantidade total de dados ingeridos de clientes Swift para este nó de armazenamento desde a última redefinição do atributo.

storagegrid_swift_data_transfers_bytes_recuperados

A quantidade total de dados recuperados pelos clientes Swift deste nó de armazenamento desde a última redefinição do atributo.

falha nas operações rápidas da grade de armazenamento

O número total de operações Swift com falha (códigos de status HTTP 4xx e 5xx), excluindo aquelas causadas por falha de autorização Swift.

storagegrid_swift_operações_bem-sucedidas

O número total de operações Swift bem-sucedidas (código de status HTTP 2xx).

storagegrid_swift_operações_não autorizadas

O número total de operações Swift com falha que são resultado de uma falha de autorização (códigos de status HTTP 401, 403, 405).

bytes de dados de uso do locatário da grade de armazenamento

O tamanho lógico de todos os objetos para o locatário.

contagem_de_objetos_de_uso_do_locatário_da_grade_de_armazenamento

O número de objetos para o inquilino.

cota_bytes_de_uso_do_locatário_da_grade_de_armazenamento

A quantidade máxima de espaço lógico disponível para os objetos do locatário. Se uma métrica de cota não for fornecida, uma quantidade ilimitada de espaço estará disponível.

Obtenha uma lista de todas as métricas

Para obter a lista completa de métricas, use a API de gerenciamento de grade.

1. Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Documentação da API**.
2. Localize as operações **métricas**.
3. Executar o GET `/grid/metric-names` operação.
4. Baixe os resultados.

Referência de arquivos de log

Referência de arquivos de log

O StorageGRID fornece logs que são usados para capturar eventos, mensagens de diagnóstico e condições de erro. Você pode ser solicitado a coletar arquivos de log e encaminhá-los ao suporte técnico para ajudar na solução de problemas.

Os logs são categorizados da seguinte forma:

- ["Registros do software StorageGRID"](#)
- ["Registros de implantação e manutenção"](#)
- ["Sobre o bycast.log"](#)



Os detalhes fornecidos para cada tipo de log são apenas para referência. Os logs são destinados à solução de problemas avançada pelo suporte técnico. Técnicas avançadas que envolvem a reconstrução do histórico de problemas usando os logs de auditoria e os arquivos de log do aplicativo estão além do escopo destas instruções.

Acessar os logs

Para acessar os logs, você pode ["coletar arquivos de log e dados do sistema"](#) de um ou mais nós como um único arquivo de log. Ou, se o nó de administração principal não estiver disponível ou não conseguir acessar um nó específico, você poderá acessar arquivos de log individuais para cada nó de grade da seguinte maneira:

1. Digite o seguinte comando: `ssh admin@grid_node_IP`
2. Digite a senha listada no `Passwords.txt` arquivo.
3. Digite o seguinte comando para alternar para root: `su -`
4. Digite a senha listada no `Passwords.txt` arquivo.

Exportar logs para o servidor syslog

Exportar os logs para o servidor syslog fornece estes recursos:

- Receba uma lista de todas as solicitações do Grid Manager e do Tenant Manager, além das solicitações do S3 e do Swift.
- Melhor visibilidade das solicitações do S3 que retornam erros, sem o impacto no desempenho causado pelos métodos de registro de auditoria.
- Acesso a solicitações de camada HTTP e códigos de erro fáceis de analisar.
- Melhor visibilidade das solicitações que foram bloqueadas pelos classificadores de tráfego no balanceador de carga.

Para exportar os logs, consulte ["Configurar mensagens de auditoria e destinos de log"](#) .

Categorias de arquivos de log

O arquivo de log do StorageGRID contém os logs descritos para cada categoria e arquivos adicionais que contém métricas e saída de comando de depuração.

Localização do arquivo	Descrição
auditoria	Mensagens de auditoria geradas durante a operação normal do sistema.
base-os-logs	Informações básicas do sistema operacional, incluindo versões de imagem do StorageGRID .

Localização do arquivo	Descrição
pacotes	Informações de configuração global (pacotes).
Cassandra	Informações do banco de dados Cassandra e logs de reparo do Reaper.
CE	Informações do VCS sobre o nó atual e informações do grupo EC por ID de perfil.
grade	Registros gerais da grade, incluindo depuração(<code>bycast.log</code>) e <code>servermanager</code> registros.
grade.json	Arquivo de configuração de grade compartilhado entre todos os nós. Adicionalmente, <code>node.json</code> é específico para o nó atual.
hagrupos	Métricas e logs de grupos de alta disponibilidade.
instalar	<code>Gdu-server</code> e instalar logs.
Lambda-árbitro	Logs relacionados à solicitação de proxy do S3 Select.
lenhador.log	Mensagens de depuração relacionadas à coleta de logs.
Métricas	Logs de serviço para Grafana, Jaeger, exportador de nós e Prometheus.
miscd	Acessos e logs de erros diversos.
MySQL	A configuração do banco de dados mariaDB e logs relacionados.
Líquido	Logs gerados por scripts relacionados à rede e pelo serviço Dynip.
nginx	Arquivos de configuração e logs do balanceador de carga e da federação de grade. Inclui também registros de tráfego do Grid Manager e do Tenant Manager.

Localização do arquivo	Descrição
nginx-gw	• <code>access.log</code>: Mensagens de log de solicitações do Grid Manager e do Tenant Manager. ◦ Essas mensagens são prefixadas com <code>mgmt</code>: quando exportado usando <code>syslog</code>. ◦ O formato dessas mensagens de log é <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$request" "\$http_host" "\$http_user_agent" "\$http_referer"</code> • <code>cgr-access.log.gz</code>: Solicitações de replicação entre grades de entrada. ◦ Essas mensagens são prefixadas com <code>cgr</code>: quando exportado usando <code>syslog</code>. ◦ O formato dessas mensagens de log é <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code> • <code>endpoint-access.log.gz</code>: Solicitações S3 e Swift para endpoints do balanceador de carga. ◦ Essas mensagens são prefixadas com <code>endpoint</code>: quando exportado usando <code>syslog</code>. ◦ O formato dessas mensagens de log é <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code> • <code>nginx-gw-dns-check.log</code>: Relacionado ao novo alerta de verificação de DNS.
ntp	Arquivo de configuração e logs do NTP.
Objetos órfãos	Registros referentes a objetos órfãos.
sistema operacional	Arquivo de estado de nó e grade, incluindo serviços <code>pid</code> .
outro	Arquivos de log em <code>/var/local/log</code> que não são coletados em outras pastas.
desempenho	Informações de desempenho para CPU, rede e E/S de disco.
prometheus-data	Métricas atuais do Prometheus, se a coleção de logs incluir dados do Prometheus.
provisionamento	Logs relacionados ao processo de provisionamento da rede.
jangada	Logs do cluster Raft usados em serviços de plataforma.

Localização do arquivo	Descrição
ssh	Logs relacionados à configuração e serviço SSH.
snmp	Configuração do agente SNMP usada para enviar notificações SNMP.
soquetes-dados	Dados de soquetes para depuração de rede.
comandos-do-sistema.txt	Saída dos comandos do contêiner StorageGRID . Contém informações do sistema, como rede e uso de disco.
pacote de recuperação de sincronização	Relacionado à manutenção da consistência do Pacote de Recuperação mais recente em todos os Nós de Administração e Nós de Armazenamento que hospedam o serviço ADC.

Registros do software StorageGRID

Você pode usar os logs do StorageGRID para solucionar problemas.



Se você deseja enviar seus logs para um servidor syslog externo ou alterar o destino das informações de auditoria, como `bycast.log` e `nms.log` , ver ["Configurar mensagens de auditoria e destinos de log"](#) .

Logs do StorageGRID geral

Nome do arquivo	Notas	Encontrado em
/var/local/log/bycast.log	O arquivo principal de solução de problemas do StorageGRID . Selecione SUORTE > Ferramentas > Topologia de grade . Em seguida, selecione Site > Nó > SSM > Eventos .	Todos os nós
/var/local/log/bycast-err.log	Contém um subconjunto de <code>bycast.log</code> (mensagens com gravidade ERRO e CRÍTICO). Mensagens CRÍTICAS também são exibidas no sistema. Selecione SUORTE > Ferramentas > Topologia de grade . Em seguida, selecione Site > Nó > SSM > Eventos .	Todos os nós

Nome do arquivo	Notas	Encontrado em
/var/local/núcleo/	Contém todos os arquivos de despejo de memória criados caso o programa seja encerrado de forma anormal. As causas possíveis incluem falhas de asserção, violações ou tempos limite de thread. Nota: O arquivo <code>`/var/local/core/kexec_cmd</code> geralmente existe em nós de dispositivos e não indica um erro.	Todos os nós

Registros relacionados à cifra

Nome do arquivo	Notas	Encontrado em
/var/local/log/ssh-config-generation.log	Contém logs relacionados à geração de configurações SSH e ao recarregamento de serviços SSH.	Todos os nós
/var/local/log/nginx/config-generation.log	Contém logs relacionados à geração de configurações nginx e ao recarregamento de serviços nginx.	Todos os nós
/var/local/log/nginx-gw/config-generation.log	Contém logs relacionados à geração de configurações do nginx-gw (e ao recarregamento de serviços do nginx-gw).	Nós de administração e gateway
/var/local/log/atualizar-configurações-de-cifra.log	Contém logs relacionados à configuração de políticas TLS e SSH.	Todos os nós

Registros de federação de grade

Nome do arquivo	Notas	Encontrado em
/var/local/log/update_grid_federation_config.log	Contém logs relacionados à geração de configurações nginx e nginx-gw para conexões de federação de grade.	Todos os nós

Registros NMS

Nome do arquivo	Notas	Encontrado em
/var/local/log/nms.log	• Captura notificações do Grid Manager e do Tenant Manager. • Captura eventos relacionados à operação do serviço NMS. Por exemplo, notificações por e-mail e alterações de configuração. • Contém atualizações de pacotes XML resultantes de alterações de configuração feitas no sistema. • Contém mensagens de erro relacionadas à redução de amostragem de atributos feita uma vez por dia. • Contém mensagens de erro do servidor web Java, por exemplo, erros de geração de página e erros HTTP Status 500.	Nós de administração
/var/local/log/nms.errlog	Contém mensagens de erro relacionadas a atualizações do banco de dados MySQL. Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Há um arquivo de log por serviço. Esses arquivos geralmente estão vazios, a menos que haja problemas com o serviço.	Nós de administração
/var/local/log/nms.requestlog	Contém informações sobre conexões de saída da API de gerenciamento para serviços internos do StorageGRID .	Nós de administração

Logs do Gerenciador de Servidores

Nome do arquivo	Notas	Encontrado em
/var/local/log/servermanager.log	Arquivo de log do aplicativo Gerenciador do Servidor em execução no servidor.	Todos os nós
/var/local/log/GridstatBackend.errlog	Arquivo de log para o aplicativo de backend da GUI do Gerenciador do Servidor.	Todos os nós
/var/local/log/gridstat.errlog	Arquivo de log para a GUI do Gerenciador do Servidor.	Todos os nós

Registros de serviços do StorageGRID

Nome do arquivo	Notas	Encontrado em
/var/local/log/acct.errlog		Nós de armazenamento executando o serviço ADC
/var/local/log/adc.errlog	Contém o fluxo de erro padrão (stderr) dos serviços correspondentes. Há um arquivo de log por serviço. Esses arquivos geralmente estão vazios, a menos que haja problemas com o serviço.	Nós de armazenamento executando o serviço ADC
/var/local/log/ams.errlog		Nós de administração
/var/local/log/cassandra/system.log	Informações para o armazenamento de metadados (banco de dados Cassandra) que podem ser usadas se ocorrerem problemas ao adicionar novos nós de armazenamento ou se a tarefa de reparo do nodetool parar.	Nós de armazenamento
/var/local/log/cassandra-reaper.log	Informações para o serviço Cassandra Reaper, que realiza reparos dos dados no banco de dados Cassandra.	Nós de armazenamento
/var/local/log/cassandra-reaper.errlog	Informações de erro para o serviço Cassandra Reaper.	Nós de armazenamento
/var/local/log/chunk.errlog		Nós de armazenamento
/var/local/log/cmn.errlog		Nós de administração
/var/local/log/cms.errlog	Este arquivo de log pode estar presente em sistemas que foram atualizados de uma versão mais antiga do StorageGRID. Ele contém informações legadas.	Nós de armazenamento
/var/local/log/dds.errlog		Nós de armazenamento
/var/local/log/dmv.errlog		Nós de armazenamento
/var/local/log/dynip*	Contém logs relacionados ao serviço dynip, que monitora a grade em busca de alterações dinâmicas de IP e atualiza a configuração local.	Todos os nós

Nome do arquivo	Notas	Encontrado em
/var/local/log/grafana.log	O log associado ao serviço Grafana, que é usado para visualização de métricas no Grid Manager.	Nós de administração
/var/local/log/hagroups.log	O log associado aos grupos de alta disponibilidade.	Nós de administração e nós de gateway
/var/local/log/hagroups_events.log	Rastreia mudanças de estado, como transição de BACKUP para MASTER ou FAULT.	Nós de administração e nós de gateway
/var/local/log/idnt.errlog		Nós de armazenamento executando o serviço ADC
/var/local/log/jaeger.log	O log associado ao serviço jaeger, que é usado para coleta de rastreamento.	Todos os nós
/var/local/log/kstn.errlog		Nós de armazenamento executando o serviço ADC
/var/local/log/lambda*	Contém logs para o serviço S3 Select.	Nós de administração e gateway Somente certos nós de administração e gateway contêm esse log. Veja o "Requisitos e limitações do S3 Select para nós de administração e gateway" .
/var/local/log/ldr.errlog		Nós de armazenamento
/var/local/log/miscd/*.log	Contém logs para o serviço MISCd (Information Service Control Daemon), que fornece uma interface para consultar e gerenciar serviços em outros nós e para gerenciar configurações ambientais no nó, como consultar o estado de serviços em execução em outros nós.	Todos os nós

Nome do arquivo	Notas	Encontrado em
/var/local/log/nginx/*.log	Contém logs para o serviço nginx, que atua como um mecanismo de autenticação e comunicação segura para vários serviços de grade (como Prometheus e Dynip) para poder se comunicar com serviços em outros nós por meio de APIs HTTPS.	Todos os nós
/var/local/log/nginx-gw/*.log	Contém logs gerais relacionados ao serviço nginx-gw, incluindo logs de erros e logs para portas de administração restritas em nós de administração.	Nós de administração e nós de gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contém logs de acesso relacionados ao tráfego de replicação entre redes.	Nós de administração, nós de gateway ou ambos, com base na configuração de federação da grade. Encontrado somente na grade de destino para replicação entre grades.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contém logs de acesso para o serviço Load Balancer, que fornece balanceamento de carga do tráfego S3 de clientes para nós de armazenamento.	Nós de administração e nós de gateway
/var/local/log/persistence*	Contém logs para o serviço Persistência, que gerencia arquivos no disco raiz que precisam persistir após uma reinicialização.	Todos os nós
/var/local/log/prometheus.log	Para todos os nós, contém o log de serviço do exportador de nós e o log de serviço de métricas do ade-exporter. Para nós de administração, também contém logs para os serviços Prometheus e Alert Manager.	Todos os nós
/var/local/log/raft.log	Contém a saída da biblioteca usada pelo serviço RSM para o protocolo Raft.	Nós de armazenamento com serviço RSM
/var/local/log/rms.errlog	Contém logs para o serviço Replicated State Machine Service (RSM), que é usado para serviços da plataforma S3.	Nós de armazenamento com serviço RSM

Nome do arquivo	Notas	Encontrado em
/var/local/log/ssm.errlog		Todos os nós
/var/local/log/atualização-s3vs-domains.log	Contém logs relacionados ao processamento de atualizações para a configuração de nomes de domínio hospedados virtuais do S3. Consulte as instruções para implementar aplicativos cliente do S3.	Nós de administração e gateway
/var/local/log/atualização-snmp-firewall.*	Contém logs relacionados às portas do firewall gerenciadas para SNMP.	Todos os nós
/var/local/log/atualização-sysl.log	Contém logs relacionados às alterações feitas na configuração do syslog do sistema.	Todos os nós
/var/local/log/atualizar-classes-de-traffic.log	Contém logs relacionados a alterações na configuração dos classificadores de tráfego.	Nós de administração e gateway
/var/local/log/update-utcn.log	Contém logs relacionados ao modo de rede de cliente não confiável neste nó.	Todos os nós

Informações relacionadas

- ["Sobre o bycast.log"](#)
- ["Usar API REST do S3"](#)

Registros de implantação e manutenção

Você pode usar os logs de implantação e manutenção para solucionar problemas.

Nome do arquivo	Notas	Encontrado em
/var/local/log/install.log	Criado durante a instalação do software. Contém um registro dos eventos de instalação.	Todos os nós
/var/local/log/expansion-progress.log	Criado durante as operações de expansão. Contém um registro dos eventos de expansão.	Nós de armazenamento
/var/local/log/pa-move.log	Criado durante a execução do <code>pa-move.sh</code> roteiro.	Nó de administração primário
/var/local/log/pa-move-new_pa.log	Criado durante a execução do <code>pa-move.sh</code> roteiro.	Nó de administração primário

Nome do arquivo	Notas	Encontrado em
/var/local/log/pa-move-old_pa.log	Criado durante a execução do <code>pa-move.sh</code> roteiro.	Nó de administração primário
/var/local/log/gdu-server.log	Criado pelo serviço GDU. Contém eventos relacionados aos procedimentos de provisionamento e manutenção gerenciados pelo nó de administração principal.	Nó de administração primário
/var/local/log/send_admin_hw.log	Criado durante a instalação. Contém informações de depuração relacionadas às comunicações de um nó com o nó de administração principal.	Todos os nós
/var/local/log/upgrade.log	Criado durante a atualização do software. Contém um registro dos eventos de atualização de software.	Todos os nós

Sobre o bycast.log

O arquivo `/var/local/log/bycast.log` é o arquivo principal de solução de problemas do software StorageGRID. Há um `bycast.log` arquivo para cada nó da grade. O arquivo contém mensagens específicas para aquele nó da grade.

O arquivo `/var/local/log/bycast-err.log` é um subconjunto de `bycast.log`. Ele contém mensagens de gravidade ERRO e CRÍTICO.

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado. Ver ["Configurar mensagens de auditoria e destinos de log"](#).

Rotação de arquivos para bycast.log

Quando o `bycast.log` o arquivo atinge 1 GB, o arquivo existente é salvo e um novo arquivo de log é iniciado.

O arquivo salvo é renomeado `bycast.log.1`, e o novo arquivo é nomeado `bycast.log`. Quando o novo `bycast.log` atinge 1 GB, `bycast.log.1` é renomeado e compactado para se tornar `bycast.log.2.gz`, e `bycast.log` é renomeado `bycast.log.1`.

O limite de rotação para `bycast.log` são 21 arquivos. Quando a 22ª versão do `bycast.log` arquivo é criado, o arquivo mais antigo é excluído.

O limite de rotação para `bycast-err.log` são sete arquivos.



Se um arquivo de log foi compactado, você não deve descompactá-lo no mesmo local em que foi gravado. Descompactar o arquivo no mesmo local pode interferir nos scripts de rotação de log.

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado. Ver ["Configurar mensagens de auditoria e destinos de log"](#).

Informações relacionadas

["Coletar arquivos de log e dados do sistema"](#)

Mensagens em bycast.log

Mensagens em `bycast.log` são escritos pelo ADE (Ambiente Distribuído Assíncrono). ADE é o ambiente de execução usado pelos serviços de cada nó da grade.

Exemplo de mensagem ADE:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685      0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

As mensagens ADE contêm as seguintes informações:

Segmento de mensagem	Valor no exemplo
ID do nó	12455685
ID do processo ADE	0357819531
Nome do módulo	SVMR
Identificador de mensagem	EVHR
Hora do sistema UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-DDTHH:MM:SS.uuuuuu)
Nível de gravidade	ERRO
Número de rastreamento interno	0906
Mensagem	SVMR: A verificação de integridade do volume 3 falhou com o motivo 'TOUT'

Gravidade das mensagens em bycast.log

As mensagens em `bycast.log` são atribuídos níveis de gravidade.

Por exemplo:

- **AVISO** — Ocorreu um evento que deveria ser registrado. A maioria das mensagens de log estão neste nível.
- **AVISO** — Ocorreu uma condição inesperada.
- **ERRO** — Ocorreu um erro grave que afetará as operações.
- **CRÍTICO** — Ocorreu uma condição anormal que interrompeu as operações normais. Você deve tratar a condição subjacente imediatamente.

Códigos de erro em `bycast.log`

A maioria das mensagens de erro em `bycast.log` contém códigos de erro.

A tabela a seguir lista códigos não numéricos comuns em `bycast.log`. O significado exato de um código não numérico depende do contexto em que ele é relatado.

Código de erro	Significado
SUCS	Nenhum erro
GERR	Desconhecido
CANC	Cancelado
ABRT	Abortado
TOTALMENTE	Tempo esgotado
INVL	Inválido
NFND	Não encontrado
VERS	Versão
CONF	Configuração
FALHAR	Fracassado
ICPL	Incompleto
FEITO	Feito
SUNV	Serviço não disponível

A tabela a seguir lista os códigos de erro numéricos em `bycast.log`.

Número do erro	Código de erro	Significado
001	EPERM	Operação não permitida
002	ENOENTE	Não existe tal arquivo ou diretório
003	ESRCH	Não existe tal processo
004	EINTR	Chamada de sistema interrompida

Número do erro	Código de erro	Significado
005	EIO	Erro de E/S
006	ENXIO	Nenhum dispositivo ou endereço desse tipo
007	E2BIG	Lista de argumentos muito longa
008	ENOEXEC	Erro de formato Exec
009	EBADF	Número de arquivo inválido
010	CRANÇA	Nenhum processo filho
011	NOVAMENTE	Tente novamente
012	ENOMEM	Sem memória
013	EACCES	Permissão negada
014	FALHA	Endereço incorreto
015	ENOTBLK	Dispositivo de bloqueio necessário
016	EBUSY	Dispositivo ou recurso ocupado
017	EEXIST	O arquivo existe
018	EXDEV	Link entre dispositivos
019	ENODEV	Nenhum dispositivo desse tipo
020	ENOTDIR	Não é um diretório
021	EISDIR	É um diretório
022	EINVAL	Argumento inválido
023	ENFILE	Estouro de tabela de arquivos
024	EMFILE	Muitos arquivos abertos
025	NÃO É NADA	Não é uma máquina de escrever
026	ETXTBSY	Arquivo de texto ocupado

Número do erro	Código de erro	Significado
027	EFBIG	Arquivo muito grande
028	ENOSPC	Não há espaço disponível no dispositivo
029	ESPIAR	Busca ilegal
030	EROFS	Sistema de arquivos somente leitura
031	EMLINK	Muitos links
032	EPIPE	Cano quebrado
033	EDOM	Argumento matemático fora do domínio da função
034	ERRANGE	Resultado matemático não representável
035	EDEADLK	Ocorreria um impasse de recursos
036	ENAMETOOLONG	Nome do arquivo muito longo
037	ENOLCK	Nenhum bloqueio de registro disponível
038	ENOSYS	Função não implementada
039	ENOTEMPTY	Diretório não vazio
040	ELOOP	Muitos links simbólicos encontrados
041		
042	ENOMSG	Nenhuma mensagem do tipo desejado
043	EIDRM	Identificador removido
044	ECHRNG	Número do canal fora do intervalo
045	EL2NSYNC	Nível 2 não sincronizado
046	EL3HLT	Nível 3 interrompido
047	EL3RST	Redefinição de nível 3
048	ELNRNG	Número do link fora do intervalo

Número do erro	Código de erro	Significado
049	EUNATCHE	Driver de protocolo não anexado
050	ENOCSE	Nenhuma estrutura CSI disponível
051	EL2HLT	Nível 2 interrompido
052	EBADE	Troca inválida
053	EBADR	Descritor de solicitação inválido
054	EXFULL	Troca completa
055	ENOANO	Sem ânodo
056	EBADRQC	Código de solicitação inválido
057	EBADSLT	Slot inválido
058		
059	EBFONT	Formato de arquivo de fonte incorreto
060	ENOSTR	O dispositivo não é um fluxo
061	ENODADOS	Nenhum dado disponível
062	ETIME	Temporizador expirado
063	ENOSR	Recursos fora dos fluxos
064	ENONET	A máquina não está na rede
065	ENOPKG	Pacote não instalado
066	REMOTO	O objeto é remoto
067	ENOLINK	O link foi rompido
068	EADV	Erro de anúncio
069	ESRMNT	Erro Srmount
070	ECOMM	Erro de comunicação no envio

Número do erro	Código de erro	Significado
071	EPROTO	Erro de protocolo
072	EMULTIHOP	Tentativa de multi-hop
073	EDOTDOT	Erro específico do RFS
074	EBADMSG	Não é uma mensagem de dados
075	E_OVERFLOW	Valor muito grande para o tipo de dados definido
076	ENOTUNIQ	Nome não exclusivo na rede
077	EBADFD	Descritor de arquivo em mau estado
078	EREMCHG	Endereço remoto alterado
079	ELIBACC	Não é possível acessar uma biblioteca compartilhada necessária
080	ELIBBAD	Acessando uma biblioteca compartilhada corrompida
081	ELIBSCN	
082	ELIBMAX	Tentando vincular muitas bibliotecas compartilhadas
083	ELIBEXEC	Não é possível executar uma biblioteca compartilhada diretamente
084	EILSEQ	Sequência de bytes ilegal
085	ERESTART	A chamada de sistema interrompida deve ser reiniciada
086	ESTRPIPE	Erro de canal de fluxos
087	USUÁRIOS	Muitos usuários
088	ENOTSOCK	Operação de soquete em não soquete
089	EDESTADDRREQ	Endereço de destino obrigatório
090	TAMANHO EMSGS	Mensagem muito longa

Número do erro	Código de erro	Significado
091	EPROTÓTIPO	Protocolo tipo errado para soquete
092	ENOPROTOOPT	Protocolo não disponível
093	EPROTONOSUPPORT	Protocolo não suportado
094	SUPORTE ESOCKTNOS	Tipo de soquete não suportado
095	EOPNOTSUPP	Operação não suportada no ponto de extremidade de transporte
096	EPFNOSUPPORT	Família de protocolo não suportada
097	APOIO EAFNOS	Família de endereços não suportada pelo protocolo
098	USO DE DRINCO PRINCIPAL	Endereço já em uso
099	EDDRNOTAVAIL	Não é possível atribuir o endereço solicitado
100	ENETDOWN	A rede está inativa
101	ENETUNREACH	A rede está inacessível
102	ENETRESET	A rede perdeu a conexão devido à reinicialização
103	ECONNABORTED	O software causou o encerramento da conexão
104	REINICIALIZAÇÃO ECONÔMICA	Conexão redefinida pelo peer
105	ENOBUFS	Não há espaço de buffer disponível
106	EISCONN	O ponto final de transporte já está conectado
107	ENOTCONN	O ponto final de transporte não está conectado
108	DESLIGAMENTO	Não é possível enviar após o desligamento do ponto de extremidade de transporte
109	ETOOMANYREFS	Muitas referências: não é possível unir
110	ETIMEDOUT	Tempo de conexão esgotado
111	ECONOMIZADO RECUSADO	Ligação recusada

Número do erro	Código de erro	Significado
112	EHOSTDOWN	O host está inativo
113	EHOSTUNREACH	Nenhuma rota para o host
114	JÁ	Operação já em andamento
115	EINPROGRESS	Operação em andamento
116		
117	EUCLEAN	Estrutura precisa de limpeza
118	ENOTNAM	Não é um arquivo do tipo nomeado XENIX
119	DISPONIBILIZAR	Nenhum semáforo XENIX disponível
120	EISNAM	É um arquivo de tipo nomeado
121	EREMOTEIO	Erro de E/S remota
122	EDQUOT	Cota excedida
123	ENOMEDIUM	Nenhum meio encontrado
124	TIPO MÉDIO	Tipo de mídia errado
125	EXCANCELADO	Operação cancelada
126	ENOKEY	Chave necessária não disponível
127	EKEY EXPIRADA	A chave expirou
128	EKEY REVOGADA	A chave foi revogada
129	EKEYREJEITADO	A chave foi rejeitada pelo serviço
130	PROPRIETÁRIO MORTO	Para mutexes robustos: O proprietário faleceu
131	ENOTRECOVERABLE	Para mutexes robustos: Estado não recuperável

Configurar destinos de mensagens e logs de auditoria

Considerações para usar um servidor syslog externo

Um servidor syslog externo é um servidor fora do StorageGRID que você pode usar para coletar informações de auditoria do sistema em um único local. Usar um servidor syslog externo permite reduzir o tráfego de rede em seus nós de administração e gerenciar as informações com mais eficiência. Para StorageGRID, o formato do pacote de mensagens syslog de saída é compatível com RFC 3164.

Os tipos de informações de auditoria que você pode enviar ao servidor syslog externo incluem:

- Registros de auditoria contendo as mensagens de auditoria geradas durante a operação normal do sistema
- Eventos relacionados à segurança, como logins e escalonamentos para root
- Logs de aplicativos que podem ser solicitados caso seja necessário abrir um caso de suporte para solucionar um problema que você encontrou

Quando usar um servidor syslog externo

Um servidor syslog externo é especialmente útil se você tiver uma grade grande, usar vários tipos de aplicativos S3 ou quiser reter todos os dados de auditoria. O envio de informações de auditoria para um servidor syslog externo permite que você:

- Colete e gerencie informações de auditoria, como mensagens de auditoria, logs de aplicativos e eventos de segurança com mais eficiência.
- Reduza o tráfego de rede em seus nós de administração porque as informações de auditoria são transferidas diretamente dos vários nós de armazenamento para o servidor syslog externo, sem precisar passar por um nó de administração.



Quando os logs são enviados para um servidor syslog externo, logs únicos maiores que 8.192 bytes são truncados no final da mensagem para estar em conformidade com as limitações comuns em implementações de servidores syslog externos.



Para maximizar as opções de recuperação completa de dados em caso de falha do servidor syslog externo, até 20 GB de logs locais de registros de auditoria(`localaudit.log`) são mantidos em cada nó.

Como configurar um servidor syslog externo

Para aprender como configurar um servidor syslog externo, consulte "[Configurar mensagens de auditoria e servidor syslog externo](#)".

Se você planeja configurar o uso do protocolo TLS ou RELP/TLS, você deve ter os seguintes certificados:

- **Certificados de CA do servidor:** Um ou mais certificados de CA confiáveis para verificar o servidor syslog externo na codificação PEM. Se omitido, o certificado Grid CA padrão será usado.
- **Certificado do cliente:** O certificado do cliente para autenticação no servidor syslog externo na codificação PEM.
- **Chave privada do cliente:** Chave privada para o certificado do cliente na codificação PEM.



Se você usar um certificado de cliente, também deverá usar uma chave privada de cliente. Se você fornecer uma chave privada criptografada, também deverá fornecer a senha. Não há benefício significativo de segurança no uso de uma chave privada criptografada porque a chave e a senha devem ser armazenadas; usar uma chave privada não criptografada, se disponível, é recomendado para simplificar.

Como estimar o tamanho do servidor syslog externo

Normalmente, sua grade é dimensionada para atingir uma taxa de transferência necessária, definida em termos de operações S3 por segundo ou bytes por segundo. Por exemplo, você pode ter um requisito para que sua grade manipule 1.000 operações S3 por segundo, ou 2.000 MB por segundo, de ingestões e recuperações de objetos. Você deve dimensionar seu servidor syslog externo de acordo com os requisitos de dados da sua grade.

Esta seção fornece algumas fórmulas heurísticas que ajudam você a estimar a taxa e o tamanho médio de mensagens de log de vários tipos que seu servidor syslog externo precisa ser capaz de manipular, expressos em termos das características de desempenho conhecidas ou desejadas da grade (operações S3 por segundo).

Use operações S3 por segundo em fórmulas de estimativa

Se sua grade foi dimensionada para uma taxa de transferência expressa em bytes por segundo, você deve converter esse dimensionamento em operações S3 por segundo para usar as fórmulas de estimativa. Para converter a taxa de transferência da grade, você deve primeiro determinar o tamanho médio do objeto, o que pode ser feito usando as informações em logs de auditoria e métricas existentes (se houver) ou usando seu conhecimento dos aplicativos que usarão o StorageGRID. Por exemplo, se sua grade foi dimensionada para atingir uma taxa de transferência de 2.000 MB/segundo, e seu tamanho médio de objeto é de 2 MB, então sua grade foi dimensionada para poder lidar com 1.000 operações S3 por segundo (2.000 MB / 2 MB).



As fórmulas para dimensionamento do servidor syslog externo nas seções a seguir fornecem estimativas de casos comuns (em vez de estimativas de pior caso). Dependendo da sua configuração e carga de trabalho, você poderá ver uma taxa maior ou menor de mensagens do syslog ou um volume de dados do syslog do que o previsto pelas fórmulas. As fórmulas devem ser usadas apenas como diretrizes.

Fórmulas de estimativa para registros de auditoria

Se você não tiver nenhuma informação sobre sua carga de trabalho do S3 além do número de operações do S3 por segundo que sua grade deve suportar, você pode estimar o volume de logs de auditoria que seu servidor syslog externo precisará manipular usando as seguintes fórmulas, supondo que você deixe os Níveis de Auditoria definidos com os valores padrão (todas as categorias definidas como Normal, exceto Armazenamento, que é definido como Erro):

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, seu servidor syslog externo deverá ser dimensionado para suportar 2.000 mensagens syslog por segundo e deverá ser capaz de receber (e normalmente armazenar) dados de log de auditoria a uma taxa de 1,6 MB por segundo.

Se você souber mais sobre sua carga de trabalho, estimativas mais precisas serão possíveis. Para logs de

auditoria, as variáveis adicionais mais importantes são a porcentagem de operações S3 que são PUTs (vs. GETs) e o tamanho médio, em bytes, dos seguintes campos S3 (as abreviações de 4 caracteres usadas na tabela são nomes de campos de log de auditoria):

Código	Campo	Descrição
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.

Vamos usar P para representar a porcentagem de operações S3 que são PUTs, onde $0 \leq P \leq 1$ (portanto, para uma carga de trabalho de 100% PUT, $P = 1$, e para uma carga de trabalho de 100% GET, $P = 0$).

Vamos usar K para representar o tamanho médio da soma dos nomes de contas S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre `my-s3-account` (13 bytes), os buckets tenham nomes de comprimento fixo como `/my/application/bucket-12345` (28 bytes) e os objetos tenham chaves de comprimento fixo como `5733a5d7-f069-41ef-8fbd-13247494c69c` (36 bytes). Então o valor de K é 90 (13+13+28+36).

Se você puder determinar valores para P e K , poderá estimar o volume de logs de auditoria que seu servidor syslog externo precisará manipular usando as seguintes fórmulas, supondo que você deixe os Níveis de Auditoria definidos como padrões (todas as categorias definidas como Normal, exceto Armazenamento, que é definido como Erro):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, sua carga de trabalho for 50% PUTs e seus nomes de conta S3, nomes de bucket e nomes de objeto tiverem em média 90 bytes, seu servidor syslog externo deverá ser dimensionado para suportar 1.500 mensagens syslog por segundo e deverá ser capaz de receber (e normalmente armazenar) dados de log de auditoria a uma taxa de aproximadamente 1 MB por segundo.

Fórmulas de estimativa para níveis de auditoria não padrão

As fórmulas fornecidas para logs de auditoria pressupõem o uso de configurações de nível de auditoria padrão (todas as categorias definidas como Normal, exceto Armazenamento, que é definido como Erro). Fórmulas detalhadas para estimar a taxa e o tamanho médio de mensagens de auditoria para configurações de nível de auditoria não padrão não estão disponíveis. No entanto, a tabela a seguir pode ser usada para fazer uma estimativa aproximada da taxa; você pode usar a fórmula de tamanho médio fornecida para logs de auditoria, mas esteja ciente de que isso provavelmente resultará em uma superestimativa porque as

mensagens de auditoria "extras" são, em média, menores que as mensagens de auditoria padrão.

Doença	Fórmula
Replicação: níveis de auditoria todos definidos como Depuração ou Normal	Taxa de log de auditoria = 8 x taxa de operações S3
Codificação de eliminação: níveis de auditoria todos definidos como Depuração ou Normal	Use a mesma fórmula das configurações padrão

Fórmulas de estimativa para eventos de segurança

Eventos de segurança não estão correlacionados com operações do S3 e normalmente produzem um volume insignificante de logs e dados. Por essas razões, nenhuma fórmula de estimativa é fornecida.

Fórmulas de estimativa para logs de aplicação

Se você não tiver nenhuma informação sobre sua carga de trabalho do S3 além do número de operações do S3 por segundo que sua grade deve suportar, você pode estimar o volume de logs de aplicativos que seu servidor syslog externo precisará manipular usando as seguintes fórmulas:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Assim, por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, seu servidor syslog externo deverá ser dimensionado para suportar 3.300 logs de aplicativos por segundo e ser capaz de receber (e armazenar) dados de log de aplicativos a uma taxa de cerca de 1,2 MB por segundo.

Se você souber mais sobre sua carga de trabalho, estimativas mais precisas serão possíveis. Para logs de aplicativos, as variáveis adicionais mais importantes são a estratégia de proteção de dados (replicação vs. codificação de eliminação), a porcentagem de operações S3 que são PUTs (vs. GETs/outros) e o tamanho médio, em bytes, dos seguintes campos S3 (as abreviações de 4 caracteres usadas na tabela são nomes de campos de log de auditoria):

Código	Campo	Descrição
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
S3BK	Balde S3	O nome do bucket S3.

Código	Campo	Descrição
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.

Exemplos de estimativas de dimensionamento

Esta seção explica casos de exemplo de como usar as fórmulas de estimativa para grades com os seguintes métodos de proteção de dados:

- Replicação
- Codificação de apagamento

Se você usar replicação para proteção de dados

Deixe P representar a porcentagem de operações S3 que são PUTs, onde $0 \leq P \leq 1$ (portanto, para uma carga de trabalho de 100% PUT, $P = 1$, e para uma carga de trabalho de 100% GET, $P = 0$).

Deixe K representar o tamanho médio da soma dos nomes de contas S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre my-s3-account (13 bytes), os buckets tenham nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes) e os objetos tenham chaves de comprimento fixo como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Então K tem um valor de 90 (13+13+28+36).

Se você puder determinar valores para P e K, poderá estimar o volume de logs de aplicativos que seu servidor syslog externo terá que ser capaz de manipular usando as seguintes fórmulas.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x K))) Bytes
```

Assim, por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, sua carga de trabalho for 50% PUTs e seus nomes de conta S3, nomes de bucket e nomes de objeto tiverem em média 90 bytes, seu servidor syslog externo deverá ser dimensionado para suportar 1.800 logs de aplicativos por segundo e receberá (e normalmente armazenará) dados de aplicativos a uma taxa de 0,5 MB por segundo.

Se você usar codificação de eliminação para proteção de dados

Deixe P representar a porcentagem de operações S3 que são PUTs, onde $0 \leq P \leq 1$ (portanto, para uma carga de trabalho de 100% PUT, $P = 1$, e para uma carga de trabalho de 100% GET, $P = 0$).

Deixe K representar o tamanho médio da soma dos nomes de contas S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre my-s3-account (13 bytes), os buckets tenham nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes) e os objetos tenham chaves de comprimento fixo como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Então K tem um valor de 90 (13+13+28+36).

Se você puder determinar valores para P e K, poderá estimar o volume de logs de aplicativos que seu servidor syslog externo terá que ser capaz de manipular usando as seguintes fórmulas.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

Portanto, por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, sua carga de trabalho for 50% PUTs e seus nomes de conta S3, nomes de bucket e nomes de objeto tiverem em média 90 bytes, seu servidor syslog externo deverá ser dimensionado para suportar 2.250 logs de aplicativos por segundo e deverá ser capaz de receber (e normalmente armazenar) dados de aplicativos a uma taxa de 0,6 MB por segundo.

Configurar mensagens de auditoria e servidor syslog externo

Você pode configurar uma série de configurações relacionadas às mensagens de auditoria. Você pode ajustar o número de mensagens de auditoria registradas; definir quaisquer cabeçalhos de solicitação HTTP que deseja incluir nas mensagens de auditoria de leitura e gravação do cliente; configurar um servidor syslog externo; e especificar para onde os logs de auditoria, logs de eventos de segurança e logs de software StorageGRID são enviados.

Mensagens e logs de auditoria registram atividades do sistema e eventos de segurança e são ferramentas essenciais para monitoramento e solução de problemas. Todos os nós do StorageGRID geram mensagens de auditoria e logs para rastrear atividades e eventos do sistema.

Opcionalmente, você pode configurar um servidor syslog externo para salvar 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. Um servidor syslog externo é especialmente útil se você tiver uma grade grande, usar vários tipos de aplicativos S3 ou quiser reter todos os dados de auditoria. Ver ["Configurar mensagens de auditoria e servidor syslog externo"](#) para mais detalhes.

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"](#).
- Se você planeja configurar um servidor syslog externo, você revisou o ["considerações para usar um servidor syslog externo"](#) e garantiu que o servidor tenha capacidade suficiente para receber e armazenar os arquivos de log.
- Se você planeja configurar um servidor syslog externo usando o protocolo TLS ou RELP/TLS, você tem a CA do servidor e os certificados de cliente necessários e a chave privada do cliente.

Alterar níveis de mensagens de auditoria

Você pode definir um nível de auditoria diferente para cada uma das seguintes categorias de mensagens no log de auditoria:

Categoria de auditoria	Configuração padrão	Mais informações
Sistema	Normal	"Mensagens de auditoria do sistema"

Categoria de auditoria	Configuração padrão	Mais informações
Armazenar	Erro	"Mensagens de auditoria de armazenamento de objetos"
Gerenciamento	Normal	"Mensagem de auditoria de gestão"
O cliente lê	Normal	"O cliente leu mensagens de auditoria"
O cliente escreve	Normal	"O cliente escreve mensagens de auditoria"
ILM	Normal	"Mensagens de auditoria do ILM"
Replicação entre grades	Erro	"CGRR: Solicitação de replicação entre redes"



Esses padrões se aplicam se você instalou inicialmente o StorageGRID usando a versão 10.3 ou posterior. Se você usou inicialmente uma versão anterior do StorageGRID, o padrão para todas as categorias é definido como Normal.



Durante as atualizações, as configurações de nível de auditoria não entrarão em vigor imediatamente.

Passos

1. Selecione **CONFIGURAÇÃO > Monitoramento > Servidor de auditoria e syslog**.
2. Para cada categoria de mensagem de auditoria, selecione um nível de auditoria na lista suspensa:

Nível de auditoria	Descrição
Desligado	Nenhuma mensagem de auditoria da categoria é registrada.
Erro	Somente mensagens de erro são registradas — mensagens de auditoria para as quais o código de resultado não foi "bem-sucedido" (SUCCS).
Normal	Mensagens transacionais padrão são registradas — as mensagens listadas nestas instruções para a categoria.
Depurar	Obsoleto. Este nível se comporta da mesma forma que o nível de auditoria Normal.

As mensagens incluídas para qualquer nível específico incluem aquelas que seriam registradas nos níveis mais altos. Por exemplo, o nível Normal inclui todas as mensagens de erro.



Se você não precisar de um registro detalhado das operações de leitura do cliente para seus aplicativos S3, opcionalmente, altere a configuração **Leituras do cliente** para **Erro** para diminuir o número de mensagens de auditoria registradas no log de auditoria.

3. Selecione **Salvar**.

Um banner verde indica que sua configuração foi salva.

Definir cabeçalhos de solicitação HTTP

Opcionalmente, você pode definir quaisquer cabeçalhos de solicitação HTTP que deseja incluir nas mensagens de auditoria de leitura e gravação do cliente. Esses cabeçalhos de protocolo se aplicam somente a solicitações S3.

Passos

1. Na seção **Cabeçalhos do protocolo de auditoria**, defina os cabeçalhos de solicitação HTTP que você deseja incluir nas mensagens de auditoria de leitura e gravação do cliente.

Use um asterisco (*) como curinga para corresponder a zero ou mais caracteres. Use a sequência de escape (*) para corresponder a um asterisco literal.

2. Selecione **Adicionar outro cabeçalho** para criar cabeçalhos adicionais, se necessário.

Quando cabeçalhos HTTP são encontrados em uma solicitação, eles são incluídos na mensagem de auditoria no campo HTRH.



Os cabeçalhos de solicitação do protocolo de auditoria serão registrados somente se o nível de auditoria para **Leituras do cliente** ou **Gravações do cliente** não for **Desativado**.

3. Selecione **Salvar**

Um banner verde indica que sua configuração foi salva.

Use um servidor syslog externo

Opcionalmente, você pode configurar um servidor syslog externo para salvar logs de auditoria, logs de aplicativos e logs de eventos de segurança em um local fora da sua grade.



Se você não quiser usar um servidor syslog externo, pule esta etapa e vá para [Selecione destinos de informações de auditoria](#).



Se as opções de configuração disponíveis neste procedimento não forem flexíveis o suficiente para atender às suas necessidades, opções de configuração adicionais podem ser aplicadas usando o `audit-destinations` endpoints, que estão na seção de API privada do ["API de gerenciamento de grade"](#). Por exemplo, você pode usar a API se quiser usar diferentes servidores syslog para diferentes grupos de nós.

Insira as informações do syslog

Acesse o assistente Configurar servidor syslog externo e forneça as informações que o StorageGRID precisa para acessar o servidor syslog externo.

Passos

1. Na página Auditoria e servidor syslog, selecione **Configurar servidor syslog externo**. Ou, se você configurou anteriormente um servidor syslog externo, selecione **Editar servidor syslog externo**.

O assistente Configurar servidor syslog externo é exibido.

2. Para a etapa **Inserir informações do syslog** do assistente, insira um nome de domínio totalmente qualificado válido ou um endereço IPv4 ou IPv6 para o servidor syslog externo no campo **Host**.
3. Insira a porta de destino no servidor syslog externo (deve ser um número inteiro entre 1 e 65535). A porta padrão é 514.
4. Selecione o protocolo usado para enviar informações de auditoria para o servidor syslog externo.

É recomendado usar **TLS** ou **RELPL/TLS**. Você deve carregar um certificado de servidor para usar qualquer uma dessas opções. O uso de certificados ajuda a proteger as conexões entre sua grade e o servidor syslog externo. Para obter mais informações, consulte "[Gerenciar certificados de segurança](#)".

Todas as opções de protocolo exigem suporte e configuração do servidor syslog externo. Você deve escolher uma opção compatível com o servidor syslog externo.



O Reliable Event Logging Protocol (RELPL) estende a funcionalidade do protocolo syslog para fornecer entrega confiável de mensagens de eventos. Usar o RELPL pode ajudar a evitar a perda de informações de auditoria caso seu servidor syslog externo precise reiniciar.

5. Selecione **Continuar**.
6. Se você selecionou **TLS** ou **RELPL/TLS**, carregue os certificados da CA do servidor, o certificado do cliente e a chave privada do cliente.
 - a. Selecione **Procurar** para o certificado ou chave que você deseja usar.
 - b. Selecione o certificado ou arquivo de chave.
 - c. Selecione **Abrir** para carregar o arquivo.

Uma marca de verificação verde aparece ao lado do nome do certificado ou do arquivo de chave, notificando que ele foi carregado com sucesso.

7. Selecione **Continuar**.

Gerenciar conteúdo do syslog

Você pode selecionar quais informações enviar para o servidor syslog externo.

Passos

1. Para a etapa **Gerenciar conteúdo do syslog** do assistente, selecione cada tipo de informação de auditoria que deseja enviar ao servidor syslog externo.
 - **Enviar logs de auditoria**: Envia eventos do StorageGRID e atividades do sistema
 - **Enviar eventos de segurança**: Envia eventos de segurança, como quando um usuário não autorizado tenta fazer login ou um usuário faz login como root
 - **Enviar logs de aplicação**: Envia "[Arquivos de log do software StorageGRID](#)" útil para solução de problemas, incluindo:
 - `broadcast-err.log`

- `bycast.log`
- `jaeger.log`
- `nms.log`(Somente nós de administração)
- `prometheus.log`
- `raft.log`
- `hagroups.log`

- **Enviar logs de acesso:** Envia logs de acesso HTTP para solicitações externas ao Grid Manager, Tenant Manager, endpoints de balanceador de carga configurados e solicitações de federação de grade de sistemas remotos.

2. Use os menus suspensos para selecionar a gravidade e a facilidade (tipo de mensagem) para cada categoria de informação de auditoria que você deseja enviar.

Definir valores de gravidade e facilidade pode ajudar você a agregar os logs de maneiras personalizáveis para facilitar a análise.

- a. Para **Gravidade**, selecione **Passagem** ou selecione um valor de gravidade entre 0 e 7.

Se você selecionar um valor, o valor selecionado será aplicado a todas as mensagens deste tipo. Informações sobre diferentes gravidades serão perdidas se você substituir a gravidade por um valor fixo.

Gravidade	Descrição
Passagem	Cada mensagem enviada ao syslog externo deve ter o mesmo valor de gravidade de quando foi registrada localmente no nó: • Para logs de auditoria, a gravidade é "info". • Para eventos de segurança, os valores de gravidade são gerados pela distribuição Linux nos nós. • Para logs de aplicativos, as gravidades variam entre "info" e "notice", dependendo do problema. Por exemplo, adicionar um servidor NTP e configurar um grupo HA fornece um valor de "info", enquanto interromper intencionalmente o serviço SSM ou RSM fornece um valor de "notice". • Para logs de acesso, a gravidade é "info".
0	Emergência: O sistema está inutilizável
1	Alerta: Ação deve ser tomada imediatamente
2	Crítico: Condições críticas
3	Erro: Condições de erro
4	Aviso: Condições de aviso

Gravidade	Descrição
5	Aviso: Condição normal, mas significativa
6	Informativo: Mensagens informativas
7	Depuração: mensagens de nível de depuração

b. Para **Instalação**, selecione **Passthrough** ou selecione um valor de instalação entre 0 e 23.

Se você selecionar um valor, ele será aplicado a todas as mensagens deste tipo. Informações sobre diferentes instalações serão perdidas se você substituir a instalação por um valor fixo.

Instalação	Descrição
Passagem	Cada mensagem enviada ao syslog externo deve ter o mesmo valor de recurso de quando foi registrada localmente no nó: • Para logs de auditoria, o recurso enviado ao servidor syslog externo é "local7". • Para eventos de segurança, os valores de facilidade são gerados pela distribuição Linux nos nós. • Para logs de aplicativos, os logs de aplicativos enviados ao servidor syslog externo têm os seguintes valores de facilidade: ◦ <code>bcast.log</code>: usuário ou daemon ◦ <code>bcast-err.log</code>: usuário, daemon, local3 ou local4 ◦ <code>jaeger.log</code>: local2 ◦ <code>nms.log</code>: local3 ◦ <code>prometheus.log</code>: local4 ◦ <code>raft.log</code>: local5 ◦ <code>hagroups.log</code>: local6 • Para logs de acesso, o recurso enviado ao servidor syslog externo é "local0".
0	kern (mensagens do kernel)
1	usuário (mensagens em nível de usuário)
2	correspondência
3	daemon (daemons do sistema)
4	auth (mensagens de segurança/autorização)

Instalação	Descrição
5	syslog (mensagens geradas internamente pelo syslogd)
6	lpr (subsistema de impressora de linha)
7	notícias (subsistema de notícias da rede)
8	UUCP
9	cron (daemon do relógio)
10	segurança (mensagens de segurança/autorização)
11	FTP
12	NTP
13	logaudit (auditoria de log)
14	logalert (alerta de registro)
15	relógio (daemon do relógio)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Selecione **Continuar**.

Enviar mensagens de teste

Antes de começar a usar um servidor syslog externo, você deve solicitar que todos os nós na sua grade enviem mensagens de teste para o servidor syslog externo. Você deve usar essas mensagens de teste para

ajudar a validar toda a sua infraestrutura de coleta de logs antes de se comprometer a enviar dados para o servidor syslog externo.



Não use a configuração do servidor syslog externo até confirmar que o servidor syslog externo recebeu uma mensagem de teste de cada nó na sua grade e que a mensagem foi processada conforme o esperado.

Passos

1. Se você não quiser enviar mensagens de teste porque tem certeza de que seu servidor syslog externo está configurado corretamente e pode receber informações de auditoria de todos os nós em sua grade, selecione **Ignorar e concluir**.

Um banner verde indica que a configuração foi salva.

2. Caso contrário, selecione **Enviar mensagens de teste** (recomendado).

Os resultados dos testes aparecem continuamente na página até você interromper o teste. Enquanto o teste estiver em andamento, suas mensagens de auditoria continuarão sendo enviadas para os destinos configurados anteriormente.

3. Se você receber algum erro durante a configuração do servidor syslog ou em tempo de execução, corrija-o e selecione **Enviar mensagens de teste** novamente.

Ver "[Solucionar problemas de um servidor syslog externo](#)" para ajudar você a resolver quaisquer erros.

4. Aguarde até ver um banner verde indicando que todos os nós passaram no teste.
5. Verifique seu servidor syslog para determinar se as mensagens de teste estão sendo recebidas e processadas conforme o esperado.



Se você estiver usando UDP, verifique toda a sua infraestrutura de coleta de logs. O protocolo UDP não permite uma detecção de erros tão rigorosa quanto os outros protocolos.

6. Selecione **Parar e finalizar**.

Você retornará à página **Auditoria e servidor syslog**. Um banner verde indica que a configuração do servidor syslog foi salva.



As informações de auditoria do StorageGRID não são enviadas ao servidor syslog externo até que você selecione um destino que inclua o servidor syslog externo.

Selecione destinos de informações de auditoria

Você pode especificar onde os logs de auditoria, logs de eventos de segurança e "[Registros do software StorageGRID](#)" são enviados.

O StorageGRID assume como padrão os destinos de auditoria de nós locais e armazena as informações de auditoria em `/var/local/log/localaudit.log`.



Ao usar `/var/local/log/localaudit.log`, as entradas de log de auditoria do Grid Manager e do Tenant Manager podem ser enviadas para um nó de armazenamento. Você pode descobrir qual nó tem as entradas mais recentes usando o `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` comando.

Alguns destinos só estarão disponíveis se você tiver configurado um servidor syslog externo.

Passos

1. Na página Auditoria e servidor syslog, selecione o destino para as informações de auditoria.



Somente nós locais e servidor syslog externo geralmente oferecem melhor desempenho.

Opção	Descrição
Somente nós locais (padrão)	Mensagens de auditoria, logs de eventos de segurança e logs de aplicativos não são enviados aos nós de administração. Em vez disso, eles são salvos apenas nos nós que os geraram ("o nó local"). As informações de auditoria geradas em cada nó local são armazenadas em <code>/var/local/log/localaudit.log</code>. Observação: O StorageGRID remove periodicamente logs locais em uma rotação para liberar espaço. Quando o arquivo de log de um nó atinge 1 GB, o arquivo existente é salvo e um novo arquivo de log é iniciado. O limite de rotação do log é de 21 arquivos. Quando a 22ª versão do arquivo de log é criada, o arquivo de log mais antigo é excluído. Em média, cerca de 20 GB de dados de log são armazenados em cada nó.
Nós de administração/nós locais	As mensagens de auditoria são enviadas para o log de auditoria nos nós de administração, e os logs de eventos de segurança e logs de aplicativos são armazenados nos nós que os geraram. As informações de auditoria são armazenadas nos seguintes arquivos: • Nós de administração (primários e não primários): <code>/var/local/audit/export/audit.log</code> • Todos os nós: O <code>/var/local/log/localaudit.log</code> o arquivo normalmente está vazio ou ausente. Pode conter informações secundárias, como uma cópia adicional de algumas mensagens.
Servidor syslog externo	As informações de auditoria são enviadas para um servidor syslog externo e salvas nos nós locais(<code>/var/local/log/localaudit.log</code>). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção é habilitada somente após você configurar um servidor syslog externo.

Opção	Descrição
Nó de administração e servidor syslog externo	As mensagens de auditoria são enviadas para o log de auditoria(/var/local/audit/export/audit.log) em nós de administração, e as informações de auditoria são enviadas ao servidor syslog externo e salvas no nó local(/var/local/log/localaudit.log). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção é habilitada somente após você configurar um servidor syslog externo.

2. Selecione **Salvar**.

Uma mensagem de aviso é exibida.

3. Selecione **OK** para confirmar que deseja alterar o destino das informações de auditoria.

Um banner verde indica que a configuração de auditoria foi salva.

Novos logs são enviados para os destinos selecionados. Os registros existentes permanecem em seu local atual.

Usar monitoramento SNMP

Usar monitoramento SNMP

Se você quiser monitorar o StorageGRID usando o Protocolo Simples de Gerenciamento de Rede (SNMP), deverá configurar o agente SNMP incluído no StorageGRID.

- ["Configurar o agente SNMP"](#)
- ["Atualizar o agente SNMP"](#)

Capacidades

Cada nó StorageGRID executa um agente SNMP, ou daemon, que fornece um MIB. O MIB StorageGRID contém definições de tabela e notificação para alertas. O MIB também contém informações de descrição do sistema, como plataforma e número do modelo para cada nó. Cada nó StorageGRID também suporta um subconjunto de objetos MIB-II.



Ver ["Acessar arquivos MIB"](#) se você quiser baixar os arquivos MIB nos nós da sua grade.

Inicialmente, o SNMP é desabilitado em todos os nós. Quando você configura o agente SNMP, todos os nós do StorageGRID recebem a mesma configuração.

O agente SNMP do StorageGRID suporta todas as três versões do protocolo SNMP. Ele fornece acesso MIB somente leitura para consultas e pode enviar dois tipos de notificações orientadas a eventos para um sistema de gerenciamento:

Armadilhas

Armadilhas são notificações enviadas pelo agente SNMP que não exigem confirmação pelo sistema de gerenciamento. As armadilhas servem para notificar o sistema de gerenciamento de que algo aconteceu no StorageGRID, como um alerta sendo disparado.

As armadilhas são suportadas em todas as três versões do SNMP.

Informa

As informações são semelhantes às armadilhas, mas exigem reconhecimento pelo sistema de gerenciamento. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenviará a informação até que uma confirmação seja recebida ou o valor máximo de novas tentativas seja atingido.

As informações são suportadas em SNMPv2c e SNMPv3.

Notificações de captura e informação são enviadas nos seguintes casos:

- Um alerta padrão ou personalizado é acionado em qualquer nível de gravidade. Para suprimir notificações SNMP para um alerta, você deve "[configurar um silêncio](#)" para o alerta. As notificações de alerta são enviadas pelo "[nó de administração do remetente preferencial](#)".

Cada alerta é mapeado para um dos três tipos de armadilhas com base no nível de gravidade do alerta: activeMinorAlert, activeMajorAlert e activeCriticalAlert. Para obter uma lista dos alertas que podem disparar essas armadilhas, consulte o "[Referência de alertas](#)".

Suporte à versão SNMP

A tabela fornece um resumo de alto nível do que é suportado para cada versão do SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Consultas (GET e GETNEXT)	Consultas MIB somente leitura	Consultas MIB somente leitura	Consultas MIB somente leitura
Autenticação de consulta	Cadeia de caracteres da comunidade	Cadeia de caracteres da comunidade	Usuário do Modelo de Segurança Baseado no Usuário (USM)
Notificações (ARMAZENA R e INFORMAR)	Apenas armadilhas	Armadilhas e informações	Armadilhas e informações
Autenticação de notificação	Comunidade de armadilhas padrão ou uma sequência de comunidade personalizada para cada destino de armadilha	Comunidade de armadilhas padrão ou uma sequência de comunidade personalizada para cada destino de armadilha	Usuário USM para cada destino de armadilha

Limitações

- O StorageGRID suporta acesso MIB somente leitura. O acesso de leitura e gravação não é suportado.
- Todos os nós na grade recebem a mesma configuração.

- SNMPv3: O StorageGRID não oferece suporte ao Modo de Suporte de Transporte (TSM).
- SNMPv3: O único protocolo de autenticação suportado é o SHA (HMAC-SHA-96).
- SNMPv3: O único protocolo de privacidade suportado é o AES.

Configurar o agente SNMP

Você pode configurar o agente SNMP do StorageGRID para usar um sistema de gerenciamento SNMP de terceiros para acesso MIB somente leitura e notificações.

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

O agente SNMP do StorageGRID oferece suporte a SNMPv1, SNMPv2c e SNMPv3. Você pode configurar o agente para uma ou mais versões. Para SNMPv3, somente a autenticação do Modelo de Segurança do Usuário (USM) é suportada.

Todos os nós na grade usam a mesma configuração SNMP.

Especificar configuração básica

Como primeiro passo, habilite o agente StorageGRID SMNP e forneça informações básicas.

Passos

1. Selecione **CONFIGURAÇÃO > Monitoramento > Agente SNMP**.

A página do agente SNMP é exibida.

2. Para habilitar o agente SNMP em todos os nós da grade, marque a caixa de seleção **Habilitar SNMP**.
3. Insira as seguintes informações na seção Configuração básica.

Campo	Descrição
Contato do sistema	Opcional. O contato principal do sistema StorageGRID , que é retornado em mensagens SNMP como sysContact. O contato do sistema normalmente é um endereço de e-mail. Este valor se aplica a todos os nós no sistema StorageGRID . Contato do sistema pode ter no máximo 255 caracteres.
Localização do sistema	Opcional. A localização do sistema StorageGRID , que é retornada em mensagens SNMP como sysLocation. A localização do sistema pode ser qualquer informação útil para identificar onde seu sistema StorageGRID está localizado. Por exemplo, você pode usar o endereço de uma instalação. Este valor se aplica a todos os nós no sistema StorageGRID . Localização do sistema pode ter no máximo 255 caracteres.

Campo	Descrição
Habilitar notificações do agente SNMP	• Se selecionado, o agente SNMP StorageGRID envia notificações de interceptação e informação. • Se não for selecionado, o agente SNMP suportará acesso MIB somente leitura, mas não enviará nenhuma notificação SNMP.
Habilitar armadilhas de autenticação	Se selecionado, o agente SNMP do StorageGRID enviará interceptações de autenticação se receber mensagens de protocolo autenticadas incorretamente.

Insira as sequências da comunidade

Se você usar SNMPv1 ou SNMPv2c, preencha a seção Strings da comunidade.

Quando o sistema de gerenciamento consulta o StorageGRID MIB, ele envia uma string de comunidade. Se a sequência de caracteres da comunidade corresponder a um dos valores especificados aqui, o agente SNMP enviará uma resposta ao sistema de gerenciamento.

Passos

1. Para **Comunidade somente leitura**, insira opcionalmente uma sequência de caracteres de comunidade para permitir acesso MIB somente leitura em endereços de agente IPv4 e IPv6.



Para garantir a segurança do seu sistema StorageGRID, não use "public" como string de comunidade. Se você deixar este campo em branco, o agente SNMP usará o ID da grade do seu sistema StorageGRID como a string da comunidade.

Cada sequência de caracteres da comunidade pode ter no máximo 32 caracteres e não pode conter espaços em branco.

2. Selecione **Adicionar outra sequência de comunidade** para adicionar sequências adicionais.

São permitidas até cinco strings.

Criar destinos de armadilha

Use a guia Destinos de interceptação na seção Outras configurações para definir um ou mais destinos para interceptação do StorageGRID ou informar notificações. Quando você habilita o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. Notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifDown e coldStart).

Passos

1. Para o campo **Comunidade de interceptação padrão**, insira opcionalmente a sequência de caracteres da comunidade padrão que você deseja usar para destinos de interceptação SNMPv1 ou SNMPv2.

Conforme necessário, você pode fornecer uma sequência de caracteres de comunidade diferente ("personalizada") ao definir um destino de captura específico.

Comunidade de trap padrão pode ter no máximo 32 caracteres e não pode conter espaços em branco.

2. Para adicionar um destino de armadilha, selecione **Criar**.
3. Selecione qual versão SNMP será usada para este destino de trap.
4. Preencha o formulário Criar destino de armadilha para a versão selecionada.

SNMPv1

Se você selecionou SNMPv1 como a versão, preencha estes campos.

Campo	Descrição
Tipo	Deve ser Trap para SNMPv1.
Hospedar	Um endereço IPv4 ou IPv6 ou um nome de domínio totalmente qualificado (FQDN) para receber a armadilha.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo de interceptação SNMP padrão, a menos que você precise usar TCP.
Cadeia de caracteres da comunidade	Use a comunidade de armadilha padrão, se uma foi especificada, ou insira uma sequência de caracteres de comunidade personalizada para este destino de armadilha. A sequência de caracteres da comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaços em branco.

SNMPv2c

Se você selecionou SNMPv2c como a versão, preencha estes campos.

Campo	Descrição
Tipo	Se o destino será usado para armadilhas ou informações.
Hospedar	Um endereço IPv4 ou IPv6 ou FQDN para receber a interceptação.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo de interceptação SNMP padrão, a menos que você precise usar TCP.
Cadeia de caracteres da comunidade	Use a comunidade de armadilha padrão, se uma foi especificada, ou insira uma sequência de caracteres de comunidade personalizada para este destino de armadilha. A sequência de caracteres da comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaços em branco.

SNMPv3

Se você selecionou SNMPv3 como a versão, preencha estes campos.

Campo	Descrição
Tipo	Se o destino será usado para armadilhas ou informações.
Hospedar	Um endereço IPv4 ou IPv6 ou FQDN para receber a interceptação.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo de interceptação SNMP padrão, a menos que você precise usar TCP.
Usuário USM	O usuário USM que será usado para autenticação. • Se você selecionou Trap, somente usuários do USM sem IDs de mecanismo autoritativos serão exibidos. • Se você selecionou Informar, somente usuários do USM com IDs de mecanismo autoritativos serão exibidos. • Se nenhum usuário for exibido: i. Crie e salve o destino da armadilha. ii. Vá para Criar usuários USM e criar o usuário. iii. Retorne à aba Destinos da armadilha, selecione o destino salvo na tabela e selecione Editar. iv. Selecione o usuário.

5. Selecione **Criar**.

O destino da armadilha é criado e adicionado à tabela.

Criar endereços de agentes

Opcionalmente, use a guia Endereços do agente na seção Outras configurações para especificar um ou mais "endereços de escuta". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

Se você não configurar um endereço de agente, o endereço de escuta padrão será a porta UDP 161 em todas as redes StorageGRID .

Passos

1. Selecione **Criar**.
2. Insira as seguintes informações.

Campo	Descrição
Protocolo de internet	Se este endereço usará IPv4 ou IPv6. Por padrão, o SNMP usa IPv4.
Protocolo de transporte	Se este endereço usará UDP ou TCP. Por padrão, o SNMP usa UDP.
Rede StorageGRID	Em qual rede StorageGRID o agente irá escutar. • Redes de grade, administração e cliente: o agente SNMP escutará consultas em todas as três redes. • Rede de grade • Rede de administração • Rede de clientes Observação: se você usar a Rede do Cliente para dados inseguros e criar um endereço de agente para a Rede do Cliente, esteja ciente de que o tráfego SNMP também será inseguro.
Porta	Opcionalmente, o número da porta na qual o agente SNMP deve escutar. A porta UDP padrão para um agente SNMP é 161, mas você pode inserir qualquer número de porta não utilizado. Observação: quando você salva o agente SNMP, o StorageGRID abre automaticamente as portas de endereço do agente no firewall interno. Você deve garantir que todos os firewalls externos permitam acesso a essas portas.

3. Selecione **Criar**.

O endereço do agente é criado e adicionado à tabela.

Criar usuários USM

Se você estiver usando SNMPv3, use a guia Usuários do USM na seção Outras configurações para definir os usuários do USM que estão autorizados a consultar o MIB ou a receber traps e informações.



Os destinos SNMPv3 *inform* devem ter usuários com IDs de mecanismo. O destino SNMPv3 *trap* não pode ter usuários com IDs de mecanismo.

Essas etapas não se aplicam se você estiver usando apenas SNMPv1 ou SNMPv2c.

Passos

1. Selecione **Criar**.

2. Insira as seguintes informações.

Campo	Descrição
Nome de usuário	Um nome exclusivo para este usuário USM. Os nomes de usuário podem ter no máximo 32 caracteres e não podem conter espaços em branco. O nome de usuário não pode ser alterado após a criação do usuário.
Acesso MIB somente leitura	Se selecionado, este usuário deverá ter acesso somente leitura ao MIB.
ID do mecanismo autoritativo	Se este usuário for usado em um destino de informação, o ID do mecanismo autoritativo para este usuário. Digite de 10 a 64 caracteres hexadecimais (5 a 32 bytes) sem espaços. Este valor é necessário para usuários do USM que serão selecionados em destinos de trap para informações. Este valor não é permitido para usuários do USM que serão selecionados em destinos de armadilhas para armadilhas. Observação: Este campo não será exibido se você selecionar Acesso MIB somente leitura porque os usuários do USM que têm acesso MIB somente leitura não podem ter IDs de mecanismo.
Nível de segurança	O nível de segurança para o usuário USM: • authPriv: Este usuário se comunica com autenticação e privacidade (criptografia). Você deve especificar um protocolo de autenticação e uma senha, bem como um protocolo de privacidade e uma senha. • authNoPriv: Este usuário se comunica com autenticação e sem privacidade (sem criptografia). Você deve especificar um protocolo de autenticação e uma senha.
Protocolo de autenticação	Sempre definido como SHA, que é o único protocolo suportado (HMAC-SHA-96).
Senha	A senha que este usuário usará para autenticação.
Protocolo de privacidade	Exibido somente se você selecionou authPriv e sempre definiu como AES, que é o único protocolo de privacidade suportado.
Senha	Exibido somente se você selecionou authPriv . A senha que este usuário usará para privacidade.

3. Selecione **Criar**.

O usuário USM é criado e adicionado à tabela.

4. Quando tiver concluído a configuração do agente SNMP, selecione **Salvar**.

A nova configuração do agente SNMP fica ativa.

Atualizar o agente SNMP

Você pode desabilitar notificações SNMP, atualizar strings de comunidade ou adicionar ou remover endereços de agentes, usuários USM e destinos de interceptação.

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

Ver ["Configurar o agente SNMP"](#) para obter detalhes sobre cada campo na página do agente SNMP. Você deve selecionar **Salvar** na parte inferior da página para confirmar quaisquer alterações feitas em cada guia.

Passos

1. Selecione **CONFIGURAÇÃO > Monitoramento > Agente SNMP**.

A página do agente SNMP é exibida.

2. Para desabilitar o agente SNMP em todos os nós da grade, desmarque a caixa de seleção **Habilitar SNMP** e selecione **Salvar**.

Se você reativar o agente SNMP, todas as configurações SNMP anteriores serão mantidas.

3. Opcionalmente, atualize as informações na seção Configuração básica:

- a. Conforme necessário, atualize o **Contato do sistema** e o **Local do sistema**.
- b. Opcionalmente, marque ou desmarque a caixa de seleção **Habilitar notificações do agente SNMP** para controlar se o agente SNMP do StorageGRID envia notificações de interceptação e informação.

Quando esta caixa de seleção está desmarcada, o agente SNMP suporta acesso MIB somente leitura, mas não envia notificações SNMP.

- c. Opcionalmente, marque ou desmarque a caixa de seleção **Ativar armadilhas de autenticação** para controlar se o agente SNMP do StorageGRID envia armadilhas de autenticação quando recebe mensagens de protocolo autenticadas incorretamente.
4. Se você usar SNMPv1 ou SNMPv2c, opcionalmente atualize ou adicione uma **Comunidade somente leitura** na seção Strings da comunidade.
 5. Para atualizar destinos de armadilhas, selecione a aba Destinos de armadilhas na seção Outras configurações.

Use esta guia para definir um ou mais destinos para notificações de interceptação ou informação do StorageGRID . Quando você habilita o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando os alertas são acionados. Notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifDown e coldStart).

Para obter detalhes sobre o que inserir, consulte ["Criar destinos de armadilhas"](#) .

- Opcionalmente, atualize ou remova a comunidade de armadilhas padrão.

Se você remover a comunidade de armadilhas padrão, primeiro deverá garantir que todos os destinos de armadilhas existentes usem uma sequência de caracteres de comunidade personalizada.

- Para adicionar um destino de armadilha, selecione **Criar**.
- Para editar um destino de armadilha, selecione o botão de opção e selecione **Editar**.
- Para remover um destino de armadilha, selecione o botão de opção e selecione **Remover**.
- Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

6. Para atualizar endereços de agentes, selecione a guia Endereços de agentes na seção Outras configurações.

Use esta aba para especificar um ou mais "endereços de escuta". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

Para obter detalhes sobre o que inserir, consulte "[Criar endereços de agentes](#)".

- Para adicionar um endereço de agente, selecione **Criar**.
- Para editar o endereço de um agente, selecione o botão de opção e selecione **Editar**.
- Para remover um endereço de agente, selecione o botão de opção e selecione **Remover**.
- Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

7. Para atualizar usuários do USM, selecione a guia Usuários do USM na seção Outras configurações.

Use esta guia para definir os usuários do USM que estão autorizados a consultar o MIB ou a receber armadilhas e informações.

Para obter detalhes sobre o que inserir, consulte "[Criar usuários USM](#)".

- Para adicionar um usuário USM, selecione **Criar**.
- Para editar um usuário USM, selecione o botão de opção e selecione **Editar**.

O nome de usuário de um usuário USM existente não pode ser alterado. Se precisar alterar um nome de usuário, você deverá removê-lo e criar um novo.



Se você adicionar ou remover o ID de mecanismo autoritativo de um usuário e esse usuário estiver selecionado para um destino, você deverá editar ou remover o destino. Caso contrário, ocorrerá um erro de validação ao salvar a configuração do agente SNMP.

- Para remover um usuário do USM, selecione o botão de opção e selecione **Remover**.



Se o usuário que você removeu estiver selecionado para um destino de interceptação, você deverá editar ou remover o destino. Caso contrário, ocorrerá um erro de validação ao salvar a configuração do agente SNMP.

- Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

8. Quando você tiver atualizado a configuração do agente SNMP, selecione **Salvar**.

Acessar arquivos MIB

Os arquivos MIB contêm definições e informações sobre as propriedades dos recursos e serviços gerenciados para os nós na sua grade. Você pode acessar arquivos MIB que

definem os objetos e notificações para StorageGRID. Esses arquivos podem ser úteis para monitorar sua grade.

Ver ["Usar monitoramento SNMP"](#) para mais informações sobre arquivos SNMP e MIB.

Acessar arquivos MIB

Siga estas etapas para acessar os arquivos MIB.

Passos

1. Selecione **CONFIGURAÇÃO > Monitoramento > Agente SNMP**.
2. Na página do agente SNMP, selecione o arquivo que deseja baixar:
 - **NETAPP-STORAGEGRID-MIB.txt**: Define a tabela de alertas e notificações (traps) acessíveis em todos os nós de administração.
 - **ES-NETAPP-06-MIB.mib**: Define objetos e notificações para dispositivos baseados na Série E.
 - **MIB_1_10.zip**: Define objetos e notificações para dispositivos com uma interface BMC .



Você também pode acessar arquivos MIB no seguinte local em qualquer nó do StorageGRID : `/usr/share/snmp/mibs`

3. Para extrair os OIDs do StorageGRID do arquivo MIB:

- a. Obtenha o OID da raiz do StorageGRID MIB:

```
root@user-adml:~ # snmptranslate -On -IR storagegrid
```

Resultado: `.1.3.6.1.4.1.789.28669` (28669 é sempre o OID para StorageGRID)

- a. Grep para o OID StorageGRID em toda a árvore (usando `paste` para unir linhas):

```
root@user-adml:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



O `snmptranslate` O comando tem muitas opções úteis para explorar o MIB. Este comando está disponível em qualquer nó StorageGRID .

Conteúdo do arquivo MIB

Todos os objetos estão sob o OID StorageGRID .

Nome do objeto	ID do objeto (OID)	Descrição
		O módulo MIB para entidades NetApp StorageGRID .

Objetos MIB

Nome do objeto	ID do objeto (OID)	Descrição
Contagem de Alerta Ativo		O número de alertas ativos na activeAlertTable.
Tabela de Alerta Ativo		Uma tabela de alertas ativos no StorageGRID.
ID de alerta ativo		O ID do alerta. Único no conjunto atual de alertas ativos.
NomeAlertaAtivo		O nome do alerta.
instância de alerta ativo		O nome da entidade que gerou o alerta, normalmente o nome do nó.
activeAlertSeverity		A gravidade do alerta.
hora de início do alerta ativo		Data e hora em que o alerta foi disparado.

Tipos de notificação (armadilhas)

Todas as notificações incluem as seguintes variáveis como varbinds:

- ID de alerta ativo
- NomeAlertaAtivo
- instância de alerta ativo
- activeAlertSeverity
- hora de início do alerta ativo

Tipo de notificação	ID do objeto (OID)	Descrição
Alerta Menor Ativo		Um alerta com gravidade menor
AlertaMaiorAtivo		Um alerta com grande gravidade
AlertaCríticoAtivo		Um alerta com gravidade crítica

Coletar dados adicionais do StorageGRID

Use tabelas e gráficos

Você pode usar gráficos e relatórios para monitorar o estado do sistema StorageGRID e solucionar problemas.

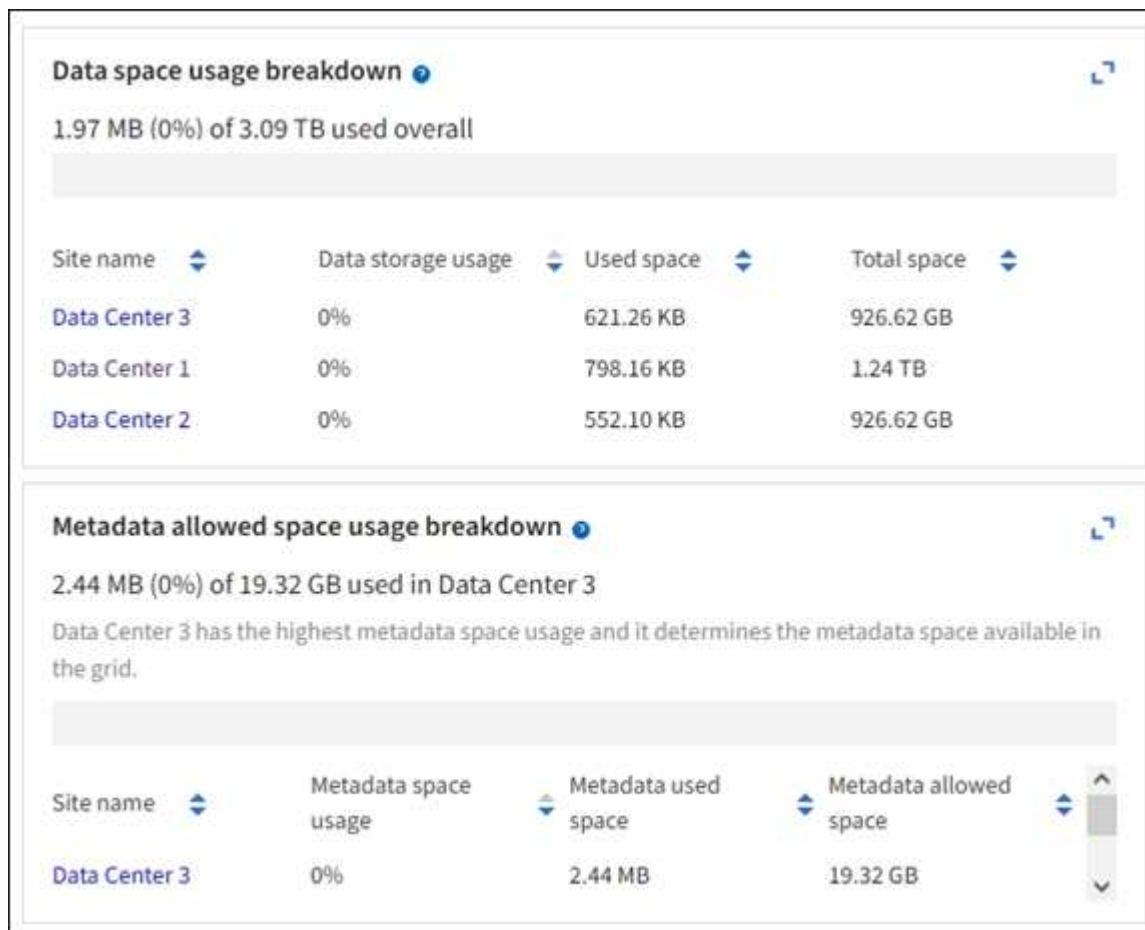


O Grid Manager é atualizado a cada versão e pode não corresponder às capturas de tela de exemplo nesta página.

Tipos de gráficos

Gráficos e tabelas resumem os valores de métricas e atributos específicos do StorageGRID .

O painel do Grid Manager inclui cartões que resumem o armazenamento disponível para a grade e cada site.



O painel de uso de armazenamento no painel do Gerenciador de locatários exibe o seguinte:

- Uma lista dos maiores buckets (S3) ou contêineres (Swift) para o locatário
- Um gráfico de barras que representa os tamanhos relativos dos maiores baldes ou recipientes
- A quantidade total de espaço utilizado e, se uma cota for definida, a quantidade e a porcentagem de espaço restante

Dashboard

16 Buckets
[View buckets](#)

2 Platform services
endpoints
[View endpoints](#)

0 Groups
[View groups](#)

1 User
[View users](#)

Storage usage ?

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage ?

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details ?

Name: Tenant02

ID: 3341 1240 0546 8283 2208

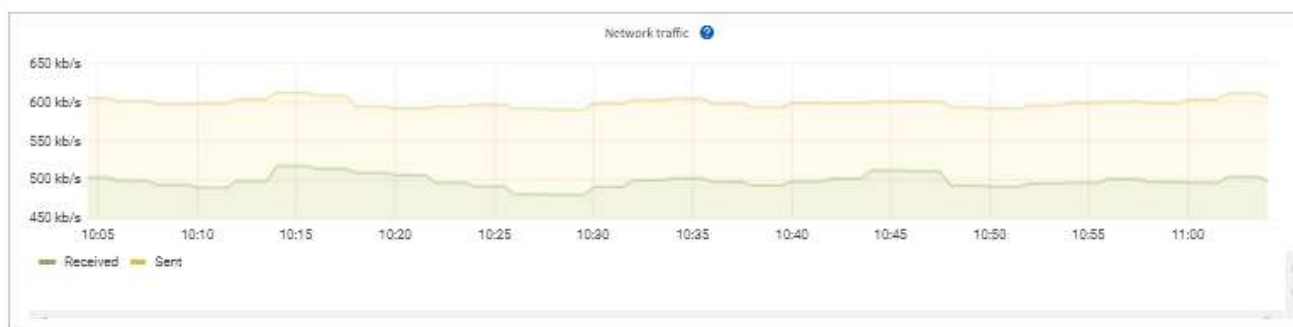
- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Além disso, gráficos que mostram como as métricas e os atributos do StorageGRID mudam ao longo do tempo estão disponíveis na página Nós e na página **SUPORTE > Ferramentas > Topologia de grade**.

Existem quatro tipos de gráficos:

- **Gráficos Grafana:** Exibidos na página Nós, os gráficos Grafana são usados para plotar os valores das métricas do Prometheus ao longo do tempo. Por exemplo, a guia **NÓS > Rede** para um Nó de Armazenamento inclui um gráfico Grafana para tráfego de rede.

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

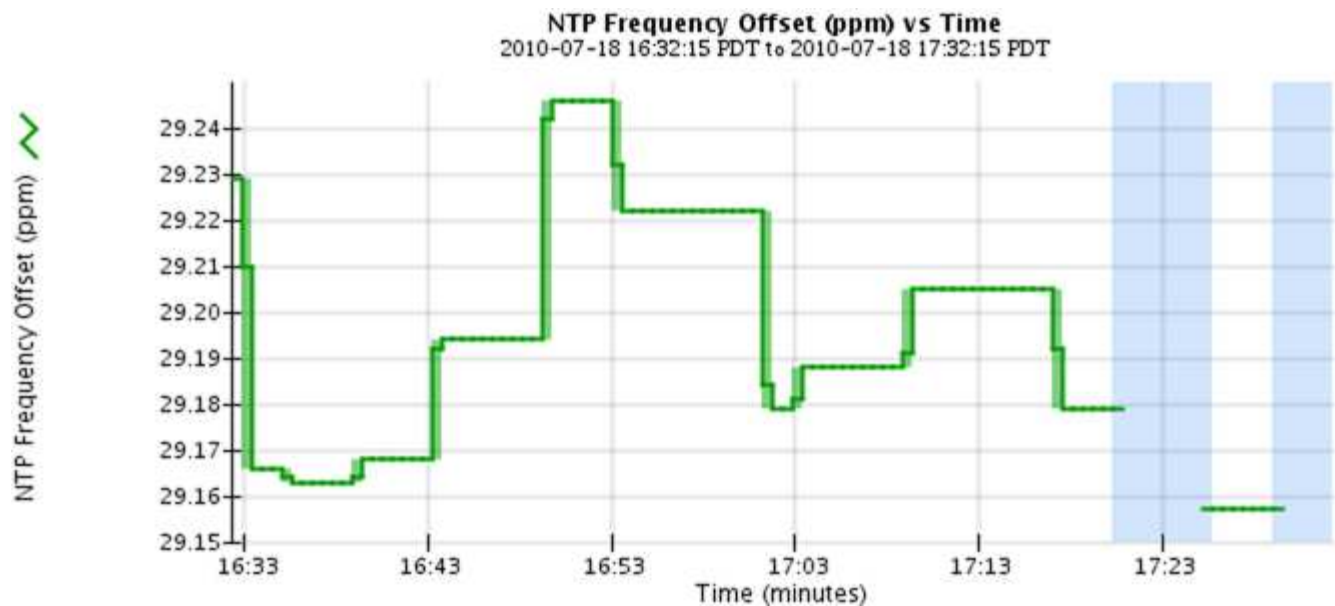
Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

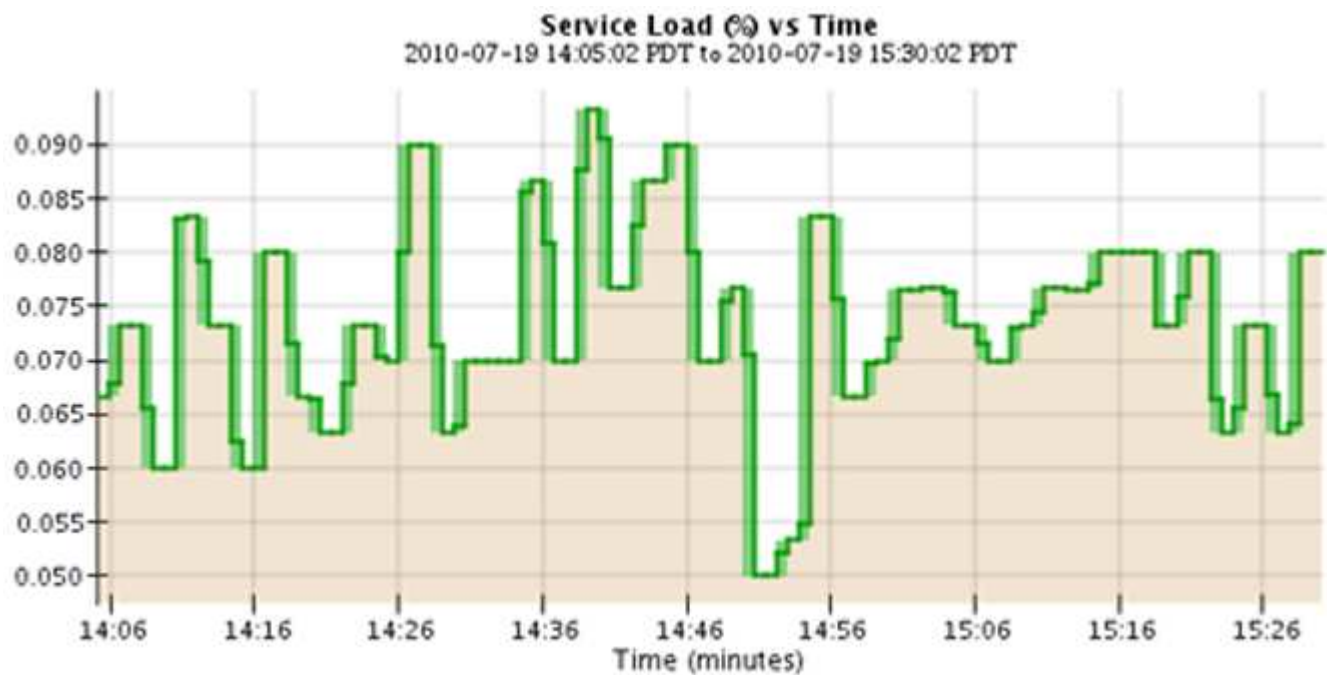


Os gráficos do Grafana também estão incluídos nos painéis pré-construídos disponíveis na página **SUPORTE > Ferramentas > Métricas**.

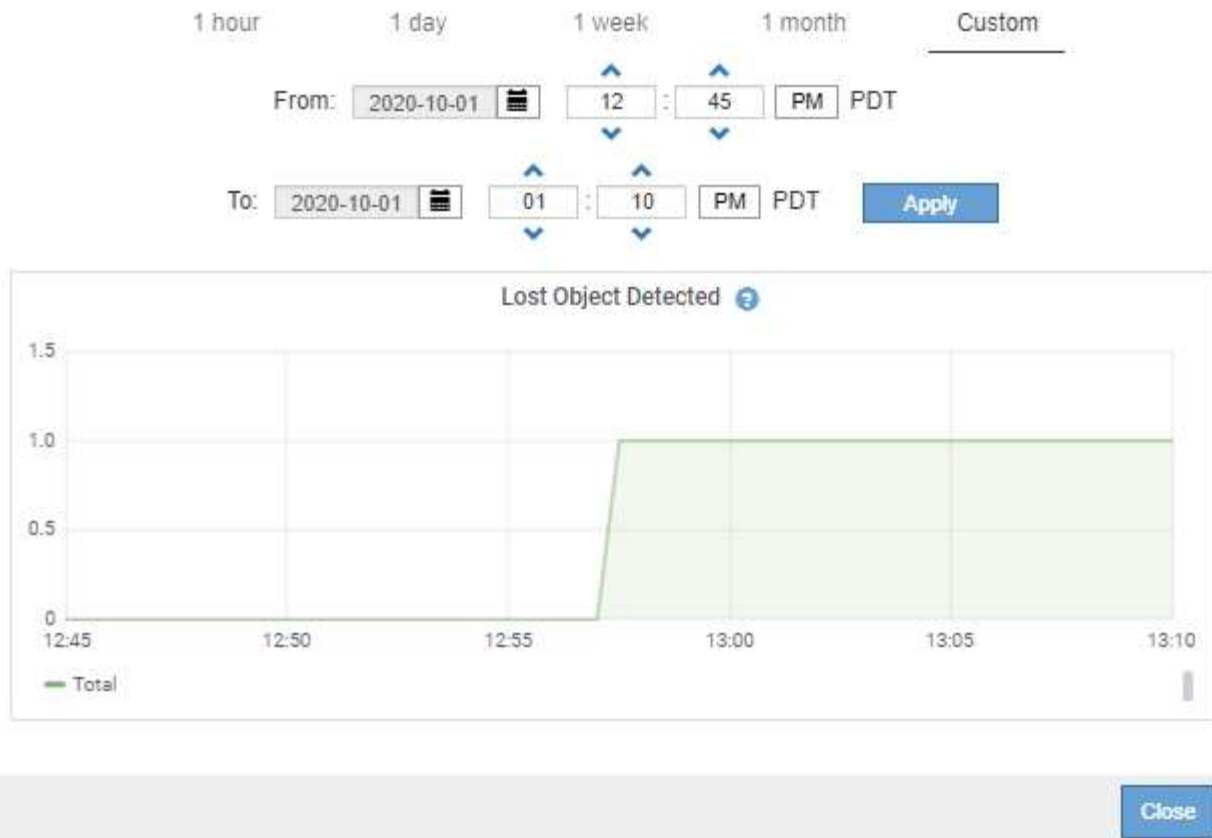
- **Gráficos de linha:** Disponíveis na página Nós e na página **SUPORTE > Ferramentas > Topologia de grade** (selecione o ícone do gráfico  após um valor de dados), gráficos de linha são usados para plotar os valores dos atributos StorageGRID que têm um valor unitário (como deslocamento de frequência NTP, em ppm). As alterações no valor são plotadas em intervalos de dados regulares (bins) ao longo do tempo.



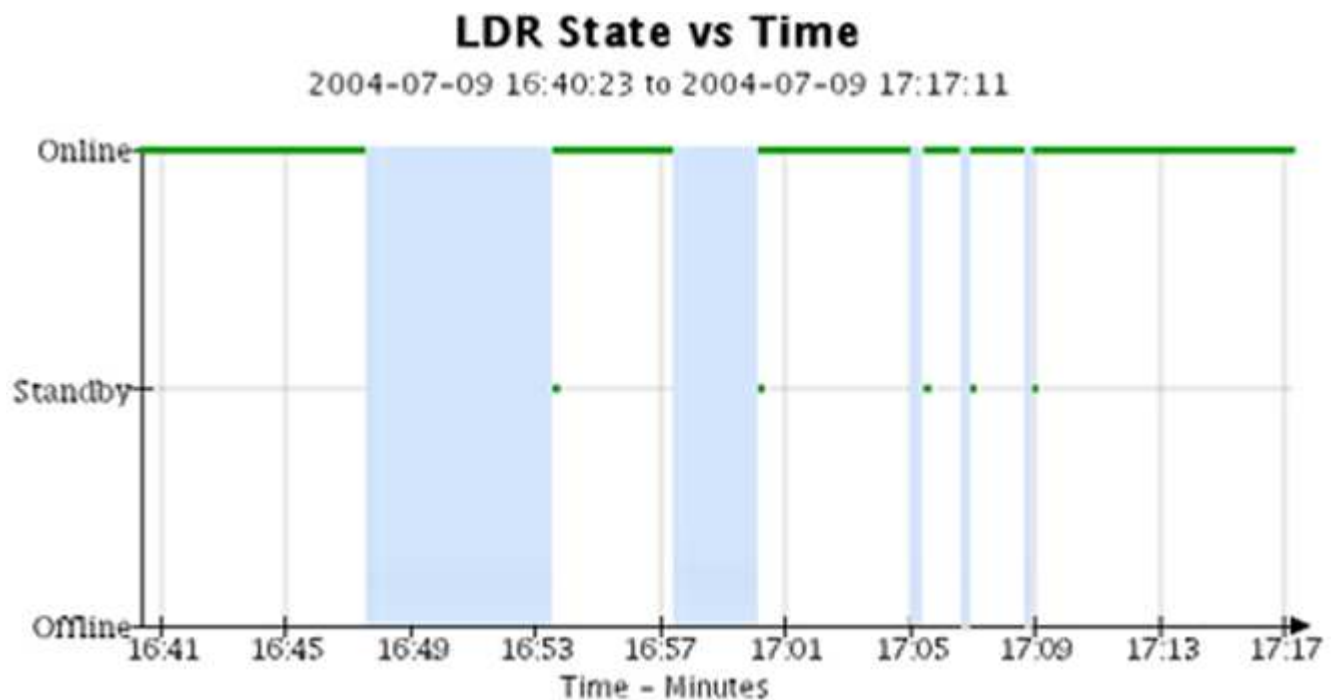
- **Gráficos de área:** Disponíveis na página Nós e na página **SUPORTE > Ferramentas > Topologia de grade** (selecione o ícone do gráfico  após um valor de dados), gráficos de área são usados para plotar quantidades de atributos volumétricos, como contagens de objetos ou valores de carga de serviço. Os gráficos de área são semelhantes aos gráficos de linhas, mas incluem um sombreamento marrom claro abaixo da linha. As alterações no valor são plotadas em intervalos de dados regulares (bins) ao longo do tempo.



- Alguns gráficos são indicados com um tipo diferente de ícone de gráfico  e têm um formato diferente:



- **Gráfico de estado:** Disponível na página **SUPORTE > Ferramentas > Topologia de grade** (selecione o ícone do gráfico  após um valor de dados), os gráficos de estado são usados para plotar valores de atributos que representam estados distintos, como um estado de serviço que pode ser online, em espera ou offline. Os gráficos de estado são semelhantes aos gráficos de linha, mas a transição é descontínua; ou seja, o valor salta de um valor de estado para outro.



Informações relacionadas

- ["Ver a página de nós"](#)
- ["Visualizar a árvore de topologia da grade"](#)
- ["Revisar métricas de suporte"](#)

Legenda do gráfico

As linhas e cores usadas para desenhar gráficos têm um significado específico.

Exemplo	Significado
	Os valores de atributos relatados são plotados usando linhas verde-escuras.
	O sombreamento verde claro ao redor das linhas verde escuro indica que os valores reais nesse intervalo de tempo variam e foram "agrupados" para uma plotagem mais rápida. A linha escura representa a média ponderada. O intervalo em verde claro indica os valores máximo e mínimo dentro do compartimento. O sombreamento marrom claro é usado em gráficos de área para indicar dados volumétricos.
	Áreas em branco (sem dados plotados) indicam que os valores dos atributos não estavam disponíveis. O fundo pode ser azul, cinza ou uma mistura de cinza e azul, dependendo do estado do serviço que relata o atributo.
	O sombreamento azul claro indica que alguns ou todos os valores de atributo naquele momento eram indeterminados; o atributo não estava relatando valores porque o serviço estava em um estado desconhecido.
	O sombreamento cinza indica que alguns ou todos os valores de atributos naquele momento não eram conhecidos porque o serviço que relatava os atributos estava administrativamente inativo.
	Uma mistura de sombreamento cinza e azul indica que alguns dos valores de atributos no momento eram indeterminados (porque o serviço estava em um estado desconhecido), enquanto outros não eram conhecidos porque o serviço que relatava os atributos estava administrativamente inativo.

Exibir tabelas e gráficos

A página Nós contém os gráficos e tabelas que você deve acessar regularmente para monitorar atributos como capacidade de armazenamento e taxa de transferência. Em alguns casos, especialmente ao trabalhar com suporte técnico, você pode usar a página **SUPORTE > Ferramentas > Topologia de grade** para acessar gráficos adicionais.

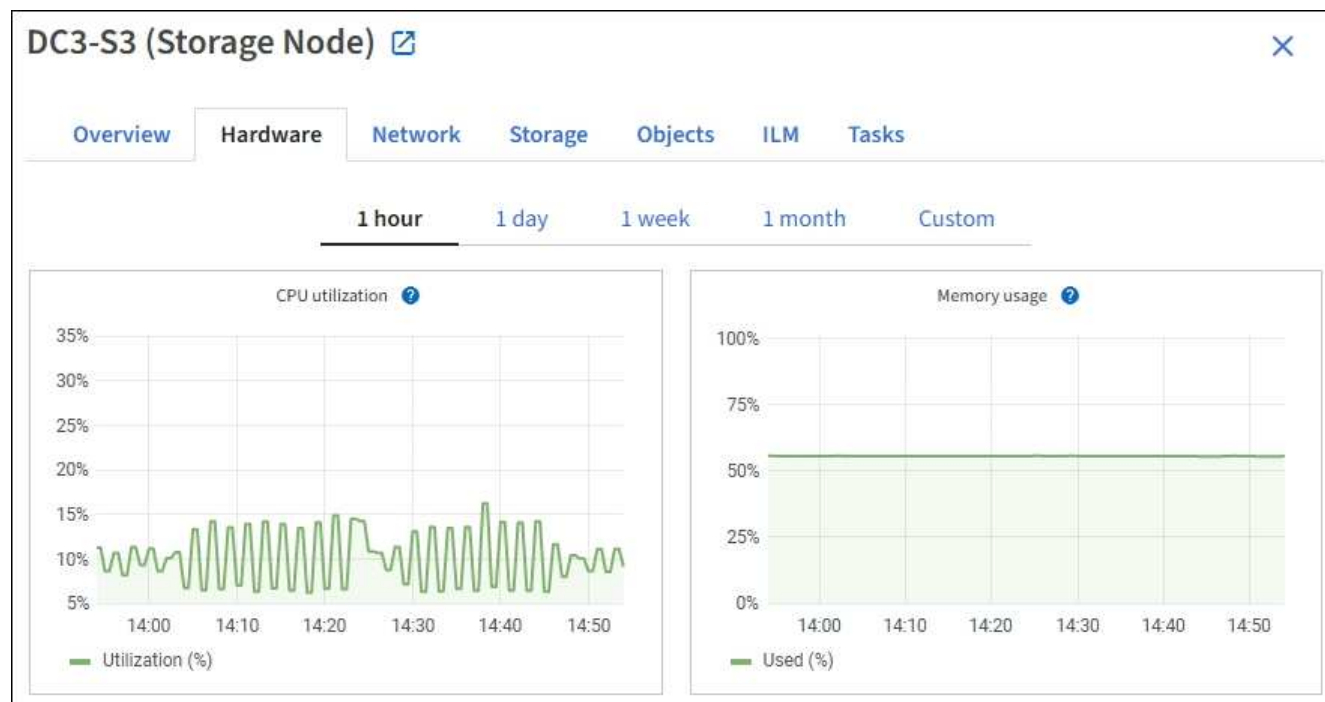
Antes de começar

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

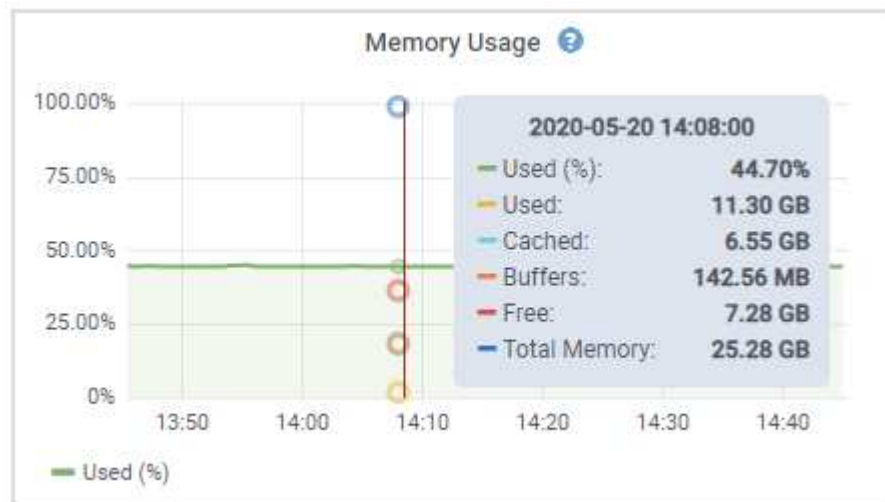
Passos

1. Selecione **NODES**. Em seguida, selecione um nó, um site ou a grade inteira.
2. Selecione a aba cujas informações você deseja visualizar.

Algumas guias incluem um ou mais gráficos Grafana, que são usados para plotar os valores das métricas do Prometheus ao longo do tempo. Por exemplo, a guia **NÓS > Hardware** para um nó inclui dois gráficos Grafana.



3. Opcionalmente, posicione o cursor sobre o gráfico para ver valores mais detalhados de um determinado momento.



4. Conforme necessário, muitas vezes você pode exibir um gráfico para um atributo ou métrica específica. Na tabela na página Nós, selecione o ícone do gráfico  à direita do nome do atributo.



Os gráficos não estão disponíveis para todas as métricas e atributos.

Exemplo 1: Na guia Objetos de um Nó de Armazenamento, você pode selecionar o ícone do gráfico  para ver o número total de consultas bem-sucedidas do repositório de metadados para o nó de armazenamento.



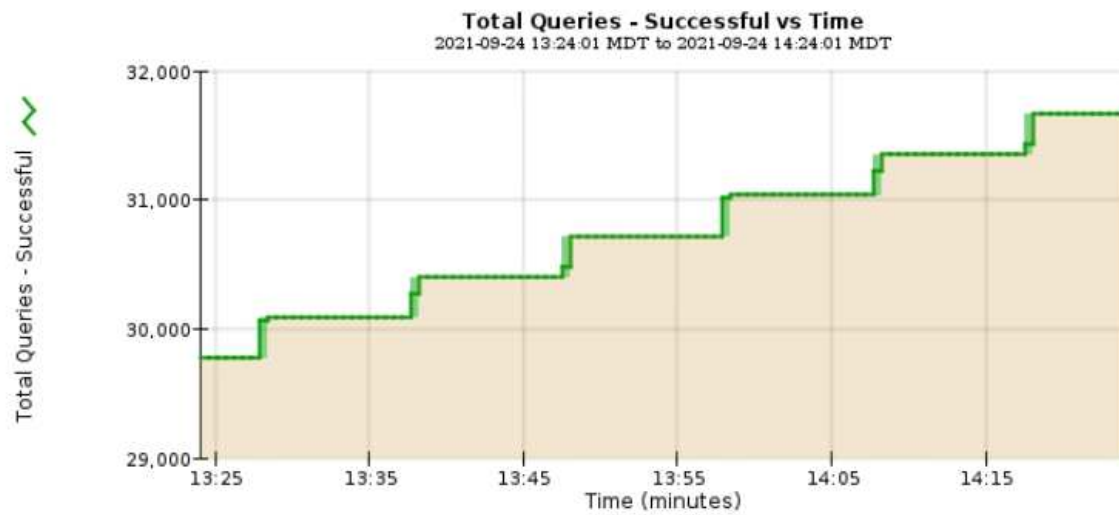
Reports (Charts): DDS (DC1-S1) - Data Store



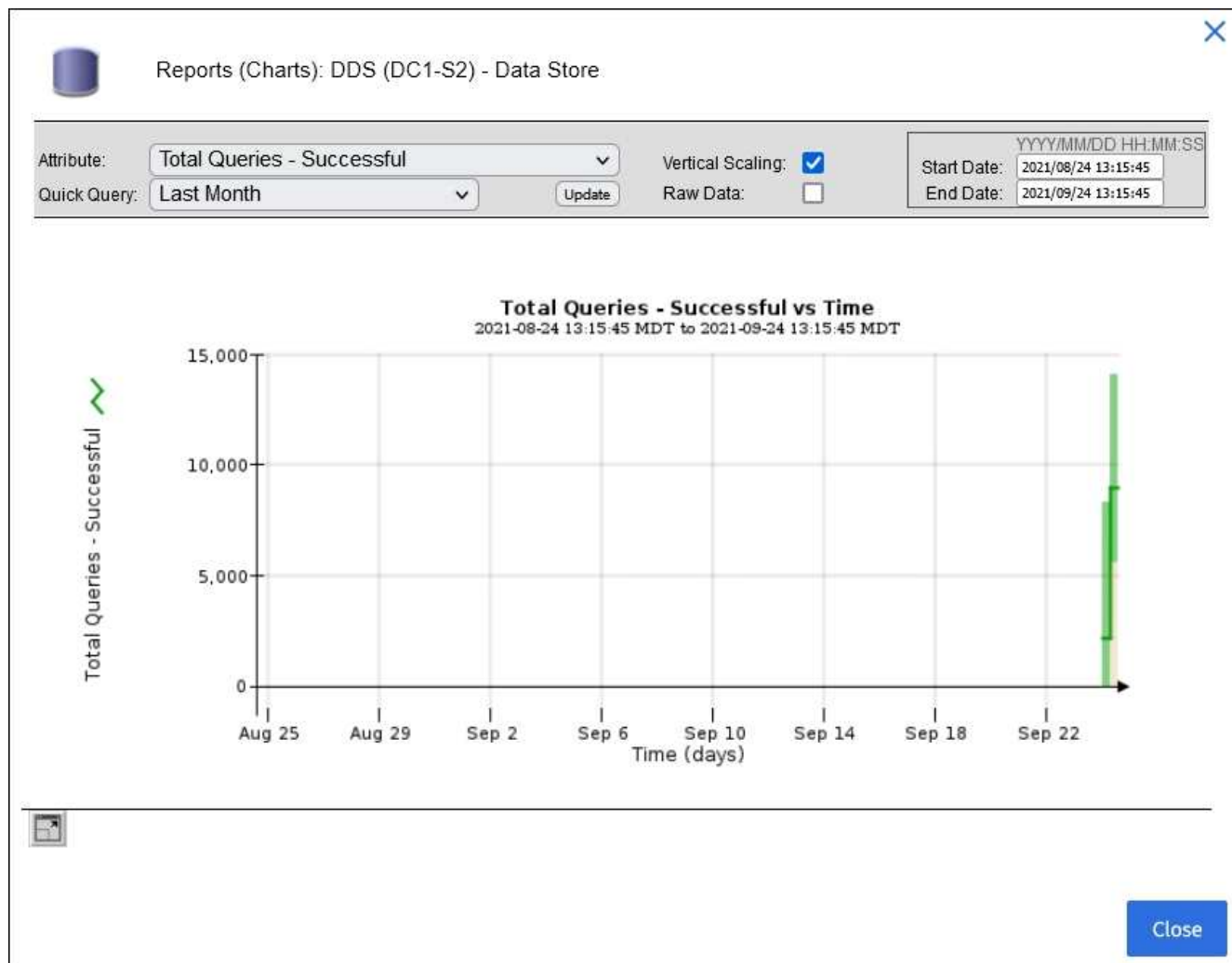
Attribute: Total Queries - Successful
Quick Query: Last Hour

Vertical Scaling: ☒
Raw Data: ☐

Start Date: 2021/09/24 13:24:01
End Date: 2021/09/24 14:24:01

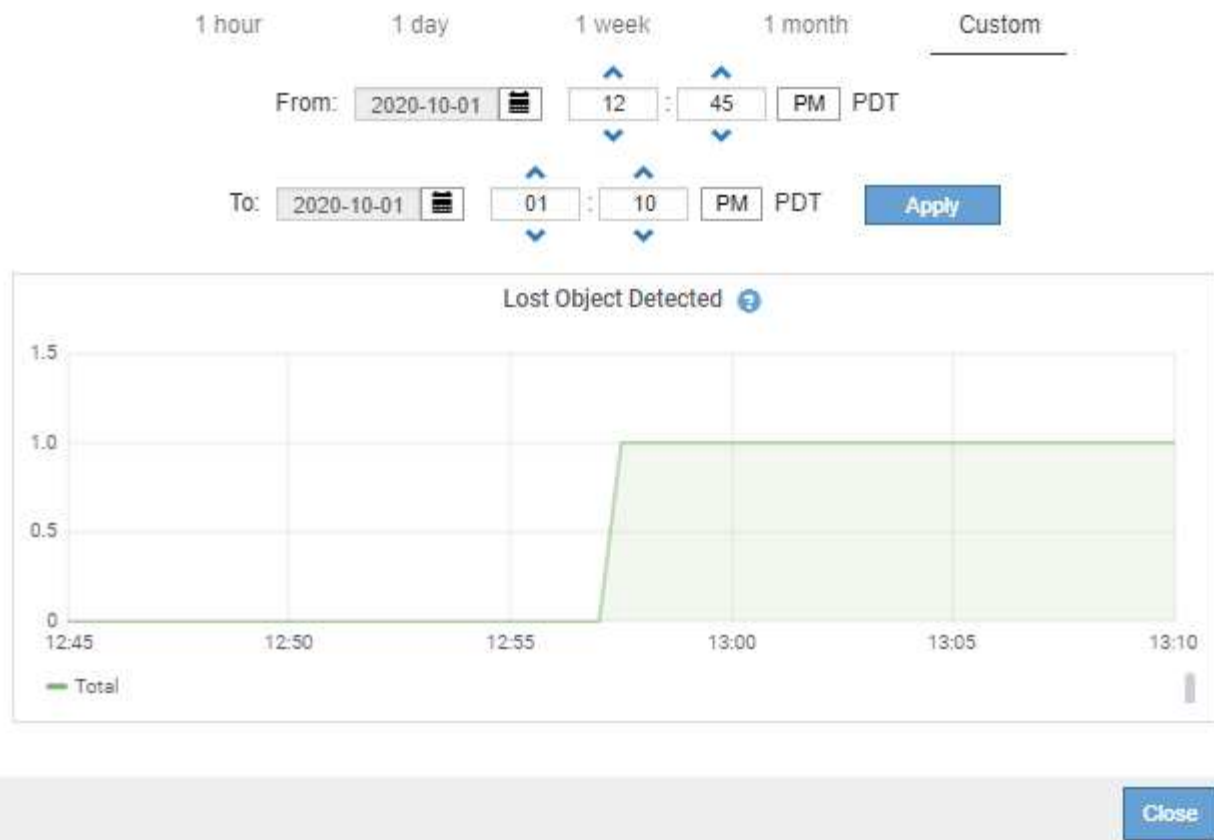


Close



Exemplo 2: Na guia Objetos de um nó de armazenamento, você pode selecionar o ícone do gráfico para ver o gráfico Grafana da contagem de objetos perdidos detectados ao longo do tempo.

Object Counts		
Total Objects	1	
Lost Objects	1	
S3 Buckets and Swift Containers	1	



5. Para exibir gráficos para atributos que não são mostrados na página Nó, selecione **SUPORTE > Ferramentas > Topologia de grade**.
6. Selecione *nó de grade > componente ou serviço > Visão geral > Principal*.

Overview

Alarms

Reports

Configuration

Main



Overview: SSM (DC1-ADM1) - Resources
 Updated: 2018-05-07 16:29:52 MDT

Computational Resources

Service Restarts:	1	
Service Runtime:	6 days	
Service Uptime:	6 days	
Service CPU Seconds:	10666 s	
Service Load:	0.266 %	

Memory

Installed Memory:	8.38 GB	
Available Memory:	2.9 GB	

Processors

Processor Number	Vendor	Type	Cache
1	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
2	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
3	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
4	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
5	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
6	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
7	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
8	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB

7. Selecione o ícone do gráfico  ao lado do atributo.

A exibição muda automaticamente para a página **Relatórios > Gráficos**. O gráfico exibe os dados do atributo no último dia.

Gerar gráficos

Os gráficos exibem uma representação gráfica dos valores de dados de atributos. Você pode gerar relatórios sobre um site de data center, nó de grade, componente ou serviço.

Antes de começar

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

Passos

1. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
2. Selecione **grid node > component or service > Relatórios > Gráficos**.
3. Selecione o atributo a ser relatado na lista suspensa **Atributo**.
4. Para forçar o eixo Y a começar em zero, desmarque a caixa de seleção **Escala vertical**.
5. Para mostrar valores com precisão total, marque a caixa de seleção **Dados Brutos** ou, para arredondar

os valores para um máximo de três casas decimais (por exemplo, para atributos relatados como porcentagens), desmarque a caixa de seleção **Dados Brutos**.

6. Selecione o período de tempo para relatar na lista suspensa **Consulta rápida**.

Selecione a opção Consulta personalizada para selecionar um intervalo de tempo específico.

O gráfico aparece depois de alguns instantes. Reserve vários minutos para tabulação de intervalos de tempo longos.

7. Se você selecionou Consulta personalizada, personalize o período do gráfico inserindo a **Data de início** e a **Data de término**.

Use o formato *YYYY/MM/DDHH:MM:SS* no horário local. Zeros à esquerda são necessários para corresponder ao formato. Por exemplo, 2017/4/6 7:30:00 falha na validação. O formato correto é: 2017/04/06 07:30:00.

8. Selecione **Atualizar**.

Um gráfico é gerado após alguns segundos. Reserve vários minutos para tabulação de intervalos de tempo longos. Dependendo do período definido para a consulta, um relatório de texto bruto ou um relatório de texto agregado será exibido.

Usar relatórios de texto

Os relatórios de texto exibem uma representação textual dos valores de dados de atributos que foram processados pelo serviço NMS. Há dois tipos de relatórios gerados dependendo do período de tempo em que você está relatando: relatórios de texto bruto para períodos inferiores a uma semana e relatórios de texto agregado para períodos superiores a uma semana.

Relatórios de texto bruto

Um relatório de texto bruto exibe detalhes sobre o atributo selecionado:

- Hora de recebimento: data e hora locais em que um valor de amostra dos dados de um atributo foi processado pelo serviço NMS.
- Hora da amostra: data e hora locais em que um valor de atributo foi amostrado ou alterado na origem.
- Valor: Valor do atributo no momento da amostra.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Relatórios de texto agregado

Um relatório de texto agregado exibe dados durante um período de tempo mais longo (geralmente uma semana) do que um relatório de texto bruto. Cada entrada é o resultado do resumo de vários valores de atributos (um agregado de valores de atributos) pelo serviço NMS ao longo do tempo em uma única entrada com valores médios, máximos e mínimos derivados da agregação.

Cada entrada exibe as seguintes informações:

- Hora agregada: última data e hora local em que o serviço NMS agregou (coletou) um conjunto de valores de atributos alterados.
- Valor médio: a média do valor do atributo ao longo do período de tempo agregado.
- Valor mínimo: o valor mínimo ao longo do período de tempo agregado.
- Valor máximo: o valor máximo durante o período de tempo agregado.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Gerar relatórios de texto

Os relatórios de texto exibem uma representação textual dos valores de dados de atributos que foram processados pelo serviço NMS. Você pode gerar relatórios sobre um site de data center, nó de grade, componente ou serviço.

Antes de começar

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

Sobre esta tarefa

Para dados de atributos que devem mudar continuamente, esses dados de atributos são amostrados pelo serviço NMS (na origem) em intervalos regulares. Para dados de atributo que mudam com pouca frequência (por exemplo, dados baseados em eventos como alterações de estado ou status), um valor de atributo é enviado ao serviço NMS quando o valor muda.

O tipo de relatório exibido depende do período de tempo configurado. Por padrão, relatórios de texto agregados são gerados para períodos maiores que uma semana.

O texto em cinza indica que o serviço estava administrativamente inativo durante o período em que foi amostrado. O texto azul indica que o serviço estava em um estado desconhecido.

Passos

1. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
2. Selecione **nó de grade > componente ou serviço > Relatórios > Texto**.
3. Selecione o atributo a ser relatado na lista suspensa **Atributo**.
4. Selecione o número de resultados por página na lista suspensa **Resultados por página**.
5. Para arredondar valores para um máximo de três casas decimais (por exemplo, para atributos relatados como porcentagens), desmarque a caixa de seleção **Dados Brutos**.
6. Selecione o período de tempo para relatar na lista suspensa **Consulta rápida**.

Selecione a opção Consulta personalizada para selecionar um intervalo de tempo específico.

O relatório aparece depois de alguns instantes. Reserve vários minutos para tabulação de intervalos de tempo longos.

- Se você selecionou Consulta personalizada, precisará personalizar o período de tempo do relatório inserindo a **Data de início** e a **Data de término**.

Use o formato YYYY/MM/DDHH:MM:SS no horário local. Zeros à esquerda são necessários para corresponder ao formato. Por exemplo, 2017/4/6 7:30:00 falha na validação. O formato correto é: 2017/04/06 07:30:00.

- Clique em **Atualizar**.

Um relatório de texto é gerado após alguns instantes. Reserve vários minutos para tabulação de intervalos de tempo longos. Dependendo do período definido para a consulta, um relatório de texto bruto ou um relatório de texto agregado será exibido.

Exportar relatórios de texto

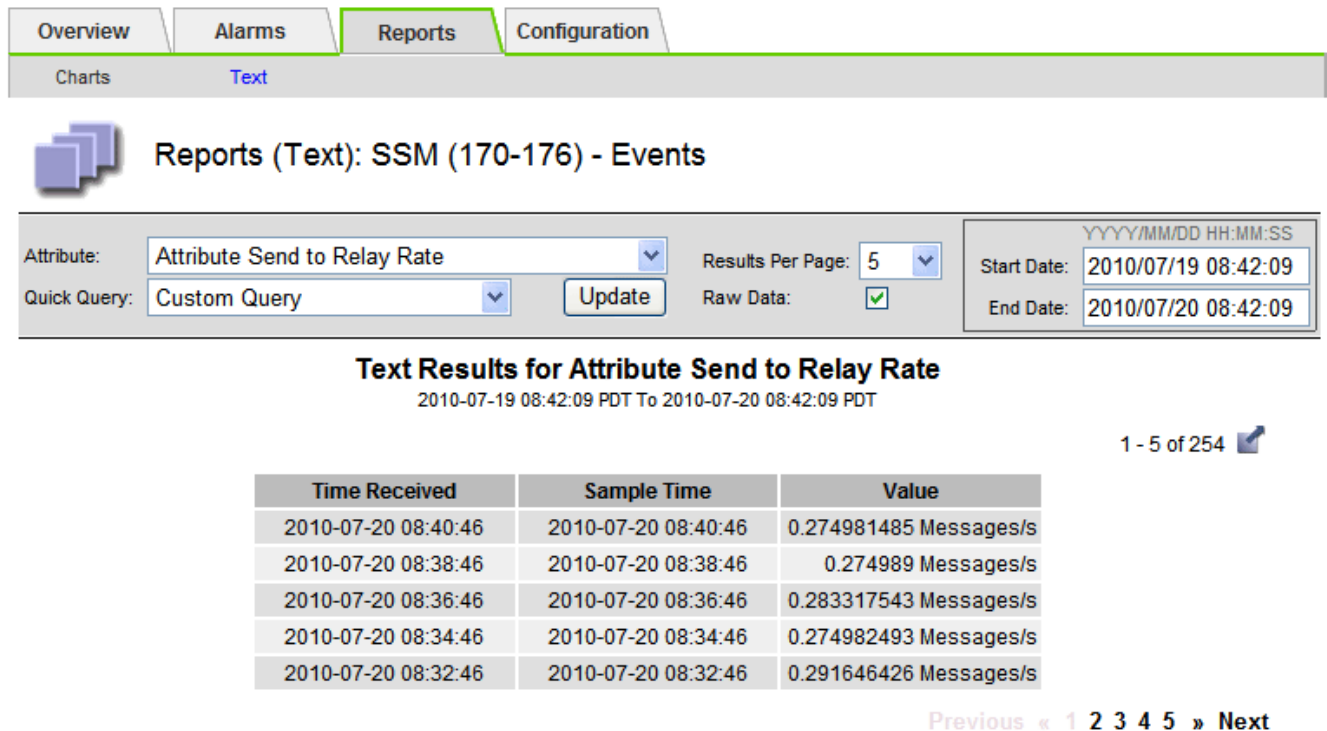
Os relatórios de texto exportados abrem uma nova guia do navegador, que permite selecionar e copiar os dados.

Sobre esta tarefa

Os dados copiados podem então ser salvos em um novo documento (por exemplo, uma planilha) e usados para analisar o desempenho do sistema StorageGRID .

Passos

- Selecione **SUPORTE > Ferramentas > Topologia de grade**.
- Crie um relatório de texto.
- Clique em *Exportar*.



The screenshot shows the 'Reports (Text): SSM (170-176) - Events' interface. It includes tabs for Overview, Alarms, Reports, and Configuration. Under Reports, there are sub-tabs for Charts and Text. The main content area displays the 'Attribute Send to Relay Rate' report. The report title is 'Text Results for Attribute Send to Relay Rate' with a subtitle '2010-07-19 08:42:09 PDT To 2010-07-20 08:42:09 PDT'. The report shows a table of results with columns 'Time Received', 'Sample Time', and 'Value'. The table contains 5 rows of data. Below the table, there is a pagination control showing '1 - 5 of 254' and a 'Next' button.

Time Received	Sample Time	Value
2010-07-20 08:40:46	2010-07-20 08:40:46	0.274981485 Messages/s
2010-07-20 08:38:46	2010-07-20 08:38:46	0.274989 Messages/s
2010-07-20 08:36:46	2010-07-20 08:36:46	0.283317543 Messages/s
2010-07-20 08:34:46	2010-07-20 08:34:46	0.274982493 Messages/s
2010-07-20 08:32:46	2010-07-20 08:32:46	0.291646426 Messages/s

A janela Exportar Relatório de Texto é aberta exibindo o relatório.

Grid ID: 000 000
 OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
 Node Path: Site/170-176/SSM/Events
 Attribute: Attribute Send to Relay Rate (ABSR)
 Query Start Date: 2010-07-19 08:42:09 PDT
 Query End Date: 2010-07-20 08:42:09 PDT
 Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
 2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
 2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
 2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
 2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
 2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
 2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
 2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
 2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
 2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
 2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
 2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
 2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
 2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

4. Selecione e copie o conteúdo da janela Exportar Relatório de Texto.

Esses dados agora podem ser colados em um documento de terceiros, como uma planilha.

Monitore o desempenho de PUT e GET

Você pode monitorar o desempenho de determinadas operações, como armazenamento e recuperação de objetos, para ajudar a identificar alterações que podem exigir investigação adicional.

Sobre esta tarefa

Para monitorar o desempenho de PUT e GET, você pode executar comandos S3 diretamente de uma estação de trabalho ou usando o aplicativo S3tester de código aberto. O uso desses métodos permite avaliar o desempenho independentemente de fatores externos ao StorageGRID, como problemas com um aplicativo cliente ou problemas com uma rede externa.

Ao executar testes de operações PUT e GET, use as seguintes diretrizes:

- Use tamanhos de objetos comparáveis aos objetos que você normalmente ingere em sua grade.
- Execute operações em sites locais e remotos.

Mensagens no ["registro de auditoria"](#) indicar o tempo total necessário para executar determinadas operações. Por exemplo, para determinar o tempo total de processamento de uma solicitação S3 GET, você pode revisar o valor do atributo TIME na mensagem de auditoria SGET. Você também pode encontrar o atributo TIME nas mensagens de auditoria para as seguintes operações do S3: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Ao analisar os resultados, observe o tempo médio necessário para atender a uma solicitação, bem como o rendimento geral que você pode atingir. Repita os mesmos testes regularmente e registre os resultados para que você possa identificar tendências que possam exigir investigação.

- Você pode "[baixe o S3tester do github](#)".

Monitorar operações de verificação de objetos

O sistema StorageGRID pode verificar a integridade dos dados de objetos nos nós de armazenamento, verificando se há objetos corrompidos e ausentes.

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](#)".

Sobre esta tarefa

Dois "[processos de verificação](#)" trabalhar em conjunto para garantir a integridade dos dados:

- **A verificação de antecedentes** é executada automaticamente, verificando continuamente a exatidão dos dados do objeto.

A verificação em segundo plano verifica automática e continuamente todos os nós de armazenamento para determinar se há cópias corrompidas de dados de objetos replicados e codificados para eliminação. Se forem encontrados problemas, o sistema StorageGRID tenta automaticamente substituir os dados do objeto corrompidos de cópias armazenadas em outro lugar no sistema. A verificação em segundo plano não é executada em objetos em um pool de armazenamento em nuvem.



O alerta **Objeto corrompido não identificado detectado** é acionado se o sistema detectar um objeto corrompido que não pode ser corrigido automaticamente.

- **A verificação de existência de objetos** pode ser acionada por um usuário para verificar mais rapidamente a existência (mas não a exatidão) dos dados do objeto.

A verificação de existência de objetos verifica se todas as cópias replicadas esperadas de objetos e fragmentos codificados para eliminação existem em um nó de armazenamento. A verificação de existência de objetos fornece uma maneira de verificar a integridade dos dispositivos de armazenamento, especialmente se um problema recente de hardware pode ter afetado a integridade dos dados.

Você deve revisar os resultados das verificações de antecedentes e verificações de existência de objetos regularmente. Investigue imediatamente quaisquer instâncias de dados de objetos corrompidos ou ausentes para determinar a causa raiz.

Passos

1. Revise os resultados das verificações de antecedentes:
 - a. Selecione **NÓS > Nó de Armazenamento > Objetos**.
 - b. Confira os resultados da verificação:
 - Para verificar a verificação de dados de objetos replicados, observe os atributos na seção Verificação.

Verification		
Status: ?	No errors	
Percent complete: ?	0.00%	
Average stat time: ?	0.00 microseconds	
Objects verified: ?	0	
Object verification rate: ?	0.00 objects / second	
Data verified: ?	0 bytes	
Data verification rate: ?	0.00 bytes / second	
Missing objects: ?	0	
Corrupt objects: ?	0	
Corrupt objects unidentified: ?	0	
Quarantined objects: ?	0	

- Para verificar a verificação de fragmentos codificados por eliminação, selecione **Storage Node > ILM** e observe os atributos na seção Verificação de codificação de eliminação.

Erasure coding verification		
Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Selecione o ponto de interrogação (?) ao lado do nome de um atributo para exibir o texto de ajuda.

- Revise os resultados dos trabalhos de verificação de existência de objetos:
 - Selecione **MANUTENÇÃO > Verificação de existência do objeto > Histórico de tarefas**.
 - Examine a coluna Cópias de objetos ausentes detectadas. Se algum trabalho resultou em 100 ou mais cópias de objetos ausentes e o alerta **Objetos perdidos** foi acionado, entre em contato com o suporte técnico.

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify that objects defined by your ILM policy, still exist on the volumes.

Active job

Job history

Delete

Search...

☐

Job ID ?

Status ?

Nodes (volumes) ?

Missing object copies detected ?

☐

15816859223101303015

Completed

DC2-S1 (3 volumes)

0

☐

12538643155010477372

Completed

DC1-S3 (1 volume)

0

☐

5490044849774982476

Completed

DC1-S2 (1 volume)

0

☐

3395284277055907678

Completed

DC1-S1 (3 volumes)
DC1-S2 (3 volumes)
DC1-S3 (3 volumes)
and 7 more

0

Monitorar eventos

Você pode monitorar eventos detectados por um nó de grade, incluindo eventos personalizados que você criou para rastrear eventos registrados no servidor syslog. A mensagem Último Evento exibida no Grid Manager fornece mais informações sobre o evento mais recente.

As mensagens de eventos também são listadas no `/var/local/log/bycast-err.log` arquivo de log. Veja o "[Referência de arquivos de log](#)".

O alarme SMTT (Total de eventos) pode ser disparado repetidamente por problemas como problemas de rede, quedas de energia ou atualizações. Esta seção contém informações sobre como investigar eventos para que você possa entender melhor por que esses alarmes ocorreram. Se um evento ocorreu devido a um problema conhecido, é seguro redefinir os contadores de eventos.

Passos

- Revise os eventos do sistema para cada nó da grade:
 - Selecione **SUPORTE > Ferramentas > Topologia de grade**.
 - Selecione **site > grid node > SSM > Eventos > Visão geral > Principal**.
- Gere uma lista de mensagens de eventos anteriores para ajudar a isolar problemas que ocorreram no passado:

- Selecione **SUPORTE > Ferramentas > Topologia de grade.**
- Selecione **site > grid node > SSM > Eventos > Relatórios.**
- Selecione **Texto.**

O atributo **Último Evento** não é mostrado no "visualização de gráficos". Para visualizá-lo:

- Altere **Atributo** para **Último Evento**.
- Opcionalmente, selecione um período de tempo para **Consulta rápida.**
- Selecione **Atualizar.**

Time Received	Sample Time	Value
2009-04-15 15:24:22	2009-04-15 15:24:22	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }
2009-04-15 15:24:11	2009-04-15 15:23:39	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }

Criar eventos syslog personalizados

Eventos personalizados permitem que você rastreie todos os eventos de kernel, daemon, erro e nível crítico do usuário registrados no servidor syslog. Um evento personalizado pode ser útil para monitorar a ocorrência de mensagens de log do sistema (e, portanto, eventos de segurança de rede e falhas de hardware).

Sobre esta tarefa

Considere criar eventos personalizados para monitorar problemas recorrentes. As considerações a seguir se aplicam a eventos personalizados.

- Depois que um evento personalizado é criado, cada ocorrência dele é monitorada.
- Para criar um evento personalizado com base em palavras-chave no `/var/local/log/messages` arquivos, os logs nesses arquivos devem ser:
 - Gerado pelo kernel
 - Gerado pelo daemon ou programa do usuário no nível de erro ou crítico

Nota: Nem todas as entradas no `/var/local/log/messages` os arquivos serão correspondidos, a menos que satisfaçam os requisitos declarados acima.

Passos

- Selecione **SUPORTE > Alarmes (antigo) > Eventos personalizados.**
- Clique em *Editar* (ou *Inserir* se este não for o primeiro evento).

3. Insira uma sequência de eventos personalizada, por exemplo, desligamento

Events
Updated: 2021-10-22 11:15:34 MDT

Custom Events (1 - 1 of 1)

Event	Actions
shutdown	

Show 10 Records Per Page Refresh Previous 1 Next

Apply Changes

4. Selecione **Aplicar alterações**.

5. Selecione **SUPORTE > Ferramentas > Topologia de grade**.

6. Selecione **grid node > SSM > Eventos**.

7. Localize a entrada para Eventos personalizados na tabela Eventos e monitore o valor para **Contagem**.

Se a contagem aumentar, um evento personalizado que você está monitorando será acionado naquele nó da grade.

Overview
Alarms
Reports
Configuration

Main



Overview: SSM (DC1-ADM1) - Events
Updated: 2021-10-22 11:19:18 MDT

System Events

Log Monitor State: Connected
Total Events: 0
Last Event: No Events

Description	Count
Abnormal Software Events	0
Account Service Events	0
Cassandra Errors	0
Cassandra Heap Out Of Memory Errors	0
Chunk Service Events	0
Custom Events	0
Data-Mover Service Events	0
File System Errors	0
Forced Termination Events	0
Grid Node Errors	0
Hotfix Installation Failure Events	0
I/O Errors	0
IDE Errors	0
Identity Service Events	0
Kernel Errors	0
Kernel Memory Allocation Failure	0
Keystone Service Events	0
Network Receive Errors	0
Network Transmit Errors	0
Out Of Memory Errors	0
Replicated State Machine Service Events	0
SCSI Errors	0

Redefina a contagem de eventos personalizados para zero

Se você quiser zerar o contador apenas para eventos personalizados, use a página Topologia de grade no menu Suporte.

Redefinir um contador faz com que o alarme seja disparado pelo próximo evento. Por outro lado, quando você reconhece um alarme, ele só é disparado novamente se o próximo nível limite for atingido.

Passos

1. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
2. Selecione **grid node > SSM > Eventos > Configuração > Principal**.
3. Selecione a caixa de seleção **Redefinir** para Eventos personalizados.

Overview

Alarms

Reports

Configuration

Main

Alarms



Configuration: SSM (DC2-ADM1) - Events

Updated: 2018-04-11 10:35:44 MDT

Description	Count	Reset
Abnormal Software Events	0	☐
Account Service Events	0	☐
Cassandra Errors	0	☐
Cassandra Heap Out Of Memory Errors	0	☐
Custom Events	0	☒
File System Errors	0	☐
Forced Termination Events	0	☐

4. Selecione **Aplicar alterações**.

Revisar mensagens de auditoria

As mensagens de auditoria podem ajudar você a entender melhor as operações detalhadas do seu sistema StorageGRID . Você pode usar logs de auditoria para solucionar problemas e avaliar o desempenho.

Durante a operação normal do sistema, todos os serviços do StorageGRID geram mensagens de auditoria, como a seguir:

- As mensagens de auditoria do sistema estão relacionadas ao próprio sistema de auditoria, aos estados dos nós da grade, à atividade de tarefas em todo o sistema e às operações de backup de serviço.
- As mensagens de auditoria de armazenamento de objetos estão relacionadas ao armazenamento e gerenciamento de objetos no StorageGRID, incluindo armazenamento e recuperações de objetos, transferências de nó de grade para nó de grade e verificações.
- As mensagens de auditoria de leitura e gravação do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para criar, modificar ou recuperar um objeto.
- As mensagens de auditoria de gerenciamento registram solicitações do usuário para a API de gerenciamento.

Cada nó de administração armazena mensagens de auditoria em arquivos de texto. O compartilhamento de auditoria contém o arquivo ativo (audit.log), bem como logs de auditoria compactados de dias anteriores. Cada nó na grade também armazena uma cópia das informações de auditoria geradas no nó.

Você pode acessar arquivos de log de auditoria diretamente da linha de comando do nó de administração.

O StorageGRID pode enviar informações de auditoria por padrão, ou você pode alterar o destino:

- O StorageGRID assume como padrão os destinos de auditoria de nós locais.
- As entradas de log de auditoria do Grid Manager e do Tenant Manager podem ser enviadas para um nó de

armazenamento.

- Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado.
- ["Saiba mais sobre como configurar mensagens de auditoria e destinos de log"](#) .

Para obter detalhes sobre o arquivo de log de auditoria, o formato das mensagens de auditoria, os tipos de mensagens de auditoria e as ferramentas disponíveis para analisar mensagens de auditoria, consulte ["Revisar logs de auditoria"](#) .

Coletar arquivos de log e dados do sistema

Você pode usar o Grid Manager para recuperar arquivos de log e dados do sistema (incluindo dados de configuração) para seu sistema StorageGRID .

Antes de começar

- Você deve estar conectado ao Grid Manager no nó de administração primário usando um ["navegador da web compatível"](#) .
- Você tem ["permissões de acesso específicas"](#) .
- Você deve ter a senha de provisionamento.

Sobre esta tarefa

Você pode usar o Grid Manager para reunir ["arquivos de log"](#) , dados do sistema e dados de configuração de qualquer nó de grade para o período de tempo selecionado. Os dados são coletados e arquivados em um arquivo .tar.gz que você pode baixar para seu computador local.

Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado. Ver ["Configurar mensagens de auditoria e destinos de log"](#) .

Passos

1. Selecione **SUPORTE > Ferramentas > Registros**.

2. Selecione os nós da grade para os quais você deseja coletar arquivos de log.

Conforme necessário, você pode coletar arquivos de log para toda a grade ou para um site de data center inteiro.

3. Selecione uma **Hora de início** e uma **Hora de término** para definir o intervalo de tempo dos dados a serem incluídos nos arquivos de log.

Se você selecionar um período de tempo muito longo ou coletar logs de todos os nós em uma grade grande, o arquivo de log poderá ficar muito grande para ser armazenado em um nó ou muito grande para ser coletado no nó de administração principal para download. Se isso ocorrer, você deverá reiniciar a coleta de logs com um conjunto menor de dados.

4. Selecione os tipos de logs que você deseja coletar.

- **Logs de aplicativos:** logs específicos do aplicativo que o suporte técnico usa com mais frequência para solução de problemas. Os logs coletados são um subconjunto dos logs de aplicativos disponíveis.
- **Registros de auditoria:** Registros contendo as mensagens de auditoria geradas durante a operação normal do sistema.
- **Rastreamento de rede:** Logs usados para depuração de rede.
- **Banco de dados Prometheus:** métricas de séries temporais dos serviços em todos os nós.

5. Opcionalmente, insira notas sobre os arquivos de log que você está coletando na caixa de texto **Notas**.

Você pode usar essas notas para fornecer informações de suporte técnico sobre o problema que o levou a coletar os arquivos de log. Suas notas são adicionadas a um arquivo chamado `info.txt`, juntamente com outras informações sobre a coleção de arquivos de log. O `info.txt` o arquivo é salvo no pacote de

arquivo de log.

6. Digite a senha de provisionamento do seu sistema StorageGRID na caixa de texto **Senha de provisionamento**.
7. Selecione **Coletar Logs**.

Quando você envia uma nova solicitação, a coleção anterior de arquivos de log é excluída.

Você pode usar a página Logs para monitorar o progresso da coleta de arquivos de log para cada nó da grade.

Se você receber uma mensagem de erro sobre o tamanho do log, tente coletar logs por um período de tempo mais curto ou para menos nós.

8. Selecione **Download** quando a coleta do arquivo de log estiver concluída.

O arquivo `.tar.gz` contém todos os arquivos de log de todos os nós da grade onde a coleta de log foi bem-sucedida. Dentro do arquivo combinado `.tar.gz`, há um arquivo de log para cada nó da grade.

Depois que você terminar

Você pode baixar novamente o pacote de arquivo de log mais tarde, se necessário.

Opcionalmente, você pode selecionar **Excluir** para remover o pacote de arquivamento do arquivo de log e liberar espaço em disco. O pacote de arquivo de log atual será removido automaticamente na próxima vez que você coletar arquivos de log.

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.



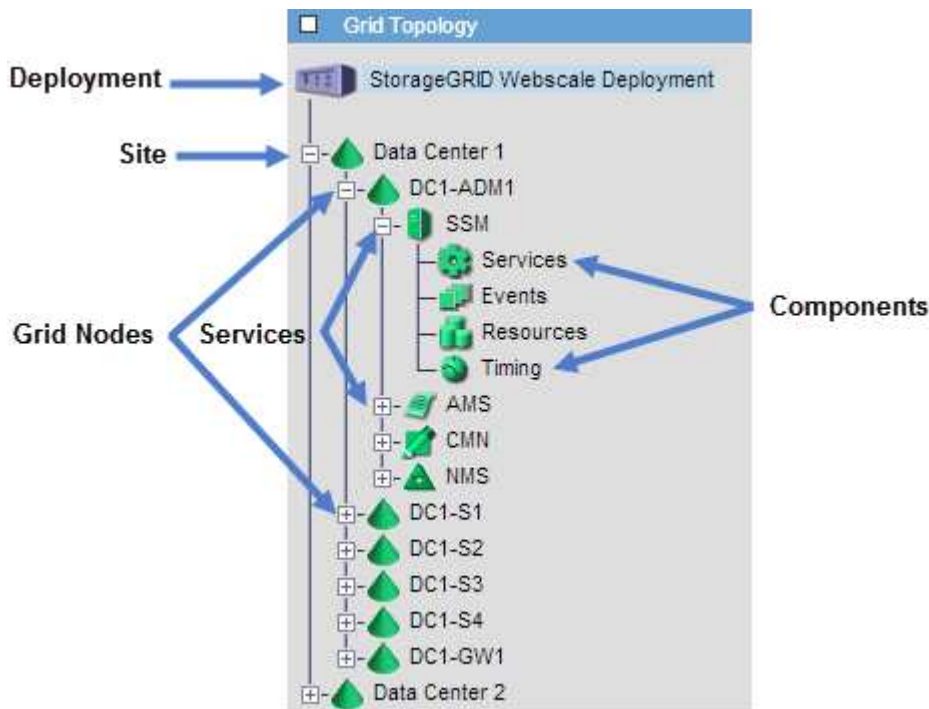
Após enviar um pacote de AutoSupport acionado pelo usuário, atualize a página de AutoSupport no seu navegador após 1 minuto para acessar os resultados mais recentes.

Visualizar a árvore de topologia da grade

A árvore de topologia de grade fornece acesso a informações detalhadas sobre os elementos do sistema StorageGRID , incluindo sites, nós de grade, serviços e

componentes. Na maioria dos casos, você só precisa acessar a árvore de topologia de grade quando instruído na documentação ou ao trabalhar com o suporte técnico.

Para acessar a árvore Topologia de grade, selecione **SUPORTE > Ferramentas > Topologia de grade**.



Para expandir ou recolher a árvore de topologia de grade, clique em **+** ou **-** no nível do site, nó ou serviço. Para expandir ou recolher todos os itens em todo o site ou em cada nó, mantenha pressionada a tecla **<Ctrl>** e clique.

Atributos StorageGRID

Os atributos relatam valores e status para muitas das funções do sistema StorageGRID . Os valores de atributo estão disponíveis para cada nó da grade, cada site e toda a grade.

Os atributos StorageGRID são usados em vários lugares no Grid Manager:

- **Página Nós:** Muitos dos valores mostrados na página Nós são atributos do StorageGRID . (As métricas do Prometheus também são mostradas nas páginas de nós.)
- **Árvore de topologia de grade:** os valores dos atributos são mostrados na árvore de topologia de grade (**SUPORTE > Ferramentas > Topologia de grade**).
- **Eventos:** Eventos do sistema ocorrem quando determinados atributos registram um erro ou condição de falha para um nó, incluindo erros como erros de rede.

Valores de atributos

Os atributos são relatados com base no melhor esforço e estão aproximadamente corretos. As atualizações de atributos podem ser perdidas em algumas circunstâncias, como a falha de um serviço ou a falha e reconstrução de um nó de grade.

Além disso, atrasos de propagação podem retardar o relato de atributos. Os valores atualizados para a maioria dos atributos são enviados ao sistema StorageGRID em intervalos fixos. Pode levar vários minutos até que uma atualização fique visível no sistema, e dois atributos que mudam mais ou menos

simultaneamente podem ser relatados em momentos ligeiramente diferentes.

Revisar métricas de suporte

Ao solucionar um problema, você pode trabalhar com o suporte técnico para revisar métricas e gráficos detalhados do seu sistema StorageGRID .

Antes de começar

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

Sobre esta tarefa

A página Métricas permite que você acesse as interfaces de usuário do Prometheus e do Grafana. Prometheus é um software de código aberto para coleta de métricas. Grafana é um software de código aberto para visualização de métricas.



As ferramentas disponíveis na página Métricas são destinadas ao uso do suporte técnico. Alguns recursos e itens de menu dessas ferramentas são intencionalmente não funcionais e estão sujeitos a alterações. Veja a lista de ["métricas Prometheus comumente usadas"](#) .

Passos

1. Conforme instruído pelo suporte técnico, selecione **SUORTE > Ferramentas > Métricas**.

Um exemplo da página Métricas é mostrado aqui:

Metrics

Access charts and metrics to help troubleshoot issues.

 The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- [https://\[redacted\]](https://[redacted])

Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	EC Overview	Replicated Read Path Overview
Account Service Overview	Grid	S3 - Node
Alertmanager	ILM	S3 Overview
Audit Overview	Identity Service Overview	S3 Select
Cassandra Cluster Overview	Ingests	Site
Cassandra Network Overview	Node	Support
Cassandra Node Overview	Node (Internal Use)	Traces
Cross Grid Replication	OSL - AsyncIO	Traffic Classification Policy
Cloud Storage Pool Overview	Platform Services Commits	Usage Processing
EC - ADE	Platform Services Overview	Virtual Memory (vmstat)
EC - Chunk Service	Platform Services Processing	

2. Para consultar os valores atuais das métricas do StorageGRID e visualizar gráficos dos valores ao longo do tempo, clique no link na seção Prometheus.

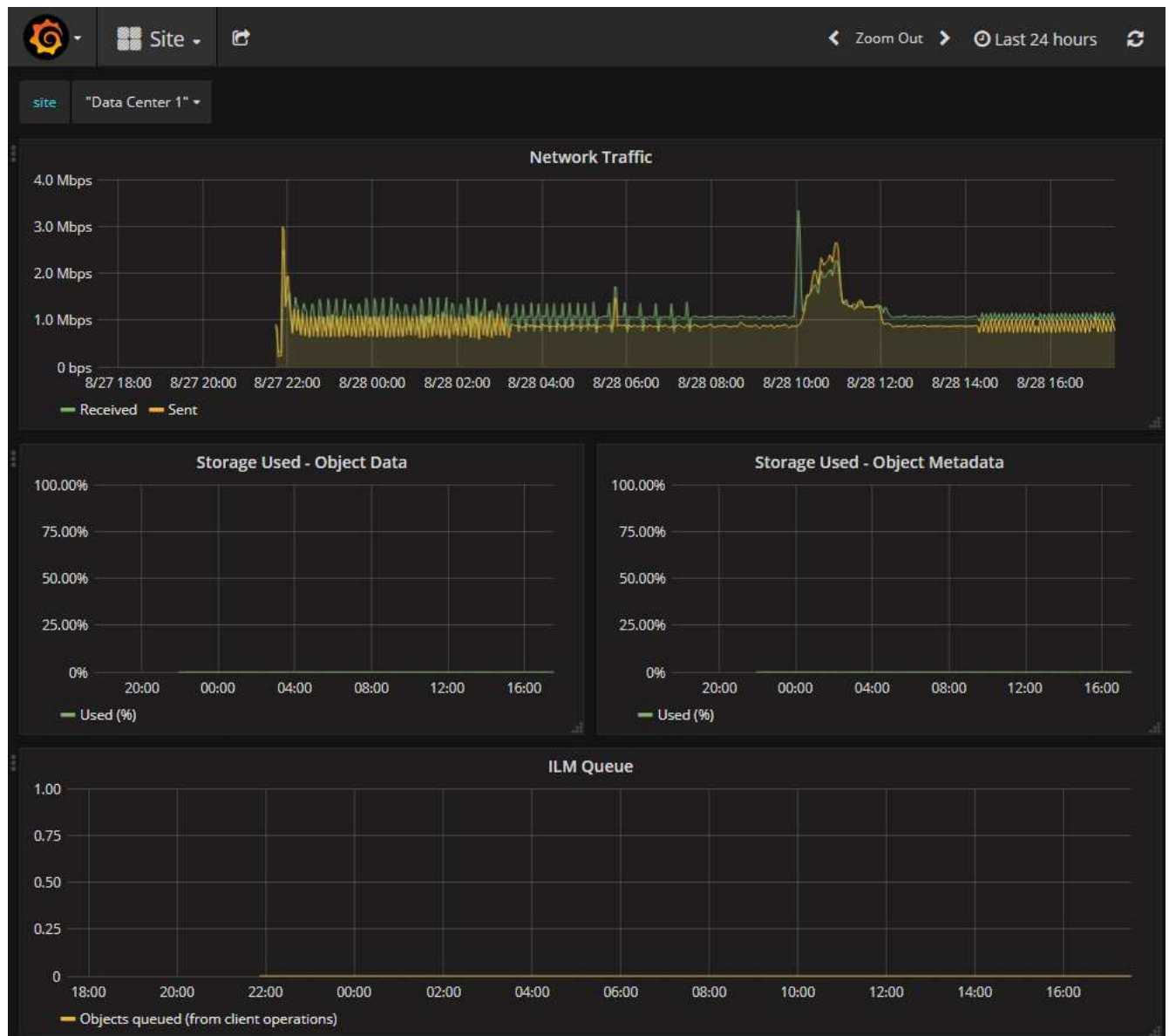
A interface do Prometheus é exibida. Você pode usar esta interface para executar consultas nas métricas do StorageGRID disponíveis e criar gráficos das métricas do StorageGRID ao longo do tempo.



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

3. Para acessar painéis pré-construídos contendo gráficos de métricas do StorageGRID ao longo do tempo, clique nos links na seção Grafana.

A interface do Grafana para o link selecionado é exibida.



Executar diagnósticos

Ao solucionar um problema, você pode trabalhar com o suporte técnico para executar diagnósticos no seu sistema StorageGRID e revisar os resultados.

- ["Revisar métricas de suporte"](#)
- ["Métricas do Prometheus comumente usadas"](#)

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 página Diagnóstico executa um conjunto de verificações de diagnóstico no estado atual da grade. Cada verificação de diagnóstico pode ter um dos três status:

-

✓ **Normal:** Todos os valores estão dentro da faixa normal.

• ⚠ **Atenção:** Um ou mais valores estão fora da faixa normal.

• ✖ **Cuidado:** Um ou mais valores estão significativamente fora da faixa normal.

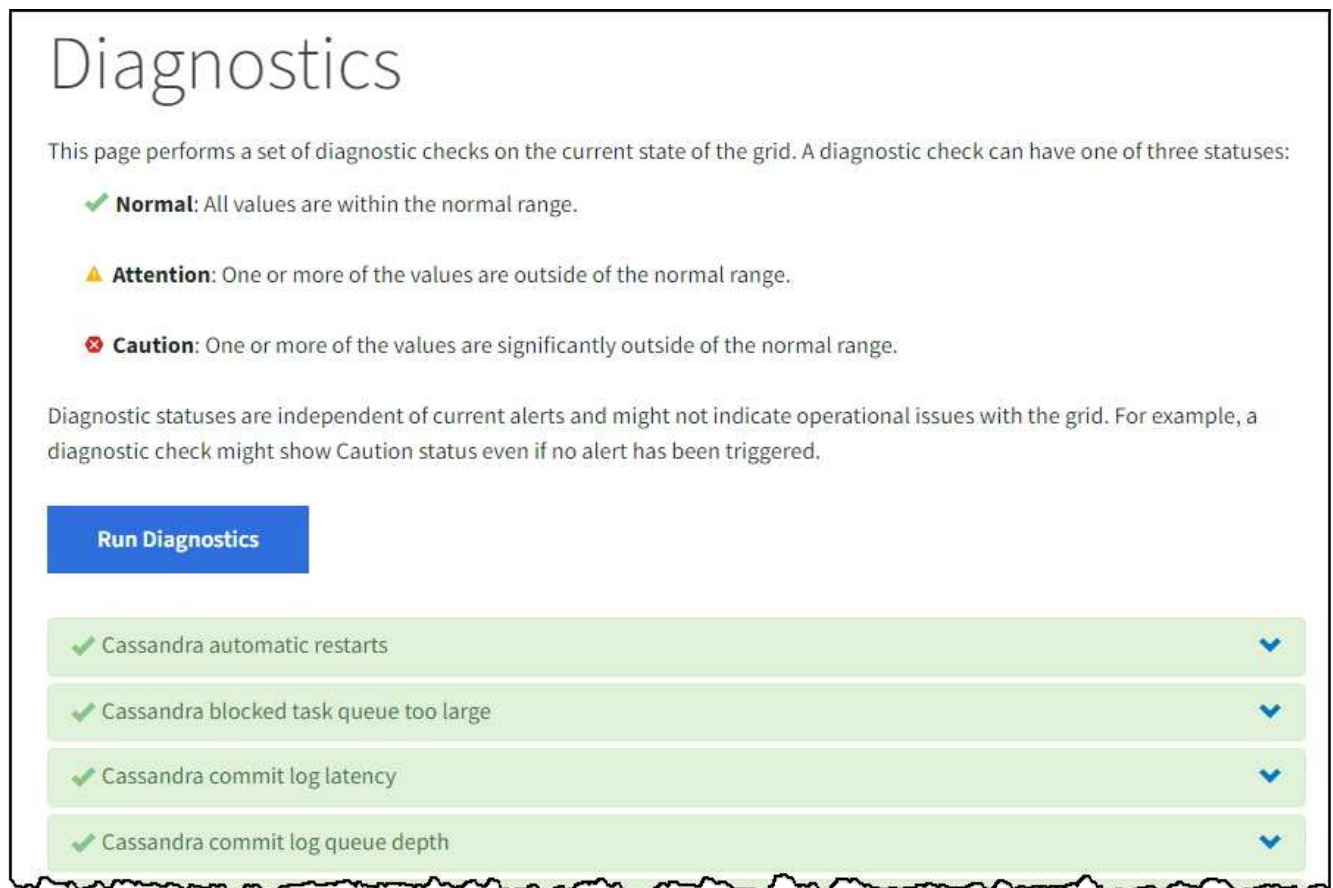
Os status de diagnóstico são independentes dos alertas atuais e podem não indicar problemas operacionais com a rede. Por exemplo, uma verificação de diagnóstico pode mostrar o status Cuidado mesmo que nenhum alerta tenha sido disparado.

Passos

1. Selecione **SUPORTE > Ferramentas > Diagnóstico**.

A página Diagnóstico é exibida e lista os resultados de cada verificação de diagnóstico. Os resultados são classificados por gravidade (Cuidado, Atenção e Normal). Dentro de cada gravidade, os resultados são classificados em ordem alfabética.

Neste exemplo, todos os diagnósticos têm status Normal.



Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

- ✓ **Normal:** All values are within the normal range.
- ⚠ **Attention:** One or more of the values are outside of the normal range.
- ✖ **Caution:** One or more of the values are significantly outside of the normal range.

Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.

Run Diagnostics

- ✓ Cassandra automatic restarts
- ✓ Cassandra blocked task queue too large
- ✓ Cassandra commit log latency
- ✓ Cassandra commit log queue depth

2. Para saber mais sobre um diagnóstico específico, clique em qualquer lugar da linha.

Detalhes sobre o diagnóstico e seus resultados atuais aparecem. Os seguintes detalhes estão listados:

- **Status:** O status atual deste diagnóstico: Normal, Atenção ou Cuidado.
- **Consulta Prometheus:** Se usada para diagnóstico, a expressão Prometheus que foi usada para gerar os valores de status. (Uma expressão Prometheus não é usada para todos os diagnósticos.)

- **Limites:** Se disponíveis para o diagnóstico, os limites definidos pelo sistema para cada status de diagnóstico anormal. (Os valores limite não são usados para todos os diagnósticos.)



Você não pode alterar esses limites.

- **Valores de status:** Uma tabela que mostra o status e o valor do diagnóstico em todo o sistema StorageGRID . Neste exemplo, é mostrada a utilização atual da CPU para cada nó em um sistema StorageGRID . Todos os valores dos nós estão abaixo dos limites de Atenção e Cuidado, portanto, o status geral do diagnóstico é Normal.

CPU utilization

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the [Node Grafana dashboard](#).

Status Normal

Prometheus query `sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))`

[View in Prometheus](#)

Thresholds

- Attention $\geq 75\%$
- Caution $\geq 95\%$

Status	Instance	CPU Utilization
	DC1-ADM1	2.598%
	DC1-ARC1	0.937%
	DC1-G1	2.119%
	DC1-S1	8.708%
	DC1-S2	8.142%
	DC1-S3	9.669%
	DC2-ADM1	2.515%
	DC2-ARC1	1.152%
	DC2-S1	8.204%
	DC2-S2	5.000%
	DC2-S3	10.469%

3. **Opcional:** Para ver gráficos do Grafana relacionados a este diagnóstico, clique no link **Painel do Grafana**.

Este link não é exibido para todos os diagnósticos.

O painel relacionado do Grafana aparece. Neste exemplo, o painel do nó aparece mostrando a utilização da CPU ao longo do tempo para este nó, bem como outros gráficos do Grafana para o nó.



Você também pode acessar os painéis pré-construídos do Grafana na seção Grafana da página **SUPORTE > Ferramentas > Métricas**.



4. **Opcional:** Para ver um gráfico da expressão do Prometheus ao longo do tempo, clique em **Exibir no Prometheus**.

Aparece um gráfico do Prometheus da expressão usada no diagnóstico.

☐ Enable query history

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode))
```

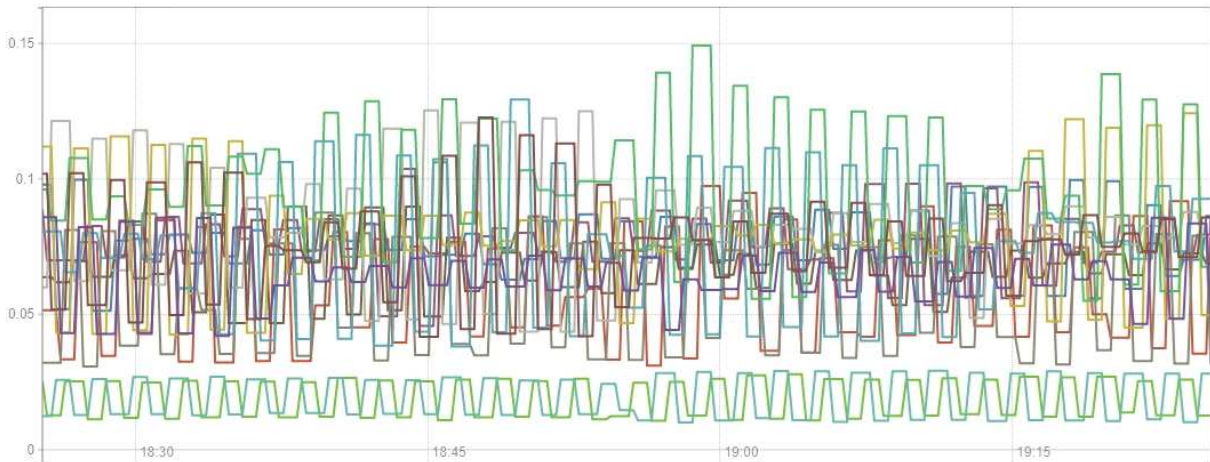
Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

- insert metric at cursor - ▾

Graph Console

- 1h + ⏪ Until ⏩ Res. (s) ☐ stacked



- ✓ {instance="DC3-S3"}
- ✓ {instance="DC3-S2"}
- ✓ {instance="DC3-S1"}
- ✓ {instance="DC2-S3"}
- ✓ {instance="DC2-S2"}
- ✓ {instance="DC2-S1"}
- ✓ {instance="DC2-ADM1"}
- ✓ {instance="DC1-S3"}
- ✓ {instance="DC1-S2"}
- ✓ {instance="DC1-S1"}
- ✓ {instance="DC1-G1"}
- ✓ {instance="DC1-ARC1"}
- ✓ {instance="DC1-ADM1"}

Remove Graph

Add Graph

Crie aplicativos de monitoramento personalizados

Você pode criar aplicativos de monitoramento e painéis personalizados usando as métricas do StorageGRID disponíveis na API de gerenciamento de grade.

Se você quiser monitorar métricas que não são exibidas em uma página existente do Grid Manager ou se quiser criar painéis personalizados para o StorageGRID, poderá usar a API de gerenciamento de grade para consultar as métricas do StorageGRID .

Você também pode acessar as métricas do Prometheus diretamente com uma ferramenta de monitoramento externa, como o Grafana. O uso de uma ferramenta externa exige que você carregue ou gere um certificado de cliente administrativo para permitir que o StorageGRID autentique a ferramenta para segurança. Veja o ["instruções para administrar o StorageGRID"](#) .

Para visualizar as operações da API de métricas, incluindo a lista completa das métricas disponíveis, acesse o Grid Manager. No topo da página, selecione o ícone de ajuda e selecione **Documentação da API > métricas** .

GET

`/grid/metric-labels/{label}/values` Lists the values for a metric label

GET

`/grid/metric-names` Lists all available metric names

GET

`/grid/metric-query` Performs an instant metric query at a single point in time

GET

`/grid/metric-query-range` Performs a metric query over a range of time

Os detalhes de como implementar um aplicativo de monitoramento personalizado estão além do escopo desta documentação.

Solucionar problemas do sistema StorageGRID

Solucionar problemas de um sistema StorageGRID

Se você encontrar um problema ao usar um sistema StorageGRID, consulte as dicas e diretrizes nesta seção para obter ajuda para determinar e resolver o problema.

Muitas vezes, você pode resolver problemas sozinho; no entanto, pode ser necessário encaminhar alguns problemas ao suporte técnico.

Defina o problema

O primeiro passo para resolver um problema é defini-lo claramente.

Esta tabela fornece exemplos dos tipos de informações que você pode coletar para definir um problema:

Pergunta	Exemplo de resposta
O que o sistema StorageGRID está fazendo ou não fazendo? Quais são os sintomas?	Os aplicativos clientes estão relatando que objetos não podem ser ingeridos no StorageGRID.
Quando o problema começou?	A ingestão de objetos foi negada pela primeira vez por volta das 14h50 do dia 8 de janeiro de 2020.
Como você percebeu o problema pela primeira vez?	Notificado pelo aplicativo do cliente. Também recebi notificações de alerta por e-mail.
O problema acontece constantemente ou apenas às vezes?	O problema continua.
Se o problema acontece regularmente, quais etapas fazem com que ele ocorra?	O problema acontece sempre que um cliente tenta ingerir um objeto.

Pergunta	Exemplo de resposta
Se o problema acontece intermitentemente, quando ele ocorre? Registre os horários de cada incidente que você tiver conhecimento.	O problema não é intermitente.
Você já viu esse problema antes? Com que frequência você teve esse problema no passado?	Esta é a primeira vez que vejo esse problema.

Avaliar o risco e o impacto no sistema

Depois de definir o problema, avalie seu risco e impacto no sistema StorageGRID . Por exemplo, a presença de alertas críticos não significa necessariamente que o sistema não esteja prestando serviços essenciais.

Esta tabela resume o impacto que o problema de exemplo está tendo nas operações do sistema:

Pergunta	Exemplo de resposta
O sistema StorageGRID pode ingerir conteúdo?	Não.
Os aplicativos clientes podem recuperar conteúdo?	Alguns objetos podem ser recuperados e outros não.
Os dados estão em risco?	Não.
A capacidade de conduzir negócios é severamente afetada?	Sim, porque os aplicativos clientes não podem armazenar objetos no sistema StorageGRID e os dados não podem ser recuperados de forma consistente.

Coletar dados

Depois de definir o problema e avaliar seu risco e impacto, colete dados para análise. O tipo de dado mais útil para coletar depende da natureza do problema.

Tipo de dados a coletar	Por que coletar esses dados	Instruções
Criar cronograma de mudanças recentes	Alterações no seu sistema StorageGRID , sua configuração ou seu ambiente podem causar novos comportamentos.	Crie uma linha do tempo das mudanças recentes

Tipo de dados a coletar	Por que coletar esses dados	Instruções
Alertas de revisão	Os alertas podem ajudar você a determinar rapidamente a causa raiz de um problema, fornecendo pistas importantes sobre os problemas subjacentes que podem estar causando isso. Revise a lista de alertas atuais para ver se o StorageGRID identificou a causa raiz de um problema para você. Revise os alertas acionados no passado para obter insights adicionais.	• "Ver alertas atuais e resolvidos"
Monitorar eventos	Eventos incluem qualquer erro de sistema ou eventos de falha para um nó, incluindo erros como erros de rede. Monitore eventos para saber mais sobre problemas ou para ajudar na solução de problemas.	• "Monitorar eventos"
Identifique tendências usando gráficos e relatórios de texto	As tendências podem fornecer pistas valiosas sobre quando os problemas surgiram pela primeira vez e podem ajudar você a entender a rapidez com que as coisas estão mudando.	• "Use tabelas e gráficos" • "Usar relatórios de texto"
Estabelecer linhas de base	Colete informações sobre os níveis normais de vários valores operacionais. Esses valores de base e desvios dessas linhas de base podem fornecer pistas valiosas.	• Estabelecer linhas de base
Realizar testes de ingestão e recuperação	Para solucionar problemas de desempenho com ingestão e recuperação, use uma estação de trabalho para armazenar e recuperar objetos. Compare os resultados com aqueles vistos ao usar o aplicativo cliente.	• "Monitore o desempenho de PUT e GET"
Revisar mensagens de auditoria	Revise as mensagens de auditoria para acompanhar as operações do StorageGRID em detalhes. Os detalhes nas mensagens de auditoria podem ser úteis para solucionar muitos tipos de problemas, incluindo problemas de desempenho.	• "Revisar mensagens de auditoria"
Verifique a localização dos objetos e a integridade do armazenamento	Se você estiver tendo problemas de armazenamento, verifique se os objetos estão sendo colocados onde você espera. Verifique a integridade dos dados do objeto em um nó de armazenamento.	• "Monitorar operações de verificação de objetos" • "Confirmar a localização dos dados do objeto" • "Verificar integridade do objeto"

Tipo de dados a coletar	Por que coletar esses dados	Instruções
Coletar dados para suporte técnico	O suporte técnico pode solicitar que você colete dados ou revise informações específicas para ajudar a solucionar problemas.	• "Coletar arquivos de log e dados do sistema" • "Acionar manualmente um pacote AutoSupport" • "Revisar métricas de suporte"

Criar uma linha do tempo das mudanças recentes

Quando ocorre um problema, você deve considerar o que mudou recentemente e quando essas mudanças ocorreram.

- Alterações no seu sistema StorageGRID , sua configuração ou seu ambiente podem causar novos comportamentos.
- Um cronograma de mudanças pode ajudar você a identificar quais mudanças podem ser responsáveis por um problema e como cada mudança pode ter afetado seu desenvolvimento.

Crie uma tabela de alterações recentes no seu sistema que inclua informações sobre quando cada alteração ocorreu e quaisquer detalhes relevantes sobre a alteração, como informações sobre o que mais estava acontecendo enquanto a alteração estava em andamento:

Tempo de mudança	Tipo de mudança	Detalhes
Por exemplo: • Quando você iniciou a recuperação do nó? • Quando a atualização do software foi concluída? • Você interrompeu o processo?	O que aconteceu? O que você fez?	Documente quaisquer detalhes relevantes sobre a mudança. Por exemplo: • Detalhes das alterações na rede. • Qual hotfix foi instalado. • Como as cargas de trabalho dos clientes mudaram. Não deixe de anotar se mais de uma alteração estava acontecendo ao mesmo tempo. Por exemplo, essa alteração foi feita enquanto uma atualização estava em andamento?

Exemplos de mudanças recentes significativas

Aqui estão alguns exemplos de mudanças potencialmente significativas:

- O sistema StorageGRID foi instalado, expandido ou recuperado recentemente?
- O sistema foi atualizado recentemente? Foi aplicado algum hotfix?
- Algum hardware foi reparado ou trocado recentemente?
- A política do ILM foi atualizada?

- A carga de trabalho do cliente mudou?
- O aplicativo cliente ou seu comportamento mudou?
- Você alterou os balanceadores de carga ou adicionou ou removeu um grupo de alta disponibilidade de nós de administração ou nós de gateway?
- Alguma tarefa foi iniciada e pode levar muito tempo para ser concluída? Exemplos incluem:
 - Recuperação de um nó de armazenamento com falha
 - Descomissionamento do nó de armazenamento
- Alguma alteração foi feita na autenticação do usuário, como adicionar um locatário ou alterar a configuração do LDAP?
- A migração de dados está ocorrendo?
- Os serviços da plataforma foram habilitados ou alterados recentemente?
- A conformidade foi ativada recentemente?
- Os pools de armazenamento em nuvem foram adicionados ou removidos?
- Alguma alteração foi feita na compactação ou criptografia do armazenamento?
- Houve alguma mudança na infraestrutura de rede? Por exemplo, VLANs, roteadores ou DNS.
- Alguma alteração foi feita nas fontes NTP?
- Foram feitas alterações nas interfaces de rede Grid, Admin ou Client Network?
- Alguma outra alteração foi feita no sistema StorageGRID ou em seu ambiente?

Estabelecer linhas de base

Você pode estabelecer linhas de base para seu sistema registrando os níveis normais de vários valores operacionais. No futuro, você poderá comparar os valores atuais com essas linhas de base para ajudar a detectar e resolver valores anormais.

Propriedade	Valor	Como obter
Consumo médio de armazenamento	GB consumidos/dia Porcentagem consumida/dia	Acesse o Gerenciador de Grade. Na página Nós, selecione a grade inteira ou um site e vá para a guia Armazenamento. No gráfico Armazenamento usado - Dados do objeto, encontre um período em que a linha seja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar quanto armazenamento é consumido a cada dia Você pode coletar essas informações para todo o sistema ou para um data center específico.

Propriedade	Valor	Como obter
Consumo médio de metadados	GB consumidos/dia Porcentagem consumida/dia	Acesse o Gerenciador de Grade. Na página Nós, selecione a grade inteira ou um site e vá para a guia Armazenamento. No gráfico Armazenamento usado - Metadados do objeto, encontre um período em que a linha seja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar quanto armazenamento de metadados é consumido a cada dia Você pode coletar essas informações para todo o sistema ou para um data center específico.
Taxa de operações S3/Swift	Operações/segundo	No painel do Grid Manager, selecione Desempenho > Operações S3 ou Desempenho > Operações Swift. Para ver as taxas e contagens de ingestão e recuperação de um site ou nó específico, selecione NÓS > site ou Nó de Armazenamento > Objetos. Posicione o cursor sobre o gráfico Ingestão e Recuperação do S3.
Operações S3/Swift com falha	Operações	Selecione SUPORTE > Ferramentas > Topologia de grade . Na guia Visão geral na seção Operações da API, visualize o valor para Operações do S3 - Falha ou Operações do Swift - Falha.
Taxa de avaliação do ILM	Objetos/segundo	Na página Nós, selecione grid > ILM. No gráfico de fila do ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de base para a Taxa de avaliação do seu sistema.
Taxa de varredura ILM	Objetos/segundo	Selecione NÓS > grade > ILM. No gráfico de fila do ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de base para Taxa de varredura para seu sistema.
Objetos enfileirados de operações do cliente	Objetos/segundo	Selecione NÓS > grade > ILM. No gráfico de fila do ILM, encontre um período em que a linha esteja razoavelmente estável. Posicione o cursor sobre o gráfico para estimar um valor de base para Objetos na fila (de operações do cliente) para seu sistema.

Propriedade	Valor	Como obter
Latência média de consulta	Milissegundos	Selecione NÓS > Nó de Armazenamento > Objetos . Na tabela Consultas, visualize o valor de Latência Média.

Analisar dados

Use as informações coletadas para determinar a causa do problema e possíveis soluções.

A análise depende do problema, mas em geral:

- Localize pontos de falha e gargalos usando os alertas.
- Reconstrua o histórico do problema usando o histórico de alertas e gráficos.
- Use gráficos para encontrar anomalias e comparar a situação problemática com a operação normal.

Lista de verificação de informações de escalonamento

Se você não conseguir resolver o problema sozinho, entre em contato com o suporte técnico. Antes de entrar em contato com o suporte técnico, reúna as informações listadas na tabela a seguir para facilitar a resolução do problema.

	Item	Notas
	Declaração do problema	Quais são os sintomas do problema? Quando o problema começou? Isso acontece de forma consistente ou intermitente? Se intermitentemente, em que horários isso ocorreu? Defina o problema
	Avaliação de impacto	Qual é a gravidade do problema? Qual é o impacto no aplicativo cliente? • O cliente já se conectou com sucesso antes? • O cliente pode ingerir, recuperar e excluir dados?
	ID do sistema StorageGRID	Selecione MANUTENÇÃO > Sistema > Licença . O ID do sistema StorageGRID é exibido como parte da licença atual.
	Versão do software	Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione Sobre para ver a versão do StorageGRID .

	Item	Notas
	Personalização	Resuma como seu sistema StorageGRID está configurado. Por exemplo, liste o seguinte: • A grade usa compactação de armazenamento, criptografia de armazenamento ou conformidade? • A ILM cria objetos replicados ou codificados para eliminação? O ILM garante redundância do site? As regras do ILM usam os comportamentos de ingestão Balanceado, Estrito ou Dual Commit?
	Arquivos de log e dados do sistema	Colete arquivos de log e dados do sistema para seu sistema. Selecione SUPORTE > Ferramentas > Registros. Você pode coletar logs para toda a grade ou para nós selecionados. Se você estiver coletando logs apenas para nós selecionados, certifique-se de incluir pelo menos um nó de armazenamento que tenha o serviço ADC. (Os três primeiros nós de armazenamento em um site incluem o serviço ADC.) "Coletar arquivos de log e dados do sistema"
	Informações de base	Colete informações básicas sobre operações de ingestão, operações de recuperação e consumo de armazenamento. Estabelecer linhas de base
	Linha do tempo das mudanças recentes	Crie uma linha do tempo que resuma quaisquer alterações recentes no sistema ou em seu ambiente. Crie uma linha do tempo das mudanças recentes
	Histórico de esforços para diagnosticar o problema	Se você tomou medidas para diagnosticar ou solucionar o problema sozinho, registre as etapas realizadas e o resultado.

Solucionar problemas de objetos e armazenamento

Confirmar a localização dos dados do objeto

Dependendo do problema, você pode querer ["confirmar onde os dados do objeto estão sendo armazenados"](#). Por exemplo, você pode querer verificar se a política do ILM está funcionando conforme o esperado e se os dados do objeto estão sendo armazenados onde pretendido.

Antes de começar

- Você deve ter um identificador de objeto, que pode ser um dos seguintes:

- **UUID:** Identificador Universalmente Único do objeto. Digite o UUID em letras maiúsculas.
- **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 do "[Interface S3](#)" , o aplicativo cliente usa uma combinação de chave de bucket e objeto para armazenar e identificar o objeto.

Passos

1. Selecione **ILM > Consulta de metadados do objeto**.
2. Digite o identificador do objeto no campo **Identificador**.

Você pode inserir um UUID, CBID, chave de objeto/bucket S3 ou nome de objeto/contêiner Swift.

3. Se você quiser consultar uma versão específica do objeto, insira o ID da versão (opcional).

4. Selecione **Procurar**.

O "[resultados da pesquisa de metadados do objeto](#)" aparecer. Esta página lista os seguintes tipos de informações:

- Metadados do sistema, incluindo o ID do objeto (UUID), o ID da versão (opcional), o nome do objeto, o nome do contêiner, 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, 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.

O exemplo a seguir mostra os resultados da pesquisa de metadados de objeto para um objeto de teste S3 armazenado como duas cópias replicadas.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAW": "2",

```

Falhas de armazenamento de objetos (volume de armazenamento)

O armazenamento subjacente em um nó de armazenamento é dividido em armazenamentos de objetos. Os armazenamentos de objetos também são conhecidos como volumes de armazenamento.

Você pode visualizar informações de armazenamento de objetos para cada nó de armazenamento. Os armazenamentos de objetos são mostrados na parte inferior da página **NODES > Storage Node > Storage**.

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
sdC(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

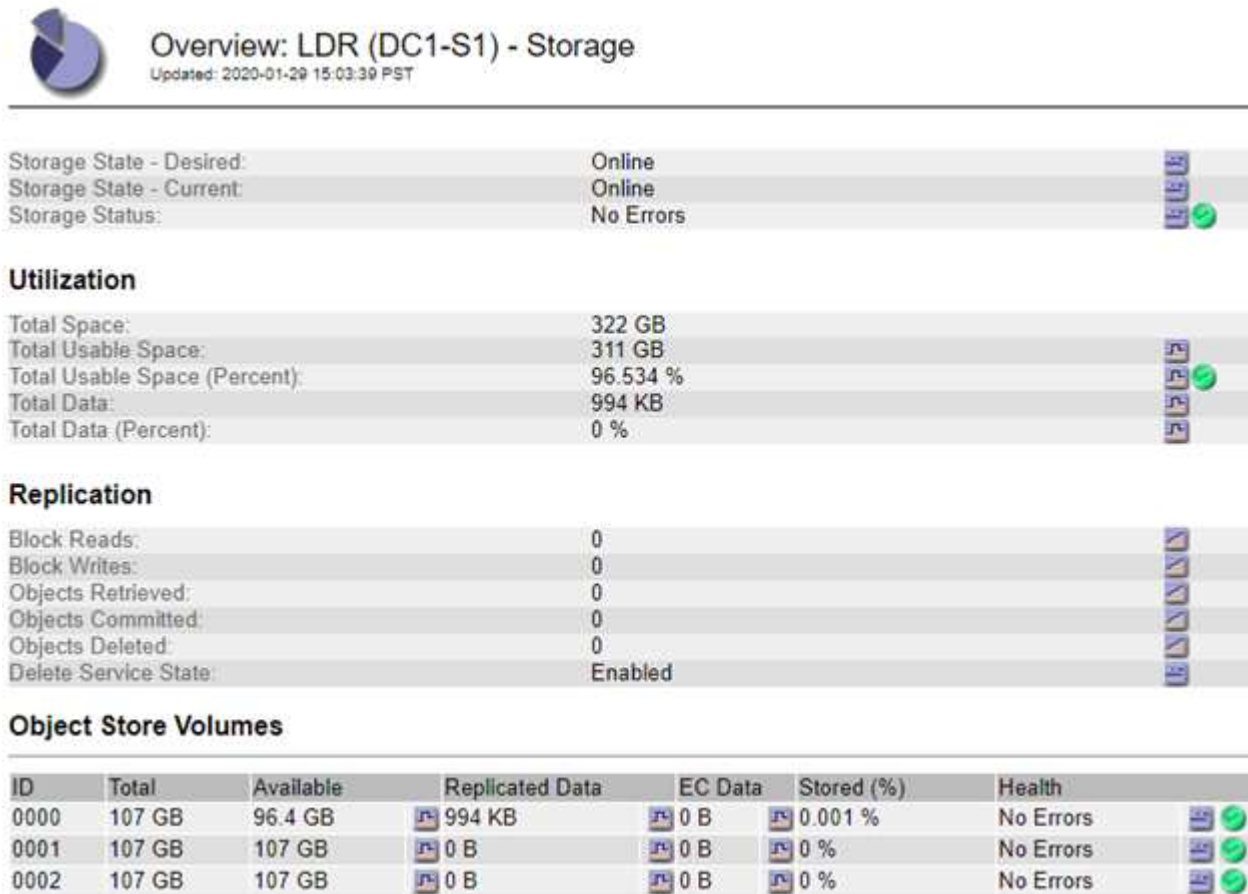
Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdC	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB 	Enabled

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB 	1.55 MB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0003	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0004	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

Para ver mais "detalhes sobre cada nó de armazenamento", siga estes passos:

1. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
2. Selecione **site > Nó de armazenamento > LDR > Armazenamento > Visão geral > Principal**.



Dependendo da natureza da falha, falhas em um volume de armazenamento podem ser refletidas em "alertas de volume de armazenamento". Se um volume de armazenamento falhar, você deverá reparar o volume de armazenamento com falha para restaurar o Nó de Armazenamento à funcionalidade completa o mais rápido possível. Se necessário, você pode ir até a aba **Configuração** e "coloque o nó de armazenamento em um estado somente leitura" para que o sistema StorageGRID possa usá-lo para recuperação de dados enquanto você se prepara para uma recuperação completa do servidor.

Verificar integridade do objeto

O sistema StorageGRID verifica a integridade dos dados de objetos nos nós de armazenamento, verificando se há objetos corrompidos e ausentes.

Existem dois processos de verificação: verificação em segundo plano e verificação de existência de objetos (anteriormente chamada de verificação em primeiro plano). Eles trabalham juntos para garantir a integridade dos dados. A verificação de antecedentes é executada automaticamente e verifica continuamente a exatidão dos dados do objeto. A verificação de existência de objetos pode ser acionada por um usuário para verificar mais rapidamente a existência (mas não a exatidão) dos objetos.

O que é verificação de antecedentes?

O processo de verificação em segundo plano verifica automática e continuamente os nós de armazenamento

em busca de cópias corrompidas de dados de objetos e tenta reparar automaticamente quaisquer problemas encontrados.

A verificação de antecedentes verifica a integridade de objetos replicados e objetos codificados para eliminação, da seguinte forma:

- **Objetos replicados:** Se o processo de verificação em segundo plano encontrar um objeto replicado corrompido, a cópia corrompida será removida de seu local e colocada em quarentena em outro lugar no nó de armazenamento. Em seguida, uma nova cópia não corrompida é gerada e colocada para satisfazer as políticas ativas do ILM. A nova cópia pode não ser colocada no nó de armazenamento que foi usado para a cópia original.



Dados de objetos corrompidos são colocados em quarentena em vez de excluídos do sistema, para que ainda possam ser acessados. Para obter mais informações sobre como acessar dados de objetos em quarentena, entre em contato com o suporte técnico.

- **Objetos com codificação de eliminação:** Se o processo de verificação em segundo plano detectar que um fragmento de um objeto com codificação de eliminação está corrompido, o StorageGRID tenta automaticamente reconstruir o fragmento ausente no mesmo nó de armazenamento, usando os dados restantes e os fragmentos de paridade. Se o fragmento corrompido não puder ser reconstruído, será feita uma tentativa de recuperar outra cópia do objeto. Se a recuperação for bem-sucedida, uma avaliação do ILM será realizada para criar uma cópia de substituição do objeto codificado para eliminação.

O processo de verificação em segundo plano verifica objetos somente em nós de armazenamento. Ele não verifica objetos em um pool de armazenamento em nuvem. Os objetos devem ter mais de quatro dias para se qualificarem para verificação de antecedentes.

A verificação de antecedentes é executada em uma taxa contínua e projetada para não interferir nas atividades normais do sistema. A verificação de antecedentes não pode ser interrompida. No entanto, você pode aumentar a taxa de verificação em segundo plano para verificar mais rapidamente o conteúdo de um nó de armazenamento se suspeitar de um problema.

Alertas relacionados à verificação de antecedentes

Se o sistema detectar um objeto corrompido que não pode ser corrigido automaticamente (porque a corrupção impede que o objeto seja identificado), o alerta **Objeto corrompido não identificado detectado** será acionado.

Se a verificação de antecedentes não puder substituir um objeto corrompido porque não consegue localizar outra cópia, o alerta **Objetos perdidos** será acionado.

Alterar a taxa de verificação de antecedentes

Você pode alterar a taxa na qual a verificação em segundo plano verifica os dados de objetos replicados em um nó de armazenamento se tiver preocupações sobre a integridade dos dados.

Antes de começar

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

Sobre esta tarefa

Você pode alterar a Taxa de Verificação para verificação em segundo plano em um Nó de Armazenamento:

- **Adaptável:** configuração padrão. A tarefa foi projetada para verificar no máximo 4 MB/s ou 10 objetos/s (o que for excedido primeiro).
- **Alto:** a verificação do armazenamento ocorre rapidamente, a uma taxa que pode retardar as atividades comuns do sistema.

Use a taxa de verificação Alta somente quando suspeitar que uma falha de hardware ou software pode ter corrompido os dados do objeto. Após a conclusão da verificação de antecedentes de alta prioridade, a Taxa de verificação é redefinida automaticamente para Adaptável.

Passos

1. Selecione **SUORTE > Ferramentas > Topologia de grade**.
2. Selecione **Nó de armazenamento > LDR > Verificação**.
3. Selecione **Configuração > Principal**.
4. Vá para **LDR > Verificação > Configuração > Principal**.
5. Em Verificação de antecedentes, selecione **Taxa de verificação > Alta** ou **Taxa de verificação > Adaptável**.

Overview Alarms Reports Configuration

Main

 Configuration: LDR (StorageGrid) - Verification
Updated: 2021-11-11 07:13:00 MST

Reset Missing Objects Count ☐

Background Verification

Verification Rate Adaptive

Reset Corrupt Objects Count ☐

Quarantined Objects

Delete Quarantined Objects ☐

Apply Changes 

6. Clique em **Aplicar alterações**.
7. Monitore os resultados da verificação de antecedentes para objetos replicados.
 - a. Vá para **NÓS > Nó de Armazenamento > Objetos**.
 - b. Na seção Verificação, monitore os valores para **Objetos Corrompidos** e **Objetos Corrompidos Não Identificados**.

Se a verificação de antecedentes encontrar dados de objetos replicados corrompidos, a métrica **Objetos Corrompidos** será incrementada e o StorageGRID tentará extrair o identificador de objeto dos dados, da seguinte maneira:

- Se o identificador do objeto puder ser extraído, o StorageGRID criará automaticamente uma nova

cópia dos dados do objeto. A nova cópia pode ser feita em qualquer lugar no sistema StorageGRID que satisfaça as políticas de ILM ativas.

- Se o identificador do objeto não puder ser extraído (porque foi corrompido), a métrica **Objetos corrompidos não identificados** será incrementada e o alerta **Objeto corrompido não identificado detectado** será acionado.

c. Se forem encontrados dados de objetos replicados corrompidos, entre em contato com o suporte técnico para determinar a causa raiz da corrupção.

8. Monitore os resultados da verificação de antecedentes para objetos codificados por eliminação.

Se a verificação de antecedentes encontrar fragmentos corrompidos de dados de objetos codificados para eliminação, o atributo Fragmentos Corrompidos Detectados será incrementado. O StorageGRID se recupera reconstruindo o fragmento corrompido no mesmo nó de armazenamento.

a. Selecione **SUORTE > Ferramentas > Topologia de grade**.

b. Selecione **Nó de Armazenamento > LDR > Codificação de Apagamento**.

c. Na tabela Resultados da Verificação, monitore o atributo Fragmentos Corrompidos Detectados (ECCD).

9. Depois que os objetos corrompidos forem restaurados automaticamente pelo sistema StorageGRID, redefine a contagem de objetos corrompidos.

a. Selecione **SUORTE > Ferramentas > Topologia de grade**.

b. Selecione **Nó de armazenamento > LDR > Verificação > Configuração**.

c. Selecione **Redefinir contagem de objetos corrompidos**.

d. Clique em **Aplicar alterações**.

10. Se tiver certeza de que os objetos em quarentena não são necessários, você pode excluí-los.



Se o alerta **Objetos perdidos** for acionado, o suporte técnico pode querer acessar os objetos em quarentena para ajudar a depurar o problema subjacente ou tentar recuperar os dados.

a. Selecione **SUORTE > Ferramentas > Topologia de grade**.

b. Selecione **Nó de armazenamento > LDR > Verificação > Configuração**.

c. Selecione **Excluir objetos em quarentena**.

d. Selecione **Aplicar alterações**.

O que é verificação de existência de objetos?

A verificação de existência de objetos verifica se todas as cópias replicadas esperadas de objetos e fragmentos codificados para eliminação existem em um nó de armazenamento. A verificação de existência do objeto não verifica os dados do objeto em si (a verificação em segundo plano faz isso); em vez disso, ela fornece uma maneira de verificar a integridade dos dispositivos de armazenamento, especialmente se um problema recente de hardware pode ter afetado a integridade dos dados.

Ao contrário da verificação de antecedentes, que ocorre automaticamente, você deve iniciar manualmente um trabalho de verificação de existência de objeto.

A verificação de existência de objetos lê os metadados de cada objeto armazenado no StorageGRID e verifica a existência de cópias de objetos replicadas e fragmentos de objetos codificados para eliminação. Quaisquer dados ausentes são tratados da seguinte forma:

- **Cópias replicadas:** Se uma cópia dos dados do objeto replicado estiver faltando, o StorageGRID tentará automaticamente substituir a cópia por uma cópia armazenada em outro lugar no sistema. O nó de armazenamento executa uma cópia existente por meio de uma avaliação de ILM, que determinará que a política de ILM atual não está mais sendo atendida para este objeto porque outra cópia está faltando. Uma nova cópia é gerada e colocada para satisfazer as políticas de ILM ativas do sistema. Esta nova cópia pode não ser colocada no mesmo local onde a cópia ausente foi armazenada.
- **Fragmentos codificados por eliminação:** se um fragmento de um objeto codificado por eliminação estiver ausente, o StorageGRID tenta reconstruir automaticamente o fragmento ausente no mesmo nó de armazenamento usando os fragmentos restantes. Se o fragmento ausente não puder ser reconstruído (porque muitos fragmentos foram perdidos), o ILM tenta encontrar outra cópia do objeto, que pode ser usada para gerar um novo fragmento codificado por apagamento.

Executar verificação de existência de objeto

Você cria e executa uma tarefa de verificação de existência de objeto por vez. Ao criar um trabalho, você seleciona os nós de armazenamento e os volumes que deseja verificar. Você também seleciona a consistência do trabalho.

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 garantiu que os nós de armazenamento que deseja verificar estão online. Selecione **NÓS** para visualizar a tabela de nós. Certifique-se de que nenhum ícone de alerta apareça ao lado do nome do nó para os nós que você deseja verificar.
- Você garantiu que os seguintes procedimentos **não** estão em execução nos nós que deseja verificar:
 - Expansão da grade para adicionar um nó de armazenamento
 - Desativação do nó de armazenamento
 - Recuperação de um volume de armazenamento com falha
 - Recuperação de um nó de armazenamento com uma unidade de sistema com falha
 - Reequilíbrio da CE
 - Clone do nó do dispositivo

A verificação de existência do objeto não fornece informações úteis enquanto esses procedimentos estão em andamento.

Sobre esta tarefa

Uma tarefa de verificação de existência de objeto pode levar dias ou semanas para ser concluída, dependendo do número de objetos na grade, dos nós e volumes de armazenamento selecionados e da consistência selecionada. Você pode executar apenas uma tarefa por vez, mas pode selecionar vários nós de armazenamento e volumes ao mesmo tempo.

Passos

1. Selecione **MANUTENÇÃO > Tarefas > Verificação de existência de objeto**.
2. Selecione **Criar trabalho**. O assistente Criar uma tarefa de verificação de existência de objeto é exibido.
3. Selecione os nós que contêm os volumes que você deseja verificar. Para selecionar todos os nós on-line, marque a caixa de seleção **Nome do nó** no cabeçalho da coluna.

Você pode pesquisar por nome do nó ou site.

Você não pode selecionar nós que não estejam conectados à grade.

4. Selecione **Continuar**.

5. Selecione um ou mais volumes para cada nó na lista. Você pode pesquisar volumes usando o número do volume de armazenamento ou o nome do nó.

Para selecionar todos os volumes para cada nó selecionado, marque a caixa de seleção **Volume de armazenamento** no cabeçalho da coluna.

6. Selecione **Continuar**.

7. Selecione a consistência para o trabalho.

A consistência determina quantas cópias de metadados do objeto são usadas para a verificação da existência do objeto.

- **Strong-site**: Duas cópias de metadados em um único site.
- **Strong-global**: Duas cópias de metadados em cada site.
- **Todos** (padrão): Todas as três cópias de metadados em cada site.

Para obter mais informações sobre consistência, consulte as descrições no assistente.

8. Selecione **Continuar**.

9. Revise e verifique suas seleções. Você pode selecionar **Anterior** para ir para uma etapa anterior no assistente e atualizar suas seleções.

Um trabalho de verificação de existência de objeto é gerado e executado até que ocorra uma das seguintes situações:

- O trabalho foi concluído.
- Você pausa ou cancela o trabalho. Você pode retomar um trabalho que foi pausado, mas não pode retomar um trabalho que foi cancelado.
- O trabalho estagna. O alerta **A verificação de existência do objeto foi interrompida** é acionado. Siga as ações corretivas especificadas para o alerta.
- O trabalho falha. O alerta **Falha na verificação de existência do objeto** é acionado. Siga as ações corretivas especificadas para o alerta.
- Aparece uma mensagem "Serviço indisponível" ou "Erro interno do servidor". Após um minuto, atualize a página para continuar monitorando o trabalho.



Conforme necessário, você pode sair da página de verificação de existência do objeto e retornar para continuar monitorando o trabalho.

10. Conforme o trabalho é executado, visualize a guia **Trabalho ativo** e observe o valor de Cópias de objetos ausentes detectadas.

Este valor representa o número total de cópias ausentes de objetos replicados e objetos codificados por eliminação com um ou mais fragmentos ausentes.

Se o número de cópias de objetos ausentes detectadas for maior que 100, pode haver um problema com o armazenamento do nó de armazenamento.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job

Job history

Status: Accepted

Consistency control: All

Job ID: 2334602652907829302

Start time: 2021-11-10 14:43:02 MST

Missing object copies detected: 0

Elapsed time: —

Progress: 0%

Estimated time to completion: —

Pause

Cancel

Volumes

Details

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. Após a conclusão do trabalho, execute quaisquer ações adicionais necessárias:

- Se o número de cópias de objetos ausentes detectadas for zero, nenhum problema foi encontrado. Nenhuma ação é necessária.
- Se o número de cópias de objetos ausentes detectadas for maior que zero e o alerta **Objetos perdidos** não tiver sido acionado, todas as cópias ausentes foram reparadas pelo sistema. Verifique se quaisquer problemas de hardware foram corrigidos para evitar danos futuros às cópias de objetos.
- Se o número de cópias de objetos ausentes detectadas for maior que zero e o alerta **Objetos perdidos** tiver sido acionado, a integridade dos dados poderá ser afetada. Entre em contato com o suporte técnico.
- Você pode investigar cópias de objetos perdidos usando grep para extrair as mensagens de auditoria `LLST: grep LLST audit_file_name`.

Este procedimento é semelhante ao de "[investigando objetos perdidos](#)", embora para cópias de objetos você procure por LLST em vez de OLST.

12. Se você selecionou a consistência strong-site ou strong-global para o trabalho, aguarde aproximadamente três semanas pela consistência dos metadados e execute o trabalho novamente nos mesmos volumes.

Quando o StorageGRID tiver tempo para atingir a consistência de metadados para os nós e volumes incluídos no trabalho, a nova execução do trabalho poderá limpar cópias de objetos ausentes relatadas erroneamente ou fazer com que cópias adicionais de objetos sejam verificadas se estiverem ausentes.

a. Selecione **MANUTENÇÃO > Verificação de existência do objeto > Histórico de tarefas**.

- b. Determine quais tarefas estão prontas para serem executadas novamente:
 - i. Veja a coluna **Hora de término** para determinar quais tarefas foram executadas há mais de três semanas.
 - ii. Para esses trabalhos, verifique a coluna Controle de consistência para strong-site ou strong-global.
- c. Marque a caixa de seleção de cada tarefa que você deseja executar novamente e selecione **Executar novamente**.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job | Job history

Delete | **Rerun** | Search by Job ID/ node name/ consistency control/ start time

Displaying 4 results

☐	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
☒	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
☐	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

- d. No assistente de execução repetida de trabalhos, revise os nós e volumes selecionados e a consistência.
- e. Quando estiver pronto para executar novamente os trabalhos, selecione **Executar novamente**.

A guia Trabalho ativo é exibida. Todos os trabalhos selecionados serão executados novamente como um único trabalho com consistência de strong-site. Um campo **Trabalhos relacionados** na seção Detalhes lista os IDs dos trabalhos originais.

Depois que você terminar

Se você ainda tiver dúvidas sobre a integridade dos dados, vá para **SUPORTE > Ferramentas > Topologia de grade > site > Nó de armazenamento > LDR > Verificação > Configuração > Principal** e aumente a Taxa de verificação em segundo plano. A verificação de antecedentes verifica a exatidão de todos os dados de objetos armazenados e repara quaisquer problemas encontrados. Encontrar e reparar possíveis problemas o mais rápido possível reduz o risco de perda de dados.

Solucionar problemas de alerta de tamanho de objeto S3 PUT muito grande

O alerta de tamanho de objeto S3 PUT muito grande é acionado se um locatário tentar uma operação PutObject não multiparte que exceda o limite de tamanho S3 de 5 GiB.

Antes de começar

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

Determine quais locatários usam objetos maiores que 5 GiB para que você possa notificá-los.

Passos

1. Vá para **CONFIGURAÇÃO > Monitoramento > Servidor de auditoria e syslog**.
2. Se as gravações do cliente estiverem normais, acesse o log de auditoria:

- a. Digitar `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 `#` .

- e. Mude para o diretório onde os logs de auditoria estão localizados.

O diretório do log de auditoria e os nós aplicáveis dependem das configurações de destino da auditoria.

Opção	Destino
Nós locais (padrão)	<code>/var/local/log/localaudit.log</code>
Nós de administração/nós locais	• Nós de administração (primários e não primários): <code>/var/local/audit/export/audit.log</code> • Todos os nós: O <code>/var/local/log/localaudit.log</code> o arquivo normalmente está vazio ou ausente neste modo.
Servidor syslog externo	<code>/var/local/log/localaudit.log</code>

Dependendo das configurações de destino da auditoria, insira: `cd /var/local/log` ou `/var/local/audit/export/`

Para saber mais, consulte ["Selecione destinos de informações de auditoria"](#) .

- f. Identifique quais locatários estão usando objetos maiores que 5 GiB.
 - i. Digitar `zgrep SPUT * | egrep "CSIZ\ (UI64\): ([5-9] | [1-9] [0-9]+) [0-9]{9}"`
 - ii. Para cada mensagem de auditoria nos resultados, observe `S3AI` campo para determinar o ID da conta do locatário. Use os outros campos na mensagem para determinar qual endereço IP foi usado pelo cliente, pelo bucket e pelo objeto:

Código	Descrição
SAIP	IP de origem
S3AI	ID do inquilino
S3BK	Balde
S3KY	Objeto
CSIZ	Tamanho (bytes)

Exemplo de resultados de log de auditoria

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"]][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Se as gravações do cliente não forem normais, use o ID do locatário do alerta para identificá-lo:

- Vá para **SUPORTE > Ferramentas > Registros**. Colete logs de aplicativos para o nó de armazenamento no alerta. Especifique 15 minutos antes e depois do alerta.
- Extraia o arquivo e vá para `broadcast.log`:

```
/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/broadcast.log
```

- Pesquise no log por `method=PUT` e identificar o cliente no `clientIP` campo.

Exemplo broadcast.log

```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE 1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. Informe aos locatários que o tamanho máximo do `PutObject` é 5 GiB e que devem usar uploads multipartes para objetos maiores que 5 GiB.

5. Ignore o alerta por uma semana se o aplicativo tiver sido alterado.

Solucionar problemas de dados de objetos perdidos e ausentes

Solucionar problemas de dados de objetos perdidos e ausentes

Os objetos podem ser recuperados por vários motivos, incluindo solicitações de leitura de um aplicativo cliente, verificações em segundo plano de dados de objetos replicados, reavaliações de ILM e restauração de dados de objetos durante a recuperação de um nó de armazenamento.

O sistema StorageGRID usa informações de localização nos metadados de um objeto para determinar de qual local recuperar o objeto. Se uma cópia do objeto não for encontrada no local esperado, o sistema tentará recuperar outra cópia do objeto de outro lugar no sistema, supondo que a política do ILM contenha uma regra para fazer duas ou mais cópias do objeto.

Se essa recuperação for bem-sucedida, o sistema StorageGRID substituirá a cópia ausente do objeto. Caso contrário, o alerta **Objetos perdidos** é acionado, da seguinte forma:

- Para cópias replicadas, se outra cópia não puder ser recuperada, o objeto será considerado perdido e o alerta será acionado.
- Para cópias codificadas para eliminação, se uma cópia não puder ser recuperada do local esperado, o atributo Cópias Corrompidas Detectadas (ECOR) será incrementado em um antes de uma tentativa de recuperar uma cópia de outro local. Se nenhuma outra cópia for encontrada, o alerta será disparado.

Você deve investigar todos os alertas de **Objetos perdidos** imediatamente para determinar a causa raiz da perda e para determinar se o objeto ainda pode existir em um Nós de Armazenamento offline ou indisponível no momento. Ver "[Investigar objetos perdidos](#)".

No caso de dados de objetos sem cópias serem perdidos, não há solução de recuperação. No entanto, você deve zerar o contador de objetos perdidos para evitar que objetos perdidos conhecidos mascarem quaisquer novos objetos perdidos. Ver "[Redefinir contagens de objetos perdidos e desaparecidos](#)".

Investigar objetos perdidos

Quando o alerta **Objetos perdidos** for acionado, você deve investigar imediatamente. Colete informações sobre os objetos afetados e entre em contato com o suporte técnico.

Antes de começar

- Você deve estar conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- Você tem "[permissões de acesso específicas](#)".
- Você deve ter o `Passwords.txt` arquivo.

Sobre esta tarefa

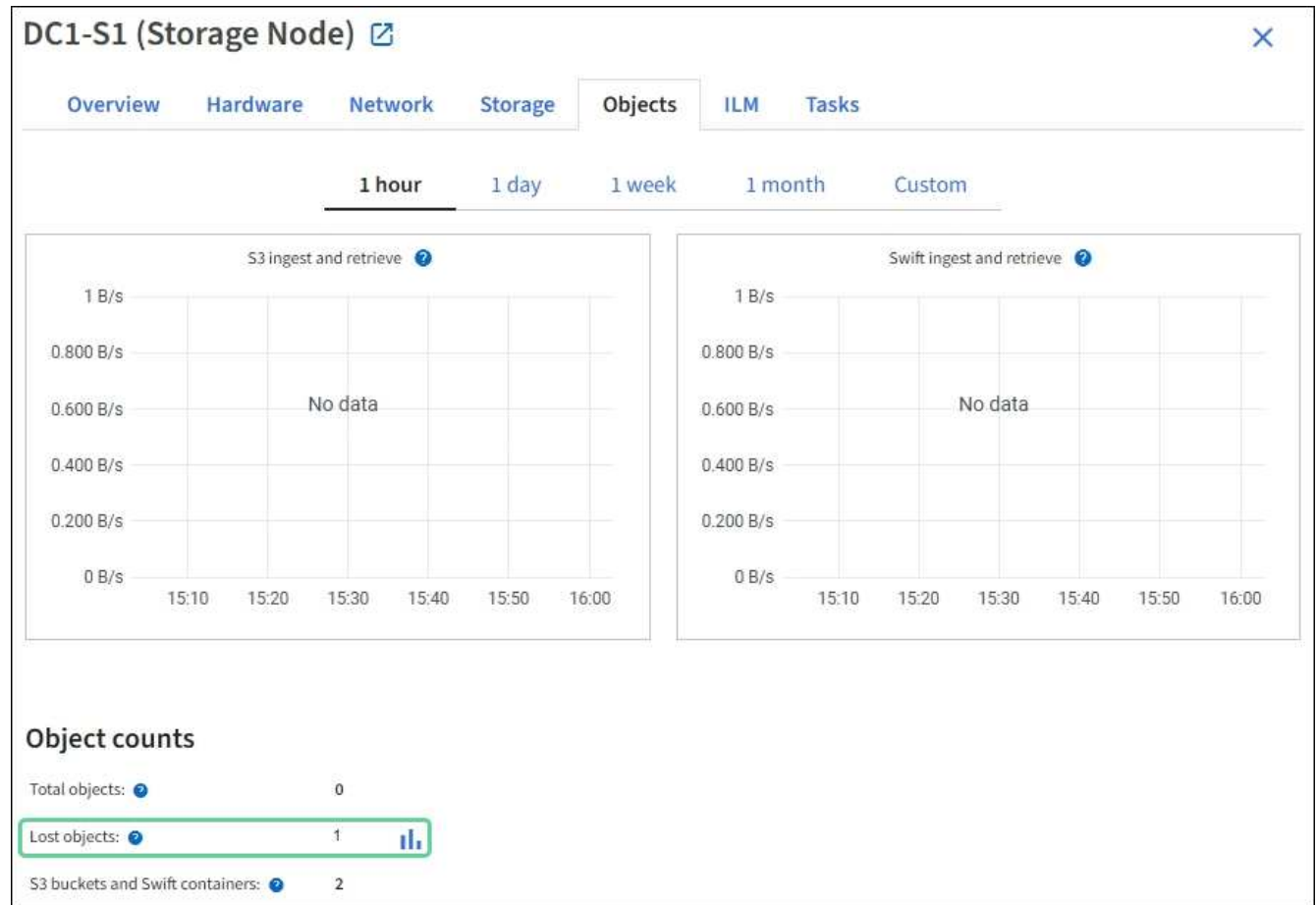
O alerta **Objetos perdidos** indica que o StorageGRID acredita que não há cópias de um objeto na grade. Os dados podem ter sido perdidos permanentemente.

Investigue imediatamente alertas de objetos perdidos. Talvez seja necessário tomar medidas para evitar mais perdas de dados. Em alguns casos, você pode restaurar um objeto perdido se agir rapidamente.

Passos

1. Selecione **NODES**.
2. Selecione **Nó de Armazenamento > Objetos**.
3. Revise o número de objetos perdidos mostrado na tabela Contagem de objetos.

Este número indica o número total de objetos que este nó de grade detecta como ausentes em todo o sistema StorageGRID . O valor é a soma dos contadores de objetos perdidos do componente de armazenamento de dados nos serviços LDR e DDS.



4. De um nó de administração, "acessar o log de auditoria" para determinar o identificador exclusivo (UUID) do objeto que acionou o alerta **Objetos perdidos**:
 - a. Efetue login no nó da grade:
 - i. Digite o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Digite a senha listada no `Passwords.txt` arquivo.
 - iii. Digite o seguinte comando para alternar para root: `su -`
 - iv. Digite a senha listada no `Passwords.txt` arquivo. Quando você está logado como root, o prompt muda de `$` para `#`.
 - b. Mude para o diretório onde os logs de auditoria estão localizados.

O diretório do log de auditoria e os nós aplicáveis dependem das configurações de destino da auditoria.

Opção	Destino
Nós locais (padrão)	/var/local/log/localaudit.log
Nós de administração/nós locais	- Nós de administração (primários e não primários): /var/local/audit/export/audit.log - Todos os nós: O /var/local/log/localaudit.log o arquivo normalmente está vazio ou ausente neste modo.
Servidor syslog externo	/var/local/log/localaudit.log

Dependendo das configurações de destino da auditoria, insira: `cd /var/local/log` ou `/var/local/audit/export/`

Para saber mais, consulte ["Selecione destinos de informações de auditoria"](#).

- c. Use `grep` para extrair as mensagens de auditoria de Objeto Perdido (OLST). Digitar: `grep OLST audit_file_name`
- d. Observe o valor do UUID incluído na mensagem.

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5] [UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"] [NOID(UI32):12288733] [VOL1(UI64):3222345986]
[RSLT(FC32):NONE] [AVER(UI32):10]
[ATIM(UI64):1581535134780426] [ATYP(FC32):OLST] [ANID(UI32):12448208] [AMID(FC32):ILMX] [ATID(UI64):7729403978647354233]]
```

5. Procure os metadados do objeto perdido usando o UUID:
 - a. Selecione **ILM > Consulta de metadados do objeto**.
 - b. Digite o UUID e selecione **Procurar**.
 - c. Revise os locais nos metadados e tome as medidas apropriadas:

Metadados	Conclusão
Objeto <object_identifier> não encontrado	Se o objeto não for encontrado, a mensagem "ERROR":"" será retornada. Se o objeto não for encontrado, você pode zerar a contagem de Objetos perdidos para limpar o alerta. A ausência de um objeto indica que o objeto foi excluído intencionalmente.

Metadados	Conclusão
Locais > 0	Se houver locais listados na saída, o alerta Objetos perdidos pode ser um falso positivo. Confirme se os objetos existem. Use o ID do nó e o caminho do arquivo listados na saída para confirmar se o arquivo de objeto está no local listado. (O procedimento para "procurando por objetos potencialmente perdidos" explica como usar o ID do nó para encontrar o nó de armazenamento correto.) Se os objetos existirem, você pode zerar a contagem de Objetos perdidos para limpar o alerta.
Locais = 0	Se não houver locais listados na saída, o objeto está potencialmente ausente. Você pode tentar "procurar e restaurar o objeto" você mesmo ou entre em contato com o suporte técnico. O suporte técnico pode solicitar que você determine se há um procedimento de recuperação de armazenamento em andamento. Veja as informações sobre "restaurando dados de objetos usando o Grid Manager" e "restaurando dados de objetos para um volume de armazenamento".

Pesquisar e restaurar objetos potencialmente perdidos

Pode ser possível encontrar e restaurar objetos que acionaram um alerta de **Objeto perdido** e um alarme legado de Objetos Perdidos (LOST) e que você identificou como potencialmente perdidos.

Antes de começar

- Você tem o UUID de qualquer objeto perdido, conforme identificado em "[Investigar objetos perdidos](#)".
- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

Você pode seguir este procedimento para procurar cópias replicadas do objeto perdido em outro lugar na grade. Na maioria dos casos, o objeto perdido não será encontrado. No entanto, em alguns casos, você pode encontrar e restaurar um objeto replicado perdido se agir imediatamente.



Entre em contato com o suporte técnico para obter assistência com este procedimento.

Passos

1. Em um nó de administração, pesquise nos logs de auditoria possíveis localizações de objetos:
 - a. Efetue login no nó da grade:
 - i. Digite o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Digite a senha listada no `Passwords.txt` arquivo.

- iii. Digite o seguinte comando para alternar para root: `su -`
 - iv. Digite a senha listada no `Passwords.txt` arquivo. Quando você está logado como root, o prompt muda de `$` para `#`.
- b. Altere para o diretório onde os logs de auditoria estão localizados.

O diretório do log de auditoria e os nós aplicáveis dependem das configurações de destino da auditoria.

Opção	Destino
Nós locais (padrão)	<code>/var/local/log/localaudit.log</code>
Nós de administração/nós locais	• Nós de administração (primários e não primários): <code>/var/local/audit/export/audit.log</code> • Todos os nós: O <code>/var/local/log/localaudit.log</code> o arquivo normalmente está vazio ou ausente neste modo.
Servidor syslog externo	<code>/var/local/log/localaudit.log</code>

Dependendo das configurações de destino da auditoria, insira: `cd /var/local/log` ou `/var/local/audit/export/`

Para saber mais, consulte ["Selecione destinos de informações de auditoria"](#).

- c. Use `grep` para extrair o ["mensagens de auditoria associadas ao objeto potencialmente perdido"](#) e enviá-los para um arquivo de saída. Digitar: `grep uuid-value audit_file_name > output_file_name`

Por exemplo:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_lost_object.txt
```

- d. Use `grep` para extrair as mensagens de auditoria de Localização Perdida (LLST) deste arquivo de saída. Digitar: `grep LLST output_file_name`

Por exemplo:

```
Admin: # grep LLST /var/local/tmp/messages_about_lost_objects.txt
```

Uma mensagem de auditoria LLST se parece com esta mensagem de exemplo.

```
[AUDT: [NOID (UI32) :12448208] [CBIL (UI64) :0x38186FE53E3C49A5]
[UUID (CSTR) : "926026C4-00A4-449B-AC72-BCCA72DD1311"] [LTYP (FC32) :CLDI]
[PCLD (CSTR) : "/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6"]
[TSRC (FC32) :SYST] [RSLT (FC32) :NONE] [AVER (UI32) :10] [ATIM (UI64) :15815351
34379225]
[ATYP (FC32) :LLST] [ANID (UI32) :12448208] [AMID (FC32) :CLSM] [ATID (UI64) :70
86871083190743409]]
```

e. Localize o campo PCLD e o campo NOID na mensagem LLST.

Se presente, o valor de PCLD é o caminho completo no disco para a cópia do objeto replicado ausente. O valor de NOID é o ID do nó do LDR onde uma cópia do objeto pode ser encontrada.

Se você encontrar a localização de um objeto, poderá restaurá-lo.

a. Encontre o nó de armazenamento associado a este ID de nó LDR. No Grid Manager, selecione **SUPOORTE > Ferramentas > Topologia de grade**. Em seguida, selecione **Data Center > Storage Node > LDR**.

O ID do nó para o serviço LDR está na tabela Informações do nó. Revise as informações de cada nó de armazenamento até encontrar aquele que hospeda este LDR.

2. Determine se o objeto existe no nó de armazenamento indicado na mensagem de auditoria:

a. Efetue login no nó da grade:

- i. Digite o seguinte comando: `ssh admin@grid_node_IP`
- ii. Digite a senha listada no `Passwords.txt` arquivo.
- iii. Digite o seguinte comando para alternar para root: `su -`
- iv. Digite a senha listada no `Passwords.txt` arquivo.

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

b. Determine se o caminho do arquivo para o objeto existe.

Para o caminho do arquivo do objeto, use o valor de PCLD da mensagem de auditoria LLST.

Por exemplo, insira:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6'
```



Sempre coloque o caminho do arquivo objeto entre aspas simples nos comandos para escapar de quaisquer caracteres especiais.

- Se o caminho do objeto não for encontrado, o objeto será perdido e não poderá ser restaurado usando este procedimento. Entre em contato com o suporte técnico.
- Se o caminho do objeto for encontrado, continue com a próxima etapa. Você pode tentar restaurar o objeto encontrado de volta para StorageGRID.

3. Se o caminho do objeto foi encontrado, tente restaurar o objeto para StorageGRID:
 - a. No mesmo nó de armazenamento, altere a propriedade do arquivo de objeto para que ele possa ser gerenciado pelo StorageGRID. Digitar: `chown ldr-user:bycast 'file_path_of_object'`
 - b. Faça telnet para o host local 1402 para acessar o console LDR. Digitar: `telnet 0 1402`
 - c. Digitar: `cd /proc/STOR`
 - d. Digitar: `Object_Found 'file_path_of_object'`

Por exemplo, insira:

```
Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Emitindo o `Object_Found` O comando notifica a grade sobre a localização do objeto. Ele também aciona as políticas ILM ativas, que fazem cópias adicionais conforme especificado em cada política.



Se o nó de armazenamento onde você encontrou o objeto estiver offline, você poderá copiar o objeto para qualquer nó de armazenamento que esteja online. Coloque o objeto em qualquer diretório `/var/local/rangedb` do nó de armazenamento online. Em seguida, emita o `Object_Found` comando usando esse caminho de arquivo para o objeto.

- Se o objeto não puder ser restaurado, o `Object_Found` o comando falha. Entre em contato com o suporte técnico.
- Se o objeto foi restaurado com sucesso para StorageGRID, uma mensagem de sucesso será exibida. Por exemplo:

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

Continue com o próximo passo.

4. Se o objeto foi restaurado com sucesso para StorageGRID, verifique se os novos locais foram criados:
 - a. Sign in no Grid Manager usando um ["navegador da web compatível"](#).
 - b. Selecione **ILM > Consulta de metadados do objeto**.
 - c. Digite o UUID e selecione **Procurar**.
 - d. Revise os metadados e verifique os novos locais.
5. Em um nó de administração, pesquise nos logs de auditoria a mensagem de auditoria ORLM para este objeto para confirmar se o gerenciamento do ciclo de vida das informações (ILM) colocou cópias conforme necessário.

a. Efetue login no nó da grade:

- i. Digite o seguinte comando: `ssh admin@grid_node_IP`
- ii. Digite a senha listada no `Passwords.txt` arquivo.
- iii. Digite o seguinte comando para alternar para root: `su -`
- iv. Digite a senha listada no `Passwords.txt` arquivo. Quando você está logado como root, o prompt muda de `$` para `#`.

b. Mude para o diretório onde os logs de auditoria estão localizados. Consulte [subetapa 1. b](#).

c. Use `grep` para extrair as mensagens de auditoria associadas ao objeto para um arquivo de saída.

Digitar: `grep uuid-value audit_file_name > output_file_name`

Por exemplo:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_restored_object.txt
```

d. Use `grep` para extrair as mensagens de auditoria do Object Rules Met (ORLM) deste arquivo de saída.

Digitar: `grep ORLM output_file_name`

Por exemplo:

```
Admin: # grep ORLM /var/local/tmp/messages_about_restored_object.txt
```

Uma mensagem de auditoria ORLM se parece com esta mensagem de exemplo.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. Encontre o campo `LOCS` na mensagem de auditoria.

Se presente, o valor de `CLDI` em `LOCS` é o ID do nó e o ID do volume onde uma cópia do objeto foi criada. Esta mensagem mostra que o ILM foi aplicado e que duas cópias de objeto foram criadas em dois locais na grade.

6. "[Redefinir a contagem de objetos perdidos e desaparecidos](#)"no Gerenciador de Grade.

Redefinir contagens de objetos perdidos e desaparecidos

Depois de investigar o sistema StorageGRID e verificar se todos os objetos perdidos registrados foram perdidos permanentemente ou se é um alarme falso, você pode

redefinir o valor do atributo Objetos Perdidos para zero.

Antes de começar

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

Sobre esta tarefa

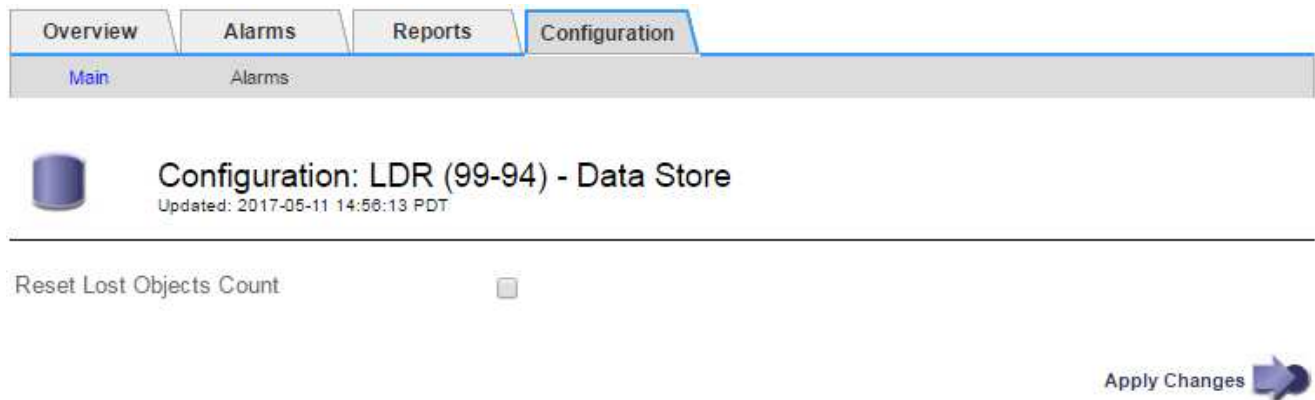
Você pode zerar o contador de Objetos Perdidos em qualquer uma das seguintes páginas:

- **SUPORTE > Ferramentas > Topologia de grade > Site > Nó de armazenamento > LDR > Armazenamento de dados > Visão geral > Principal**
- **SUPORTE > Ferramentas > Topologia de grade > Site > Nó de armazenamento > DDS > Armazenamento de dados > Visão geral > Principal**

Estas instruções mostram como redefinir o contador na página **LDR > Data Store**.

Passos

1. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
2. Selecione **Site > Nó de Armazenamento > LDR > Armazenamento de Dados > Configuração** para o Nó de Armazenamento que tem o alerta **Objetos perdidos** ou o alarme PERDIDO.
3. Selecione **Redefinir contagem de objetos perdidos**.



4. Clique em **Aplicar alterações**.

O atributo Objetos Perdidos é redefinido para 0 e o alerta **Objetos perdidos** e o alarme PERDIDO são apagados, o que pode levar alguns minutos.

5. Opcionalmente, redefina outros valores de atributos relacionados que podem ter sido incrementados no processo de identificação do objeto perdido.
 - a. Selecione **Site > Nó de Armazenamento > LDR > Codificação de Apagamento > Configuração**.
 - b. Selecione **Redefinir contagem de falhas de leitura** e **Redefinir contagem de cópias corrompidas detectadas**.
 - c. Clique em **Aplicar alterações**.
 - d. Selecione **Site > Nó de Armazenamento > LDR > Verificação > Configuração**.
 - e. Selecione **Redefinir contagem de objetos ausentes** e **Redefinir contagem de objetos corrompidos**.

- f. Se tiver certeza de que os objetos em quarentena não são necessários, você pode selecionar **Excluir objetos em quarentena**.

Objetos em quarentena são criados quando a verificação em segundo plano identifica uma cópia corrompida do objeto replicado. Na maioria dos casos, o StorageGRID substitui automaticamente o objeto corrompido e é seguro excluir os objetos em quarentena. Entretanto, se o alerta **Objetos perdidos** ou o alarme PERDIDO for acionado, o suporte técnico pode querer acessar os objetos em quarentena.

- g. Clique em **Aplicar alterações**.

Pode levar alguns instantes para que os atributos sejam redefinidos após você clicar em **Aplicar alterações**.

Solucionar problemas do alerta de armazenamento de dados de objeto baixo

O alerta **Armazenamento de dados de objeto baixo** monitora quanto espaço está disponível para armazenar dados de objeto em cada nó 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

O alerta **Baixo armazenamento de dados de objeto** é acionado quando a quantidade total de dados de objeto replicados e codificados para eliminação em um nó de armazenamento atende a uma das condições configuradas na regra de alerta.

Por padrão, um alerta principal é acionado quando esta condição é avaliada como verdadeira:

```
(storagegrid_storage_utilization_data_bytes/  
(storagegrid_storage_utilization_data_bytes +  
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

Nessa condição:

- ``storagegrid_storage_utilization_data_bytes`` é uma estimativa do tamanho total de dados de objetos replicados e codificados para eliminação para um nó de armazenamento.
- ``storagegrid_storage_utilization_usable_space_bytes`` é a quantidade total de espaço de armazenamento de objetos restante para um nó de armazenamento.

Se um alerta maior ou menor de **Baixo armazenamento de dados de objeto** for acionado, você deverá executar um procedimento de expansão o mais rápido possível.

Passos

1. Selecione **ALERTAS > Atual**.

A página Alertas é exibida.

2. Na tabela de alertas, expanda o grupo de alertas **Armazenamento de dados de objeto baixo**, se necessário, e selecione o alerta que deseja visualizar.

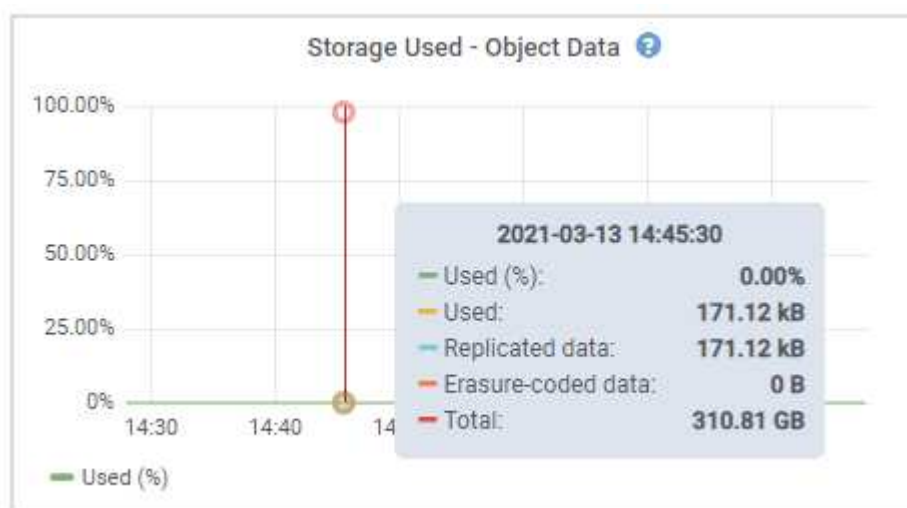


Selecione o alerta, não o título de um grupo de alertas.

3. Revise os detalhes na caixa de diálogo e observe o seguinte:
 - Tempo acionado
 - O nome do site e do nó
 - Os valores atuais das métricas para este alerta
4. Selecione **NÓS > Nó ou Site de Armazenamento > Armazenamento**.
5. Posicione o cursor sobre o gráfico Armazenamento usado - Dados do objeto.

Os seguintes valores são mostrados:

- **Usado (%)**: A porcentagem do espaço total utilizável que foi usada para dados do objeto.
- **Usado**: A quantidade de espaço total utilizável que foi usada para dados do objeto.
- **Dados replicados**: Uma estimativa da quantidade de dados de objetos replicados neste nó, site ou grade.
- **Dados codificados por eliminação**: Uma estimativa da quantidade de dados de objetos codificados por eliminação neste nó, site ou grade.
- **Total**: A quantidade total de espaço utilizável neste nó, site ou grade. O valor usado é o `storagegrid_storage_utilization_data_bytes` métrica.



6. Selecione os controles de tempo acima do gráfico para visualizar o uso do armazenamento em diferentes períodos de tempo.

Analisar o uso do armazenamento ao longo do tempo pode ajudar você a entender quanto armazenamento foi usado antes e depois do alerta ser disparado e pode ajudar você a estimar quanto tempo pode levar para o espaço restante do nó ficar cheio.

7. O mais breve possível, "[adicionar capacidade de armazenamento](#)" para sua grade.

Você pode adicionar volumes de armazenamento (LUNs) aos nós de armazenamento existentes ou adicionar novos nós de armazenamento.



Para obter mais informações, consulte "[Gerenciar nós de armazenamento completos](#)".

Solucionar problemas de alertas de substituição de marca d'água somente leitura

Se você usar valores personalizados para marcas d'água de volume de armazenamento, talvez seja necessário resolver o alerta **Substituição de marca d'água somente leitura baixa**. Se possível, você deve atualizar seu sistema para começar a usar os valores otimizados.

Em lançamentos anteriores, os três "**marcas d'água de volume de armazenamento**" eram configurações globais — os mesmos valores aplicados a cada volume de armazenamento em cada nó de armazenamento. A partir do StorageGRID 11.6, o software pode otimizar essas marcas d'água para cada volume de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

Ao atualizar para o StorageGRID 11.6 ou superior, marcas d'água otimizadas somente leitura e leitura/gravação são aplicadas automaticamente a todos os volumes de armazenamento, a menos que uma das seguintes condições seja verdadeira:

- Seu sistema está próximo da capacidade máxima e não conseguirá aceitar novos dados se marcas d'água otimizadas forem aplicadas. O StorageGRID não alterará as configurações da marca d'água neste caso.
- Você definiu anteriormente qualquer uma das marcas d'água do volume de armazenamento para um valor personalizado. O StorageGRID não substituirá as configurações de marca d'água personalizadas por valores otimizados. No entanto, o StorageGRID pode disparar o alerta **Substituição de marca d'água somente leitura baixa** se o seu valor personalizado para a marca d'água somente leitura do volume de armazenamento for muito pequeno.

Entenda o alerta

Se você usar valores personalizados para marcas d'água de volume de armazenamento, o alerta **Substituição de marca d'água somente leitura baixa** poderá ser acionado para um ou mais nós de armazenamento.

Cada instância do alerta indica que o valor personalizado da marca d'água somente leitura do volume de armazenamento é menor que o valor mínimo otimizado para esse nó de armazenamento. Se você continuar a usar a configuração personalizada, o Nó de Armazenamento poderá ficar com pouco espaço antes de poder fazer a transição segura para o estado somente leitura. Alguns volumes de armazenamento podem ficar inacessíveis (desmontados automaticamente) quando o nó atinge a capacidade.

Por exemplo, suponha que você tenha definido anteriormente a marca d'água somente leitura do volume de armazenamento para 5 GB. Agora suponha que o StorageGRID tenha calculado os seguintes valores otimizados para os quatro volumes de armazenamento no Nó de Armazenamento A:

Volume 0	12 GB
Volume 1	12 GB
Volume 2	11 GB
Volume 3	15 GB

O alerta **Substituição de marca d'água somente leitura baixa** é acionado para o Nó de Armazenamento A porque sua marca d'água personalizada (5 GB) é menor que o valor mínimo otimizado para todos os volumes

naquele nó (11 GB). Se você continuar usando a configuração personalizada, o nó poderá ficar com pouco espaço antes de poder fazer a transição segura para o estado somente leitura.

Resolva o alerta

Siga estas etapas se um ou mais alertas de **Substituição de marca d'água somente leitura baixa** tiverem sido acionados. Você também pode usar estas instruções se atualmente usa configurações de marca d'água personalizadas e deseja começar a usar configurações otimizadas mesmo que nenhum alerta tenha sido acionado.

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"](#) .

Sobre esta tarefa

Você pode resolver o alerta **Substituição de marca d'água somente leitura baixa** atualizando as configurações de marca d'água personalizadas para as novas substituições de marca d'água. No entanto, se um ou mais nós de armazenamento estiverem quase cheios ou se você tiver requisitos especiais de ILM, primeiro você deve visualizar as marcas d'água de armazenamento otimizadas e determinar se é seguro usá-las.

Avalie o uso de dados do objeto para toda a grade

Passos

1. Selecione **NODES**.
2. Para cada site na grade, expanda a lista de nós.
3. Revise os valores percentuais mostrados na coluna **Dados do objeto usados** para cada nó de armazenamento em cada site.

Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 13

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID	Grid	61%	4%	—
▲ Data Center 1	Site	56%	3%	—
DC1-ADM	Primary Admin Node	—	—	6%
DC1-GW	Gateway Node	—	—	1%
! DC1-SN1	Storage Node	71%	3%	30%
! DC1-SN2	Storage Node	25%	3%	42%
! DC1-SN3	Storage Node	63%	3%	42%
! DC1-SN4	Storage Node	65%	3%	41%

4. Siga o passo apropriado:

- Se nenhum dos nós de armazenamento estiver quase cheio (por exemplo, todos os valores de **Dados do objeto usados** forem inferiores a 80%), você poderá começar a usar as configurações de substituição. Vá para [Use marcas d'água otimizadas](#).
- Se as regras do ILM usarem o comportamento de ingestão estrito ou se pools de armazenamento específicos estiverem quase cheios, execute as etapas em [Exibir marcas d'água de armazenamento otimizadas](#) e [Determine se você pode usar marcas d'água otimizadas](#).

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.

Passos

- Selecione **SUORTE > Ferramentas > Métricas**.
- Na seção Prometheus, selecione o link para acessar a interface do usuário do Prometheus.
- 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.

5. Observe o valor máximo otimizado para cada nó de armazenamento.

Determine se você pode usar marcas d'água otimizadas

Passos

1. Selecione **NODES**.
2. Repita estas etapas para cada nó de armazenamento on-line:
 - a. Selecione **Nó de armazenamento > Armazenamento**.
 - b. Role para baixo até a tabela Object Stores.
 - c. Compare o valor **Disponível** para cada armazenamento de objetos (volume) com a marca d'água máxima otimizada que você anotou para esse Nó de Armazenamento.
3. Se pelo menos um volume em cada nó de armazenamento on-line tiver mais espaço disponível do que a marca d'água otimizada máxima para esse nó, vá para [Use marcas d'água otimizadas](#) para começar a usar as marcas d'água otimizadas.

Caso contrário, expanda a grade o mais rápido possível. Qualquer ["adicionar volumes de armazenamento"](#) para um nó existente ou ["adicionar novos nós de armazenamento"](#). Então vá para [Use marcas d'água otimizadas](#) para atualizar as configurações da marca d'água.

4. Se você precisar continuar usando valores personalizados para as marcas d'água do volume de armazenamento, ["silêncio"](#) ou ["desabilitar"](#) o alerta **Substituição de marca d'água somente leitura baixa**.



Os mesmos valores de marca d'água personalizados são aplicados a cada volume de armazenamento em cada nó de armazenamento. Usar valores menores que os recomendados para marcas d'água de volume de armazenamento pode fazer com que alguns volumes de armazenamento se tornem inacessíveis (desmontados automaticamente) quando o nó atingir a capacidade.

Use marcas d'água otimizadas

Passos

1. Vá para **SUPORTE > Outros > Marcas d'água de armazenamento**.
2. Marque a caixa de seleção **Usar valores otimizados**.
3. Selecione **Salvar**.

As configurações otimizadas de marca d'água do volume de armazenamento agora estão em vigor para cada volume de armazenamento, com base no tamanho do nó de armazenamento e na capacidade relativa do volume.

Solucionar problemas de metadados

Se ocorrerem problemas de metadados, os alertas informarão a origem dos problemas e as ações recomendadas a serem tomadas. Em particular, você deve adicionar novos nós de armazenamento se o alerta de armazenamento de metadados baixo for acionado.

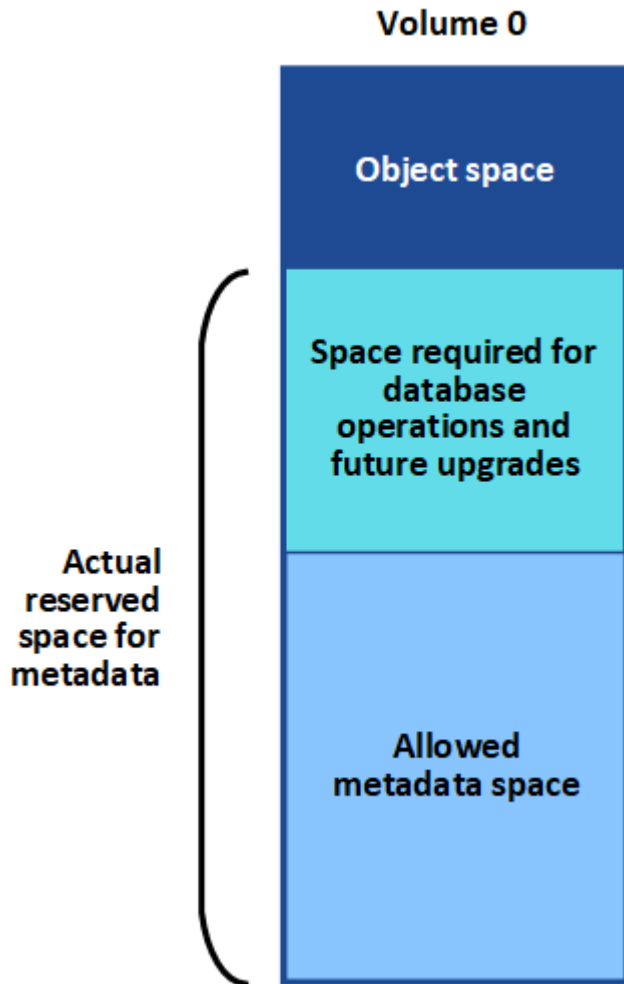
Antes de começar

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

Sobre esta tarefa

Siga as ações recomendadas para cada alerta relacionado a metadados que for acionado. Se o alerta **Armazenamento de metadados baixo** for acionado, você deverá adicionar novos Nós de Armazenamento.

O StorageGRID reserva uma certa quantidade de espaço no volume 0 de cada nó de armazenamento para metadados de objetos. Este espaço, conhecido como *espaço reservado real*, é subdividido no espaço permitido para metadados de objetos (o espaço de metadados permitido) e no espaço necessário para operações essenciais do banco de dados, como compactação e reparo. O espaço de metadados permitido controla a capacidade geral do objeto.



Se os metadados do objeto consumirem mais de 100% do espaço permitido para metadados, as operações do banco de dados não poderão ser executadas com eficiência e ocorrerão erros.

Você pode ["monitorar a capacidade de metadados do objeto para cada nó de armazenamento"](#) para ajudar você a antecipar erros e corrigi-los antes que eles ocorram.

O StorageGRID usa a seguinte métrica do Prometheus para medir o quão cheio está o espaço de metadados permitido:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Quando essa expressão do Prometheus atinge certos limites, o alerta **Armazenamento de metadados baixo** é acionado.

- **Menor:** Os metadados do objeto estão usando 70% ou mais do espaço de metadados permitido. Você deve adicionar novos nós de armazenamento o mais rápido possível.
- **Principal:** Os metadados do objeto estão usando 90% ou mais do espaço de metadados permitido. Você deve adicionar novos nós de armazenamento imediatamente.



Quando os metadados do objeto estão usando 90% ou mais do espaço de metadados permitido, um aviso aparece no painel. Se esse aviso aparecer, você deverá adicionar novos Nós de Armazenamento imediatamente. Você nunca deve permitir que metadados de objetos usem mais de 100% do espaço permitido.

- **Crítico:** Os metadados do objeto estão usando 100% ou mais do espaço de metadados permitido e estão começando a consumir o espaço necessário para operações essenciais do banco de dados. Você deve interromper a ingestão de novos objetos e adicionar novos Nós de Armazenamento imediatamente.



Se o tamanho do volume 0 for menor que a opção de armazenamento Espaço Reservado de Metadados (por exemplo, em um ambiente de não produção), o cálculo do alerta **Armazenamento de metadados baixo** poderá ser impreciso.

Passos

1. Selecione **ALERTAS > Atual**.
2. Na tabela de alertas, expanda o grupo de alertas **Armazenamento de metadados baixo**, se necessário, e selecione o alerta específico que deseja visualizar.
3. Revise os detalhes na caixa de diálogo de alerta.
4. Se um alerta importante ou crítico de **Baixo armazenamento de metadados** for acionado, execute uma expansão para adicionar nós de armazenamento imediatamente.



Como o StorageGRID mantém cópias completas de todos os metadados do objeto em cada site, a capacidade de metadados de toda a grade é limitada pela capacidade de metadados do menor site. Se você precisar adicionar capacidade de metadados a um site, você também deve [expandir quaisquer outros sites](#) pelo mesmo número de nós de armazenamento.

Depois de executar a expansão, o StorageGRID redistribui os metadados do objeto existentes para os novos nós, o que aumenta a capacidade geral de metadados da grade. Nenhuma ação do usuário é necessária. O alerta **Baixo armazenamento de metadados** foi removido.

Solucionar erros de certificado

Se você observar um problema de segurança ou de certificado ao tentar se conectar ao

StorageGRID usando um navegador da Web, um cliente S3 ou uma ferramenta de monitoramento externa, verifique o certificado.

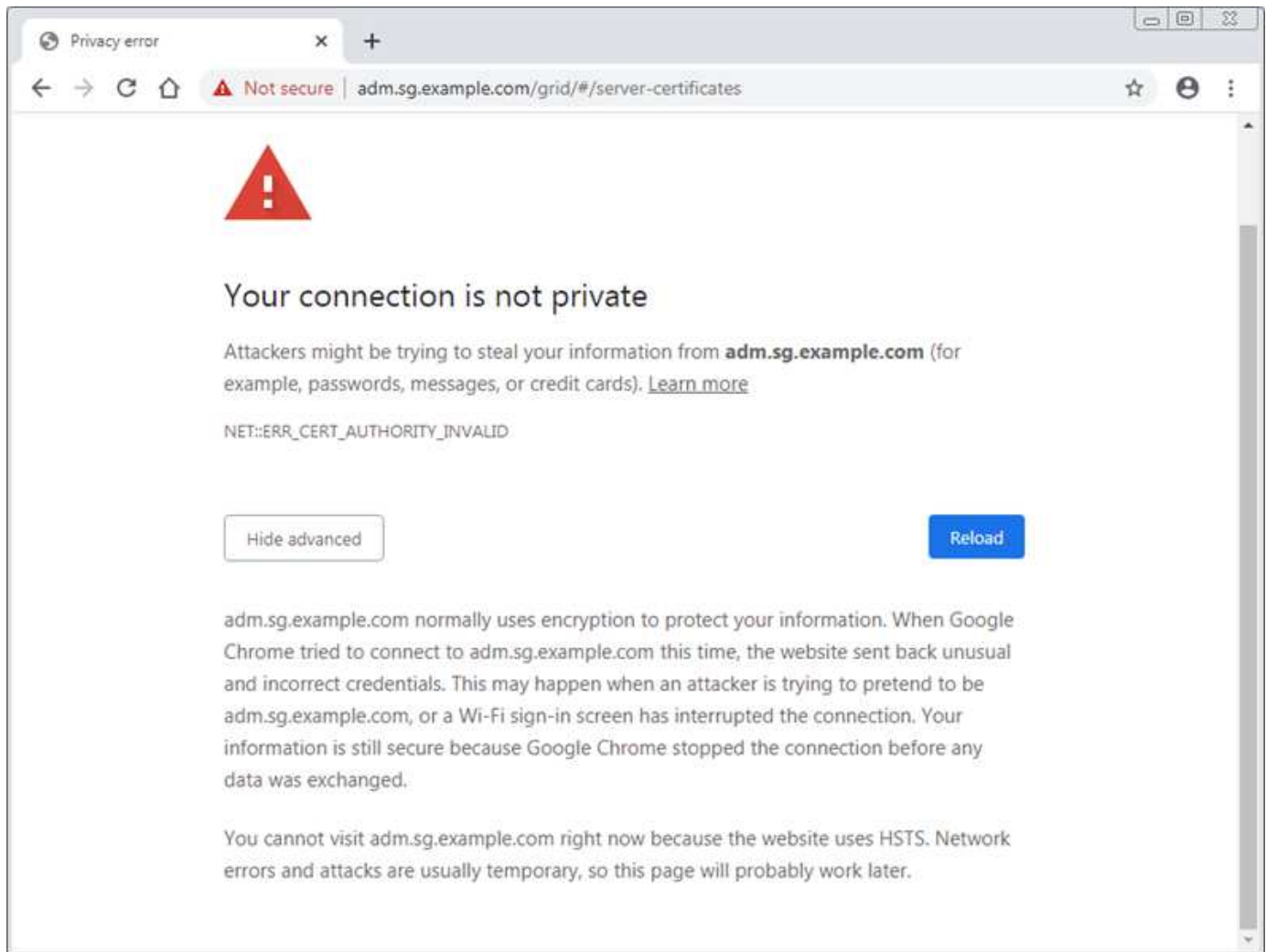
Sobre esta tarefa

Erros de certificado podem causar problemas quando você tenta se conectar ao StorageGRID usando o Grid Manager, a Grid Management API, o Tenant Manager ou a Tenant Management API. Erros de certificado também podem ocorrer quando você tenta se conectar a um cliente S3 ou a uma ferramenta de monitoramento externa.

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 reverte de um certificado de interface de gerenciamento personalizado para o certificado de servidor padrão.

O exemplo a seguir mostra um erro de certificado quando o certificado da interface de gerenciamento personalizada expirou:



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 o certificado do servidor está prestes a expirar.

Ao usar certificados de cliente para integração externa do Prometheus, erros de certificado podem ser causados pelo certificado da interface de gerenciamento do StorageGRID ou por certificados de cliente. O alerta **Expiração de certificados de cliente configurados na página Certificados** é acionado quando um certificado de cliente está prestes a expirar.

Passos

Se você recebeu uma notificação de alerta sobre um certificado expirado, acesse os detalhes do certificado: .
Selecione **CONFIGURAÇÃO > Segurança > Certificados** e então "[selecione a aba de certificado apropriada](#)" .

1. Verifique o período de validade do certificado. + Alguns navegadores da Web e clientes S3 não aceitam certificados com período de validade superior a 398 dias.
2. Se o certificado expirou ou irá expirar em breve, carregue ou gere um novo certificado.
 - Para um certificado de servidor, consulte as etapas para "[configurando um certificado de servidor personalizado para o Grid Manager e o Tenant Manager](#)" .
 - Para um certificado de cliente, consulte as etapas para "[configurando um certificado de cliente](#)" .
3. Para erros de certificado de servidor, tente uma ou ambas as opções a seguir:
 - Certifique-se de que o Nome Alternativo do Assunto (SAN) do certificado esteja preenchido e que o SAN corresponda ao endereço IP ou nome do host do nó ao qual você está se conectando.
 - Se você estiver tentando se conectar ao StorageGRID usando um nome de domínio:
 - i. Digite o endereço IP do nó de administração em vez do nome de domínio para ignorar o erro de conexão e acessar o Grid Manager.
 - ii. No Grid Manager, selecione **CONFIGURAÇÃO > Segurança > Certificados** e então "[selecione a aba de certificado apropriada](#)" para instalar um novo certificado personalizado ou continuar com o certificado padrão.
 - iii. Nas instruções para administrar o StorageGRID, veja as etapas para "[configurando um certificado de servidor personalizado para o Grid Manager e o Tenant Manager](#)" .

Solucionar problemas do nó de administração e da interface do usuário

Você pode executar várias tarefas para ajudar a determinar a origem dos problemas relacionados aos nós de administração e à interface do usuário do StorageGRID .

Erros de login do nó de administração

Se você tiver um erro ao fazer login em um nó de administração do StorageGRID , seu sistema pode ter um problema com um "[rede](#)" ou "[ferragens](#)" problema, uma questão com "[Serviços do nó de administração](#)" , ou um "[problema com o banco de dados Cassandra](#)" em nós de armazenamento conectados.

Antes de começar

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

Sobre esta tarefa

Use estas diretrizes de solução de problemas se você vir alguma das seguintes mensagens de erro ao tentar fazer login em um nó de administração:

- Your credentials for this account were invalid. Please try again.
- Waiting for services to start...
- Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.
- Unable to communicate with server. Reloading page...

Passos

1. Aguarde 10 minutos e tente fazer login novamente.

Se o erro não for resolvido automaticamente, vá para a próxima etapa.

2. Se o seu sistema StorageGRID tiver mais de um nó de administração, tente fazer login no Grid Manager de outro nó de administração para verificar o status de um nó de administração indisponível.
 - Se você conseguir fazer login, poderá usar as opções **Painel**, **NÓS**, **Alertas** e **SUPORTE** para ajudar a determinar a causa do erro.
 - Se você tiver apenas um nó de administração ou ainda não conseguir fazer login, vá para a próxima etapa.
3. Determine se o hardware do nó está offline.
4. Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID , consulte as etapas para "[configurando logon único](#)".

Pode ser necessário desabilitar e reabilitar temporariamente o SSO para um único nó de administração para resolver quaisquer problemas.



Se o SSO estiver habilitado, você não poderá fazer logon usando uma porta restrita. Você deve usar a porta 443.

5. Determine se a conta que você está usando pertence a um usuário federado.

Se a conta de usuário federada não estiver funcionando, tente entrar no Grid Manager como um usuário local, como root.

- Se o usuário local puder efetuar login:
 - i. Revisar alertas.
 - ii. Selecione **CONFIGURAÇÃO > Controle de acesso > Federação de identidade**.
 - iii. Clique em **Testar conexão** para validar suas configurações de conexão para o servidor LDAP.
 - iv. Se o teste falhar, resolva quaisquer erros de configuração.
 - Se o usuário local não conseguir fazer login e você tiver certeza de que as credenciais estão corretas, vá para a próxima etapa.
6. Use o Secure Shell (ssh) para efetuar login no 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 # .

7. Visualize o status de todos os serviços em execução no nó da grade: `storagegrid-status`

Certifique-se de que os serviços de API nms, mi, nginx e mgmt estejam todos em execução.

A saída é atualizada imediatamente se o status de um serviço mudar.

```
$ storagegrid-status
Host Name                99-211
IP Address                10.96.99.211
Operating System Kernel  4.19.0                Verified
Operating System Environment Debian 10.1            Verified
StorageGRID Webscale Release 11.4.0                Verified
Networking                Verified
Storage Subsystem        Verified
Database Engine           5.5.9999+default Running
Network Monitoring        11.4.0                Running
Time Synchronization      1:4.2.8p10+dfsg Running
ams                        11.4.0                Running
cmn                        11.4.0                Running
nms                        11.4.0                Running
ssm                        11.4.0                Running
mi                         11.4.0                Running
dynip                     11.4.0                Running
nginx                     1.10.3                Running
tomcat                    9.0.27                Running
grafana                   6.4.3                Running
mgmt api                  11.4.0                Running
prometheus                11.4.0                Running
persistence               11.4.0                Running
ade exporter              11.4.0                Running
alertmanager              11.4.0                Running
attrDownPurge             11.4.0                Running
attrDownSamp1             11.4.0                Running
attrDownSamp2             11.4.0                Running
node exporter              0.17.0+ds             Running
sg snmp agent             11.4.0                Running
```

8. Confirme se o serviço nginx-gw está em execução # `service nginx-gw status`

9. Use o Lumberjack para coletar toras: # `/usr/local/sbin/lumberjack.rb`

Se a autenticação com falha ocorreu no passado, você pode usar as opções de script `--start` e `--end` do Lumberjack para especificar o intervalo de tempo apropriado. Use `lumberjack -h` para obter detalhes sobre essas opções.

A saída para o terminal indica onde o arquivo de log foi copiado.

10. Revise os seguintes logs:

- `/var/local/log/bycast.log`
- `/var/local/log/bycast-err.log`
- `/var/local/log/nms.log`
- `**/*commands.txt`

11. Se você não conseguir identificar nenhum problema com o nó de administração, emita um dos seguintes comandos para determinar os endereços IP dos três nós de armazenamento que executam o serviço ADC no seu site. Normalmente, esses são os três primeiros nós de armazenamento instalados no local.

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

Os nós de administração usam o serviço ADC durante o processo de autenticação.

12. No nó de administração, use ssh para efetuar login em cada um dos nós de armazenamento do ADC, usando os endereços IP que você identificou.

13. Visualize o status de todos os serviços em execução no nó da grade: `storagegrid-status`

Certifique-se de que os serviços `idnt`, `acct`, `nginx` e `cassandra` estejam todos em execução.

14. Repita os passos [Use o Lenhador para coletar toras](#) e [Registros de revisão](#) para revisar os logs nos nós de armazenamento.

15. Se você não conseguir resolver o problema, entre em contato com o suporte técnico.

Forneça os logs coletados ao suporte técnico. Veja também ["Referência de arquivos de log"](#) .

Problemas de interface do usuário

A interface do usuário do Grid Manager ou do Tenant Manager pode não responder conforme o esperado após a atualização do software StorageGRID .

Passos

1. Certifique-se de que você está usando um ["navegador da web compatível"](#) .
2. Limpe o cache do seu navegador.

Limpar o cache remove recursos desatualizados usados pela versão anterior do software StorageGRID e permite que a interface do usuário opere corretamente novamente. Para obter instruções, consulte a documentação do seu navegador.

Solucionar problemas de rede, hardware e plataforma

Há várias tarefas que você pode executar para ajudar a determinar a origem dos problemas relacionados à rede, hardware e plataforma do StorageGRID .

Erros "422: Entidade não processável"

O erro 422: Entidade não processável pode ocorrer por diferentes motivos. Verifique a mensagem de erro para determinar o que causou o problema.

Se você vir uma das mensagens de erro listadas, tome a ação recomendada.

Mensagem de erro	Causa raiz e ação corretiva
422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839	Esta mensagem pode ocorrer se você selecionar a opção Não usar TLS para Segurança da Camada de Transporte (TLS) ao configurar a federação de identidade usando o Windows Active Directory (AD). O uso da opção Não usar TLS não é suportado para uso com servidores AD que impõem assinatura LDAP. Você deve selecionar a opção Usar STARTTLS ou a opção Usar LDAPS para TLS.

Mensagem de erro	Causa raiz e ação corretiva
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)</pre>	Esta mensagem aparece se você tentar usar uma cifra não suportada para fazer uma conexão TLS (Transport Layer Security) do StorageGRID para um sistema externo usado para identificar federações ou pools de armazenamento em nuvem. Verifique as cifras oferecidas pelo sistema externo. O sistema deve utilizar um dos cifras suportadas pelo StorageGRID para conexões TLS de saída, conforme mostrado nas instruções para administrar o StorageGRID.

Alerta de incompatibilidade de MTU da rede de grade

O alerta **Incompatibilidade de MTU da rede de grade** é acionado quando a configuração da unidade máxima de transmissão (MTU) para a interface da rede de grade (eth0) difere significativamente entre os nós da grade.

Sobre esta tarefa

As diferenças nas configurações de MTU podem indicar que algumas, mas não todas, redes eth0 estão configuradas para quadros jumbo. Uma incompatibilidade de tamanho de MTU maior que 1000 pode causar problemas de desempenho de rede.

Passos

1. Liste as configurações de MTU para eth0 em todos os nós.
 - Use a consulta fornecida no Grid Manager.
 - Navegar para *primary Admin Node IP address/metrics/graph* e insira a seguinte consulta: `node_network_mtu_bytes{device="eth0"}`
2. ["Modificar as configurações de MTU"](#) conforme necessário para garantir que sejam os mesmos para a interface da rede Grid (eth0) em todos os nós.
 - Para nós baseados em Linux e VMware, use o seguinte comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

Exemplo: `change-ip.py -n node 1500 grid admin`

Observação: Em nós baseados em Linux, se o valor de MTU desejado para a rede no contêiner exceder o valor já configurado na interface do host, você deve primeiro configurar a interface do host para ter o valor de MTU desejado e, em seguida, usar o `change-ip.py` script para alterar o valor de MTU da rede no contêiner.

Use os seguintes argumentos para modificar a MTU em nós baseados em Linux ou VMware.

Argumentos posicionais	Descrição
<code>mtu</code>	A MTU a ser definida. Deve estar no intervalo de 1280 a 9216.
<code>network</code>	As redes às quais a MTU será aplicada. Inclua um ou mais dos seguintes tipos de rede: • grade • administrador • cliente

+

Argumentos opcionais	Descrição
<code>-h, - help</code>	Mostrar a mensagem de ajuda e sair.
<code>-n node, --node node</code>	O nó. O padrão é o nó local.

Alerta de erro de quadro de recepção de rede de nó

Alertas de **Erro de quadro de recepção de rede de nó** podem ser causados por problemas de conectividade entre o StorageGRID e seu hardware de rede. Este alerta desaparece sozinho depois que o problema subjacente é resolvido.

Sobre esta tarefa

Os alertas de **Erro de quadro de recepção de rede de nó** podem ser causados pelos seguintes problemas com o hardware de rede que se conecta ao StorageGRID:

- A correção de erros antecipada (FEC) é necessária e não está em uso
- Incompatibilidade de porta do switch e MTU da placa de rede
- Altas taxas de erro de link
- Estouro do buffer de anel da placa de rede

Passos

1. Siga as etapas de solução de problemas para todas as possíveis causas desse alerta, de acordo com sua configuração de rede.
2. Execute as seguintes etapas dependendo da causa do erro:

Incompatibilidade de FEC



Essas etapas são aplicáveis somente para alertas de **Erro de quadro de recepção de rede de nó** causados por incompatibilidade de FEC em dispositivos StorageGRID .

- a. Verifique o status FEC da porta no switch conectado ao seu dispositivo StorageGRID .
- b. Verifique a integridade física dos cabos do aparelho até o switch.
- c. Se você quiser alterar as configurações do FEC para tentar resolver o alerta, primeiro certifique-se de que o dispositivo esteja configurado para o modo **Automático** na página Configuração de link do instalador do dispositivo StorageGRID (consulte as instruções para seu dispositivo):
 - "SG6160"
 - "SGF6112"
 - "SG6000"
 - "SG5800"
 - "SG5700"
 - "SG110 e SG1100"
 - "SG100 e SG1000"
- d. Altere as configurações de FEC nas portas do switch. As portas do dispositivo StorageGRID ajustarão suas configurações de FEC para corresponder, se possível.

Não é possível configurar as definições do FEC em dispositivos StorageGRID . Em vez disso, os dispositivos tentam descobrir e espelhar as configurações de FEC nas portas do switch às quais estão conectados. Se os links forem forçados a velocidades de rede de 25 GbE ou 100 GbE, o switch e a NIC podem falhar ao negociar uma configuração FEC comum. Sem uma configuração FEC comum, a rede retornará ao modo "sem FEC". Quando o FEC não está habilitado, as conexões ficam mais suscetíveis a erros causados por ruído elétrico.



Os dispositivos StorageGRID são compatíveis com Firecode (FC) e Reed Solomon (RS) FEC, além de nenhum FEC.

Incompatibilidade de porta do switch e MTU da placa de rede

Se o alerta for causado por uma incompatibilidade de MTU entre a porta do switch e a NIC, verifique se o tamanho da MTU configurado no nó é o mesmo que a configuração de MTU para a porta do switch.

O tamanho da MTU configurado no nó pode ser menor que a configuração na porta do switch à qual o nó está conectado. Se um nó StorageGRID receber um quadro Ethernet maior que sua MTU, o que é possível com essa configuração, o alerta **Erro de quadro de recepção de rede do nó** poderá ser relatado. Se você acredita que isso é o que está acontecendo, altere a MTU da porta do switch para corresponder à MTU da interface de rede StorageGRID ou altere a MTU da interface de rede StorageGRID para corresponder à porta do switch, dependendo de suas metas ou requisitos de MTU de ponta a ponta.



Para obter o melhor desempenho da rede, todos os nós devem ser configurados com valores de MTU semelhantes em suas interfaces de rede de grade. O alerta **Incompatibilidade de MTU da rede de grade** é acionado se houver uma diferença significativa nas configurações de MTU da rede de grade em nós individuais. Os valores de MTU não precisam ser os mesmos para todos os tipos de rede. Ver [Solucionar problemas de alerta de incompatibilidade de MTU da rede de grade](#) para maiores informações.



Veja também ["Alterar configuração de MTU"](#) .

Altas taxas de erro de link

- Habilite o FEC, caso ainda não esteja habilitado.
- Verifique se o cabeamento da sua rede é de boa qualidade e não está danificado ou conectado incorretamente.
- Se os cabos não parecerem ser o problema, entre em contato com o suporte técnico.



Você pode notar altas taxas de erro em um ambiente com alto ruído elétrico.

Estouro do buffer de anel da placa de rede

Se o erro for um estouro do buffer de anel da NIC, entre em contato com o suporte técnico.

O buffer de anel pode ser estourado quando o sistema StorageGRID está sobrecarregado e não consegue processar eventos de rede em tempo hábil.

- Monitore o problema e entre em contato com o suporte técnico se o alerta não for resolvido.

Erros de sincronização de tempo

Você pode ver problemas com a sincronização de tempo na sua grade.

Se você encontrar problemas de sincronização de tempo, verifique se especificou pelo menos quatro fontes NTP externas, cada uma fornecendo uma referência Stratum 3 ou melhor, e se todas as fontes NTP externas estão operando normalmente e são acessíveis pelos seus nós StorageGRID .



Quando ["especificando a fonte NTP externa"](#) para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft para uso em ambientes de alta precisão, como o StorageGRID.

Linux: Problemas de conectividade de rede

Você pode ver problemas com a conectividade de rede para nós do StorageGRID hospedados em hosts Linux.

Clonagem de endereço MAC

Em alguns casos, problemas de rede podem ser resolvidos usando clonagem de endereço MAC. Se você estiver usando hosts virtuais, defina o valor da chave de clonagem de endereço MAC para cada uma das suas redes como "true" no arquivo de configuração do nó. Esta configuração faz com que o endereço MAC do

contêiner StorageGRID use o endereço MAC do host. Para criar arquivos de configuração de nó, consulte as instruções para ["Red Hat Enterprise Linux"](#) ou ["Ubuntu ou Debian"](#) .



Crie interfaces de rede virtuais separadas para uso pelo sistema operacional host Linux. Usar as mesmas interfaces de rede para o sistema operacional host Linux e o contêiner StorageGRID pode fazer com que o sistema operacional host fique inacessível se o modo promíscuo não estiver habilitado no hipervisor.

Para obter mais informações sobre como habilitar a clonagem de MAC, consulte as instruções para ["Red Hat Enterprise Linux"](#) ou ["Ubuntu ou Debian"](#) .

Modo promíscuo

Se você não quiser usar a clonagem de endereço MAC e preferir permitir que todas as interfaces recebam e transmitam dados para endereços MAC diferentes daqueles atribuídos pelo hipervisor, certifique-se de que as propriedades de segurança nos níveis de switch virtual e grupo de portas estejam definidas como **Aceitar** para Modo Promíscuo, Alterações de Endereço MAC e Transmissões Falsificadas. Os valores definidos no switch virtual podem ser substituídos pelos valores no nível do grupo de portas, portanto, certifique-se de que as configurações sejam as mesmas em ambos os locais.

Para obter mais informações sobre o uso do Modo Promíscuo, consulte as instruções para ["Red Hat Enterprise Linux"](#) ou ["Ubuntu ou Debian"](#) .

Linux: o status do nó é "órfão"

Um nó Linux em estado órfão geralmente indica que o serviço storagegrid ou o daemon do nó StorageGRID que controla o contêiner do nó morreu inesperadamente.

Sobre esta tarefa

Se um nó Linux relatar que está em um estado órfão, você deve:

- Verifique os logs em busca de erros e mensagens.
- Tente iniciar o nó novamente.
- Se necessário, use comandos do mecanismo de contêiner para parar o contêiner do nó existente.
- Reinicie o nó.

Passos

1. Verifique os logs do daemon de serviço e do nó órfão em busca de erros óbvios ou mensagens sobre saída inesperada.
2. Efetue login no host como root ou use uma conta com permissão sudo.
3. Tente iniciar o nó novamente executando o seguinte comando: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Se o nó for órfão, a resposta é

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. No Linux, pare o mecanismo de contêiner e quaisquer processos de controle do storagegrid-node. Por exemplo: `sudo docker stop --time secondscontainer-name`

Para `seconds`, insira o número de segundos que você deseja esperar para que o contêiner pare (normalmente 15 minutos ou menos). Por exemplo:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Reinicie o nó: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux: Solucionar problemas de suporte a IPv6

Talvez seja necessário habilitar o suporte a IPv6 no kernel se você tiver instalado nós StorageGRID em hosts Linux e perceber que endereços IPv6 não foram atribuídos aos contêineres de nós conforme o esperado.

Sobre esta tarefa

Para ver o endereço IPv6 que foi atribuído a um nó de grade:

1. Selecione **NÓS** e selecione o nó.
2. Selecione **Mostrar endereços IP adicionais** ao lado de **Endereços IP** na guia Visão geral.

Se o endereço IPv6 não for exibido e o nó estiver instalado em um host Linux, siga estas etapas para habilitar o suporte a IPv6 no kernel.

Passos

1. Efetue login no host como root ou use uma conta com permissão sudo.
2. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

O resultado deve ser 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Se o resultado não for 0, consulte a documentação do seu sistema operacional para alterar `sysctl` configurações. Em seguida, altere o valor para 0 antes de continuar.

3. Digite o contêiner do nó StorageGRID: `storagegrid node enter node-name`
4. Execute o seguinte comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

O resultado deve ser 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```



Se o resultado não for 1, este procedimento não se aplica. Entre em contato com o suporte técnico.

5. Sair do contêiner: `exit`

```
root@DC1-S1:~ # exit
```

6. Como root, edite o seguinte arquivo: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Localize as duas linhas a seguir e remova as tags de comentário. Em seguida, salve e feche o arquivo.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Execute estes comandos para reiniciar o contêiner StorageGRID :

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Solucionar problemas de um servidor syslog externo

A tabela a seguir descreve as mensagens de erro que podem estar relacionadas ao uso de um servidor syslog externo e lista as ações corretivas.

Esses erros são exibidos pelo assistente Configurar servidor syslog externo se você tiver problemas para enviar mensagens de teste para validar se o servidor syslog externo está configurado corretamente.

Problemas em tempo de execução podem ser relatados pelo ["Erro de encaminhamento do servidor syslog"](#)

[externo](#)" alerta. Se você receber este alerta, siga as instruções no alerta para reenviar as mensagens de teste para que você possa obter mensagens de erro detalhadas.

Para obter mais informações sobre como enviar informações de auditoria para um servidor syslog externo, consulte:

- ["Considerações para usar um servidor syslog externo"](#)
- ["Configurar mensagens de auditoria e servidor syslog externo"](#)

Mensagem de erro	Descrição e ações recomendadas
Não é possível resolver o nome do host	O FQDN inserido para o servidor syslog não pôde ser resolvido para um endereço IP. 1. Verifique o nome do host que você digitou. Se você inseriu um endereço IP, certifique-se de que seja um endereço IP válido na notação WXYZ ("decimal com ponto"). 2. Verifique se os servidores DNS estão configurados corretamente. 3. Confirme se cada nó pode acessar os endereços IP do servidor DNS.
Ligação recusada	Uma conexão TCP ou TLS com o servidor syslog foi recusada. Pode não haver nenhum serviço escutando na porta TCP ou TLS do host, ou um firewall pode estar bloqueando o acesso. 1. Verifique se você inseriu o FQDN ou endereço IP, a porta e o protocolo corretos para o servidor syslog. 2. Confirme se o host do serviço syslog está executando um daemon syslog que está escutando na porta especificada. 3. Confirme se um firewall não está bloqueando o acesso às conexões TCP/TLS dos nós ao IP e à porta do servidor syslog.
Rede inacessível	O servidor syslog não está em uma sub-rede conectada diretamente. Um roteador retornou uma mensagem de falha de ICMP para indicar que não conseguiu encaminhar as mensagens de teste dos nós listados para o servidor syslog. 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Para cada nó listado, verifique a Lista de sub-redes da rede de grade, as Listas de sub-redes das redes de administração e os gateways da rede do cliente. Confirme se eles estão configurados para rotear o tráfego para o servidor syslog pela interface de rede e gateway esperados (Grid, Admin ou Cliente).

Mensagem de erro	Descrição e ações recomendadas
Host inacessível	O servidor syslog está em uma sub-rede conectada diretamente (sub-rede usada pelos nós listados para seus endereços IP de grade, administrador ou cliente). Os nós tentaram enviar mensagens de teste, mas não receberam respostas às solicitações ARP para o endereço MAC do servidor syslog. 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Verifique se o host que executa o serviço syslog está ativo.
Tempo de conexão esgotado	Uma tentativa de conexão TCP/TLS foi feita, mas nenhuma resposta foi recebida do servidor syslog por um longo tempo. Pode haver uma configuração incorreta de roteamento ou um firewall pode estar descartando tráfego sem enviar nenhuma resposta (uma configuração comum). 1. Verifique se você inseriu o FQDN ou endereço IP correto para o servidor syslog. 2. Para cada nó listado, verifique a Lista de sub-redes da rede de grade, as Listas de sub-redes das redes de administração e os gateways da rede do cliente. Confirme se eles estão configurados para rotear o tráfego para o servidor syslog usando a interface de rede e o gateway (Grid, Admin ou Cliente) pelos quais você espera que o servidor syslog seja alcançado. 3. Confirme se um firewall não está bloqueando o acesso às conexões TCP/TLS dos nós listados para o IP e a porta do servidor syslog.
Conexão fechada pelo parceiro	Uma conexão TCP com o servidor syslog foi estabelecida com sucesso, mas foi fechada posteriormente. Os motivos para isso podem incluir: • O servidor syslog pode ter sido reiniciado ou reinicializado. • O nó e o servidor syslog podem ter configurações TCP/TLS diferentes. • Um firewall intermediário pode estar fechando conexões TCP ociosas. • Um servidor não syslog escutando na porta do servidor syslog pode ter fechado a conexão. Para resolver esse problema: 1. Verifique se você inseriu o FQDN ou endereço IP, a porta e o protocolo corretos para o servidor syslog. 2. Se você estiver usando TLS, confirme se o servidor syslog também está usando TLS. Se você estiver usando TCP, confirme se o servidor syslog também está usando TCP. 3. Verifique se um firewall intermediário não está configurado para fechar conexões TCP ociosas.

Mensagem de erro	Descrição e ações recomendadas
Erro de certificado TLS	O certificado do servidor recebido do servidor syslog não era compatível com o pacote de certificados da CA e o certificado do cliente que você forneceu. 1. Confirme se o pacote de certificados da CA e o certificado do cliente (se houver) são compatíveis com o certificado do servidor no servidor syslog. 2. Confirme se as identidades no certificado do servidor do servidor syslog incluem os valores de IP ou FQDN esperados.
Encaminhamento suspenso	Os registros do Syslog não estão mais sendo encaminhados para o servidor Syslog e o StorageGRID não consegue detectar o motivo. Revise os logs de depuração fornecidos com este erro para tentar determinar a causa raiz.
Sessão TLS encerrada	O servidor syslog encerrou a sessão TLS e o StorageGRID não consegue detectar o motivo. 1. Revise os logs de depuração fornecidos com este erro para tentar determinar a causa raiz. 2. Verifique se você inseriu o FQDN ou endereço IP, a porta e o protocolo corretos para o servidor syslog. 3. Se você estiver usando TLS, confirme se o servidor syslog também está usando TLS. Se você estiver usando TCP, confirme se o servidor syslog também está usando TCP. 4. Confirme se o pacote de certificados da CA e o certificado do cliente (se houver) são compatíveis com o certificado do servidor do servidor syslog. 5. Confirme se as identidades no certificado do servidor do servidor syslog incluem os valores de IP ou FQDN esperados.
Falha na consulta de resultados	O nó de administração usado para configuração e teste do servidor syslog não consegue solicitar resultados de teste dos nós listados. Um ou mais nós podem estar inativos. 1. Siga as etapas padrão de solução de problemas para garantir que os nós estejam online e todos os serviços esperados estejam em execução. 2. Reinicie o serviço miscd nos nós listados.

Revisar logs de auditoria

Mensagens e logs de auditoria

Estas instruções contêm informações sobre a estrutura e o conteúdo das mensagens de auditoria e dos logs de auditoria do StorageGRID . Você pode usar essas informações para ler e analisar a trilha de auditoria da atividade do sistema.

Estas instruções são para administradores responsáveis por produzir relatórios de atividade e uso do sistema

que exigem análise das mensagens de auditoria do sistema StorageGRID .

Para usar o arquivo de log de texto, você deve ter acesso ao compartilhamento de auditoria configurado no nó de administração.

Para obter informações sobre como configurar níveis de mensagens de auditoria e usar um servidor syslog externo, consulte "[Configurar mensagens de auditoria e destinos de log](#)".

Fluxo e retenção de mensagens de auditoria

Todos os serviços do StorageGRID geram mensagens de auditoria durante a operação normal do sistema. Você deve entender como essas mensagens de auditoria se movem pelo sistema StorageGRID para o `audit.log` arquivo.

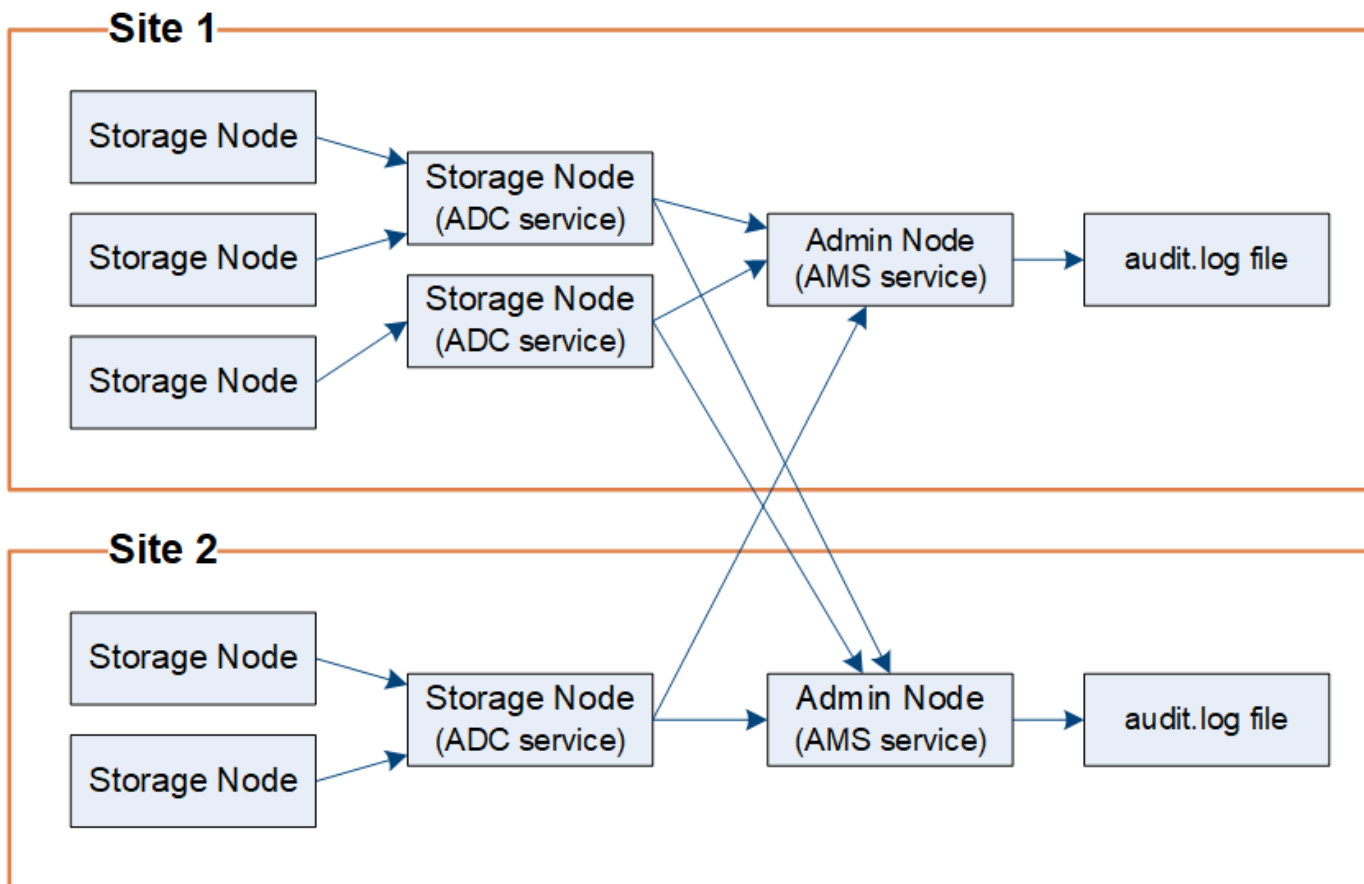
Fluxo de mensagens de auditoria

As mensagens de auditoria são processadas pelos nós de administração e pelos nós de armazenamento que têm um serviço de controlador de domínio administrativo (ADC).

Conforme mostrado no diagrama de fluxo de mensagens de auditoria, cada nó StorageGRID envia suas mensagens de auditoria para um dos serviços do ADC no site do data center. O serviço ADC é habilitado automaticamente para os três primeiros nós de armazenamento instalados em cada site.

Por sua vez, cada serviço ADC atua como um retransmissor e envia sua coleção de mensagens de auditoria para cada nó administrativo no sistema StorageGRID , o que fornece a cada nó administrativo um registro completo da atividade do sistema.

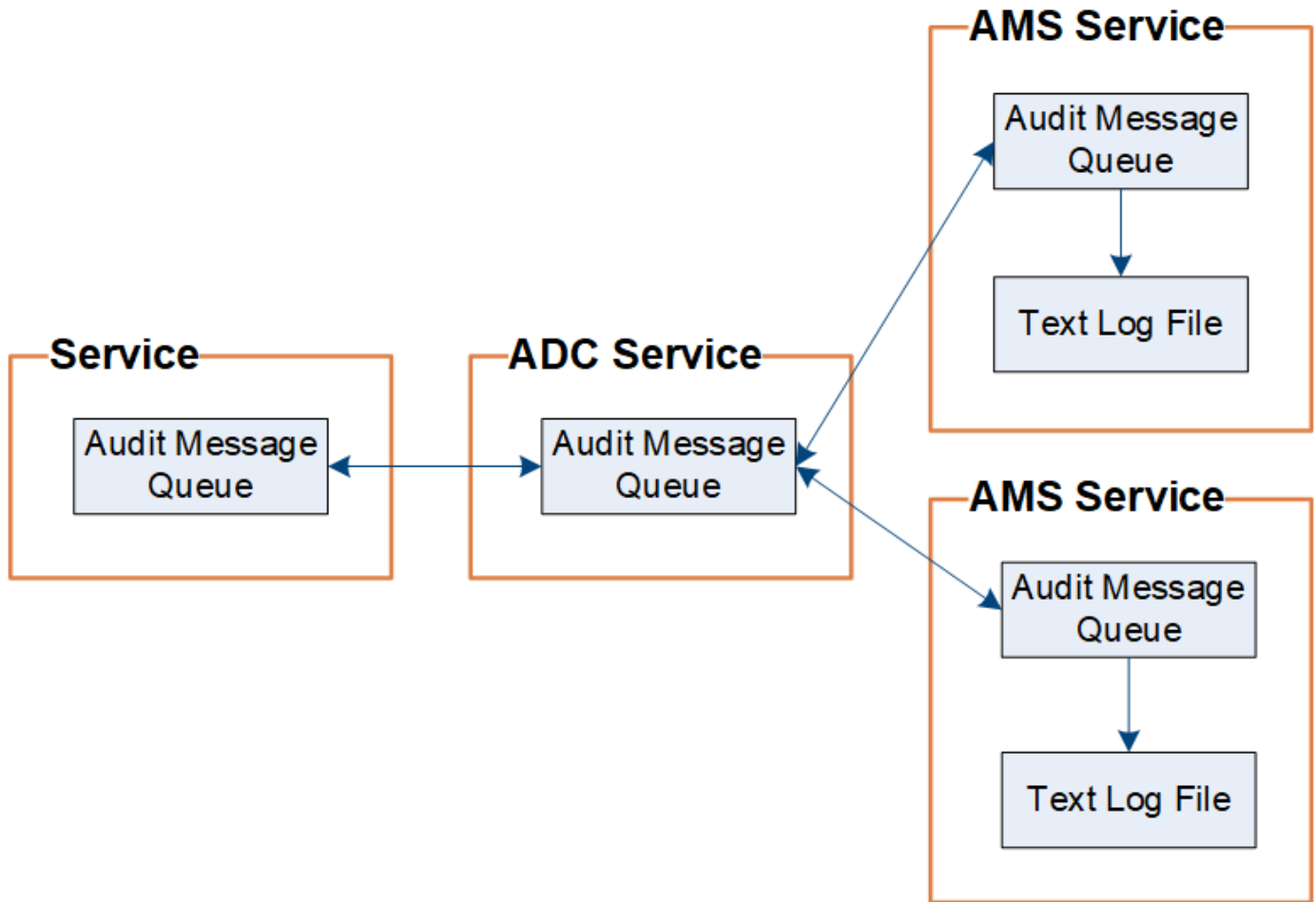
Cada nó de administração armazena mensagens de auditoria em arquivos de log de texto; o arquivo de log ativo é denominado `audit.log`.



Retenção de mensagens de auditoria

O StorageGRID usa um processo de copiar e excluir para garantir que nenhuma mensagem de auditoria seja perdida antes de ser gravada no log de auditoria.

Quando um nó gera ou retransmite uma mensagem de auditoria, a mensagem é armazenada em uma fila de mensagens de auditoria no disco do sistema do nó da grade. Uma cópia da mensagem é sempre mantida em uma fila de mensagens de auditoria até que a mensagem seja gravada no arquivo de log de auditoria no nó de administração. `/var/local/log` diretório. Isso ajuda a evitar a perda de uma mensagem de auditoria durante o transporte.



A fila de mensagens de auditoria pode aumentar temporariamente devido a problemas de conectividade de rede ou capacidade de auditoria insuficiente. À medida que as filas aumentam, elas consomem mais espaço disponível em cada nó `/var/local/` diretório. Se o problema persistir e o diretório de mensagens de auditoria de um nó ficar muito cheio, os nós individuais priorizarão o processamento de seu backlog e ficarão temporariamente indisponíveis para novas mensagens.

Especificamente, você pode ver os seguintes comportamentos:

- Se o `/var/local/log` o diretório usado por um nó de administração ficar cheio, o nó de administração será sinalizado como indisponível para novas mensagens de auditoria até que o diretório não esteja mais cheio. As solicitações do cliente S3 não são afetadas. O alarme XAMS (Repositórios de auditoria inacessíveis) é acionado quando um repositório de auditoria fica inacessível.
- Se o `/var/local/` o diretório usado por um nó de armazenamento com o serviço ADC ficar 92% cheio, o nó será sinalizado como indisponível para mensagens de auditoria até que o diretório esteja apenas 87% cheio. As solicitações do cliente S3 para outros nós não são afetadas. O alarme NRLY (Relés de auditoria disponíveis) é acionado quando os relés de auditoria estão inacessíveis.



Se não houver nós de armazenamento disponíveis com o serviço ADC, os nós de armazenamento armazenam as mensagens de auditoria localmente no `/var/local/log/localaudit.log` arquivo.

- Se o `/var/local/` diretório usado por um nó de armazenamento ficar 85% cheio, o nó começará a recusar solicitações de cliente S3 com `503 Service Unavailable`.

Os seguintes tipos de problemas podem fazer com que as filas de mensagens de auditoria fiquem muito grandes:

- A interrupção de um nó de administração ou de um nó de armazenamento com o serviço ADC. Se um dos nós do sistema estiver inativo, os nós restantes poderão ficar acumulados.
- Uma taxa de atividade sustentada que excede a capacidade de auditoria do sistema.
- O `/var/local/` espaço em um nó de armazenamento ADC ficando cheio por motivos não relacionados a mensagens de auditoria. Quando isso acontece, o nó para de aceitar novas mensagens de auditoria e prioriza seu backlog atual, o que pode causar backlogs em outros nós.

Alerta de fila de auditoria grande e alarme de mensagens de auditoria na fila (AMQS)

Para ajudar você a monitorar o tamanho das filas de mensagens de auditoria ao longo do tempo, o alerta **Fila de auditoria grande** e o alarme AMQS legado são acionados quando o número de mensagens em uma fila de nó de armazenamento ou fila de nó de administração atinge determinados limites.

Se o alerta **Grande fila de auditoria** ou o alarme AMQS legado for acionado, comece verificando a carga no sistema. Se houver um número significativo de transações recentes, o alerta e o alarme deverão ser resolvidos com o tempo e poderão ser ignorados.

Se o alerta ou alarme persistir e aumentar em gravidade, visualize um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para Gravações do Cliente e Leituras do Cliente para Erro ou Desligado. Ver "[Configurar mensagens de auditoria e destinos de log](#)".

Mensagens duplicadas

O sistema StorageGRID adota uma abordagem conservadora caso ocorra uma falha de rede ou nó. Por esse motivo, podem existir mensagens duplicadas no log de auditoria.

Arquivo de log de auditoria de acesso

O compartilhamento de auditoria contém o ativo `audit.log` arquivo e quaisquer arquivos de log de auditoria compactados. Você pode acessar arquivos de log de auditoria diretamente da linha de comando do nó de administração.

Antes de começar

- Você tem "[permissões de acesso específicas](#)".
- Você deve ter o `Passwords.txt` arquivo.
- Você deve saber o endereço IP de um nó de administração.

Passos

1. Efetue login em um nó de administração:
 - 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. Vá para o diretório que contém os arquivos de log de auditoria:

```
cd /var/local/log
```

3. Visualize o arquivo de log de auditoria atual ou salvo, conforme necessário.

Rotação do arquivo de log de auditoria

Os arquivos de logs de auditoria são salvos em um nó de administração `/var/local/log` diretório. Os arquivos de log de auditoria ativos são nomeados `audit.log` .



Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado. Ver ["Configurar mensagens de auditoria e destinos de log"](#) .

Uma vez por dia, o ativo `audit.log` o arquivo é salvo e um novo `audit.log` o arquivo é iniciado. O nome do arquivo salvo indica quando ele foi salvo, no formato `yyyy-mm-dd.txt` . Se mais de um log de auditoria for criado em um único dia, os nomes dos arquivos usarão a data em que o arquivo foi salvo, anexada por um número, no formato `yyyy-mm-dd.txt.n` . Por exemplo, `2018-04-15.txt` e `2018-04-15.txt.1` são o primeiro e o segundo arquivos de log criados e salvos em 15 de abril de 2018.

Após um dia, o arquivo salvo é compactado e renomeado, no formato `yyyy-mm-dd.txt.gz` , que preserva a data original. Com o tempo, isso resulta no consumo de armazenamento alocado para logs de auditoria no nó de administração. Um script monitora o consumo de espaço do log de auditoria e exclui os arquivos de log conforme necessário para liberar espaço no `/var/local/log` diretório. Os logs de auditoria são excluídos com base na data em que foram criados, sendo os mais antigos excluídos primeiro. Você pode monitorar as ações do script no seguinte arquivo: `/var/local/log/manage-audit.log` .

Este exemplo mostra o ativo `audit.log` arquivo, arquivo do dia anterior(`2018-04-15.txt`), e o arquivo compactado do dia anterior(`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formato de arquivo de log de auditoria

Formato de arquivo de log de auditoria

Os arquivos de log de auditoria são encontrados em cada nó administrativo e contêm uma coleção de mensagens de auditoria individuais.

Cada mensagem de auditoria contém o seguinte:

- O Tempo Universal Coordenado (UTC) do evento que disparou a mensagem de auditoria (ATIM) no formato ISO 8601, seguido por um espaço:

YYYY-MM-DDTHH:MM:SS.UUUUUU, onde UUUUUU são microssegundos.

- A própria mensagem de auditoria, entre colchetes e começando com AUDT .

O exemplo a seguir mostra três mensagens de auditoria em um arquivo de log de auditoria (quebras de linha adicionadas para facilitar a leitura). Essas mensagens foram geradas quando um locatário criou um bucket S3 e adicionou dois objetos a esse bucket.

```
2019-08-07T18:43:30.247711
```

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-  
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547  
18:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc  
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]  
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142  
142472611085]]
```

```
2019-08-07T18:43:30.783597
```

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-  
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547  
18:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc  
ket1"][S3KY(CSTR):"fh-small-0"]  
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-  
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]  
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F  
C32):S3RQ][ATID(UI64):8439606722108456022]]
```

```
2019-08-07T18:43:30.784558
```

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-  
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547  
18:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc  
ket1"][S3KY(CSTR):"fh-small-2000"]  
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-  
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]  
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F  
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

No formato padrão, as mensagens de auditoria nos arquivos de log de auditoria não são fáceis de ler ou

interpretar. Você pode usar o "[ferramenta audit-explain](#)" para obter resumos simplificados das mensagens de auditoria no log de auditoria. Você pode usar o "[ferramenta de soma de auditoria](#)" para resumir quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações levaram.

Use a ferramenta audit-explain

Você pode usar o `audit-explain` ferramenta para traduzir as mensagens de auditoria no log de auditoria para um formato fácil de ler.

Antes de começar

- Você tem "[permissões de acesso específicas](#)".
- Você deve ter o `Passwords.txt` arquivo.
- Você deve saber o endereço IP do nó de administração primário.

Sobre esta tarefa

O `audit-explain` A ferramenta, disponível no nó de administração principal, fornece resumos simplificados das mensagens de auditoria em um log de auditoria.



O `audit-explain` A ferramenta destina-se principalmente ao uso pelo suporte técnico durante operações de solução de problemas. Processamento `audit-explain` consultas podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID .

Este exemplo mostra a saída típica do `audit-explain` ferramenta. Esses quatro "[CUSPIR](#)" mensagens de auditoria foram geradas quando o locatário do S3 com ID de conta 92484777680322627870 usou solicitações S3 PUT para criar um bucket chamado "bucket1" e adicionar três objetos a esse bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

O `audit-explain` ferramenta pode fazer o seguinte:

- Processe logs de auditoria simples ou compactados. Por exemplo:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Processe vários arquivos simultaneamente. Por exemplo:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/log/*
```

- Aceitar entrada de um pipe, o que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Como os logs de auditoria podem ser muito grandes e lentos para analisar, você pode economizar tempo filtrando as partes que deseja examinar e executando `audit-explain` nas partes, em vez do arquivo inteiro.



O `audit-explain` a ferramenta não aceita arquivos compactados como entrada canalizada. Para processar arquivos compactados, forneça seus nomes de arquivo como argumentos de linha de comando ou use o `zcat` ferramenta para descompactar os arquivos primeiro. Por exemplo:

```
zcat audit.log.gz | audit-explain
```

Use o `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-explain -h
```

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. Digite o seguinte comando, onde `/var/local/log/audit.log` representa o nome e o local do arquivo ou arquivos que você deseja analisar:

```
$ audit-explain /var/local/log/audit.log
```

O `audit-explain` A ferramenta imprime interpretações legíveis por humanos de todas as mensagens no arquivo ou arquivos especificados.



Para reduzir o comprimento das linhas e facilitar a leitura, os registros de data e hora não são exibidos por padrão. Se você quiser ver os carimbos de data/hora, use o carimbo de data/hora (`-t`) opção.

Use a ferramenta audit-sum

Você pode usar o `audit-sum` ferramenta para contar as mensagens de auditoria de gravação, leitura, cabeçalho e exclusão e para ver o tempo mínimo, máximo e médio (ou tamanho) para cada tipo de operação.

Antes de começar

- Você tem ["permissões de acesso específicas"](#) .
- Você deve ter o `Passwords.txt` arquivo.
- Você deve saber o endereço IP do nó de administração primário.

Sobre esta tarefa

O `audit-sum` A ferramenta, disponível no nó de administração principal, resume quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações levaram.



O `audit-sum` A ferramenta destina-se principalmente ao uso pelo suporte técnico durante operações de solução de problemas. Processamento `audit-sum` consultas podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID .

Este exemplo mostra a saída típica do `audit-sum` ferramenta. Este exemplo mostra quanto tempo demoraram as operações do protocolo.

```
message group          count      min(sec)      max(sec)
average(sec)
=====
=====
IDEL                  274
SDEL                 213371      0.004         20.934
0.352
SGET                 201906      0.010         1740.290
1.132
SHEA                 22716       0.005          2.349
0.272
SPUT                 1771398     0.011         1770.563
0.487
```

O `audit-sum` A ferramenta fornece contagens e tempos para as seguintes mensagens de auditoria do S3, Swift e ILM em um log de auditoria.



Os códigos de auditoria são removidos do produto e da documentação, pois os recursos são descontinuados. Se você encontrar um código de auditoria que não esteja listado aqui, verifique as versões anteriores deste tópico para versões mais antigas do SG. Por exemplo, ["Documentação da ferramenta de soma de auditoria do StorageGRID 11.8"](#) .

Código	Descrição	Consulte
IDEL	Exclusão iniciada pelo ILM: registra quando o ILM inicia o processo de exclusão de um objeto.	"IDEL: Exclusão iniciada pelo ILM"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou bucket.	"SDEL: S3 EXCLUIR"

Código	Descrição	Consulte
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket.	"SGET: S3 OBTER"
KARITÉ	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	"SHEA: CABEÇA S3"
CUSPIR	S3 PUT: Registra uma transação bem-sucedida para criar um novo objeto ou bucket.	"SPUT: S3 PUT"
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contêiner.	"WDEL: Swift EXCLUIR"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contêiner.	"WGET: GET rápido"
WHEA	Swift HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contêiner.	"WHEA: CABEÇA Rápida"
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contêiner.	"WPUT: PUT rápido"

O `audit-sum` ferramenta pode fazer o seguinte:

- Processe logs de auditoria simples ou compactados. Por exemplo:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Processe vários arquivos simultaneamente. Por exemplo:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/log/*
```

- Aceitar entrada de um pipe, o que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```



Esta ferramenta não aceita arquivos compactados como entrada canalizada. Para processar arquivos compactados, forneça seus nomes de arquivo como argumentos de linha de comando ou use o `zcat` ferramenta para descompactar os arquivos primeiro. Por exemplo:

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

Você pode usar opções de linha de comando para resumir operações em buckets separadamente de operações em objetos ou para agrupar resumos de mensagens por nome de bucket, por período de tempo ou por tipo de destino. Por padrão, os resumos mostram o tempo mínimo, máximo e médio de operação, mas você pode usar o `size (-s)` opção para olhar o tamanho do objeto.

Use o `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-sum -h
```

Passos

1. Efetue login no nó de administração principal:

- Digite o seguinte comando: `ssh admin@primary_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. Se você quiser analisar todas as mensagens relacionadas às operações de gravação, leitura, cabeçalho e exclusão, siga estas etapas:

- Digite o seguinte comando, onde `/var/local/log/audit.log` representa o nome e o local do arquivo ou arquivos que você deseja analisar:

```
$ audit-sum /var/local/log/audit.log
```

Este exemplo mostra a saída típica do `audit-sum` ferramenta. Este exemplo mostra quanto tempo demoraram as operações do protocolo.

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

Neste exemplo, as operações SGET (S3 GET) são as mais lentas, em média, com 1,13 segundos, mas as operações SGET e SPUT (S3 PUT) mostram tempos longos de pior caso, de cerca de 1.770 segundos.

- b. Para mostrar as 10 operações de recuperação mais lentas, use o comando `grep` para selecionar apenas mensagens SGET e adicione a opção de saída longa(-l) para incluir caminhos de objetos:

```
grep SGET audit.log | audit-sum -l
```

Os resultados incluem o tipo (objeto ou bucket) e o caminho, o que permite que você pesquise no log de auditoria outras mensagens relacionadas a esses objetos específicos.

```

Total:          201906 operations
Slowest:        1740.290 sec
Average:        1.132 sec
Fastest:        0.010 sec
Slowest operations:
      time(usec)      source ip      type      size(B) path
      =====
      1740289662      10.96.101.125      object      5663711385
backup/r90l0aQ8JB-1566861764-4519.iso
      1624414429      10.96.101.125      object      5375001556
backup/r90l0aQ8JB-1566861764-6618.iso
      1533143793      10.96.101.125      object      5183661466
backup/r90l0aQ8JB-1566861764-4518.iso
      70839      10.96.101.125      object      28338
bucket3/dat.1566861764-6619
      68487      10.96.101.125      object      27890
bucket3/dat.1566861764-6615
      67798      10.96.101.125      object      27671
bucket5/dat.1566861764-6617
      67027      10.96.101.125      object      27230
bucket5/dat.1566861764-4517
      60922      10.96.101.125      object      26118
bucket3/dat.1566861764-4520
      35588      10.96.101.125      object      11311
bucket3/dat.1566861764-6616
      23897      10.96.101.125      object      10692
bucket3/dat.1566861764-4516

```

+

A partir deste exemplo de saída, você pode ver que as três solicitações GET do S3 mais lentas foram para objetos com cerca de 5 GB de tamanho, o que é muito maior do que os outros objetos. O tamanho grande é responsável pelos tempos de recuperação lentos no pior caso.

3. Se você quiser determinar quais tamanhos de objetos estão sendo ingeridos e recuperados de sua grade, use a opção de tamanho(-s):

```
audit-sum -s audit.log
```

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

Neste exemplo, o tamanho médio do objeto para SPUT é inferior a 2,5 MB, mas o tamanho médio para SGET é muito maior. O número de mensagens SPUT é muito maior que o número de mensagens SGET, indicando que a maioria dos objetos nunca é recuperada.

4. Se você quiser determinar se as recuperações foram lentas ontem:

- Emita o comando no log de auditoria apropriado e use a opção `group-by-time(-gt )`, seguido pelo período de tempo (por exemplo, 15M, 1H, 10S):

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Esses resultados mostram que o tráfego S3 GET atingiu o pico entre 06:00 e 07:00. Os tempos máximo e médio também são consideravelmente maiores nesses momentos e não aumentam gradualmente conforme a contagem aumenta. Isso sugere que a capacidade foi excedida em algum lugar, talvez na rede ou na capacidade da grade de processar solicitações.

- b. Para determinar o tamanho dos objetos que foram recuperados a cada hora ontem, adicione a opção de tamanho(-s) ao comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Esses resultados indicam que algumas recuperações muito grandes ocorreram quando o tráfego geral de recuperação estava no máximo.

- c. Para ver mais detalhes, use o ["ferramenta audit-explain"](#) para revisar todas as operações do SGET durante aquela hora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se a saída do comando `grep` for esperada em muitas linhas, adicione o `less` comando para mostrar o conteúdo do arquivo de log de auditoria uma página (uma tela) por vez.

5. Se você quiser determinar se as operações SPUT em buckets são mais lentas do que as operações SPUT para objetos:

- a. Comece usando o `-go` opção, que agrupa mensagens para operações de objeto e bucket separadamente:

```
grep SPUT sample.log | audit-sum -go
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.bucket 0.125	1	0.125	0.125
SPUT.object 0.236	12	0.025	1.019

Os resultados mostram que as operações SPUT para buckets têm características de desempenho diferentes das operações SPUT para objetos.

- b. Para determinar quais buckets têm as operações SPUT mais lentas, use o `-gb` opção, que agrupa mensagens por bucket:

```
grep SPUT audit.log | audit-sum -gb
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.cho-non-versioning 1.571	71943	0.046	1770.563
SPUT.cho-versioning 1.415	54277	0.047	1736.633
SPUT.cho-west-region 1.329	80615	0.040	55.557
SPUT.ldt002 0.361	1564563	0.011	51.569

- c. Para determinar quais buckets têm o maior tamanho de objeto SPUT, use ambos `-gb` e o `-s` opções:

```
grep SPUT audit.log | audit-sum -gb -s
```


message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ltd002 0.352	1564563	0.000	999.972

Formato de mensagem de auditoria

Formato de mensagem de auditoria

As mensagens de auditoria trocadas dentro do sistema StorageGRID incluem informações padrão comuns a todas as mensagens e conteúdo específico descrevendo o evento ou atividade que está sendo relatada.

Se as informações resumidas fornecidas pelo ["auditoria-explicação"](#) e ["soma de auditoria"](#) ferramentas for insuficiente, consulte esta seção para entender o formato geral de todas as mensagens de auditoria.

A seguir está um exemplo de mensagem de auditoria como ela pode aparecer no arquivo de log de auditoria:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):9445736326500603516]]
```

Cada mensagem de auditoria contém uma sequência de elementos de atributo. A sequência inteira está entre colchetes([]), e cada elemento de atributo na string tem as seguintes características:

- Entre parênteses []
- Introduzido pela corda AUDT , que indica uma mensagem de auditoria
- Sem delimitadores (sem vírgulas ou espaços) antes ou depois
- Terminado por um caractere de quebra de linha \n

Cada elemento inclui um código de atributo, um tipo de dado e um valor que são relatados neste formato:

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

O número de elementos de atributo na mensagem depende do tipo de evento da mensagem. Os elementos de atributo não são listados em nenhuma ordem específica.

A lista a seguir descreve os elementos de atributo:

- `ATTR` é um código de quatro caracteres para o atributo que está sendo relatado. Há alguns atributos que são comuns a todas as mensagens de auditoria e outros que são específicos do evento.
- `type` é um identificador de quatro caracteres do tipo de dados de programação do valor, como `UI64`, `FC32` e assim por diante. O tipo está entre parênteses ``()`.
- `value` é o conteúdo do atributo, normalmente um valor numérico ou de texto. Os valores sempre seguem dois pontos `(: `)`. Valores do tipo de dados `CSTR` são colocados entre aspas duplas `" "`.

Tipos de dados

Diferentes tipos de dados são usados para armazenar informações em mensagens de auditoria.

Tipo	Descrição
UI32	Inteiro longo sem sinal (32 bits); pode armazenar os números de 0 a 4.294.967.295.
UI64	Inteiro duplo longo sem sinal (64 bits); pode armazenar os números de 0 a 18.446.744.073.709.551.615.
FC32	Constante de quatro caracteres; um valor inteiro sem sinal de 32 bits representado como quatro caracteres ASCII, como "ABCD".
iPad	Usado para endereços IP.
CSTR	Uma matriz de comprimento variável de caracteres UTF-8. Os caracteres podem ser escapados com as seguintes convenções: • A barra invertida é <code>\\</code>. • O retorno de carro é <code>\r</code>. • Aspas duplas são <code>\"</code>. • A quebra de linha (nova linha) é <code>\n</code>. • Os caracteres podem ser substituídos por seus equivalentes hexadecimais (no formato <code>\xHH</code>, onde <code>HH</code> é o valor hexadecimal que representa o caractere).

Dados específicos do evento

Cada mensagem de auditoria no log de auditoria registra dados específicos de um evento do sistema.

Após a abertura `[AUDT:` contêiner que identifica a mensagem em si, o próximo conjunto de atributos fornece informações sobre o evento ou ação descrita pela mensagem de auditoria. Esses atributos são destacados no

exemplo a seguir:

```
2018-12-05T08:24:45.921845 [AUDT:*[RSLT\(\FC32\):SUCS\]*
\[TIME\(\UI64\):11454\]\[SAIP\(\IPAD\):"10.224.0.100"\]\[S3AI\(\CSTR\):"60025621595611246499"\]
\[SACC\(\CSTR\):"conta"\]\[S3AK\(\CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJ
A=="\]\[SUSR\(\CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(\CSTR\):"60025621595611246499"\]\[SBAC\(\CSTR\):"conta"\]\[S3BK\(\CSTR\):"bucket"\]
\[S3KY\(\CSTR\):"objeto"\]\[CBID\(\UI64\):0xCC128B9B9E428347\]\[UUID\(\CSTR\):"B975D2CE-E4DA-
4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\(\UI64\):30720\]\[AVER\(\UI32\):10]
\[ATIM\(\UI64\):1543998285921845\]\[ATYP\(\FC32\):SHEA\]\[ANID\(\UI32\):12281045\]\[AMID\(\FC32\):S3RQ]
\[ATID\(\UI64\):15552417629170647261\]
```

O `ATYP` elemento (sublinhado no exemplo) identifica qual evento gerou a mensagem. Esta mensagem de exemplo inclui o **"KARITÉ"** código de mensagem (`[ATYP(FC32):SHEA]`), indicando que foi gerado por uma solicitação S3 HEAD bem-sucedida.

Elementos comuns em mensagens de auditoria

Todas as mensagens de auditoria contêm os elementos comuns.

Código	Tipo	Descrição
ENTRE	FC32	ID do módulo: um identificador de quatro caracteres do ID do módulo que gerou a mensagem. Isso indica o segmento de código no qual a mensagem de auditoria foi gerada.
ANID	UI32	ID do nó: ID do nó da grade atribuído ao serviço que gerou a mensagem. Cada serviço recebe um identificador exclusivo no momento em que o sistema StorageGRID é configurado e instalado. Este ID não pode ser alterado.
ASES	UI64	Identificador de Sessão de Auditoria: Em versões anteriores, esse elemento indicava o horário em que o sistema de auditoria foi inicializado após o serviço ser iniciado. Este valor de tempo foi medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1º de janeiro de 1970). Observação: Este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ASQN	UI64	Contagem de sequência: em versões anteriores, esse contador era incrementado para cada mensagem de auditoria gerada no nó da grade (ANID) e zerado na reinicialização do serviço. Observação: Este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ATID	UI64	ID de rastreamento: um identificador compartilhado pelo conjunto de mensagens que foram acionadas por um único evento.

Código	Tipo	Descrição
ATIM	UI64	Carimbo de data/hora: hora em que o evento foi gerado e que disparou a mensagem de auditoria, medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1º de janeiro de 1970). Observe que a maioria das ferramentas disponíveis para converter o registro de data e hora em data e hora locais são baseadas em milissegundos. Pode ser necessário arredondar ou truncar o registro de data e hora registrado. O tempo legível por humanos que aparece no início da mensagem de auditoria no <code>audit.log</code> arquivo é o atributo ATIM no formato ISO 8601. A data e a hora são representadas como <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, onde o T é um caractere de sequência literal que indica o início do segmento de tempo da data. <code>UUUUUU</code> são microssegundos.
ATYP	FC32	Tipo de evento: um identificador de quatro caracteres do evento que está sendo registrado. Isso rege o conteúdo "payload" da mensagem: os atributos que são incluídos.
MÉDIO	UI32	Versão: A versão da mensagem de auditoria. À medida que o software StorageGRID evolui, novas versões de serviços podem incorporar novos recursos em relatórios de auditoria. Este campo permite a compatibilidade com versões anteriores no serviço AMS para processar mensagens de versões mais antigas dos serviços.
RSLT	FC32	Resultado: O resultado de um evento, processo ou transação. Se não for relevante para uma mensagem, NONE é usado em vez de SUCS para que a mensagem não seja filtrada acidentalmente.

Exemplos de mensagens de auditoria

Você pode encontrar informações detalhadas em cada mensagem de auditoria. Todas as mensagens de auditoria usam o mesmo formato.

A seguir está um exemplo de mensagem de auditoria como ela pode aparecer no `audit.log` arquivo:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

A mensagem de auditoria contém informações sobre o evento que está sendo registrado, bem como informações sobre a própria mensagem de auditoria.

Para identificar qual evento é registrado pela mensagem de auditoria, procure o atributo ATYP (destacado abaixo):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"]
[S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

O valor do atributo ATYP é SPUT. "CUSPIR" representa uma transação S3 PUT, que registra a ingestão de um objeto em um bucket.

A seguinte mensagem de auditoria também mostra o bucket ao qual o objeto está associado:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"]
[S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK\ (CSTR\): "s3small11"] [S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Para descobrir quando o evento PUT ocorreu, observe o registro de data e hora do Tempo Universal Coordenado (UTC) no início da mensagem de auditoria. Este valor é uma versão legível do atributo ATIM da própria mensagem de auditoria:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"]
[S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\ (UI64\): 1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

O ATIM registra o tempo, em microssegundos, desde o início da era UNIX. No exemplo, o valor 1405631878959669 traduz para quinta-feira, 17-jul-2014 21:17:59 UTC.

Mensagens de auditoria e o ciclo de vida do objeto

Quando as mensagens de auditoria são geradas?

Mensagens de auditoria são geradas sempre que um objeto é ingerido, recuperado ou excluído. Você pode identificar essas transações no log de auditoria localizando mensagens de auditoria específicas da API do S3.

As mensagens de auditoria são vinculadas por meio de identificadores específicos para cada protocolo.

Protocolo	Código
Vinculando operações S3	S3BK (balde), S3KY (chave) ou ambos
Vinculando operações Swift	WCON (contêiner), WOBJ (objeto) ou ambos
Vinculando operações internas	CBDID (identificador interno do objeto)

Cronometragem das mensagens de auditoria

Devido a fatores como diferenças de tempo entre nós da grade, tamanho do objeto e atrasos na rede, a ordem das mensagens de auditoria geradas pelos diferentes serviços pode variar daquela mostrada nos exemplos desta seção.

Transações de ingestão de objetos

Você pode identificar transações de ingestão de clientes no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de ingestão estão listadas nas tabelas a seguir. Somente as mensagens necessárias para rastrear a transação de ingestão são incluídas.

Mensagens de auditoria de ingestão do S3

Código	Nome	Descrição	Rastro	Ver
CUSPIR	Transação S3 PUT	Uma transação de ingestão S3 PUT foi concluída com sucesso.	CBDI, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regras de Objetos Atendidas	A política do ILM foi satisfeita para este objeto.	CBDI	"ORLM: Regras de Objeto Atendidas"

Mensagens de auditoria de ingestão rápida

Código	Nome	Descrição	Rastro	Ver
WPUT	Transação Swift PUT	Uma transação de ingestão Swift PUT foi concluída com sucesso.	CBDI, WCON, WOBJ	"WPUT: PUT rápido"

Código	Nome	Descrição	Rastro	Ver
ORLM	Regras de Objetos Atendidas	A política do ILM foi satisfeita para este objeto.	CBDI	"ORLM: Regras de Objeto Atendidas"

Exemplo: ingestão de objeto S3

A série de mensagens de auditoria abaixo é um exemplo das mensagens de auditoria geradas e salvas no log de auditoria quando um cliente S3 ingere um objeto em um nó de armazenamento (serviço LDR).

Neste exemplo, a política ILM ativa inclui a regra ILM Fazer 2 Cópias.



Nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Somente aqueles relacionados à transação de ingestão S3 (SPUT) são listados.

Este exemplo pressupõe que um bucket S3 foi criado anteriormente.

SPUT: S3 PUT

A mensagem SPUT é gerada para indicar que uma transação S3 PUT foi emitida para criar um objeto em um bucket específico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\ (UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\ (FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Regras de Objeto Atendidas

A mensagem ORLM indica que a política ILM foi satisfeita para este objeto. A mensagem inclui o CBID do objeto e o nome da regra ILM que foi aplicada.

Para objetos replicados, o campo LOCS inclui o ID do nó LDR e o ID do volume dos locais do objeto.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID(UI64):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Para objetos codificados por eliminação, o campo LOCS inclui o ID do perfil de codificação de eliminação e o ID do grupo de codificação de eliminação

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP(FC32):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

O campo PATH inclui informações de bucket e chave do S3 ou informações de contêiner e objeto do Swift, dependendo de qual API foi usada.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Transações de exclusão de objetos

Você pode identificar transações de exclusão de objetos no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de exclusão estão listadas nas tabelas a seguir. Somente mensagens necessárias para rastrear a transação de exclusão são incluídas.

Mensagens de auditoria de exclusão do S3

Código	Nome	Descrição	Rastro	Ver
SDEL	S3 Excluir	Solicitação feita para excluir o objeto de um bucket.	CBDI, S3KY	"SDEL: S3 EXCLUIR"

Mensagens de auditoria de exclusão rápida

Código	Nome	Descrição	Rastro	Ver
WDEL	Exclusão rápida	Solicitação feita para excluir o objeto de um contêiner, ou o contêiner.	CBDI, WOBJ	"WDEL: Swift EXCLUIR"

Exemplo: exclusão de objeto S3

Quando um cliente S3 exclui um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.



Nem todas as mensagens de auditoria geradas durante uma transação de exclusão estão listadas no exemplo abaixo. Somente aqueles relacionados à transação de exclusão do S3 (SDEL) são listados.

SDEL: S3 Excluir

A exclusão de objetos começa quando o cliente envia uma solicitação DeleteObject para um serviço LDR. A mensagem contém o bucket do qual o objeto deve ser excluído e a chave S3 do objeto, que é usada para identificá-lo.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\ (CSTR\):"example"\]\[S3KY\ (CSTR\):"testobject-0-
7"\][CBID\ (UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\ (FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Transações de recuperação de objetos

Você pode identificar transações de recuperação de objetos no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de recuperação estão listadas nas tabelas a seguir. Somente mensagens necessárias para rastrear a transação de recuperação são incluídas.

Mensagens de auditoria de recuperação S3

Código	Nome	Descrição	Rastro	Ver
SGET	S3 GET	Solicitação feita para recuperar um objeto de um bucket.	CBDI, S3BK, S3KY	"SGET: S3 OBTER"

Mensagens de auditoria de recuperação rápida

Código	Nome	Descrição	Rastro	Ver
WGET	Rápido GET	Solicitação feita para recuperar um objeto de um contêiner.	CBDI, WCON, WOBJ	"WGET: GET rápido"

Exemplo: recuperação de objeto S3

Quando um cliente S3 recupera um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Somente aqueles relacionados à transação de recuperação S3 (SGET) são listados.

SGET: S3 OBTER

A recuperação de objetos começa quando o cliente envia uma solicitação GetObject para um serviço LDR. A mensagem contém o bucket do qual recuperar o objeto e a chave S3 do objeto, que é usada para identificá-lo.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEW=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\CSTR\):"bucket-
anonymous"\]\[S3KY\CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\ (FC32\) :SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se a política do bucket permitir, um cliente poderá recuperar objetos anonimamente ou recuperar objetos de um bucket que pertence a uma conta de locatário diferente. A mensagem de auditoria contém informações sobre a conta do locatário do proprietário do bucket para que você possa rastrear essas solicitações anônimas e entre contas.

Na mensagem de exemplo a seguir, o cliente envia uma solicitação GetObject para um objeto armazenado em um bucket que não é dele. Os valores para SBAI e SBAC registram o ID e o nome da conta do locatário do proprietário do bucket, que diferem do ID e do nome da conta do locatário do cliente registrados no S3AI e no SACC.

```
2017-09-20T22:53:15.876415
```

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI\
(CSTR):"17915054115450519830"\]\[SACC(CSTR):"s3-account-
b"\]\[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="\]\[SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"\]\[SBAI(CSTR):"4397929817
8977966408"\]\[SBAC(CSTR):"s3-account-a"\]\[S3BK(CSTR):"bucket-
anonymous"]\[S3KY(CSTR):"Hello.txt"]\[CBID(UI64):0x83D70C6F1F662B02]\[CSIZ(UI
64):12]\[AVER(UI32):10]\[ATIM(UI64):1505947995876415]\[ATYP(FC32):SGET]\[ANID(
UI32):12272050]\[AMID(FC32):S3RQ]\[ATID(UI64):6888780247515624902]]
```

Exemplo: S3 Select em um objeto

Quando um cliente S3 emite uma consulta S3 Select em um objeto, mensagens de auditoria são geradas e salvas no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Somente aqueles relacionados à transação S3 Select (SelectObjectContent) são listados.

Cada consulta resulta em duas mensagens de auditoria: uma que executa a autorização da solicitação S3 Select (o campo S3SR é definido como "select") e uma operação GET padrão subsequente que recupera os dados do armazenamento durante o processamento.

```
2021-11-08T15:35:30.750038
```

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"]\[S3AI(CSTR):"63147909414576125820"]\[SACC(CSTR):"Ten
ant1636027116"]\[S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"]\[SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"]\[SBAI(CSTR):"63147909414576125820"]\[SBA
C(CSTR):"Tenant1636027116"]\[S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"]\[S3KY(CSTR):"SUB-
EST2020_ALL.csv"]\[CBID(UI64):0x0496F0408A721171]\[UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"]\[CSIZ(UI64):0]\[S3SR(CSTR):"select"]\[AVER(UI32):10]\[ATIM(UI64
):1636385730750038]\[ATYP(FC32):SPOS]\[ANID(UI32):12601166]\[AMID(FC32):S3RQ]
\[ATID(UI64):1363009709396895985]]
```

```

2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"] [S3AI(CSTR):"63147909414576125820"] [SACC(CSTR):"Tenant16
36027116"] [S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"] [SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"] [SBAI(CSTR):"63147909414576125820"] [SBAC(CST
R):"Tenant1636027116"] [S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"] [S3KY(CSTR):"SUB-
EST2020_ALL.csv"] [CBID(UI64):0x0496F0408A721171] [UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"] [CSIZ(UI64):10185581] [MTME(UI64):1636380348695262] [AVER(UI32
):10] [ATIM(UI64):1636385732604886] [ATYP(FC32):SGET] [ANID(UI32):12733063] [A
MID(FC32):S3RQ] [ATID(UI64):16562288121152341130]]

```

Mensagens de atualização de metadados

Mensagens de auditoria são geradas quando um cliente S3 atualiza os metadados de um objeto.

Mensagens de auditoria de atualização de metadados S3

Código	Nome	Descrição	Rastro	Ver
SUPD	Metadados S3 atualizados	Gerado quando um cliente S3 atualiza os metadados de um objeto ingerido.	CBDI, S3KY, HTRH	"SUPD: Metadados S3 atualizados"

Exemplo: atualização de metadados S3

O exemplo mostra uma transação bem-sucedida para atualizar os metadados de um objeto S3 existente.

SUPD: Atualização de metadados S3

O cliente S3 faz uma solicitação (SUPD) para atualizar os metadados especificados(`x-amz-meta-*`) para o objeto S3 (S3KY). Neste exemplo, os cabeçalhos de solicitação são incluídos no campo HTRH porque ele foi configurado como um cabeçalho de protocolo de auditoria (**CONFIGURAÇÃO > Monitoramento > Servidor de auditoria e syslog**). Ver ["Configurar mensagens de auditoria e destinos de log"](#).

```

2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\": \"identity\", \"authorization\": \"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\": \"0\", \"date\": \"Tue, 11 Jul 2017 21:54:03
GMT\", \"host\": \"10.96.99.163:18082\",
\"user-agent\": \"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\": \"/testbkt1/testobj1\", \"x-amz-metadata-
directive\": \"REPLACE\", \"x-amz-meta-city\": \"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]

```

Mensagens de auditoria

Descrições de mensagens de auditoria

Descrições detalhadas das mensagens de auditoria retornadas pelo sistema estão listadas nas seções a seguir. Cada mensagem de auditoria é listada primeiro em uma tabela que agrupa mensagens relacionadas pela classe de atividade que a mensagem representa. Esses agrupamentos são úteis tanto para entender os tipos de atividades que são auditadas quanto para selecionar o tipo desejado de filtragem de mensagens de auditoria.

As mensagens de auditoria também são listadas em ordem alfabética por seus códigos de quatro caracteres. Esta lista alfabética permite que você encontre informações sobre mensagens específicas.

Os códigos de quatro caracteres usados neste capítulo são os valores ATYP encontrados nas mensagens de auditoria, conforme mostrado na seguinte mensagem de exemplo:

```

2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]

```

Para obter informações sobre como definir níveis de mensagens de auditoria, alterar destinos de log e usar um servidor syslog externo para suas informações de auditoria, consulte ["Configurar mensagens de auditoria e](#)

Categorias de mensagens de auditoria

Mensagens de auditoria do sistema

As mensagens de auditoria pertencentes à categoria de auditoria do sistema são usadas para eventos relacionados ao próprio sistema de auditoria, estados de nós de grade, atividade de tarefas em todo o sistema (tarefas de grade) e operações de backup de serviço.

Código	Título e descrição da mensagem	Ver
ECMC	Fragmento de dados codificado por apagamento ausente: indica que um fragmento de dados codificado por apagamento ausente foi detectado.	"ECMC: Fragmento de dados codificado por apagamento ausente"
CEC	Fragmento de dados corrompido com codificação de eliminação: indica que um fragmento de dados corrompido com codificação de eliminação foi detectado.	"ECOC: Fragmento de dados codificados por apagamento corrompidos"
ETAF	Falha na autenticação de segurança: uma tentativa de conexão usando o Transport Layer Security (TLS) falhou.	"ETAF: Falha na autenticação de segurança"
GNRG	Registro GNDS: Um serviço atualiza ou registra informações sobre si mesmo no sistema StorageGRID .	"GNRG: Registro GNDS"
GNUR	Cancelamento de registro do GNDS: um serviço cancelou seu registro no sistema StorageGRID .	"GNUR: Cancelamento de registro do GNDS"
GTED	Tarefa de grade encerrada: o serviço CMN concluiu o processamento da tarefa de grade.	"GTED: Tarefa de grade encerrada"
GTST	Tarefa de grade iniciada: o serviço CMN começou a processar a tarefa de grade.	"GTST: Tarefa de grade iniciada"
GTSU	Tarefa de grade enviada: uma tarefa de grade foi enviada ao serviço CMN.	"GTSU: Tarefa de grade enviada"
LLST	Localização perdida: esta mensagem de auditoria é gerada quando uma localização é perdida.	"LLST: Localização Perdida"
OLST	Objeto perdido: um objeto solicitado não pode ser localizado no sistema StorageGRID .	"OLST: Sistema detectou objeto perdido"

Código	Título e descrição da mensagem	Ver
SADD	Desativar auditoria de segurança: o registro de mensagens de auditoria foi desativado.	"SADD: Desativação de auditoria de segurança"
SADE	Habilitar auditoria de segurança: o registro de mensagens de auditoria foi restaurado.	"SADE: Habilitar Auditoria de Segurança"
SVRF	Falha na verificação do Object Store: um bloco de conteúdo falhou nas verificações.	"SVRF: Falha na verificação do armazenamento de objetos"
SVRU	Object Store Verify Unknown: Dados de objeto inesperados detectados no armazenamento de objetos.	"SVRU: Verificação de armazenamento de objeto desconhecido"
SYSD	Parada do nó: um desligamento foi solicitado.	"SYSD: Parada do nó"
SISTEMA	Parada de nó: um serviço iniciou uma parada normal.	"SYST: Parada do nó"
SYSU	Início do nó: um serviço foi iniciado; a natureza do desligamento anterior é indicada na mensagem.	"SYSU: Início do nó"

Mensagens de auditoria de armazenamento de objetos

As mensagens de auditoria pertencentes à categoria de auditoria de armazenamento de objetos são usadas para eventos relacionados ao armazenamento e gerenciamento de objetos dentro do sistema StorageGRID . Isso inclui armazenamento e recuperação de objetos, transferências de nó de grade para nó de grade e verificações.



Os códigos de auditoria são removidos do produto e da documentação, pois os recursos são descontinuados. Se você encontrar um código de auditoria que não esteja listado aqui, verifique as versões anteriores deste tópico para versões mais antigas do SG. Por exemplo, "[Mensagens de auditoria de armazenamento de objetos do StorageGRID 11.8](#)".

Código	Descrição	Ver
IRMÃO	Solicitação de somente leitura de bucket: um bucket entrou ou saiu do modo somente leitura.	"BROR: Solicitação de somente leitura do bucket"
CBSE	Fim do envio do objeto: a entidade de origem concluiu uma operação de transferência de dados de um nó da grade para outro.	"CBSE: Fim do envio de objeto"

Código	Descrição	Ver
CBRE	Fim do recebimento do objeto: a entidade de destino concluiu uma operação de transferência de dados de um nó da grade para outro.	"CBRE: Objeto Recebimento Final"
CGRR	Solicitação de replicação entre grades: o StorageGRID tentou uma operação de replicação entre grades para replicar objetos entre buckets em uma conexão de federação de grade.	"CGRR: Solicitação de replicação entre redes"
EBDL	Exclusão de bucket vazio: o scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de bucket vazio).	"EBDL: Exclusão de Bucket Vazio"
EBKR	Solicitação de bucket vazio: um usuário enviou uma solicitação para ativar ou desativar o bucket vazio (ou seja, para excluir objetos do bucket ou para parar de excluir objetos).	"EBKR: Solicitação de balde vazio"
SCMT	Confirmação do armazenamento de objetos: um bloco de conteúdo foi completamente armazenado e verificado e agora pode ser solicitado.	"SCMT: Solicitação de confirmação de armazenamento de objeto"
SREM	Remoção do Object Store: Um bloco de conteúdo foi excluído de um nó de grade e não pode mais ser solicitado diretamente.	"SREM: Remoção de armazenamento de objetos"

O cliente leu mensagens de auditoria

As mensagens de auditoria de leitura do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para recuperar um objeto.

Código	Descrição	Usado por	Ver
S3SL	Solicitação S3 Select: Registra uma conclusão depois que uma solicitação S3 Select é retornada ao cliente. A mensagem S3SL pode incluir detalhes da mensagem de erro e do código de erro. A solicitação pode não ter sido bem-sucedida.	Cliente S3	"S3SL: Solicitação de seleção S3"
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket. Observação: Se a transação operar em um sub-recurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SGET: S3 OBTER"

Código	Descrição	Usado por	Ver
KARITÉ	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	Cliente S3	"SHEA: CABEÇA S3"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contêiner.	Cliente Swift	"WGET: GET rápido"
WHEA	Swift HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contêiner.	Cliente Swift	"WHEA: CABEÇA Rápida"

O cliente escreve mensagens de auditoria

As mensagens de auditoria de gravação do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para criar ou modificar um objeto.

Código	Descrição	Usado por	Ver
OVWR	Substituição de objeto: registra uma transação para substituir um objeto por outro objeto.	Clientes S3 e Swift	"OVWR: Substituição de Objeto"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou bucket. Observação: Se a transação operar em um sub-recurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SDEL: S3 EXCLUIR"
SPOS	S3 POST: Registra uma transação bem-sucedida para restaurar um objeto do armazenamento do AWS Glacier para um pool de armazenamento em nuvem.	Cliente S3	"SPOS: POSTAGEM S3"
CUSPIR	S3 PUT: Registra uma transação bem-sucedida para criar um novo objeto ou bucket. Observação: Se a transação operar em um sub-recurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SPUT: S3 PUT"
SUPD	Metadados S3 atualizados: registra uma transação bem-sucedida para atualizar os metadados de um objeto ou bucket existente.	Cliente S3	"SUPD: Metadados S3 atualizados"
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contêiner.	Cliente Swift	"WDEL: Swift EXCLUIR"

Código	Descrição	Usado por	Ver
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contêiner.	Cliente Swift	"WPUT: PUT rápido"

Mensagem de auditoria de gestão

A categoria Gerenciamento registra solicitações do usuário na API de Gerenciamento.

Código	Título e descrição da mensagem	Ver
MGAU	Mensagem de auditoria da API de gerenciamento: um log de solicitações do usuário.	"MGAU: Mensagem de auditoria de gestão"

Mensagens de auditoria do ILM

As mensagens de auditoria pertencentes à categoria de auditoria ILM são usadas para eventos relacionados às operações de gerenciamento do ciclo de vida da informação (ILM).

Código	Título e descrição da mensagem	Ver
IDEL	Exclusão iniciada pelo ILM: esta mensagem de auditoria é gerada quando o ILM inicia o processo de exclusão de um objeto.	"IDEL: Exclusão iniciada pelo ILM"
LKCU	Limpeza de objetos sobrescritos. Esta mensagem de auditoria é gerada quando um objeto substituído é removido automaticamente para liberar espaço de armazenamento.	"LKCU: Limpeza de Objetos Sobrescritos"
ORLM	Regras de objeto atendidas: esta mensagem de auditoria é gerada quando os dados do objeto são armazenados conforme especificado pelas regras do ILM.	"ORLM: Regras de Objeto Atendidas"

Referência de mensagem de auditoria

BROR: Solicitação de somente leitura do bucket

O serviço LDR gera esta mensagem de auditoria quando um bucket entra ou sai do modo somente leitura. Por exemplo, um bucket entra no modo somente leitura enquanto todos os objetos estão sendo excluídos.

Código	Campo	Descrição
BKHD	UUID do balde	O ID do bucket.

Código	Campo	Descrição
IRMÃO	Valor de solicitação somente leitura do bucket	Se o bucket está se tornando somente leitura ou está saindo do estado somente leitura (1 = somente leitura, 0 = não somente leitura).
MANOS	Motivo de somente leitura do bucket	O motivo pelo qual o bucket está se tornando somente leitura ou saindo do estado somente leitura. Por exemplo, emptyBucket.
S3AI	ID da conta do locatário S3	O ID da conta do locatário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.

CBRB: Início do recebimento do objeto

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre diferentes nós à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, esta mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se bem-sucedido, a transferência começa a partir desta contagem de sequência.

Código	Campo	Descrição
CTES	Contagem de sequência final esperada	Indica a última contagem de sequência solicitada. Se bem-sucedida, a transferência será considerada concluída quando esta contagem de sequência for recebida.
RSLT	Status de início da transferência	Status no momento em que a transferência foi iniciada: SUCS: Transferência iniciada com sucesso.

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único pedaço de conteúdo, conforme identificado pelo seu Identificador de Bloco de Conteúdo. A operação solicita dados de "Contagem de sequência inicial" até "Contagem de sequência final esperada". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar contagens de réplicas.

CBRE: Objeto Recebimento Final

Quando a transferência de um bloco de conteúdo de um nó para outro é concluída, esta mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência na qual a transferência começou.

Código	Campo	Descrição
CTAS	Contagem real da sequência final	Indica a última contagem de sequência transferida com sucesso. Se a Contagem de Sequência Final Real for a mesma que a Contagem de Sequência Inicial e o Resultado da Transferência não for bem-sucedido, nenhum dado foi trocado.
RSLT	Resultado da transferência	O resultado da operação de transferência (da perspectiva da entidade remetente): SUCS: transferência concluída com sucesso; todas as contagens de sequência solicitadas foram enviadas. CONL: conexão perdida durante a transferência CTMO: tempo limite de conexão durante estabelecimento ou transferência UNRE: ID do nó de destino inacessível CRPT: transferência encerrada devido ao recebimento de dados corrompidos ou inválidos

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi concluída. Se o resultado da transferência for bem-sucedido, a operação transfere dados de "Contagem de sequência inicial" para "Contagem de sequência final real". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e para localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, também pode ser usado para verificar contagens de réplicas.

CBSB: Início do envio de objeto

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre diferentes nós à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, esta mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.

Código	Campo	Descrição
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se bem-sucedido, a transferência começa a partir desta contagem de sequência.
CTES	Contagem de sequência final esperada	Indica a última contagem de sequência solicitada. Se bem-sucedida, a transferência será considerada concluída quando esta contagem de sequência for recebida.
RSLT	Status de início da transferência	Status no momento em que a transferência foi iniciada: SUCS: transferência iniciada com sucesso.

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único pedaço de conteúdo, conforme identificado pelo seu Identificador de Bloco de Conteúdo. A operação solicita dados de "Contagem de sequência inicial" até "Contagem de sequência final esperada". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar contagens de réplicas.

CBSE: Fim do envio de objeto

Quando a transferência de um bloco de conteúdo de um nó para outro é concluída, esta mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.

Código	Campo	Descrição
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência na qual a transferência começou.
CTAS	Contagem real da sequência final	Indica a última contagem de sequência transferida com sucesso. Se a Contagem de Sequência Final Real for a mesma que a Contagem de Sequência Inicial e o Resultado da Transferência não for bem-sucedido, nenhum dado foi trocado.
RSLT	Resultado da transferência	O resultado da operação de transferência (da perspectiva da entidade remetente): SUCS: Transferência concluída com sucesso; todas as contagens de sequência solicitadas foram enviadas. CONL: conexão perdida durante a transferência CTMO: tempo limite de conexão durante estabelecimento ou transferência UNRE: ID do nó de destino inacessível CRPT: transferência encerrada devido ao recebimento de dados corrompidos ou inválidos

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi concluída. Se o resultado da transferência for bem-sucedido, a operação transfere dados de "Contagem de sequência inicial" para "Contagem de sequência final real". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e para localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, também pode ser usado para verificar contagens de réplicas.

CGRR: Solicitação de replicação entre redes

Esta mensagem é gerada quando o StorageGRID tenta uma operação de replicação entre grades para replicar objetos entre buckets em uma conexão de federação de

grade.

Código	Campo	Descrição
CSIZ	Tamanho do objeto	O tamanho do objeto em bytes. O atributo CSIZ foi introduzido no StorageGRID 11.8. Como resultado, as solicitações de replicação entre grades abrangendo uma atualização do StorageGRID 11.7 para 11.8 podem ter um tamanho total de objeto impreciso.
S3AI	ID da conta do locatário S3	O ID da conta do locatário que possui o bucket do qual o objeto está sendo replicado.
GFID	ID de conexão da federação de grade	O ID da conexão de federação de grade que está sendo usada para replicação entre grades.
OPER	Operação CGR	O tipo de operação de replicação entre grades que foi tentada: • 0 = Replicar objeto • 1 = Replicar objeto multiparte • 2 = Replicar marcador de exclusão
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket.
VSID	ID da versão	O ID da versão específica de um objeto que estava sendo replicado.
RSLT	Código de resultado	Retorna erro bem-sucedido (SUCS) ou erro geral (GERR).

EBDL: Exclusão de Bucket Vazio

O scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de bucket vazio).

Código	Campo	Descrição
CSIZ	Tamanho do objeto	O tamanho do objeto em bytes.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
SEGC	UUID do contêiner	UUID do contêiner para o objeto segmentado. Este valor só estará disponível se o objeto for segmentado.

Código	Campo	Descrição
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
RSLT	Resultado da operação de exclusão	O resultado de um evento, processo ou transação. Se não for relevante para uma mensagem, NONE é usado em vez de SUCS para que a mensagem não seja filtrada acidentalmente.

EBKR: Solicitação de balde vazio

Esta mensagem indica que um usuário enviou uma solicitação para ativar ou desativar o bucket vazio (ou seja, para excluir objetos do bucket ou para parar de excluir objetos).

Código	Campo	Descrição
CONSTRUIR	UUID do balde	O ID do bucket.
EBJS	Configuração JSON do Bucket Vazio	Contém o JSON que representa a configuração atual do Empty Bucket.
S3AI	ID da conta do locatário S3	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.

ECMC: Fragmento de dados codificado por apagamento ausente

Esta mensagem de auditoria indica que o sistema detectou um fragmento de dados codificado para eliminação ausente.

Código	Campo	Descrição
VCMC	ID do VCS	O nome do VCS que contém o pedaço faltante.
MCID	ID do pedaço	O identificador do fragmento codificado por apagamento ausente.
RSLT	Resultado	Este campo tem o valor 'NENHUM'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem específica. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ECOC: Fragmento de dados codificados por apagamento corrompidos

Esta mensagem de auditoria indica que o sistema detectou um fragmento de dados corrompido com código de eliminação.

Código	Campo	Descrição
VCCO	ID do VCS	O nome do VCS que contém o pedaço corrompido.
VLID	ID do volume	O volume RangeDB que contém o fragmento corrompido com código de eliminação.
CCID	ID do pedaço	O identificador do fragmento corrompido codificado por apagamento.
RSLT	Resultado	Este campo tem o valor 'NENHUM'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem específica. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ETAF: Falha na autenticação de segurança

Esta mensagem é gerada quando uma tentativa de conexão usando o Transport Layer Security (TLS) falha.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP na qual a autenticação falhou.
RUID	Identidade do usuário	Um identificador dependente de serviço que representa a identidade do usuário remoto.
RSLT	Código de Razão	O motivo da falha: SCNI: Falha no estabelecimento da conexão segura. CERM: O certificado estava faltando. CERT: O certificado era inválido. CERE: O certificado expirou. CERR: O certificado foi revogado. CSGN: A assinatura do certificado era inválida. CSGU: O signatário do certificado era desconhecido. UCRM: As credenciais do usuário estavam faltando. UCRI: As credenciais do usuário eram inválidas. UCRU: Credenciais de usuário não foram permitidas. TOUT: Tempo limite de autenticação esgotado.

Quando uma conexão é estabelecida com um serviço seguro que usa TLS, as credenciais da entidade remota são verificadas usando o perfil TLS e lógica adicional incorporada ao serviço. Se essa autenticação falhar devido a certificados ou credenciais inválidos, inesperados ou não permitidos, uma mensagem de auditoria será registrada. Isso permite consultas sobre tentativas de acesso não autorizado e outros problemas de conexão relacionados à segurança.

A mensagem pode resultar de uma entidade remota com configuração incorreta ou de tentativas de apresentar credenciais inválidas ou não permitidas ao sistema. Esta mensagem de auditoria deve ser monitorada para detectar tentativas de obter acesso não autorizado ao sistema.

GNRG: Registro GNDS

O serviço CMN gera esta mensagem de auditoria quando um serviço atualiza ou registra informações sobre si mesmo no sistema StorageGRID .

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID do nó	O ID do nó do serviço que iniciou a solicitação de atualização.
GNTTP	Tipo de dispositivo	O tipo de dispositivo do nó da grade (por exemplo, BLDR para um serviço LDR).
GNDV	Versão do modelo do dispositivo	A sequência de caracteres que identifica a versão do modelo do dispositivo do nó da grade no pacote DMDL.
GNGP	Grupo	O grupo ao qual o nó da grade pertence (no contexto de custos de link e classificação de consulta de serviço).
GNIA	Endereço IP	Endereço IP do nó da grade.

Esta mensagem é gerada sempre que um nó de grade atualiza sua entrada no Pacote de Nós de Grade.

GNUR: Cancelamento de registro do GNDS

O serviço CMN gera esta mensagem de auditoria quando um serviço possui informações não registradas sobre si mesmo no sistema StorageGRID .

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID do nó	O ID do nó do serviço que iniciou a solicitação de atualização.

GTED: Tarefa de grade encerrada

Esta mensagem de auditoria indica que o serviço CMN concluiu o processamento da tarefa de grade especificada e moveu a tarefa para a tabela Histórica. Se o resultado for SUCS, ABRT ou ROLF, haverá uma mensagem de auditoria correspondente de Tarefa de grade iniciada. Os outros resultados indicam que o processamento desta tarefa de grade nunca foi iniciado.

Código	Campo	Descrição
TSID	ID da tarefa	Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa de grade seja gerenciada ao longo de seu ciclo de vida. Observação: O ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Enviadas, Iniciadas e Encerradas.
RSLT	Resultado	O resultado final do status da tarefa de grade: • SUCS: A tarefa da grade foi concluída com sucesso. • ABRT: A tarefa da grade foi encerrada sem erro de reversão. • ROLF: A tarefa da grade foi encerrada e não foi possível concluir o processo de reversão. • CANC: A tarefa da grade foi cancelada pelo usuário antes de ser iniciada. • EXPR: A tarefa de grade expirou antes de ser iniciada. • IVLD: A tarefa de grade era inválida. • AUTH: A tarefa de grade não foi autorizada. • DUPL: A tarefa de grade foi rejeitada como duplicada.

GTST: Tarefa de grade iniciada

Esta mensagem de auditoria indica que o serviço CMN começou a processar a tarefa de grade especificada. A mensagem de auditoria segue imediatamente a mensagem Grid Task Submitted para tarefas de grade iniciadas pelo serviço interno Grid Task Submission e selecionadas para ativação automática. Para tarefas de grade enviadas para a tabela Pendente, esta mensagem é gerada quando o usuário inicia a tarefa de grade.

Código	Campo	Descrição
TSID	ID da tarefa	Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. Observação: O ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Enviadas, Iniciadas e Encerradas.
RSLT	Resultado	O resultado. Este campo tem apenas um valor: • SUCS: A tarefa de grade foi iniciada com sucesso.

GTSU: Tarefa de grade enviada

Esta mensagem de auditoria indica que uma tarefa de grade foi enviada ao serviço CMN.

Código	Campo	Descrição
TSID	ID da tarefa	Identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. Observação: O ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Enviadas, Iniciadas e Encerradas.
TTYP	Tipo de tarefa	O tipo de tarefa de grade.
TVER	Versão da tarefa	Um número que indica a versão da tarefa de grade.
TDSC	Descrição da tarefa	Uma descrição legível da tarefa da grade.

Código	Campo	Descrição
IVA	Válido após o carimbo de data/hora	O primeiro momento (UINT64 microssegundos a partir de 1º de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
VBTS	Válido antes do carimbo de data/hora	O horário mais recente (UINT64 microssegundos a partir de 1º de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
TSRC	Fonte	A fonte da tarefa: • TXTB: A tarefa de grade foi enviada por meio do sistema StorageGRID como um bloco de texto assinado. • GRADE: A tarefa de grade foi enviada por meio do Serviço de Envio de Tarefas de Grade interno.
ACTV	Tipo de ativação	O tipo de ativação: • AUTO: A tarefa de grade foi enviada para ativação automática. • PEND: A tarefa da grade foi enviada para a tabela pendente. Esta é a única possibilidade para a fonte TXTB.
RSLT	Resultado	O resultado da submissão: • SUCS: A tarefa de grade foi enviada com sucesso. • FALHA: A tarefa foi movida diretamente para a tabela histórica.

IDEL: Exclusão iniciada pelo ILM

Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto.

A mensagem IDEL é gerada em qualquer uma destas situações:

- **Para objetos em buckets S3 compatíveis:** Esta mensagem é gerada quando o ILM inicia o processo de exclusão automática de um objeto porque seu período de retenção expirou (assumindo que a configuração de exclusão automática esteja ativada e a retenção legal esteja desativada).
- **Para objetos em buckets S3 não compatíveis.** Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto porque nenhuma instrução de posicionamento nas políticas ativas do ILM se aplica atualmente ao objeto.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O CBDID do objeto.

Código	Campo	Descrição
APLV	Conformidade: Exclusão automática	Somente para objetos em buckets S3 compatíveis. 0 (falso) ou 1 (verdadeiro), indicando se um objeto compatível deve ser excluído automaticamente quando seu período de retenção terminar, a menos que o bucket esteja sob retenção legal.
CMPL	Conformidade: retenção legal	Somente para objetos em buckets S3 compatíveis. 0 (falso) ou 1 (verdadeiro), indicando se o bucket está atualmente sob retenção legal.
CMPR	Conformidade: Período de retenção	Somente para objetos em buckets S3 compatíveis. A duração do período de retenção do objeto em minutos.
CTME	Conformidade: Tempo de ingestão	Somente para objetos em buckets S3 compatíveis. Tempo de ingestão do objeto. Você pode adicionar o período de retenção em minutos a esse valor para determinar quando o objeto pode ser excluído do bucket.
DMRK	Excluir ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket versionado. Operações em buckets não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LOCS	Locais	O local de armazenamento de dados de objetos dentro do sistema StorageGRID . O valor para LOCS é "" se o objeto não tiver localizações (por exemplo, ele foi excluído). CLEC: para objetos codificados por eliminação, o ID do perfil de codificação por eliminação e o ID do grupo de codificação por eliminação que são aplicados aos dados do objeto. CLDI: para objetos replicados, o ID do nó LDR e o ID do volume do local do objeto. CLNL: ID do nó ARC da localização do objeto se os dados do objeto estiverem arquivados.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.

Código	Campo	Descrição
REGRA	Etiqueta de regras	- Se um objeto em um bucket S3 compatível estiver sendo excluído automaticamente porque seu período de retenção expirou, este campo ficará em branco. - Se o objeto estiver sendo excluído porque não há mais instruções de posicionamento que se apliquem atualmente ao objeto, este campo mostrará o rótulo legível da última regra do ILM aplicada ao objeto.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

LKCU: Limpeza de Objetos Sobrescritos

Esta mensagem é gerada quando o StorageGRID remove um objeto substituído que anteriormente exigia limpeza para liberar espaço de armazenamento. Um objeto é substituído quando um cliente S3 grava um objeto em um caminho que já contém um objeto. O processo de remoção ocorre automaticamente e em segundo plano.

Código	Campo	Descrição
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LTYP	Tipo de limpeza	<i>Somente para uso interno.</i>
LUID	UUID do objeto removido	O identificador do objeto que foi removido.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
SEGC	UUID do contêiner	UUID do contêiner para o objeto segmentado. Este valor só estará disponível se o objeto for segmentado.
UUID	Identificador Universalmente Único	O identificador do objeto que ainda existe. Este valor só estará disponível se o objeto não tiver sido excluído.

Esta mensagem é gerada quando um pedaço vazado é limpo ou excluído. Um pedaço pode ser parte de um objeto replicado ou de um objeto codificado para eliminação.

Código	Campo	Descrição
CLOC	Localização do pedaço	O caminho do arquivo do pedaço vazado que foi excluído.
CTYP	Tipo de pedaço	Tipo de pedaço: ec: Erasure-coded object chunk repl: Replicated object chunk
LTYP	Tipo de vazamento	Os cinco tipos de vazamentos que podem ser detectados: object_leaked: Object doesn't exist in the grid location_leaked: Object exists in the grid, but found location doesn't belong to object mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn't contain this segment no_parent: Container object is deleted, but object segment was left out and not deleted
CTIM	Tempo de criação do bloco	Horário em que o pedaço vazado foi criado.
UUID	Identificador Universalmente Único	O identificador do objeto ao qual o pedaço pertence.
CBID	Identificador de bloco de conteúdo	CBID do objeto ao qual o pedaço vazado pertence.
CSIZ	Tamanho do conteúdo	O tamanho do pedaço em bytes.

LLST: Localização Perdida

Esta mensagem é gerada sempre que um local para uma cópia de objeto (replicada ou

codificada para eliminação) não pode ser encontrado.

Código	Campo	Descrição
CBIL	CBDI	O CBDI afetado.
ECPR	Perfil de codificação de apagamento	Para dados de objetos codificados por eliminação. O ID do perfil de codificação de eliminação usado.
LTyp	Tipo de localização	CLDI (Online): Para dados de objetos replicados CLEC (Online): Para dados de objetos codificados por apagamento CLNL (Nearline): Para dados de objetos replicados arquivados
NOID	ID do nó de origem	O ID do nó no qual os locais foram perdidos.
PCLD	Caminho para o objeto replicado	O caminho completo para o local do disco dos dados do objeto perdido. Retornado somente quando LTyp tem um valor de CLDI (ou seja, para objetos replicados). Assume a forma <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@</code>
RSLT	Resultado	Sempre NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.
TSRC	Fonte de disparo	USUÁRIO: Acionado pelo usuário SYST: Sistema acionado
UUID	ID universalmente exclusivo	O identificador do objeto afetado no sistema StorageGRID .

MG AU: Mensagem de auditoria de gestão

A categoria Gerenciamento registra solicitações do usuário na API de Gerenciamento. Cada solicitação HTTP que não é uma solicitação GET ou HEAD para um URI de API válido registra uma resposta contendo o nome de usuário, IP e tipo de solicitação para a API. URIs de API inválidos (como /api/v3-authorize) e solicitações inválidas para URIs de API válidos não são registrados.

Código	Campo	Descrição
MDIP	Endereço IP de destino	O endereço IP do servidor (destino).
MDNA	Nome de domínio	O nome do domínio do host.
MPAT	Solicitar PATH	O caminho da solicitação.
MPQP	Parâmetros de consulta de solicitação	Os parâmetros de consulta para a solicitação.
MRBD	Corpo da solicitação	O conteúdo do corpo da solicitação. Embora o corpo da resposta seja registrado por padrão, o corpo da solicitação é registrado em certos casos quando o corpo da resposta está vazio. Como as seguintes informações não estão disponíveis no corpo da resposta, elas são obtidas do corpo da solicitação para os seguintes métodos POST: • Nome de usuário e ID da conta em POST autorizar • Nova configuração de sub-redes em POST /grid/grid-networks/update • Novos servidores NTP em POST /grid/ntp-servers/update • IDs de servidores desativados em POST /grid/servers/decommission Observação: Informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).
MRMD	Método de solicitação	O método de solicitação HTTP: • PUBLICAR • COLOCAR • EXCLUIR • CORREÇÃO
MRSC	Código de resposta	O código de resposta.
MRSP	Corpo de resposta	O conteúdo da resposta (o corpo da resposta) é registrado por padrão. Observação: Informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).

Código	Campo	Descrição
MSIP	Endereço IP de origem	O endereço IP do cliente (origem).
MUUN	URN do usuário	O URN (nome uniforme do recurso) do usuário que enviou a solicitação.
RSLT	Resultado	Retorna sucesso (SUCS) ou o erro relatado pelo backend.

OLST: Sistema detectou objeto perdido

Esta mensagem é gerada quando o serviço DDS não consegue localizar nenhuma cópia de um objeto no sistema StorageGRID .

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O CBDID do objeto perdido.
NOID	ID do nó	Se disponível, a última localização direta ou próxima conhecida do objeto perdido. É possível ter apenas o ID do nó sem um ID do volume se as informações do volume não estiverem disponíveis.
CAMINHO	Balde/Chave S3	Se disponível, o nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.
UUID	ID universalmente exclusivo	O identificador do objeto perdido dentro do sistema StorageGRID .
VOLI	ID do volume	Se disponível, o ID do volume do nó de armazenamento para o último local conhecido do objeto perdido.

ORLM: Regras de Objeto Atendidas

Esta mensagem é gerada quando o objeto é armazenado e copiado com sucesso, conforme especificado pelas regras do ILM.



A mensagem ORLM não é gerada quando um objeto é armazenado com sucesso pela regra padrão Fazer 2 Cópias se outra regra na política usar o filtro avançado Tamanho do Objeto.

Código	Campo	Descrição
CONSTRUIR	Cabeçalho de balde	Campo ID do bucket. Usado para operações internas. Aparece somente se STAT for PRGD.
CBDI	Identificador de bloco de conteúdo	O CBDID do objeto.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LOCS	Locais	O local de armazenamento de dados de objetos dentro do sistema StorageGRID . O valor para LOCS é "" se o objeto não tiver localizações (por exemplo, ele foi excluído). CLEC: para objetos codificados por eliminação, o ID do perfil de codificação por eliminação e o ID do grupo de codificação por eliminação que são aplicados aos dados do objeto. CLDI: para objetos replicados, o ID do nó LDR e o ID do volume do local do objeto. CLNL: ID do nó ARC da localização do objeto se os dados do objeto estiverem arquivados.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	O rótulo legível dado à regra ILM aplicada a este objeto.
SEGC	UUID do contêiner	UUID do contêiner para o objeto segmentado. Este valor só estará disponível se o objeto for segmentado.
SGCB	CBDID do contêiner	CBID do contêiner para o objeto segmentado. Este valor está disponível somente para objetos segmentados e multipartes.

Código	Campo	Descrição
ESTATÍSTICA	Status	O status da operação do ILM. CONCLUÍDO: As operações do ILM contra o objeto foram concluídas. DFER: O objeto foi marcado para futura reavaliação do ILM. PRGD: O objeto foi excluído do sistema StorageGRID . NLOC: Os dados do objeto não podem mais ser encontrados no sistema StorageGRID . Esse status pode indicar que todas as cópias dos dados do objeto estão ausentes ou danificadas.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

A mensagem de auditoria ORLM pode ser emitida mais de uma vez para um único objeto. Por exemplo, ele é emitido sempre que ocorre um dos seguintes eventos:

- As regras do ILM para o objeto são satisfeitas para sempre.
- As regras do ILM para o objeto são satisfeitas para esta época.
- As regras do ILM excluíram o objeto.
- O processo de verificação em segundo plano detecta que uma cópia dos dados do objeto replicado está corrompida. O sistema StorageGRID executa uma avaliação do ILM para substituir o objeto corrompido.

Informações relacionadas

- ["Transações de ingestão de objetos"](#)
- ["Transações de exclusão de objetos"](#)

OVWR: Substituição de Objeto

Esta mensagem é gerada quando uma operação externa (solicitada pelo cliente) faz com que um objeto seja substituído por outro objeto.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo (novo)	O CBDID para o novo objeto.
CSIZ	Tamanho do objeto anterior	O tamanho, em bytes, do objeto que está sendo substituído.

Código	Campo	Descrição
TOCB	Identificador de bloco de conteúdo (anterior)	O CBDID do objeto anterior.
UUID	ID universalmente exclusivo (novo)	O identificador do novo objeto dentro do sistema StorageGRID .
OUID	ID universalmente exclusivo (anterior)	O identificador do objeto anterior dentro do sistema StorageGRID .
CAMINHO	Caminho do objeto S3	O caminho do objeto S3 usado para o objeto anterior e o novo
RSLT	Código de resultado	Resultado da transação de substituição de objeto. O resultado é sempre: SUCS: Bem-sucedido
SGRP	Site (Grupo)	Se presente, o objeto substituído foi excluído no site especificado, que não é o site onde o objeto substituído foi ingerido.

S3SL: Solicitação de seleção S3

Esta mensagem registra uma conclusão após uma solicitação S3 Select ter sido retornada ao cliente. A mensagem S3SL pode incluir detalhes da mensagem de erro e do código de erro. A solicitação pode não ter sido bem-sucedida.

Código	Campo	Descrição
BYSC	Bytes escaneados	Número de bytes escaneados (recebidos) dos nós de armazenamento. BYSC e BYPR provavelmente serão diferentes se o objeto for compactado. Se o objeto for compactado, BYSC terá a contagem de bytes compactados e BYPR serão os bytes após a descompactação.
BYPR	Bytes processados	Número de bytes processados. Indica quantos bytes de "Bytes escaneados" foram realmente processados ou acionados por um trabalho S3 Select.
BYRT	Bytes retornados	Número de bytes que um trabalho S3 Select retornou ao cliente.
REPR	Registros processados	Número de registros ou linhas que um trabalho S3 Select recebeu dos nós de armazenamento.

Código	Campo	Descrição
RERT	Registros Retornados	Número de registros ou linhas que um trabalho do S3 Select retornou ao cliente.
JOFI	Trabalho concluído	Indica se o trabalho S3 Select concluiu o processamento ou não. Se isso for falso, o trabalho não foi concluído e os campos de erro provavelmente conterão dados. O cliente pode ter recebido resultados parciais ou nenhum resultado.
REID	ID da solicitação	Identificador para a solicitação S3 Select.
EXTM	Tempo de execução	O tempo, em segundos, que levou para o S3 Select Job ser concluído.
ERMG	Mensagem de erro	Mensagem de erro gerada pelo trabalho S3 Select.
ERTY	Tipo de erro	Tipo de erro gerado pelo trabalho S3 Select.
ERST	Rastreamento de pilha de erros	Rastreamento de pilha de erros gerado pelo trabalho S3 Select.
S3BK	Balde S3	O nome do bucket S3.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 para o usuário que enviou a solicitação.
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket.

SADD: Desativação de auditoria de segurança

Esta mensagem indica que o serviço de origem (ID do nó) desativou o registro de mensagens de auditoria; as mensagens de auditoria não estão mais sendo coletadas ou entregues.

Código	Campo	Descrição
AETM	Método de ativação	O método usado para desabilitar a auditoria.

Código	Campo	Descrição
AEUN	Nome de usuário	O nome de usuário que executou o comando para desabilitar o registro de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.

A mensagem indica que o registro estava habilitado anteriormente, mas agora foi desabilitado. Isso normalmente é usado apenas durante ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada (SADE) e a capacidade de desabilitar a auditoria é bloqueada permanentemente.

SADE: Habilitar Auditoria de Segurança

Esta mensagem indica que o serviço de origem (ID do nó) restaurou o registro de mensagens de auditoria; as mensagens de auditoria estão sendo coletadas e entregues novamente.

Código	Campo	Descrição
AETM	Método de ativação	O método usado para permitir a auditoria.
AEUN	Nome de usuário	O nome de usuário que executou o comando para habilitar o registro de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.

A mensagem indica que o registro foi desabilitado anteriormente (SADD), mas agora foi restaurado. Isso normalmente é usado apenas durante ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada e a capacidade de desabilitar a auditoria é bloqueada permanentemente.

SCMT: Confirmação do Armazenamento de Objetos

O conteúdo da grade não é disponibilizado nem reconhecido como armazenado até que tenha sido confirmado (o que significa que foi armazenado persistentemente). O conteúdo armazenado de forma persistente foi completamente gravado no disco e passou pelas verificações de integridade relacionadas. Esta mensagem é emitida quando um bloco de conteúdo é confirmado no armazenamento.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo comprometido com armazenamento permanente.
RSLT	Código de resultado	Status no momento em que o objeto foi armazenado no disco: SUCS: Objeto armazenado com sucesso.

Esta mensagem significa que um determinado bloco de conteúdo foi completamente armazenado e verificado e agora pode ser solicitado. Ele pode ser usado para rastrear o fluxo de dados dentro do sistema.

SDEL: S3 EXCLUIR

Quando um cliente S3 emite uma transação DELETE, uma solicitação é feita para remover o objeto ou bucket especificado, ou para remover um sub-recurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. Operações em buckets não incluem este campo.
DMRK	Excluir ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket versionado. Operações em buckets não incluem este campo.
GFID	ID de conexão da federação de grade	O ID de conexão da federação de grade associada a uma solicitação de exclusão de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.
GFSA	ID da conta de origem da Federação de Grade	O ID da conta do locatário na grade de origem para uma solicitação de exclusão de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP) . `x-amz-bypass-governance-retention` é incluído automaticamente se estiver presente na solicitação.
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação DELETE. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.

Código	Campo	Descrição
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUDM	Identificador universalmente exclusivo para um marcador de exclusão	O identificador de um marcador de exclusão. As mensagens do log de auditoria especificam UUDM ou UUID, onde UUDM indica um marcador de exclusão criado como resultado de uma solicitação de exclusão de objeto, e UUID indica um objeto.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SGET: S3 OBTER

Quando um cliente S3 emite uma transação GET, uma solicitação é feita para recuperar um objeto ou listar os objetos em um bucket, ou para remover um sub-recurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. <code>`X-Forwarded-For`</code> é incluído automaticamente se estiver presente na solicitação e se o <code>`X-Forwarded-For`</code> valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP) .
LIDADE	ListObjectsV2	Uma resposta no formato v2 foi solicitada. Para mais detalhes, veja "AWS ListObjectsV2" . Somente para operações de bucket GET.
NCHD	Número de filhos	Inclui chaves e prefixos comuns. Somente para operações de bucket GET.
ALCANCE	Leitura de intervalo	Somente para operações de leitura de intervalo. Indica o intervalo de bytes que foi lido por esta solicitação. O valor após a barra (/) mostra o tamanho do objeto inteiro.
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.

Código	Campo	Descrição
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.

Código	Campo	Descrição
TRNC	Truncado ou Não Truncado	Defina como falso se todos os resultados foram retornados. Defina como verdadeiro se houver mais resultados disponíveis para retornar. Somente para operações de bucket GET.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SHEA: CABEÇA S3

Quando um cliente S3 emite uma transação HEAD, uma solicitação é feita para verificar a existência de um objeto ou bucket e recuperar os metadados sobre um objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto verificado em bytes. Operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP) .
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.

Código	Campo	Descrição
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPOS: POSTAGEM S3

Quando um cliente S3 emite uma solicitação de objeto POST, esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0.
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. <code>`X-Forwarded-For`</code> é incluído automaticamente se estiver presente na solicitação e se o <code>`X-Forwarded-For`</code> valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP) . (Não esperado para SPOS).
RSLT	Código de resultado	Resultado da solicitação RestoreObject. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável. Defina como "selecionar" para uma operação S3 Select.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SRCF	Configuração de sub-recursos	Restaurar informações.

Código	Campo	Descrição
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPUT: S3 PUT

Quando um cliente S3 emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou bucket, ou para remover um sub-recurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBID	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CMPS	Configurações de conformidade	As configurações de conformidade usadas ao criar o bucket, se presentes na solicitação (truncadas para os primeiros 1024 caracteres).
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.

Código	Campo	Descrição
GFID	ID de conexão da federação de grade	O ID de conexão da federação de grade associada a uma solicitação PUT de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.
GFSA	ID da conta de origem da Federação de Grade	O ID da conta do locatário na grade de origem para uma solicitação PUT de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP) . `x-amz-bypass-governance-retention` é incluído automaticamente se estiver presente na solicitação.
LKEN	Bloqueio de objeto habilitado	Valor do cabeçalho da solicitação <code>x-amz-bucket-object-lock-enabled</code> , se presente na solicitação.
LKLH	Bloqueio de objeto - retenção legal	Valor do cabeçalho da solicitação <code>x-amz-object-lock-legal-hold</code> , se presente na solicitação PutObject.
LKMD	Modo de retenção de bloqueio de objeto	Valor do cabeçalho da solicitação <code>x-amz-object-lock-mode</code> , se presente na solicitação PutObject.
LKRU	Bloqueio de objeto reter até a data	Valor do cabeçalho da solicitação <code>x-amz-object-lock-retain-until-date</code> , se presente na solicitação PutObject. Os valores são limitados a 100 anos a partir da data em que o objeto foi ingerido.
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação PUT. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SRCF	Configuração de sub-recursos	A nova configuração de sub-recursos (truncada para os primeiros 1024 caracteres).
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: urn:sgws:identity::03393893651506583485:root Vazio para solicitações anônimas.

Código	Campo	Descrição
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
ULID	ID de upload	Incluído somente em mensagens SPUT para operações CompleteMultipartUpload. Indica que todas as peças foram carregadas e montadas.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.
VSST	Estado de versão	O novo estado de controle de versão de um bucket. Dois estados são usados: "habilitado" ou "suspensão". Operações em objetos não incluem este campo.

SREM: Remoção de armazenamento de objetos

Esta mensagem é emitida quando o conteúdo é removido do armazenamento persistente e não está mais acessível por meio de APIs regulares.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo excluído do armazenamento permanente.
RSLT	Código de resultado	Indica o resultado das operações de remoção de conteúdo. O único valor definido é: SUCS: Conteúdo removido do armazenamento persistente

Esta mensagem de auditoria significa que um determinado bloco de conteúdo foi excluído de um nó e não pode mais ser solicitado diretamente. A mensagem pode ser usada para rastrear o fluxo de conteúdo excluído dentro do sistema.

SUPD: Metadados S3 atualizados

Esta mensagem é gerada pela API S3 quando um cliente S3 atualiza os metadados de um objeto ingerido. A mensagem é emitida pelo servidor se a atualização de metadados for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação, ao atualizar as configurações de conformidade de um bucket.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. <code>`X-Forwarded-For`</code> é incluído automaticamente se estiver presente na solicitação e se o <code>`X-Forwarded-For`</code> valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP) .
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre: SUCS: bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.

Código	Campo	Descrição
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto cujos metadados foram atualizados. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SVRF: Falha na verificação do armazenamento de objetos

Esta mensagem é emitida sempre que um bloco de conteúdo falha no processo de verificação. Cada vez que dados de objetos replicados são lidos ou gravados no disco, várias verificações e verificações de integridade são realizadas para garantir que os dados enviados ao usuário solicitante sejam idênticos aos dados originalmente inseridos no sistema. Se alguma dessas verificações falhar, o sistema colocará automaticamente

em quarentena os dados corrompidos do objeto replicado para impedir que sejam recuperados novamente.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que falhou na verificação.
RSLT	Código de resultado	Tipo de falha de verificação: CRCF: Falha na verificação de redundância cíclica (CRC). HMAC: Falha na verificação do código de autenticação de mensagem baseado em hash (HMAC). EHSB: Hash de conteúdo criptografado inesperado. PHSH: Hash de conteúdo original inesperado. SEQC: Sequência de dados incorreta no disco. PERR: Estrutura inválida do arquivo de disco. DERR: Erro de disco. FNAM: Nome de arquivo incorreto.



Esta mensagem deve ser monitorada de perto. Falhas na verificação de conteúdo podem indicar falhas iminentes de hardware.

Para determinar qual operação acionou a mensagem, consulte o valor do campo AMID (ID do módulo). Por exemplo, um valor SVFY indica que a mensagem foi gerada pelo módulo Storage Verifier, ou seja, verificação em segundo plano, e STOR indica que a mensagem foi acionada pela recuperação de conteúdo.

SVRU: Verificação de armazenamento de objeto desconhecido

O componente de armazenamento do serviço LDR verifica continuamente todas as cópias de dados de objetos replicados no armazenamento de objetos. Esta mensagem é emitida quando uma cópia desconhecida ou inesperada de dados de objetos replicados é detectada no armazenamento de objetos e movida para o diretório de quarentena.

Código	Campo	Descrição
FPTH	Caminho do arquivo	O caminho do arquivo da cópia inesperada do objeto.
RSLT	Resultado	Este campo tem o valor 'NENHUM'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.



A mensagem de auditoria SVRU: Object Store Verify Unknown deve ser monitorada de perto. Isso significa que cópias inesperadas de dados de objeto foram detectadas no armazenamento de objetos. Essa situação deve ser investigada imediatamente para determinar como essas cópias foram criadas, pois pode indicar falhas iminentes de hardware.

SYSD: Parada do nó

Quando um serviço é interrompido normalmente, esta mensagem é gerada para indicar que o desligamento foi solicitado. Normalmente, essa mensagem é enviada somente após uma reinicialização subsequente, porque a fila de mensagens de auditoria não é limpa antes do desligamento. Procure a mensagem SYST, enviada no início da sequência de desligamento, se o serviço não tiver sido reiniciado.

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza do desligamento: SUCS: O sistema foi desligado corretamente.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O RSLT de um SYSD não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SYST: Parada do nó

Quando um serviço é interrompido normalmente, esta mensagem é gerada para indicar que o desligamento foi solicitado e que o serviço iniciou sua sequência de desligamento. SYST pode ser usado para determinar se o desligamento foi solicitado antes do serviço ser reiniciado (ao contrário de SYSD, que normalmente é enviado após a reinicialização do serviço).

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza do desligamento: SUCS: O sistema foi desligado corretamente.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O código RSLT de uma mensagem SYST não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SYSU: Início do nó

Quando um serviço é reiniciado, esta mensagem é gerada para indicar se o desligamento anterior foi limpo (comandado) ou desordenado (inesperado).

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza do desligamento: SUCS: O sistema foi desligado corretamente. DSDN: O sistema não foi desligado corretamente. VRGN: O sistema foi iniciado pela primeira vez após a instalação do servidor (ou reinstalação).

A mensagem não indica se o servidor host foi iniciado, apenas o serviço de relatórios. Esta mensagem pode ser usada para:

- Detecte descontinuidade na trilha de auditoria.
- Determine se um serviço está falhando durante a operação (já que a natureza distribuída do sistema StorageGRID pode mascarar essas falhas). O Gerenciador do Servidor reinicia automaticamente um serviço com falha.

WDEL: Swift EXCLUIR

Quando um cliente Swift emite uma transação DELETE, uma solicitação é feita para remover o objeto ou contêiner especificado. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. Operações em contêineres não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.

Código	Campo	Descrição
RSLT	Código de resultado	Resultado da transação DELETE. O resultado é sempre: SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .
WCON	Contêiner Swift	O nome do contêiner Swift.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WGET: GET rápido

Quando um cliente Swift emite uma transação GET, uma solicitação é feita para recuperar um objeto, listar os objetos em um contêiner ou listar os contêineres em uma conta. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contas e contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em contas e contêineres não incluem este campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP) .
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre SUCS: bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .
WCON	Contêiner Swift	O nome do contêiner Swift. Operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contas e contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WHEA: CABEÇA Rápida

Quando um cliente Swift emite uma transação HEAD, uma solicitação é feita para verificar a existência de uma conta, contêiner ou objeto e recuperar quaisquer metadados relevantes. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contas e contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em contas e contêineres não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For` é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código de resultado	Resultado da transação HEAD. O resultado é sempre: SUCS: bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .
WCON	Contêiner Swift	O nome do contêiner Swift. Operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contas e contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WPUT: PUT rápido

Quando um cliente Swift emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou contêiner. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em contêineres não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. <code>`X-Forwarded-For`</code> é incluído automaticamente se estiver presente na solicitação e se o <code>`X-Forwarded-For`</code> valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação PUT. O resultado é sempre: SUCS: bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .

Código	Campo	Descrição
WCON	Contêiner Swift	O nome do contêiner Swift.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

Expandir uma grade

Tipos de expansão

Você pode expandir a capacidade ou os recursos do seu sistema StorageGRID sem interromper as operações do sistema.

Uma expansão StorageGRID permite que você adicione:

- Volumes de armazenamento para nós de armazenamento
- Novos nós de grade para um site existente
- Um site totalmente novo

O motivo pelo qual você está realizando a expansão determina quantos novos nós de cada tipo você deve adicionar e a localização desses novos nós. Por exemplo, há diferentes requisitos de nó se você estiver realizando uma expansão para aumentar a capacidade de armazenamento, adicionar capacidade de metadados ou adicionar redundância ou novos recursos.

Siga os passos para o tipo de expansão que você está realizando:

Adicionar volumes de armazenamento

Siga os passos para ["adicionando volumes de armazenamento aos nós de armazenamento"](#) .

Adicionar nós de grade

1. Siga os passos para ["adicionando nós de grade a um site existente"](#) .
2. ["Atualizar as sub-redes"](#) .
3. Implantar nós de grade:
 - ["Eletrodomésticos"](#)
 - ["VMware"](#)
 - ["Linux"](#)



"Linux" refere-se a uma implantação do Red Hat Enterprise Linux, Ubuntu ou Debian. Para obter uma lista de versões suportadas, consulte o ["Ferramenta de Matriz de Interoperabilidade NetApp \(IMT\)"](#) .

4. ["Executar a expansão"](#) .
5. ["Configurar o sistema expandido"](#) .

Adicionar novo site

1. Siga os passos para ["Adicionando um novo site"](#) .
2. ["Atualizar as sub-redes"](#) .
3. Implantar nós de grade:
 - ["Eletrodomésticos"](#)
 - ["VMware"](#)
 - ["Linux"](#)



"Linux" refere-se a uma implantação do Red Hat Enterprise Linux, Ubuntu ou Debian. Para obter uma lista de versões suportadas, consulte o ["Ferramenta de Matriz de Interoperabilidade NetApp \(IMT\)"](#) .

4. ["Executar a expansão"](#) .
5. ["Configurar o sistema expandido"](#) .

Plano de expansão do StorageGRID

Adicionar capacidade de armazenamento

Diretrizes para adicionar capacidade de objeto

Você pode expandir a capacidade de armazenamento de objetos do seu sistema StorageGRID adicionando volumes de armazenamento aos nós de armazenamento existentes ou adicionando novos nós de armazenamento aos sites existentes. Você deve adicionar capacidade de armazenamento de uma forma que atenda aos requisitos da

sua política de gerenciamento do ciclo de vida das informações (ILM).

Diretrizes para adicionar volumes de armazenamento

Antes de adicionar volumes de armazenamento aos nós de armazenamento existentes, revise as seguintes diretrizes e limitações:

- Você deve examinar suas regras atuais de ILM para determinar onde e quando ["adicionar volumes de armazenamento"](#) para aumentar o armazenamento disponível para ["objetos replicados"](#) ou ["objetos codificados por apagamento"](#).
- Você não pode aumentar a capacidade de metadados do seu sistema adicionando volumes de armazenamento porque os metadados do objeto são armazenados somente no volume 0.
- Cada nó de armazenamento baseado em software pode suportar no máximo 48 volumes de armazenamento. Se precisar adicionar capacidade além disso, você deverá adicionar novos Nós de Armazenamento.
- Você pode adicionar uma ou duas prateleiras de expansão a cada aparelho SG6060. Cada prateleira de expansão adiciona 16 volumes de armazenamento. Com ambas as prateleiras de expansão instaladas, o SG6060 pode suportar um total de 48 volumes de armazenamento.
- Você pode adicionar uma ou duas prateleiras de expansão a cada aparelho SG6160. Cada prateleira de expansão adiciona 60 volumes de armazenamento. Com ambas as prateleiras de expansão instaladas, o SG6160 pode suportar um total de 180 volumes de armazenamento.
- Não é possível adicionar volumes de armazenamento a nenhum outro dispositivo de armazenamento.
- Não é possível aumentar o tamanho de um volume de armazenamento existente.
- Não é possível adicionar volumes de armazenamento a um nó de armazenamento ao mesmo tempo em que você executa uma atualização do sistema, uma operação de recuperação ou outra expansão.

Depois de decidir adicionar volumes de armazenamento e determinar quais nós de armazenamento você deve expandir para atender à sua política de ILM, siga as instruções para seu tipo de nó de armazenamento:

- Para adicionar uma ou duas prateleiras de expansão a um dispositivo de armazenamento SG6060, acesse ["Adicionar prateleira de expansão ao SG6060 implantado"](#).
- Para adicionar uma ou duas prateleiras de expansão a um dispositivo de armazenamento SG6160, acesse ["Adicionar prateleira de expansão ao SG6160 implantado"](#).
- Para um nó baseado em software, siga as instruções para ["adicionando volumes de armazenamento aos nós de armazenamento"](#).

Diretrizes para adicionar nós de armazenamento

Antes de adicionar nós de armazenamento a sites existentes, revise as seguintes diretrizes e limitações:

- Você deve examinar suas regras atuais de ILM para determinar onde e quando adicionar nós de armazenamento para aumentar o armazenamento disponível para ["objetos replicados"](#) ou ["objetos codificados por apagamento"](#).
- Você não deve adicionar mais de 10 nós de armazenamento em um único procedimento de expansão.
- Você pode adicionar nós de armazenamento a mais de um site em um único procedimento de expansão.
- Você pode adicionar nós de armazenamento e outros tipos de nós em um único procedimento de expansão.
- Antes de iniciar o procedimento de expansão, você deve confirmar se todas as operações de reparo de dados executadas como parte de uma recuperação foram concluídas. Ver ["Verifique os trabalhos de"](#)

[reparo de dados](#)".

- Se você precisar remover nós de armazenamento antes ou depois de executar uma expansão, não descomissione mais de 10 nós de armazenamento em um único procedimento de descomissionamento de nó.

Diretrizes para serviço ADC em nós de armazenamento

Ao configurar a expansão, você deve escolher se deseja incluir o serviço Controlador de Domínio Administrativo (ADC) em cada novo Nó de Armazenamento. O serviço ADC monitora a localização e a disponibilidade dos serviços de rede.

- O sistema StorageGRID requer um ["quórum de serviços ADC"](#) estar disponível em cada local e em todos os momentos.
- Pelo menos três nós de armazenamento em cada site devem incluir o serviço ADC.
- Não é recomendado adicionar o serviço ADC a cada nó de armazenamento. Incluir muitos serviços ADC pode causar lentidão devido ao aumento da quantidade de comunicação entre os nós.
- Uma única grade não deve ter mais de 48 nós de armazenamento com o serviço ADC. Isso equivale a 16 locais com três serviços ADC em cada local.
- Em geral, ao selecionar a configuração **Serviço ADC** para um novo nó, você deve selecionar **Automático**. Selecione **Sim** somente se o novo nó substituir outro nó de armazenamento que incluía o serviço ADC. Como não é possível desativar um nó de armazenamento se houver poucos serviços ADC restantes, isso garante que um novo serviço ADC esteja disponível antes que o serviço antigo seja removido.
- Não é possível adicionar o serviço ADC a um nó depois que ele for implantado.

Adicionar capacidade de armazenamento para objetos replicados

Se a política de gerenciamento do ciclo de vida das informações (ILM) da sua implantação incluir uma regra que cria cópias replicadas de objetos, você deverá considerar quanto armazenamento adicionar e onde adicionar os novos volumes de armazenamento ou nós de armazenamento.

Para obter orientação sobre onde adicionar armazenamento adicional, examine as regras do ILM que criam cópias replicadas. Se as regras do ILM criarem duas ou mais cópias de objetos, planeje adicionar armazenamento em cada local onde as cópias de objetos são feitas. Como um exemplo simples, se você tiver uma grade de dois sites e uma regra ILM que cria uma cópia de objeto em cada site, você deve ["adicionar armazenamento"](#) para cada site para aumentar a capacidade geral de objetos da grade. Para obter informações sobre replicação de objetos, consulte ["O que é replicação"](#).

Por motivos de desempenho, você deve tentar manter a capacidade de armazenamento e o poder de computação equilibrados entre os sites. Portanto, para este exemplo, você deve adicionar o mesmo número de nós de armazenamento a cada site ou volumes de armazenamento adicionais em cada site.

Se você tiver uma política de ILM mais complexa que incluía regras que colocam objetos em locais diferentes com base em critérios como nome do bucket ou regras que alteram os locais dos objetos ao longo do tempo, sua análise de onde o armazenamento é necessário para a expansão será semelhante, mas mais complexa.

Mapear a rapidez com que a capacidade geral de armazenamento está sendo consumida pode ajudar você a entender quanto armazenamento adicionar na expansão e quando o espaço de armazenamento adicional será necessário. Você pode usar o Grid Manager para ["capacidade de armazenamento de monitores e gráficos"](#).

Ao planejar o momento de uma expansão, lembre-se de considerar quanto tempo pode levar para adquirir e instalar armazenamento adicional.

Adicionar capacidade de armazenamento para objetos codificados por eliminação

Se sua política de ILM incluir uma regra que faz cópias codificadas para eliminação, você deverá planejar onde adicionar novo armazenamento e quando adicioná-lo. A quantidade de armazenamento que você adiciona e o momento da adição podem afetar a capacidade de armazenamento utilizável da rede.

O primeiro passo no planejamento de uma expansão de armazenamento é examinar as regras na sua política de ILM que criam objetos codificados para eliminação. Como o StorageGRID cria $k+m$ fragmentos para cada objeto codificado por eliminação e armazena cada fragmento em um nó de armazenamento diferente, você deve garantir que pelo menos $k+m$ nós de armazenamento tenham espaço para novos dados codificados por eliminação após a expansão. Se o perfil de codificação de eliminação fornecer proteção contra perda de site, você deverá adicionar armazenamento a cada site. Ver ["O que são esquemas de codificação de apagamento"](#) para obter informações sobre perfis de codificação de eliminação.

O número de nós que você precisa adicionar também depende de quão cheios os nós existentes estarão quando você realizar a expansão.

Recomendação geral para adicionar capacidade de armazenamento para objetos codificados por eliminação

Se quiser evitar cálculos detalhados, você pode adicionar dois nós de armazenamento por site quando os nós de armazenamento existentes atingirem 70% da capacidade.

Esta recomendação geral fornece resultados razoáveis em uma ampla gama de esquemas de codificação de apagamento para grades de site único e para grades onde a codificação de apagamento fornece proteção contra perda de site.

Para entender melhor os fatores que levaram a esta recomendação ou para desenvolver um plano mais preciso para o seu site, consulte ["Considerações para rebalanceamento de dados codificados por eliminação"](#). Para uma recomendação personalizada otimizada para sua situação, entre em contato com seu consultor de serviços profissionais da NetApp.

Considerações para rebalanceamento de dados codificados por eliminação

Se você estiver executando uma expansão para adicionar nós de armazenamento e usar regras de ILM para apagar dados de código, talvez seja necessário executar o procedimento de rebalanceamento de codificação de eliminação (EC) se não puder adicionar nós de armazenamento suficientes para o esquema de codificação de eliminação que estiver usando.

Após revisar essas considerações, execute a expansão e vá para ["Rebalancear dados codificados para eliminação após adicionar nós de armazenamento"](#) para executar o procedimento.

O que é rebalanceamento de EC?

O rebalanceamento do EC é um procedimento do StorageGRID que pode ser necessário após uma expansão do nó de armazenamento. O procedimento é executado como um script de linha de comando do nó de administração principal. Quando você executa o procedimento de rebalanceamento do EC, o StorageGRID redistribui fragmentos codificados para eliminação entre os nós de armazenamento existentes e os recém-adicionados em um site.

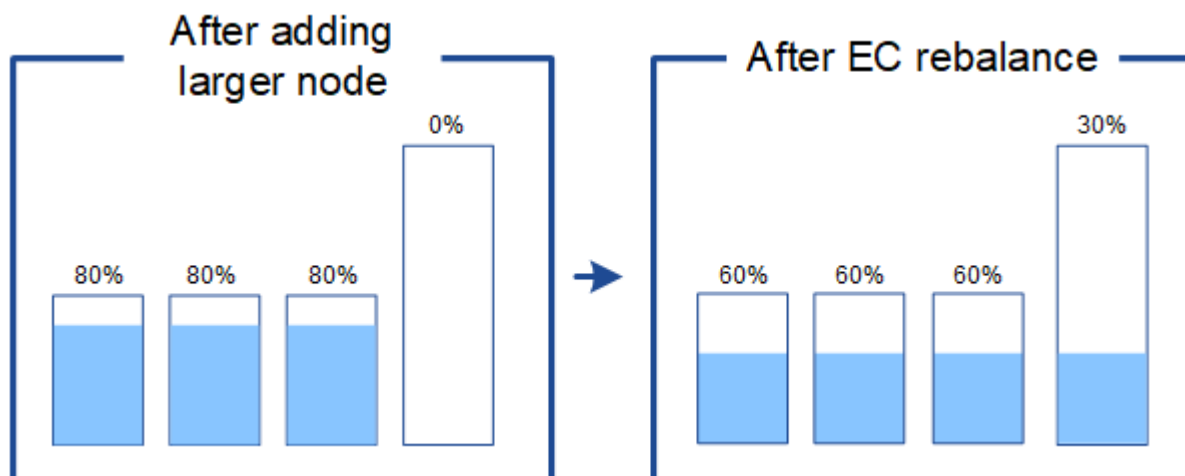
O procedimento de reequilíbrio da CE:

- Move somente dados de objetos codificados para eliminação. Ele não move dados de objetos replicados.
- Redistribui os dados dentro de um site. Ele não move dados entre sites.
- Redistribui dados entre todos os nós de armazenamento em um site. Ele não redistribui dados dentro dos volumes de armazenamento.
- Não considera o uso de dados replicados em cada nó de armazenamento ao determinar para onde mover os dados codificados para eliminação.
- Redistribui dados codificados para eliminação uniformemente entre os nós de armazenamento sem considerar as capacidades relativas de cada nó.
- Não distribuirá dados codificados para eliminação para nós de armazenamento que estejam mais de 80% cheios.
- Pode diminuir o desempenho das operações do ILM e das operações do cliente S3 quando ele é executado; recursos adicionais são necessários para redistribuir os fragmentos de codificação de eliminação.

Quando o procedimento de reequilíbrio da CE estiver concluído:

- Os dados codificados para eliminação serão movidos de nós de armazenamento com menos espaço disponível para nós de armazenamento com mais espaço disponível.
- A proteção de dados de objetos codificados para eliminação não será alterada.
- Os valores usados (%) podem ser diferentes entre os nós de armazenamento por dois motivos:
 - Cópias de objetos replicados continuarão consumindo espaço nos nós existentes; o procedimento de rebalanceamento do EC não move dados replicados.
 - Nós de maior capacidade estarão relativamente menos cheios do que nós de menor capacidade, embora todos os nós acabem com aproximadamente a mesma quantidade de dados codificados para eliminação.

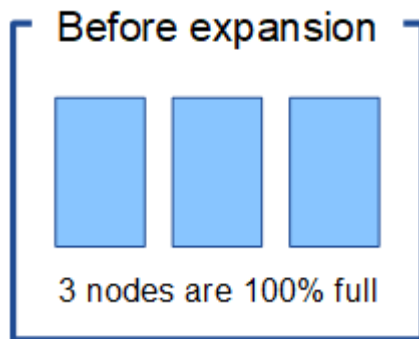
Por exemplo, suponha que três nós de 200 TB estejam cada um preenchido até 80% ($200 \times 0,8 = 160$ TB em cada nó, ou 480 TB para o site). Se você adicionar um nó de 400 TB e executar o procedimento de rebalanceamento, todos os nós terão aproximadamente a mesma quantidade de dados de código de eliminação ($480/4 = 120$ TB). Entretanto, o Usado (%) para o nó maior será menor que o Usado (%) para os nós menores.



Quando rebalancear dados codificados por eliminação

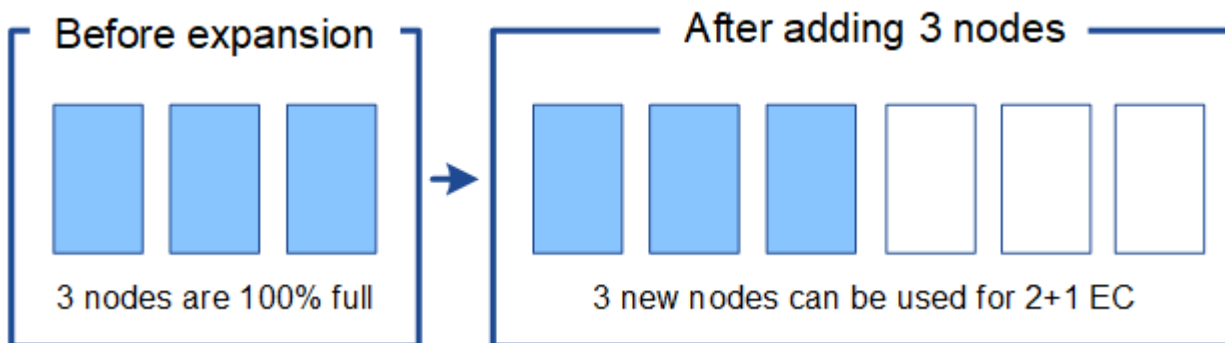
Considere o seguinte cenário:

- O StorageGRID está sendo executado em um único site, que contém três nós de armazenamento.
- A política ILM usa uma regra de codificação de eliminação 2+1 para todos os objetos maiores que 1,0 MB e uma regra de replicação de 2 cópias para objetos menores.
- Todos os nós de armazenamento ficaram completamente cheios. O alerta **Low Object Storage** foi acionado no nível de gravidade mais alto.



O rebalanceamento não é necessário se você adicionar nós suficientes

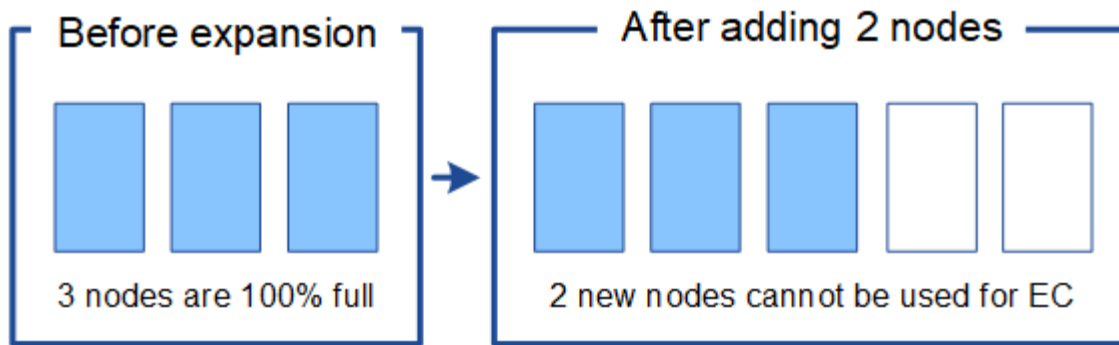
Para entender quando o rebalanceamento do EC não é necessário, suponha que você adicionou três (ou mais) novos nós de armazenamento. Neste caso, você não precisa realizar o rebalanceamento do EC. Os nós de armazenamento originais permanecerão cheios, mas novos objetos agora usarão os três novos nós para codificação de eliminação 2+1; os dois fragmentos de dados e o fragmento de paridade podem ser armazenados em um nó diferente.



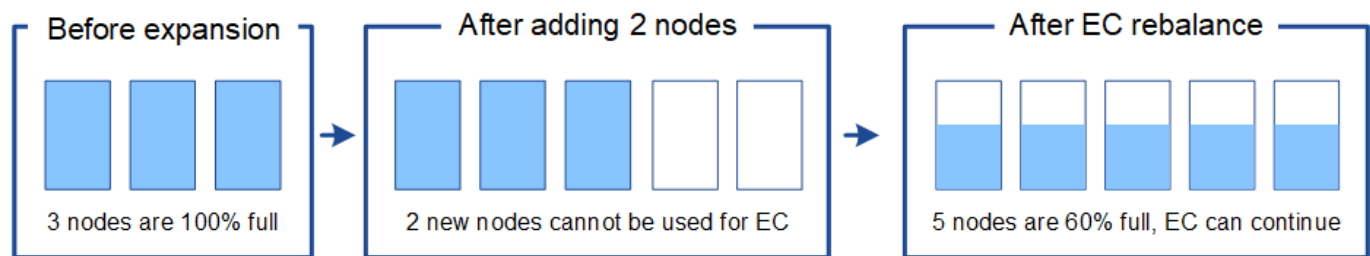
Embora você possa executar o procedimento de rebalanceamento do EC neste caso, mover os dados codificados para eliminação existentes diminuirá temporariamente o desempenho da grade, o que pode afetar as operações do cliente.

O rebalanceamento é necessário se você não puder adicionar nós suficientes

Para entender quando o rebalanceamento do EC é necessário, suponha que você só pode adicionar dois nós de armazenamento, em vez de três. Como o esquema 2+1 exige que pelo menos três nós de armazenamento tenham espaço disponível, os nós vazios não podem ser usados para novos dados codificados para eliminação.



Para utilizar os novos nós de armazenamento, você deve executar o procedimento de rebalanceamento do EC. Quando esse procedimento é executado, o StorageGRID redistribui os dados codificados por eliminação e os fragmentos de paridade existentes entre todos os nós de armazenamento no site. Neste exemplo, quando o procedimento de rebalanceamento do EC é concluído, todos os cinco nós estão agora apenas 60% cheios, e os objetos podem continuar a ser ingeridos no esquema de codificação de eliminação 2+1 em todos os nós de armazenamento.



Recomendações para o reequilíbrio da CE

A NetApp exigirá o rebalanceamento do EC se *todas* as seguintes afirmações forem verdadeiras:

- Use codificação de eliminação para seus dados de objeto.
- O alerta **Low Object Storage** foi acionado para um ou mais nós de armazenamento em um site, indicando que os nós estão 80% ou mais cheios.
- Você não consegue adicionar novos Nós de Armazenamento suficientes para o esquema de codificação de eliminação em uso. Ver ["Adicionar capacidade de armazenamento para objetos codificados por eliminação"](#).
- Seus clientes S3 podem tolerar menor desempenho em suas operações de leitura e gravação enquanto o procedimento de rebalanceamento do EC estiver em execução.

Opcionalmente, você pode executar o procedimento de rebalanceamento do EC se preferir que os nós de armazenamento sejam preenchidos com níveis semelhantes e seus clientes S3 puderem tolerar desempenho inferior para suas operações de leitura e gravação enquanto o procedimento de rebalanceamento do EC estiver em execução.

Como o procedimento de rebalanceamento da CE interage com outras tarefas de manutenção

Não é possível executar determinados procedimentos de manutenção ao mesmo tempo em que se executa o procedimento de rebalanceamento do EC.

Procedimento	Permitido durante o procedimento de rebalanceamento da CE?
Procedimentos adicionais de reequilíbrio da CE	Não. Você só pode executar um procedimento de rebalanceamento de EC por vez.
Procedimento de descomissionamento Trabalho de reparo de dados EC	Não. • Você não poderá iniciar um procedimento de descomissionamento ou um reparo de dados do EC enquanto o procedimento de rebalanceamento do EC estiver em execução. • Você está impedido de iniciar o procedimento de rebalanceamento do EC enquanto um procedimento de desativação do nó de armazenamento ou um reparo de dados do EC estiver em execução.
Procedimento de expansão	Não. Se você precisar adicionar novos nós de armazenamento em uma expansão, execute o procedimento de rebalanceamento do EC após adicionar todos os novos nós.
Procedimento de atualização	Não. Se você precisar atualizar o software StorageGRID , execute o procedimento de atualização antes ou depois de executar o procedimento de rebalanceamento do EC. Conforme necessário, você pode encerrar o procedimento de rebalanceamento do EC para realizar uma atualização de software.
Procedimento de clonagem do nó do dispositivo	Não. Se você precisar clonar um nó de armazenamento do dispositivo, execute o procedimento de rebalanceamento do EC após adicionar o novo nó.
Procedimento de correção	Sim. Você pode aplicar um hotfix do StorageGRID enquanto o procedimento de rebalanceamento do EC estiver em execução.
Outros procedimentos de manutenção	Não. Você deve encerrar o procedimento de rebalanceamento do EC antes de executar outros procedimentos de manutenção.

Como o procedimento de rebalanceamento da CE interage com o ILM

Enquanto o procedimento de rebalanceamento do EC estiver em execução, evite fazer alterações no ILM que possam alterar a localização de objetos codificados para eliminação existentes. Por exemplo, não comece a

usar uma regra ILM que tenha um perfil de codificação de eliminação diferente. Se precisar fazer tais alterações no ILM, você deverá encerrar o procedimento de rebalanceamento do EC.

Adicionar capacidade de metadados

Para garantir que haja espaço adequado disponível para metadados de objetos, talvez seja necessário executar um procedimento de expansão para adicionar novos nós de armazenamento em cada site.

O StorageGRID reserva espaço para metadados de objetos no volume 0 de cada nó de armazenamento. Três cópias de todos os metadados do objeto são mantidas em cada site, distribuídas uniformemente entre todos os nós de armazenamento.

Você pode usar o Grid Manager para monitorar a capacidade de metadados dos nós de armazenamento e estimar a rapidez com que a capacidade de metadados está sendo consumida. Além disso, o alerta **Armazenamento de metadados baixo** é acionado para um Nó de Armazenamento quando o espaço de metadados usado atinge determinados limites.

Observe que a capacidade de metadados de objetos de uma grade pode ser consumida mais rapidamente do que sua capacidade de armazenamento de objetos, dependendo de como você usa a grade. Por exemplo, se você normalmente ingere grandes quantidades de objetos pequenos ou adiciona grandes quantidades de metadados ou tags de usuário a objetos, pode ser necessário adicionar Nós de Armazenamento para aumentar a capacidade de metadados, mesmo que ainda haja capacidade de armazenamento de objetos suficiente.

Para mais informações, consulte o seguinte:

- ["Gerenciar armazenamento de metadados de objetos"](#)
- ["Monitorar a capacidade de metadados do objeto para cada nó de armazenamento"](#)

Diretrizes para aumentar a capacidade de metadados

Antes de adicionar nós de armazenamento para aumentar a capacidade de metadados, revise as seguintes diretrizes e limitações:

- Supondo que haja capacidade de armazenamento de objetos suficiente, ter mais espaço disponível para metadados de objetos aumenta o número de objetos que você pode armazenar no seu sistema StorageGRID .
- Você pode aumentar a capacidade de metadados de uma grade adicionando um ou mais nós de armazenamento a cada site.
- O espaço real reservado para metadados de objetos em qualquer nó de armazenamento depende da opção de armazenamento Espaço reservado de metadados (configuração de todo o sistema), da quantidade de RAM alocada ao nó e do tamanho do volume 0 do nó.
- Não é possível aumentar a capacidade de metadados adicionando volumes de armazenamento aos nós de armazenamento existentes, porque os metadados são armazenados somente no volume 0.
- Você não pode aumentar a capacidade de metadados adicionando um novo site.
- O StorageGRID mantém três cópias de todos os metadados de objetos em cada site. Por esse motivo, a capacidade de metadados do seu sistema é limitada pela capacidade de metadados do seu menor site.
- Ao adicionar capacidade de metadados, você deve adicionar o mesmo número de nós de armazenamento a cada site.

Os nós de armazenamento somente de metadados têm requisitos de hardware específicos:

- Ao usar dispositivos StorageGRID , nós somente de metadados podem ser configurados somente em dispositivos SGF6112 com doze unidades de 1,9 TB ou doze de 3,8 TB.
- Ao usar nós baseados em software, os recursos de nós somente de metadados devem corresponder aos recursos de nós de armazenamento existentes. Por exemplo:
 - Se o site StorageGRID existente estiver usando dispositivos SG6000 ou SG6100, os nós somente de metadados baseados em software deverão atender aos seguintes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - 8 TB SSD ou armazenamento equivalente para o banco de dados Cassandra (rangedb/0)
 - Se o site StorageGRID existente estiver usando nós de armazenamento virtuais com 24 GB de RAM, CPU de 8 núcleos e 3 TB ou 4 TB de armazenamento de metadados, os nós somente de metadados baseados em software deverão usar recursos semelhantes (24 GB de RAM, CPU de 8 núcleos e 4 TB de armazenamento de metadados (rangedb/0)).
- Ao adicionar um novo site StorageGRID , a capacidade total de metadados do novo site deve, no mínimo, corresponder aos sites StorageGRID existentes e os novos recursos do site devem corresponder aos nós de armazenamento nos sites StorageGRID existentes.

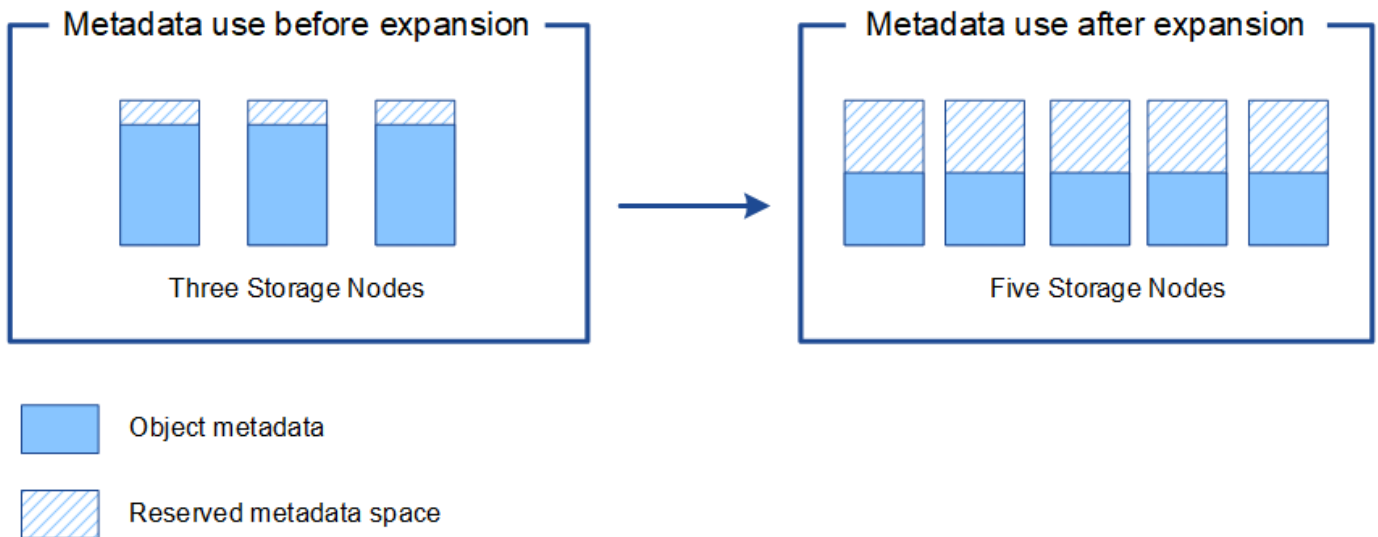
Veja o "[descrição do que é Espaço Reservado de Metadados](#)".

Como os metadados são redistribuídos quando você adiciona nós de armazenamento

Quando você adiciona nós de armazenamento em uma expansão, o StorageGRID redistribui os metadados do objeto existente para os novos nós em cada site, o que aumenta a capacidade geral de metadados da grade. Nenhuma ação do usuário é necessária.

A figura a seguir mostra como o StorageGRID redistribui metadados de objetos quando você adiciona nós de armazenamento em uma expansão. O lado esquerdo da figura representa o volume 0 de três nós de armazenamento antes de uma expansão. Os metadados estão consumindo uma parte relativamente grande do espaço de metadados disponível de cada nó, e o alerta **Armazenamento baixo de metadados** foi acionado.

O lado direito da figura mostra como os metadados existentes são redistribuídos depois que dois nós de armazenamento são adicionados ao site. A quantidade de metadados em cada nó diminuiu, o alerta **Armazenamento baixo de metadados** não é mais acionado e o espaço disponível para metadados aumentou.



Adicione nós de grade para adicionar recursos ao seu sistema

Você pode adicionar redundância ou recursos adicionais a um sistema StorageGRID adicionando novos nós de grade a sites existentes.

Por exemplo, você pode optar por adicionar nós de gateway para usar em um grupo de alta disponibilidade (HA) ou pode adicionar um nó de administração em um site remoto para permitir o monitoramento usando um nó local.

Você pode adicionar um ou mais dos seguintes tipos de nós a um ou mais sites existentes em uma única operação de expansão:

- Nós administrativos não primários
- Nós de armazenamento
- Nós de gateway

Ao se preparar para adicionar nós de grade, esteja ciente das seguintes limitações:

- O nó de administração principal é implantado durante a instalação inicial. Não é possível adicionar um nó de administração primário durante uma expansão.
- Você pode adicionar nós de armazenamento e outros tipos de nós na mesma expansão.
- Ao adicionar nós de armazenamento, você deve planejar cuidadosamente o número e a localização dos novos nós. Ver ["Diretrizes para adicionar capacidade de objeto"](#).
- Se a opção **Definir novo nó padrão** for **Não confiável** na guia Redes de clientes não confiáveis na página Controle de firewall, os aplicativos clientes que se conectam aos nós de expansão usando a Rede do cliente devem se conectar usando uma porta de ponto de extremidade do balanceador de carga (**CONFIGURAÇÃO > Segurança > Controle de firewall**). Veja as instruções para ["alterar a configuração de segurança para o novo nó"](#) e para ["configurar pontos de extremidade do balanceador de carga"](#).

Adicionar um novo site

Você pode expandir seu sistema StorageGRID adicionando um novo site.

Diretrizes para adicionar um site

Antes de adicionar um site, revise os seguintes requisitos e limitações:

- Você só pode adicionar um site por operação de expansão.
- Não é possível adicionar nós de grade a um site existente como parte da mesma expansão.
- Todos os sites devem incluir pelo menos três nós de armazenamento.
- Adicionar um novo site não aumenta automaticamente o número de objetos que você pode armazenar. A capacidade total de objetos de uma grade depende da quantidade de armazenamento disponível, da política de ILM e da capacidade de metadados em cada site.
- Ao dimensionar um novo site, você deve garantir que ele inclua capacidade de metadados suficiente.

O StorageGRID mantém uma cópia de todos os metadados do objeto em cada site. Ao adicionar um novo site, você deve garantir que ele inclua capacidade de metadados suficiente para os metadados do objeto existente e capacidade de metadados suficiente para o crescimento.

Para mais informações, consulte o seguinte:

- ["Gerenciar armazenamento de metadados de objetos"](#)
- ["Monitorar a capacidade de metadados do objeto para cada nó de armazenamento"](#)
- Você deve considerar a largura de banda de rede disponível entre os sites e o nível de latência da rede. As atualizações de metadados são continuamente replicadas entre sites, mesmo que todos os objetos sejam armazenados apenas no site onde são ingeridos.
- Como seu sistema StorageGRID permanece operacional durante a expansão, você deve revisar as regras do ILM antes de iniciar o procedimento de expansão. Você deve garantir que cópias de objetos não sejam armazenadas no novo site até que o procedimento de expansão seja concluído.

Por exemplo, antes de iniciar a expansão, determine se alguma regra usa o pool de armazenamento padrão (Todos os nós de armazenamento). Se isso acontecer, você deverá criar um novo pool de armazenamento que contenha os nós de armazenamento existentes e atualizar suas regras de ILM para usar o novo pool de armazenamento. Caso contrário, os objetos serão copiados para o novo site assim que o primeiro nó naquele site se tornar ativo.

Para obter mais informações sobre como alterar o ILM ao adicionar um novo site, consulte o ["exemplo de alteração de uma política de ILM"](#).

Reúna os materiais necessários

Antes de executar uma operação de expansão, reúna os materiais e instale e configure qualquer novo hardware e redes.

Item	Notas
Arquivo de instalação do StorageGRID	Se você estiver adicionando novos nós de grade ou um novo site, deverá baixar e extrair o arquivo de instalação do StorageGRID . Você deve usar a mesma versão que está sendo executada atualmente na grade. Para mais detalhes, consulte as instruções para baixando e extraindo os arquivos de instalação do StorageGRID . Observação: você não precisa baixar arquivos se estiver adicionando novos volumes de armazenamento aos nós de armazenamento existentes ou instalando um novo dispositivo StorageGRID .
Laptop de serviço	O laptop de serviço possui o seguinte: • Porta de rede • Cliente SSH (por exemplo, PuTTY) • "Navegador da Web compatível"
`Passwords.txt`arquivo	Contém as senhas necessárias para acessar os nós da grade na linha de comando. Incluído no Pacote de Recuperação.
Senha de provisionamento	A senha é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está no <code>Passwords.txt</code> arquivo.
Documentação do StorageGRID	• "Administrar StorageGRID" • "Notas de lançamento" • Instruções de instalação para sua plataforma ◦ "Instalar o StorageGRID no Red Hat Enterprise Linux" ◦ "Instalar o StorageGRID no Ubuntu ou Debian" ◦ "Instalar o StorageGRID no VMware"
Documentação atual para sua plataforma	Para versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade (IMT)" .

Baixe e extraia os arquivos de instalação do StorageGRID

Antes de adicionar novos nós de grade ou um novo site, você deve baixar o arquivo de instalação apropriado do StorageGRID e extrair os arquivos.

Sobre esta tarefa

Você deve executar operações de expansão usando a versão do StorageGRID que está atualmente em execução na grade.

Passos

1. Vá para "[Downloads da NetApp : StorageGRID](#)".
2. Selecione a versão do StorageGRID que está sendo executada atualmente na grade.
3. Sign in com o nome de usuário e a senha da sua conta NetApp .
4. Leia o Contrato de Licença do Usuário Final, marque a caixa de seleção e selecione **Aceitar e Continuar**.
5. Na coluna **Instalar StorageGRID** da página de download, selecione o .tgz ou .zip arquivo para sua plataforma.

A versão mostrada no arquivo de instalação deve corresponder à versão do software que está instalado no momento.

Use o .zip arquivo se você estiver executando o Windows no laptop de serviço.

Plataforma	Arquivo de instalação
Red Hat Enterprise Linux	StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .tgz
Ubuntu ou Debian ou Appliances	StorageGRID-Webscale- <i>version</i> -DEB- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -DEB- <i>uniqueID</i> .tgz
VMware	StorageGRID-Webscale- <i>version</i> -VMware- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -VMware- <i>uniqueID</i> .tgz
OpenStack/outro hipervisor	Para expandir uma implantação existente no OpenStack, você deve implantar uma máquina virtual executando uma das distribuições Linux suportadas listadas acima e seguir as instruções apropriadas para Linux.

6. Baixe e extraia o arquivo compactado.
7. Siga as etapas apropriadas para sua plataforma para escolher os arquivos necessários, com base na sua plataforma, na topologia de grade planejada e em como você expandirá seu sistema StorageGRID .

Os caminhos listados na etapa para cada plataforma são relativos ao diretório de nível superior instalado pelo arquivo compactado.

8. Se você estiver expandindo um sistema Red Hat Enterprise Linux, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID .
	Uma licença gratuita que não fornece nenhum direito de suporte para o produto.
	Pacote RPM para instalar as imagens do nó StorageGRID nos seus hosts RHEL.

Caminho e nome do arquivo	Descrição
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID .
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID .
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único estiver ativado. Você também pode usar este script para integração do Ping Federate.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> roteiro.
	Exemplo de função e manual do Ansible para configurar hosts RHEL para implantação de contêiner StorageGRID . Você pode personalizar a função ou o manual conforme necessário.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado usando o Active Directory ou o Ping Federate.
	Um script auxiliar chamado pelo companheiro <code>storagegrid-ssoauth-azure.py</code> Script Python para executar interações SSO com o Azure.
	Esquemas de API para StorageGRID. Observação: antes de executar uma atualização, você pode usar esses esquemas para confirmar se qualquer código que você escreveu para usar as APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID , caso você não tenha um ambiente StorageGRID não produtivo para testes de compatibilidade de atualização.

1. Se você estiver expandindo um sistema Ubuntu ou Debian, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID .
	Um arquivo de licença NetApp não produtivo que você pode usar para testes e implantações de prova de conceito.
	Pacote DEB para instalar as imagens do nó StorageGRID em hosts Ubuntu ou Debian.
	Soma de verificação MD5 para o arquivo /debs/storagegrid-webscale-images-version-SHA.deb .
	Pacote DEB para instalar o serviço de host StorageGRID em hosts Ubuntu ou Debian.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID .
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID .
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único estiver ativado. Você também pode usar este script para integração do Ping Federate.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> roteiro.
	Exemplo de função e manual do Ansible para configurar hosts Ubuntu ou Debian para implantação de contêiner StorageGRID . Você pode personalizar a função ou o manual conforme necessário.

Caminho e nome do arquivo	Descrição
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado usando o Active Directory ou o Ping Federate.
	Um script auxiliar chamado pelo companheiro <code>storagegrid-ssoauth-azure.py</code> Script Python para executar interações SSO com o Azure.
	Esquemas de API para StorageGRID. Observação: antes de executar uma atualização, você pode usar esses esquemas para confirmar se qualquer código que você escreveu para usar as APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID , caso você não tenha um ambiente StorageGRID não produtivo para testes de compatibilidade de atualização.

1. Se você estiver expandindo um sistema VMware, selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID .
	Uma licença gratuita que não fornece nenhum direito de suporte para o produto.
	O arquivo de disco da máquina virtual que é usado como modelo para criar máquinas virtuais de nós de grade.
	O arquivo de modelo do Open Virtualization Format(<code>.ovf</code>) e arquivo de manifesto(<code>.mf</code>) para implantar o nó de administração primário.
	O arquivo de modelo(<code>.ovf</code>) e arquivo de manifesto(<code>.mf</code>) para implantar nós administrativos não primários.
	O arquivo de modelo(<code>.ovf</code>) e arquivo de manifesto(<code>.mf</code>) para implantar nós de gateway.

Caminho e nome do arquivo	Descrição
	O arquivo de modelo(<code>.ovf</code>) e arquivo de manifesto(<code>.mf</code>) para implantar nós de armazenamento baseados em máquina virtual.
Ferramenta de script de implantação	Descrição
	Um script de shell Bash usado para automatizar a implantação de nós de grade virtual.
	Um exemplo de arquivo de configuração para uso com o <code>deploy-vsphere-ovftool.sh</code> roteiro.
	Um script Python usado para automatizar a configuração de um sistema StorageGRID .
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID .
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado. Você também pode usar este script para integração do Ping Federate.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado usando o Active Directory ou o Ping Federate.
	Um script auxiliar chamado pelo companheiro <code>storagegrid-ssoauth-azure.py</code> Script Python para executar interações SSO com o Azure.

Caminho e nome do arquivo	Descrição
	Esquemas de API para StorageGRID. Observação: antes de executar uma atualização, você pode usar esses esquemas para confirmar se qualquer código que você escreveu para usar as APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID , caso você não tenha um ambiente StorageGRID não produtivo para testes de compatibilidade de atualização.

1. Se você estiver expandindo um sistema baseado em dispositivo StorageGRID , selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Pacote DEB para instalar as imagens do nó StorageGRID em seus dispositivos.
	Soma de verificação MD5 para o arquivo /debs/storagegridwebscale-images-version-SHA.deb .



Para instalação do dispositivo, esses arquivos só são necessários se você precisar evitar tráfego de rede. O dispositivo pode baixar os arquivos necessários do nó de administração principal.

Verificar hardware e rede

Antes de iniciar a expansão do seu sistema StorageGRID , certifique-se do seguinte:

- O hardware necessário para dar suporte aos novos nós da grade ou ao novo site foi instalado e configurado.
- Todos os novos nós têm caminhos de comunicação bidirecionais para todos os nós existentes e novos (um requisito para a Rede de Grade). Em particular, confirme se as seguintes portas TCP estão abertas entre os novos nós que você está adicionando na expansão e o nó de administração principal:
 - 1055
 - 7443
 - 8011
 - 10342

Ver "[Comunicações internas do nó da rede](#)" .

- O nó de administração principal pode se comunicar com todos os servidores de expansão que devem hospedar o sistema StorageGRID .
- Se algum dos novos nós tiver um endereço IP da Grid Network em uma sub-rede não usada anteriormente, você já terá "[adicionou a nova sub-rede](#)" para a lista de sub-redes da Grid Network. Caso

contrário, você terá que cancelar a expansão, adicionar a nova sub-rede e iniciar o procedimento novamente.

- Você não está usando a tradução de endereços de rede (NAT) na Grid Network entre nós da grade ou entre sites do StorageGRID. Quando você usa endereços IPv4 privados para a Grid Network, esses endereços devem ser roteáveis diretamente de cada nó da grade em cada site. O uso de NAT para conectar a Grid Network em um segmento de rede pública só é suportado se você usar um aplicativo de tunelamento que seja transparente a todos os nós na grade, o que significa que os nós da grade não exigem conhecimento de endereços IP públicos.

Essa restrição de NAT é específica para nós de grade e para a Rede de Grade. Conforme necessário, você pode usar NAT entre clientes externos e nós de grade, como para fornecer um endereço IP público para um nó de gateway.

Adicionar volumes de armazenamento

Adicionar volumes de armazenamento aos nós de armazenamento

Você pode expandir a capacidade de armazenamento dos Nós de Armazenamento que estão abaixo do número máximo de volumes suportados. Pode ser necessário adicionar volumes de armazenamento a mais de um nó de armazenamento para atender aos requisitos de ILM para cópias replicadas ou codificadas para eliminação.

Antes de começar

Antes de adicionar volumes de armazenamento, revise o ["diretrizes para adicionar capacidade de objeto"](#) para garantir que você saiba onde adicionar volumes para atender aos requisitos da sua política de ILM.



Estas instruções se aplicam somente a nós de armazenamento baseados em software. Ver ["Adicionar prateleira de expansão ao SG6060 implantado"](#) ou ["Adicionar prateleira de expansão ao SG6160 implantado"](#) para aprender como adicionar volumes de armazenamento ao SG6060 ou SG6160 instalando prateleiras de expansão. Outros nós de armazenamento do dispositivo não podem ser expandidos.

Sobre esta tarefa

O armazenamento subjacente de um nó de armazenamento é dividido em volumes de armazenamento. Os volumes de armazenamento são dispositivos de armazenamento baseados em blocos que são formatados pelo sistema StorageGRID e montados para armazenar objetos. Cada nó de armazenamento pode suportar até 48 volumes de armazenamento, que são chamados de *armazenamentos de objetos* no Grid Manager.



Os metadados do objeto são sempre armazenados no repositório de objetos 0.

Cada armazenamento de objetos é montado em um volume que corresponde ao seu ID. Por exemplo, o armazenamento de objetos com um ID de 0000 corresponde ao `/var/local/rangedb/0` ponto de montagem.

Antes de adicionar novos volumes de armazenamento, use o Grid Manager para visualizar os armazenamentos de objetos atuais para cada nó de armazenamento, bem como os pontos de montagem correspondentes. Você pode usar essas informações ao adicionar volumes de armazenamento.

Passos

1. Selecione **NÓS > site > Nó de Armazenamento > Armazenamento**.

2. Role para baixo para ver as quantidades de armazenamento disponíveis para cada volume e armazenamento de objetos.

Para nós de armazenamento do dispositivo, o nome mundial de cada disco corresponde ao identificador mundial do volume (WWID) que aparece quando você visualiza as propriedades de volume padrão no SANtricity OS (o software de gerenciamento conectado ao controlador de armazenamento do dispositivo).

Para ajudar você a interpretar estatísticas de leitura e gravação de disco relacionadas aos pontos de montagem de volume, a primeira parte do nome mostrada na coluna **Nome** da tabela Dispositivos de disco (ou seja, *sdc*, *sdd*, *sde* e assim por diante) corresponde ao valor mostrado na coluna **Dispositivo** da tabela Volumes.

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB 	Enabled

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB 	1.55 MB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0003	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0004	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

3. Siga as instruções da sua plataforma para adicionar novos volumes de armazenamento ao Nó de Armazenamento.
 - ["VMware: Adicionar volumes de armazenamento ao nó de armazenamento"](#)
 - ["Linux: Adicionar volumes SAN ou de conexão direta ao nó de armazenamento"](#)

VMware: Adicionar volumes de armazenamento ao nó de armazenamento

Se um nó de armazenamento incluir menos de 16 volumes de armazenamento, você poderá aumentar sua capacidade usando o VMware vSphere para adicionar volumes.

Antes de começar

- Você tem acesso às instruções para instalar o StorageGRID para implantações VMware.
 - ["Instalar o StorageGRID no VMware"](#)
- Você tem o `Passwords.txt` arquivo.
- Você tem ["permissões de acesso específicas"](#) .



Não tente adicionar volumes de armazenamento a um nó de armazenamento enquanto uma atualização de software, procedimento de recuperação ou outro procedimento de expansão estiver ativo.

Sobre esta tarefa

O nó de armazenamento fica indisponível por um breve período quando você adiciona volumes de armazenamento. Você deve executar este procedimento em um nó de armazenamento por vez para evitar impactar os serviços de grade voltados para o cliente.

Passos

1. Se necessário, instale novo hardware de armazenamento e crie novos armazenamentos de dados VMware.
2. Adicione um ou mais discos rígidos à máquina virtual para uso como armazenamento (armazenamento de objetos).
 - a. Abra o VMware vSphere Client.
 - b. Edite as configurações da máquina virtual para adicionar um ou mais discos rígidos adicionais.

Os discos rígidos são normalmente configurados como Discos de Máquina Virtual (VMDKs). Os VMDKs são mais comumente usados e mais fáceis de gerenciar, enquanto os RDMs podem fornecer melhor desempenho para cargas de trabalho que usam tamanhos de objetos maiores (por exemplo, maiores que 100 MB). Para obter mais informações sobre como adicionar discos rígidos a máquinas virtuais, consulte a documentação do VMware vSphere.

3. Reinicie a máquina virtual usando a opção **Reiniciar SO convidado** no VMware vSphere Client ou inserindo o seguinte comando em uma sessão SSH na máquina virtual: `sudo reboot`



Não use **Desligar** ou **Reiniciar** para reiniciar a máquina virtual.

4. Configure o novo armazenamento para uso pelo nó de armazenamento:
 - a. Efetue login no nó da grade:
 - i. Digite o seguinte comando: `ssh admin@grid_node_IP`

- ii. Digite a senha listada no `Passwords.txt` arquivo.
- iii. Digite o seguinte comando para alternar para root: `su -`
- iv. Digite a senha listada no `Passwords.txt` arquivo. Quando você está logado como root, o prompt muda de `$` para `#`.

b. Configure os novos volumes de armazenamento:

```
sudo add_rangedbs.rb
```

Este script encontra novos volumes de armazenamento e solicita que você os formate.

- c. Digite **y** para aceitar a formatação.
- d. Se algum dos volumes tiver sido formatado anteriormente, decida se você deseja reformatá-lo.
 - Digite **y** para reformatar.
 - Digite **n** para pular a reformatação.

O `setup_rangedbs.sh` o script é executado automaticamente.

5. Verifique se os serviços iniciam corretamente:

a. Veja uma lista do status de todos os serviços no servidor:

```
sudo storagegrid-status
```

O status é atualizado automaticamente.

- a. Aguarde até que todos os serviços estejam em execução ou verificados.
- b. Sair da tela de status:

```
Ctrl+C
```

6. Verifique se o nó de armazenamento está online:

- a. Sign in no Grid Manager usando um "[navegador da web compatível](#)".
- b. Selecione **SUORTE > Ferramentas > Topologia de grade**.
- c. Selecione **site > Nó de armazenamento > LDR > Armazenamento**.
- d. Selecione a aba **Configuração** e depois a aba **Principal**.
- e. Se a lista suspensa **Estado de armazenamento - Desejado** estiver definida como Somente leitura ou Offline, selecione **Online**.
- f. Selecione **Aplicar alterações**.

7. Para ver os novos armazenamentos de objetos:

- a. Selecione **NÓS > site > Nó de Armazenamento > Armazenamento**.
- b. Veja os detalhes na tabela **Object Stores**.

Resultado

Você pode usar a capacidade expandida dos Nós de Armazenamento para salvar dados de objetos.

Linux: Adicionar volumes SAN ou de conexão direta ao nó de armazenamento

Se um nó de armazenamento incluir menos de 48 volumes de armazenamento, você poderá aumentar sua capacidade adicionando novos dispositivos de armazenamento em bloco, tornando-os visíveis aos hosts Linux e adicionando os novos mapeamentos de dispositivos em bloco ao arquivo de configuração StorageGRID usado para o nó de armazenamento.

Antes de começar

- Você tem acesso às instruções para instalar o StorageGRID na sua plataforma Linux.
 - ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
 - ["Instalar o StorageGRID no Ubuntu ou Debian"](#)
- Você tem o `Passwords.txt` arquivo.
- Você tem ["permissões de acesso específicas"](#) .



Não tente adicionar volumes de armazenamento a um nó de armazenamento enquanto uma atualização de software, procedimento de recuperação ou outro procedimento de expansão estiver ativo.

Sobre esta tarefa

O nó de armazenamento fica indisponível por um breve período quando você adiciona volumes de armazenamento. Você deve executar este procedimento em um nó de armazenamento por vez para evitar impactar os serviços de grade voltados para o cliente.

Passos

1. Instale o novo hardware de armazenamento.

Para obter mais informações, consulte a documentação fornecida pelo seu fornecedor de hardware.

2. Crie novos volumes de armazenamento em bloco dos tamanhos desejados.
 - Conecte as novas unidades e atualize a configuração do controlador RAID conforme necessário, ou aloque os novos SAN LUNs nos arrays de armazenamento compartilhados e permita que o host Linux os acesse.
 - Use o mesmo esquema de nomenclatura persistente usado para os volumes de armazenamento no nó de armazenamento existente.
 - Se você usar o recurso de migração de nó StorageGRID , torne os novos volumes visíveis para outros hosts Linux que são destinos de migração para este nó de armazenamento. Para obter mais informações, consulte as instruções para instalar o StorageGRID na sua plataforma Linux.
3. Efetue login no host Linux que suporta o Nó de Armazenamento como root ou com uma conta que tenha permissão sudo.
4. Confirme se os novos volumes de armazenamento estão visíveis no host Linux.

Talvez seja necessário verificar novamente os dispositivos.

5. Execute o seguinte comando para desabilitar temporariamente o nó de armazenamento:

```
sudo storagegrid node stop <node-name>
```

6. Usando um editor de texto como vim ou pico, edite o arquivo de configuração do nó para o nó de armazenamento, que pode ser encontrado em `/etc/storagegrid/nodes/<node-name>.conf`.
7. Localize a seção do arquivo de configuração do nó que contém os mapeamentos de dispositivos de bloco de armazenamento de objetos existentes.

No exemplo, `BLOCK_DEVICE_RANGEDB_00` para `BLOCK_DEVICE_RANGEDB_03` são os mapeamentos de dispositivos de bloco de armazenamento de objetos existentes.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. Adicione novos mapeamentos de dispositivos de bloco de armazenamento de objetos correspondentes aos volumes de armazenamento em bloco que você adicionou para este Nó de Armazenamento.

Certifique-se de começar no próximo `BLOCK_DEVICE_RANGEDB_nn`. Não deixe espaço.

- Com base no exemplo acima, comece em `BLOCK_DEVICE_RANGEDB_04`.
- No exemplo abaixo, quatro novos volumes de armazenamento em bloco foram adicionados ao nó:
`BLOCK_DEVICE_RANGEDB_04` para `BLOCK_DEVICE_RANGEDB_07`.

```

NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

```

9. Execute o seguinte comando para validar suas alterações no arquivo de configuração do nó para o nó de armazenamento:

```
sudo storagegrid node validate <node-name>
```

Resolva quaisquer erros ou avisos antes de prosseguir para a próxima etapa.

Se você observar um erro semelhante ao seguinte, significa que o arquivo de configuração do nó está tentando mapear o dispositivo de bloco usado por <node-name> para <PURPOSE> para o dado <path-name> no sistema de arquivos Linux, mas não há um arquivo especial de dispositivo de bloco válido (ou link simbólico para um arquivo especial de dispositivo de bloco) naquele local.



```

Checking configuration file for node <node-name>...
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
<path-name> is not a valid block device

```

Verifique se você inseriu o correto <path-name> .

10. Execute o seguinte comando para reiniciar o nó com os novos mapeamentos de dispositivos de bloco em vigor:

```
sudo storagegrid node start <node-name>
```

11. Efetue login no nó de armazenamento como administrador usando a senha listada no Passwords.txt arquivo.
12. Verifique se os serviços iniciam corretamente:
 - a. Veja uma lista do status de todos os serviços no servidor:

```
sudo storagegrid-status
```

O status é atualizado automaticamente.

- b. Aguarde até que todos os serviços estejam em execução ou verificados.
- c. Sair da tela de status:

```
Ctrl+C
```

13. Configure o novo armazenamento para uso pelo nó de armazenamento:

- a. Configure os novos volumes de armazenamento:

```
sudo add_rangedbs.rb
```

Este script encontra novos volumes de armazenamento e solicita que você os formate.

- b. Digite **y** para formatar os volumes de armazenamento.
- c. Se algum dos volumes tiver sido formatado anteriormente, decida se você deseja reformatá-lo.
 - Digite **y** para reformatar.
 - Digite **n** para pular a reformatação.

O `setup_rangedbs.sh` o script é executado automaticamente.

14. Verifique se o estado de armazenamento do nó de armazenamento está online:

- a. Sign in no Grid Manager usando um ["navegador da web compatível"](#).
- b. Selecione **SUORTE > Ferramentas > Topologia de grade**.
- c. Selecione **site > Nó de armazenamento > LDR > Armazenamento**.
- d. Selecione a aba **Configuração** e depois a aba **Principal**.
- e. Se a lista suspensa **Estado de armazenamento - Desejado** estiver definida como Somente leitura ou Offline, selecione **Online**.
- f. Clique em **Aplicar alterações**.

15. Para ver os novos armazenamentos de objetos:

- a. Selecione **NÓS > site > Nó de Armazenamento > Armazenamento**.
- b. Veja os detalhes na tabela **Object Stores**.

Resultado

Agora você pode usar a capacidade expandida dos Nós de Armazenamento para salvar dados de objetos.

Adicionar nós de grade ou site

Adicionar nós de grade ao site existente ou adicionar um novo site

Siga este procedimento para adicionar nós de grade a sites existentes ou para adicionar um novo site. Você só pode executar um tipo de expansão por vez.

Antes de começar

- Você tem o "[Acesso root ou permissão de manutenção](#)".
- Todos os nós existentes na grade estão ativos e funcionando em todos os sites.
- Todos os procedimentos anteriores de expansão, atualização, descomissionamento ou recuperação foram concluídos.



Você está impedido de iniciar uma expansão enquanto outro procedimento de expansão, atualização, recuperação ou desativação ativa estiver em andamento. No entanto, se necessário, você pode pausar um procedimento de desativação para iniciar uma expansão.

Passos

1. "[Atualizar sub-redes para a rede Grid](#)".
2. "[Implantar novos nós de grade](#)".
3. "[Executar expansão](#)".

Atualizar sub-redes para a rede Grid

Ao adicionar nós de grade ou um novo site em uma expansão, pode ser necessário atualizar ou adicionar sub-redes à Rede de Grade.

O StorageGRID mantém uma lista das sub-redes de rede usadas para comunicação entre nós de grade na Rede de Grade (eth0). Essas entradas incluem as sub-redes usadas para a Grid Network por cada site no seu sistema StorageGRID, bem como quaisquer sub-redes usadas para NTP, DNS, LDAP ou outros servidores externos acessados por meio do gateway da Grid Network.

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.
- Você tem os endereços de rede, em notação CIDR, das sub-redes que deseja configurar.

Sobre esta tarefa

Se algum dos novos nós tiver um endereço IP da Grid Network em uma sub-rede não usada anteriormente, você deverá adicionar a nova sub-rede à lista de sub-redes da Grid Network antes de iniciar a expansão. Caso contrário, você terá que cancelar a expansão, adicionar a nova sub-rede e iniciar o procedimento novamente.

Não use sub-redes que contenham os seguintes endereços IPv4 para a Rede de Grade, Rede de Administração ou Rede de Cliente de qualquer nó:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Por exemplo, não use os seguintes intervalos de sub-rede para a Rede de Grade, Rede de Administração ou Rede de Cliente de nenhum nó:

- 192.168.130.0/24 porque este intervalo de sub-rede contém os endereços IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 porque este intervalo de sub-rede contém os endereços IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 porque este intervalo de sub-rede contém os endereços IP 198.51.100.2 e 198.51.100.4

Passos

1. Selecione **MANUTENÇÃO > Rede > Rede de grade**.
2. Selecione **Adicionar outra sub-rede** para adicionar uma nova sub-rede na notação CIDR.

Por exemplo, insira 10.96.104.0/22 .
3. Digite a senha de provisionamento e selecione **Salvar**.
4. Aguarde até que as alterações sejam aplicadas e, em seguida, baixe um novo Pacote de Recuperação.
 - a. Selecione **MANUTENÇÃO > Sistema > Pacote de recuperação**.
 - b. Digite a **senha de provisionamento**.



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 . Ele também é usado para recuperar o nó de administração primário.

As sub-redes que você especificou são configuradas automaticamente para seu sistema StorageGRID .

Implantar novos nós de grade

As etapas para implantar novos nós de grade em uma expansão são as mesmas usadas quando a grade foi instalada pela primeira vez. Você deve implantar todos os novos nós de grade antes de poder executar a expansão.

Ao expandir uma grade, os nós adicionados não precisam corresponder aos tipos de nós existentes. Você pode adicionar nós VMware, nós baseados em contêineres Linux ou nós de dispositivos.

VMware: implantar nós de grade

Você deve implantar uma máquina virtual no VMware vSphere para cada nó VMware que deseja adicionar na expansão.

Passos

1. ["Implantar o novo nó como máquina virtual"](#) e conectá-lo a uma ou mais redes StorageGRID .

Ao implantar o nó, você pode, opcionalmente, remapear as portas do nó ou aumentar as configurações de CPU ou memória.

2. Depois de implantar todos os novos nós do VMware, ["executar o procedimento de expansão"](#) .

Linux: Implantar nós de grade

Você pode implantar nós de grade em novos hosts Linux ou em hosts Linux existentes. Se você precisar de hosts Linux adicionais para dar suporte aos requisitos de CPU, RAM e armazenamento dos nós do StorageGRID que deseja adicionar à sua grade, prepare-os da mesma forma que preparou os hosts quando os instalou pela primeira vez. Em seguida, implante os nós de expansão da mesma forma que implantou os nós de grade durante a instalação.

Antes de começar

- Você tem as instruções para instalar o StorageGRID para sua versão do Linux e revisou os requisitos de hardware e armazenamento.
 - ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
 - ["Instalar o StorageGRID no Ubuntu ou Debian"](#)
- Se você planeja implantar novos nós de grade em hosts existentes, você confirmou que os hosts existentes têm CPU, RAM e capacidade de armazenamento suficientes para os nós adicionais.
- Você tem um plano para minimizar os domínios de falha. Por exemplo, você não deve implantar todos os nós de gateway em um único host físico.



Em uma implantação de produção, não execute mais de um nó de armazenamento em um único host físico ou virtual. Usar um host dedicado para cada nó de armazenamento fornece um domínio de falha isolado.

- Se o nó StorageGRID usar armazenamento atribuído de um sistema NetApp ONTAP , confirme se o volume não tem 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.

Passos

1. Se você estiver adicionando novos hosts, acesse as instruções de instalação para implantar nós do StorageGRID .
2. Para implantar os novos hosts, siga as instruções para prepará-los.
3. Para criar arquivos de configuração de nós e validar a configuração do StorageGRID , siga as instruções para implantar nós de grade.
4. Se você estiver adicionando nós a um novo host Linux, inicie o serviço de host StorageGRID .
5. Se você estiver adicionando nós a um host Linux existente, inicie os novos nós usando a CLI do serviço do host storagegrid:
`sudo storagegrid node start [<node name>]`

Depois que você terminar

Depois de implantar todos os novos nós da grade, você pode ["realizar a expansão"](#) .

Dispositivos: Implantando nós de armazenamento, gateway ou de administração não primários

Para instalar o software StorageGRID em um nó do dispositivo, use o StorageGRID Appliance Installer, que está incluído no dispositivo. Em uma expansão, cada dispositivo de armazenamento funciona como um único nó de armazenamento, e cada dispositivo de serviços funciona como um único nó de gateway ou nó de administração não primário. Qualquer dispositivo pode se conectar à Rede de Grade, à Rede de Administração e à Rede de Cliente.

Antes de começar

- O dispositivo foi instalado em um rack ou gabinete, conectado às suas redes e ligado.
- Você concluiu o ["Configurar hardware"](#) passos.

A configuração do hardware do dispositivo inclui as etapas necessárias para configurar as conexões do StorageGRID (links de rede e endereços IP), bem como as etapas opcionais para habilitar a criptografia do nó, alterar o modo RAID e remapear as portas de rede.

- Todas as sub-redes da Rede de Grade listadas na página Configuração de IP do Instalador do Dispositivo StorageGRID foram definidas na Lista de Sub-redes da Rede de Grade no Nó de Administração primário.
- O firmware do instalador do dispositivo StorageGRID no dispositivo de substituição é compatível com a versão do software StorageGRID atualmente em execução na sua rede. Se as versões não forem compatíveis, você deverá atualizar o firmware do StorageGRID Appliance Installer.
- Você tem um laptop de serviço com um ["navegador da web compatível"](#) .
- Você conhece um dos endereços IP atribuídos ao controlador de computação do dispositivo. Você pode usar o endereço IP para qualquer rede StorageGRID conectada.

Sobre esta tarefa

O processo de instalação do StorageGRID em um nó do dispositivo tem as seguintes fases:

- Especifique ou confirme o endereço IP do nó de administração principal e o nome do nó do dispositivo.
- Você inicia a instalação e aguarda enquanto os volumes são configurados e o software é instalado.

No meio das tarefas de instalação do dispositivo, a instalação é pausada. Para retomar a instalação, faça login no Grid Manager, aprove todos os nós da grade e conclua o processo de instalação do StorageGRID .



Se você precisar implantar vários nós de dispositivo ao mesmo tempo, poderá automatizar o processo de instalação usando o `configure-sga.py` Script de instalação do aparelho.

Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação do dispositivo.

```
https://Controller_IP:8443
```

A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Na seção de conexão **Nó de administração primário**, determine se você precisa especificar o endereço IP para o nó de administração primário.

Se você já instalou outros nós neste data center, o StorageGRID Appliance Installer pode descobrir esse endereço IP automaticamente, supondo que o nó de administração principal, ou pelo menos um outro nó de grade com ADMIN_IP configurado, esteja presente na mesma sub-rede.

3. Se este endereço IP não for exibido ou você precisar alterá-lo, especifique o endereço:

Opção	Descrição
Entrada manual de IP	a. Desmarque a caixa de seleção Habilitar descoberta do nó de administração. b. Digite o endereço IP manualmente. c. Clique em Salvar. d. Aguarde até que o estado da conexão para o novo endereço IP fique pronto.
Descoberta automática de todos os nós administrativos primários conectados	a. Marque a caixa de seleção Habilitar descoberta do nó de administração. b. Aguarde até que a lista de endereços IP descobertos seja exibida. c. Selecione o nó de administração principal para a grade onde este nó de armazenamento do dispositivo será implantado. d. Clique em Salvar. e. Aguarde até que o estado da conexão para o novo endereço IP fique pronto.

4. No campo **Nome do nó**, insira o nome que deseja usar para este nó do dispositivo e selecione **Salvar**.

O nome do nó é atribuído a este nó do dispositivo no sistema StorageGRID . Ele é exibido na página Nós (guia Visão geral) no Gerenciador de grade. Se necessário, você pode alterar o nome ao aprovar o nó.

5. Na seção **Instalação**, confirme se o estado atual é "Pronto para iniciar a instalação do *nome do nó* na grade com o nó de administração primário *admin_ip*" e se o botão **Iniciar instalação** está habilitado.

Se o botão **Iniciar instalação** não estiver habilitado, talvez seja necessário alterar a configuração de rede ou as configurações de porta. Para obter instruções, consulte as instruções de manutenção do seu aparelho.

6. Na página inicial do StorageGRID Appliance Installer, selecione **Iniciar instalação**.

NetApp® StorageGRID® Appliance Installer

Home
Configure Networking ▼
Configure Hardware ▼
Monitor Installation
Advanced ▼

Home

The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node discovery
☐

Primary Admin Node IP

Connection state
Connection to 172.16.4.210 ready

Cancel

Save

Node name

Node name

Cancel

Save

Installation

Current state
Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

Start Installation

O estado atual muda para "A instalação está em andamento" e a página Instalação do monitor é exibida.

- Se sua expansão incluir vários nós de dispositivo, repita as etapas anteriores para cada dispositivo.



Se você precisar implantar vários nós de armazenamento do dispositivo ao mesmo tempo, poderá automatizar o processo de instalação usando o script de instalação do dispositivo `configure-sga.py`.

- Se precisar acessar manualmente a página de instalação do monitor, selecione **Instalação do monitor** na barra de menu.

A página Instalação do Monitor mostra o progresso da instalação.

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller		Complete	
Clear existing configuration		Complete	
Configure volumes		Creating volume StorageGRID-obj-00	
Configure host settings		Pending	

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

A barra de status azul indica qual tarefa está em andamento. Barras de status verdes indicam tarefas que foram concluídas com sucesso.



O instalador garante que as tarefas concluídas em uma instalação anterior não sejam executadas novamente. Se você estiver executando uma instalação novamente, todas as tarefas que não precisam ser executadas novamente serão exibidas com uma barra de status verde e o status "Ignorada".

9. Revise o progresso dos dois primeiros estágios da instalação.

1. Configurar aparelho

Durante esta fase, ocorre um dos seguintes processos:

- Para um dispositivo de armazenamento, o instalador se conecta ao controlador de armazenamento, limpa qualquer configuração existente, se comunica com o SANtricity OS para configurar volumes e define as configurações do host.
- Para um dispositivo de serviços, o instalador limpa qualquer configuração existente das unidades no controlador de computação e define as configurações do host.

2. Instalar SO

Durante esta etapa, o instalador copia a imagem base do sistema operacional do StorageGRID para o dispositivo.

10. Continue monitorando o progresso da instalação até que uma mensagem apareça na janela do console, solicitando que você use o Grid Manager para aprovar o nó.



Aguarde até que todos os nós adicionados nesta expansão estejam prontos para aprovação antes de ir ao Grid Manager para aprovar os nós.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

Executar expansão

Quando você executa a expansão, os novos nós de grade são adicionados à sua implantação existente do StorageGRID .

Antes de começar

- Você está conectado ao Grid Manager usando um [navegador da web compatível](#) .
- Você tem a senha de provisionamento.
- Você implantou todos os nós de grade que estão sendo adicionados nesta expansão.
- Você tem o [Permissão de acesso de manutenção ou root](#) .

- Se você estiver adicionando nós de armazenamento, terá confirmado que todas as operações de reparo de dados executadas como parte de uma recuperação foram concluídas. Ver "[Verifique os trabalhos de reparo de dados](#)".
- Se você estiver adicionando nós de armazenamento e quiser atribuir um grau de armazenamento personalizado a esses nós, você já deve ter "[criou o grau de armazenamento personalizado](#)". Você também tem a permissão de acesso Root ou as permissões de Manutenção e ILM.
- Se você estiver adicionando um novo site, você revisou e atualizou as regras do ILM. Você deve garantir que cópias de objetos não sejam armazenadas no novo site até que a expansão seja concluída. Por exemplo, se uma regra usa o pool de armazenamento padrão (**Todos os nós de armazenamento**), você deve "[criar um novo pool de armazenamento](#)" que contém apenas os nós de armazenamento existentes e "[atualizar regras do ILM](#)" e a política do ILM para usar esse novo pool de armazenamento. Caso contrário, os objetos serão copiados para o novo site assim que o primeiro nó naquele site se tornar ativo.

Sobre esta tarefa

A execução da expansão inclui estas tarefas principais do usuário:

1. Configurar a expansão.
2. Inicie a expansão.
3. Baixe um novo arquivo do pacote de recuperação.
4. Monitore as etapas e estágios de expansão até que todos os novos nós sejam instalados e configurados e todos os serviços tenham sido iniciados.



Algumas etapas e estágios de expansão podem levar um tempo significativo para serem executados em uma grade grande. Por exemplo, transmitir o Cassandra para um novo nó de armazenamento pode levar apenas alguns minutos se o banco de dados do Cassandra estiver vazio. No entanto, se o banco de dados Cassandra incluir uma grande quantidade de metadados de objetos, essa etapa poderá levar várias horas ou mais. Não reinicie nenhum nó de armazenamento durante os estágios "Expandindo o cluster do Cassandra" ou "Iniciando o Cassandra e transmitindo dados".

Passos

1. Selecione **MANUTENÇÃO > Tarefas > Expansão**.

A página Expansão da grade é exibida. A seção Nós pendentes lista os nós que estão prontos para serem adicionados.

Grid Expansion

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Configure Expansion

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve

✕ Remove

Search 

	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:a7:7a:c0	rlao-010-096-106-151	Storage Node	VMware VM	10.96.106.151/22
☐	00:50:56:a7:0f:2e	rlao-010-096-106-156	API Gateway Node	VMware VM	10.96.106.156/22

2. Selecione **Configurar expansão**.

A caixa de diálogo Seleção de Site é exibida.

3. Selecione o tipo de expansão que você está iniciando:

- Se você estiver adicionando um novo site, selecione **Novo** e insira o nome do novo site.
- Se você estiver adicionando um ou mais nós a um site existente, selecione **Existente**.

4. Selecione **Salvar**.

5. Revise a lista **Nós pendentes** e confirme se ela mostra todos os nós de grade que você implantou.

Conforme necessário, você pode posicionar o cursor sobre o **Endereço MAC da rede Grid** de um nó para ver detalhes sobre esse nó.

Pending Nodes

Grid nodes are listed as

+

 Approve

x

 Remove

Grid Network MAC Address

00:50:56:a7:7a:c0

00:50:56:a7:0f:2e

Approved Nodes

leo-010-096-106-151

Storage Node

Network

Grid Network	10.96.106.151/22	10.96.104.1
Admin Network	Name	Type
Client Network		

Hardware

VMware VM

4 CPUs

8 GB RAM

Disks

55 GB

55 GB

55 GB



Se um nó estiver faltando, confirme se ele foi implantado com sucesso.

6. Na lista de nós pendentes, aprove os nós que deseja adicionar nesta expansão.
 - a. Selecione o botão de opção ao lado do primeiro nó de grade pendente que você deseja aprovar.
 - b. Selecione **Aprovar**.

O formulário de configuração do nó da grade é exibido.

- c. Conforme necessário, modifique as configurações gerais:

Campo	Descrição
Site	O nome do site ao qual o nó da grade será associado. Se você estiver adicionando vários nós, certifique-se de selecionar o site correto para cada nó. Se você estiver adicionando um novo site, todos os nós serão adicionados ao novo site.
Nome	O nome do sistema para o nó. Os nomes do sistema são necessários para operações internas do StorageGRID e não podem ser alterados.
Tipo de armazenamento (somente nós de armazenamento)	• Dados e metadados ("combinados"): Nó de armazenamento de dados e metadados de objetos • Somente dados: nó de armazenamento contendo apenas dados de objeto (sem metadados) • Somente metadados: nó de armazenamento contendo apenas metadados (sem dados de objeto)

Campo	Descrição
Função NTP	A função do Protocolo de Tempo de Rede (NTP) do nó da grade: • Selecione Automático (padrão) para atribuir automaticamente a função NTP ao nó. A função Primária será atribuída a nós de administração, nós de armazenamento com serviços ADC, nós de gateway e quaisquer nós de grade que tenham endereços IP não estáticos. A função Cliente será atribuída a todos os outros nós da grade. • Selecione Primário para atribuir manualmente a função NTP Primário ao nó. Pelo menos dois nós em cada site devem ter a função Primária para fornecer acesso redundante do sistema a fontes de tempo externas. • Selecione Cliente para atribuir manualmente a função NTP do Cliente ao nó.
Serviço ADC (nós de armazenamento combinados ou somente de metadados)	Se este nó de armazenamento executará o serviço Controlador de Domínio Administrativo (ADC). O serviço ADC monitora a localização e a disponibilidade dos serviços de rede. Pelo menos três nós de armazenamento em cada site devem incluir o serviço ADC. Não é possível adicionar o serviço ADC a um nó depois que ele for implantado. • Selecione Sim se o nó de armazenamento que você está substituindo incluir o serviço ADC. Como não é possível desativar um nó de armazenamento se houver poucos serviços ADC restantes, isso garante que um novo serviço ADC esteja disponível antes que o serviço antigo seja removido. • Selecione Automático para permitir que o sistema determine se este nó requer o serviço ADC. Aprenda sobre o "Quórum do ADC" .
Grau de armazenamento (nós de armazenamento combinados ou somente de dados)	Use o grau de armazenamento Padrão ou selecione o grau de armazenamento personalizado que deseja atribuir a este novo nó. Os níveis de armazenamento são usados pelos pools de armazenamento do ILM, portanto sua seleção pode afetar quais objetos serão colocados no Nó de Armazenamento.

d. Conforme necessário, modifique as configurações da Rede de grade, Rede de administração e Rede de cliente.

- **Endereço IPv4 (CIDR):** O endereço de rede CIDR para a interface de rede. Por exemplo:
172.16.10.100/24



Se você descobrir que os nós têm endereços IP duplicados na Grid Network enquanto estiver aprovando nós, será necessário cancelar a expansão, reimplantar as máquinas virtuais ou os dispositivos com um IP não duplicado e reiniciar a expansão.

- **Gateway:** O gateway padrão do nó da grade. Por exemplo: 172.16.10.1
- **Sub-redes (CIDR):** Uma ou mais sub-redes para a Rede de Administração.

e. Selecione **Salvar**.

O nó de grade aprovado é movido para a lista de nós aprovados.

- Para modificar as propriedades de um nó de grade aprovado, selecione seu botão de opção e selecione **Editar**.
- Para mover um nó de grade aprovado de volta para a lista de Nós Pendentes, selecione seu botão de opção e selecione **Redefinir**.
- Para remover permanentemente um nó de rede aprovado, desligue-o. Em seguida, selecione o botão de opção e selecione **Remover**.

f. Repita essas etapas para cada nó de grade pendente que você deseja aprovar.



Se possível, você deve aprovar todas as notas de grade pendentes e executar uma única expansão. Mais tempo será necessário se você realizar várias pequenas expansões.

7. Quando você tiver aprovado todos os nós da grade, insira a **Senha de provisionamento** e selecione **Expandir**.

Após alguns minutos, esta página é atualizada para exibir o status do procedimento de expansão. Quando tarefas que afetam nós de grade individuais estão em andamento, a seção Status do nó de grade lista o status atual de cada nó de grade.



Durante a etapa "Instalando nós de grade" para um novo dispositivo, o Instalador do Dispositivo StorageGRID mostra a instalação passando do Estágio 3 para o Estágio 4, Finalizar instalação. Quando o Estágio 4 estiver concluído, o controlador será reiniciado.

Expansion Progress

Lists the status of grid configuration tasks required to change the grid topology. These grid configuration tasks are run automatically by the StorageGRID system.

1. Installing grid nodes

In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

Search



Name	Site	Grid Network IPv4 Address	Progress	Stage
rleo-010-096-106-151	Data Center 1	10.96.106.151/22		Waiting for Dynamic IP Service peers
rleo-010-096-106-156	Data Center 1	10.96.106.156/22		Waiting for NTP to synchronize

2. Initial configuration

Pending

3. Distributing the new grid node's certificates to the StorageGRID system.

Pending

4. Assigning Storage Nodes to storage grade

Pending

5. Starting services on the new grid nodes

Pending

6. Starting background process to clean up unused Cassandra keys

Pending



Uma expansão do site inclui uma tarefa adicional para configurar o Cassandra para o novo site.

8. Assim que o link **Baixar pacote de recuperação** aparecer, baixe o arquivo do pacote de recuperação.

Você deve baixar uma cópia atualizada do arquivo do pacote de recuperação o mais rápido possível após fazer alterações na topologia da grade no sistema StorageGRID . O arquivo Recovery Package permite restaurar o sistema caso ocorra uma falha.

- Selecione o link para download.
- Digite a senha de provisionamento e selecione **Iniciar download**.
- Quando o download for concluído, abra o .zip arquivo e confirme que você pode acessar o conteúdo, incluindo o `Passwords.txt` arquivo.
- Copie o arquivo do pacote de recuperação baixado(.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 .

9. Se você estiver adicionando nós de armazenamento a um site existente ou adicionando um site, monitore os estágios do Cassandra, que ocorrem quando os serviços são iniciados nos novos nós da grade.



Não reinicie nenhum nó de armazenamento durante os estágios "Expandindo o cluster do Cassandra" ou "Iniciando o Cassandra e transmitindo dados". Esses estágios podem levar muitas horas para serem concluídos para cada novo nó de armazenamento, especialmente se os nós de armazenamento existentes contiverem uma grande quantidade de metadados de objetos.

Adicionando nós de armazenamento

Se você estiver adicionando nós de armazenamento a um site existente, revise a porcentagem mostrada na mensagem de status "Iniciando o Cassandra e transmitindo dados".

5. Starting services on the new grid nodes

In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

⚠ Do not reboot any Storage Nodes during Step 4. The "Starting Cassandra and streaming data" stage might take hours, especially if existing Storage Nodes contain a large amount of object metadata.

Name	Site	Grid Network IPv4 Address	Progress	Stage
rleo-010-096-106-151	Data Center 1	10.96.106.151/22		Starting Cassandra and streaming data (20.4% streamed)
rleo-010-096-106-156	Data Center 1	10.96.106.156/22		Starting services

Essa porcentagem estima o quão completa é a operação de streaming do Cassandra, com base na quantidade total de dados do Cassandra disponíveis e na quantidade que já foi gravada no novo nó.

Adicionando site

Se você estiver adicionando um novo site, use `nodetool status` para monitorar o progresso do streaming do Cassandra e ver quantos metadados foram copiados para o novo site durante o estágio "Expandindo o cluster do Cassandra". A carga total de dados no novo site deve estar em cerca de 20% do total de um site atual.

- Continue monitorando a expansão até que todas as tarefas sejam concluídas e o botão **Configurar expansão** reapareça.

Depois que você terminar

Dependendo dos tipos de nós de grade que você adicionou, execute etapas adicionais de integração e configuração. Ver ["Etapas de configuração após expansão"](#).

Configurar sistema expandido

Etapas de configuração após expansão

Após concluir uma expansão, você deve executar etapas adicionais de integração e configuração.

Sobre esta tarefa

Você deve concluir as tarefas de configuração listadas abaixo para os nós de grade ou sites que você está adicionando à sua expansão. Algumas tarefas podem ser opcionais, dependendo das opções selecionadas ao instalar e administrar seu sistema, e de como você deseja configurar os nós e sites adicionados durante a expansão.

Passos

1. Se você adicionou um site:

- ["Criar um pool de armazenamento"](#) para o site e cada nível de armazenamento selecionado para os novos Nós de Armazenamento.
- Confirme se a política de ILM atende aos novos requisitos. Se forem necessárias alterações nas regras, ["criar novas regras"](#) e ["atualizar a política do ILM"](#). Se as regras já estiverem corretas, ["ativar uma nova política"](#) sem alterações de regras para garantir que o StorageGRID use os novos nós.
- Confirme se os servidores do Network Time Protocol (NTP) estão acessíveis nesse site. Ver ["Gerenciar servidores NTP"](#).



Certifique-se de que pelo menos dois nós em cada site possam acessar pelo menos quatro fontes NTP externas. Se apenas um nó em um site puder alcançar as fontes NTP, ocorrerão problemas de tempo se esse nó ficar inativo. Além disso, designar dois nós por site como fontes primárias de NTP garante um tempo preciso se um site estiver isolado do restante da rede.

2. Se você adicionou um ou mais nós de armazenamento a um site existente:

- ["Ver detalhes do pool de armazenamento"](#) para confirmar se cada nó adicionado está incluído nos pools de armazenamento esperados e usado nas regras de ILM esperadas.
- Confirme se a política de ILM atende aos novos requisitos. Se forem necessárias alterações nas regras, ["criar novas regras"](#) e ["atualizar a política do ILM"](#). Se as regras já estiverem corretas, ["ativar uma nova política"](#) sem alterações de regras para garantir que o StorageGRID use os novos nós.
- ["Verifique se o nó de armazenamento está ativo"](#) e capaz de ingerir objetos.
- Se você não conseguiu adicionar o número recomendado de nós de armazenamento, rebalanceie os dados codificados para eliminação. Ver ["Rebalancear dados codificados para eliminação após adicionar nós de armazenamento"](#).

3. Se você adicionou um nó de gateway:

- Se grupos de alta disponibilidade (HA) forem usados para conexões de cliente, opcionalmente, adicione o nó de gateway a um grupo de HA. Selecione **CONFIGURAÇÃO > Rede > Grupos de alta disponibilidade** para revisar a lista de grupos de HA existentes e adicionar o novo nó. Ver ["Configurar grupos de alta disponibilidade"](#).

4. Se você adicionou um nó de administração:

- a. Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID, crie uma parte confiável para o novo nó de administração. Você não pode fazer login no nó até criar essa confiança de terceira parte confiável. Ver ["Configurar logon único"](#).
- b. Se você planeja usar o serviço Load Balancer em nós de administração, opcionalmente adicione o novo nó de administração a um grupo de HA. Selecione **CONFIGURAÇÃO > Rede > Grupos de alta disponibilidade** para revisar a lista de grupos de HA existentes e adicionar o novo nó. Ver ["Configurar grupos de alta disponibilidade"](#).
- c. Opcionalmente, copie o banco de dados do nó administrativo do nó administrativo principal para o nó administrativo de expansão se desejar manter as informações de atributo e auditoria consistentes em

cada nó administrativo. Ver ["Copiar o banco de dados do nó de administração"](#) .

- d. Opcionalmente, copie o banco de dados Prometheus do nó de administração principal para o nó de administração de expansão se quiser manter as métricas históricas consistentes em cada nó de administração. Ver ["Copiar métricas do Prometheus"](#) .
- e. Opcionalmente, copie os logs de auditoria existentes do nó de administração principal para o nó de administração de expansão se desejar manter as informações de log histórico consistentes em cada nó de administração. Ver ["Copiar logs de auditoria"](#) .

5. Para verificar se os nós de expansão foram adicionados com uma Rede de Cliente não confiável ou para alterar se a Rede de Cliente de um nó é confiável ou não confiável, vá para **CONFIGURAÇÃO > Segurança > Controle de Firewall**.

Se a rede do cliente no nó de expansão não for confiável, as conexões com o nó na rede do cliente deverão ser feitas usando um ponto de extremidade do balanceador de carga. Ver ["Configurar pontos de extremidade do balanceador de carga"](#) e ["Gerenciar controles de firewall"](#) .

6. Configurar o DNS.

Se você tiver especificado configurações de DNS separadamente para cada nó da grade, deverá adicionar configurações de DNS personalizadas por nó para os novos nós. Ver ["Modificar a configuração de DNS para um único nó de grade"](#) .

Para garantir a operação correta, especifique dois ou três servidores DNS. Se você especificar mais de três, é possível que apenas três sejam usados devido a limitações conhecidas do sistema operacional em algumas plataformas. Se você tiver restrições de roteamento em seu ambiente, você pode ["personalizar a lista de servidores DNS"](#) para nós individuais (normalmente todos os nós em um site) usar um conjunto diferente de até três servidores DNS.

Se possível, use servidores DNS que cada site possa acessar localmente para garantir que um site isolado possa resolver os FQDNs para destinos externos.

Verifique se o nó de armazenamento está ativo

Após a conclusão de uma operação de expansão que adiciona novos nós de armazenamento, o sistema StorageGRID deve começar a usar automaticamente os novos nós de armazenamento. Você deve usar o sistema StorageGRID para verificar se o novo nó de armazenamento está ativo.

Passos

1. Sign in no Grid Manager usando um ["navegador da web compatível"](#) .
2. Selecione **NÓS > Nó de Armazenamento de Expansão > Armazenamento**.
3. Posicione o cursor sobre o gráfico **Armazenamento usado - Dados do objeto** para visualizar o valor de **Usado**, que é a quantidade de espaço total utilizável que foi usada para dados do objeto.
4. Verifique se o valor de **Usado** está aumentando à medida que você move o cursor para a direita no gráfico.

Copiar banco de dados do nó de administração

Ao adicionar nós de administração por meio de um procedimento de expansão, você pode, opcionalmente, copiar o banco de dados do nó de administração principal para o

novo nó de administração. Copiar o banco de dados permite que você retenha informações históricas sobre atributos, alertas e alertas.

Antes de começar

- Você concluiu as etapas de expansão necessárias para adicionar um nó de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

O processo de ativação do software StorageGRID cria um banco de dados vazio para o serviço NMS no nó de administração de expansão. Quando o serviço NMS é iniciado no nó de administração de expansão, ele registra informações de servidores e serviços que atualmente fazem parte do sistema ou foram adicionados posteriormente. Este banco de dados do nó de administração inclui as seguintes informações:

- Histórico de alertas
- Dados de atributos históricos, que são usados em gráficos de estilo legado na página Nós

Para garantir que o banco de dados do Nó de Administração seja consistente entre os nós, você pode copiar o banco de dados do Nó de Administração principal para o Nó de Administração de expansão.



A cópia do banco de dados do nó administrativo principal (o nó administrativo de origem) para um nó administrativo de expansão pode levar várias horas para ser concluída. Durante esse período, o Grid Manager fica inacessível.

Use estas etapas para interromper o serviço MI e o serviço da API de gerenciamento no nó de administração principal e no nó de administração de expansão antes de copiar o banco de dados.

Passos

1. Conclua as seguintes etapas no nó de administração principal:
 - a. Efetue login no nó de administração:
 - i. Digite o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Digite a senha listada no `Passwords.txt` arquivo.
 - iii. Digite o seguinte comando para alternar para root: `su -`
 - iv. Digite a senha listada no `Passwords.txt` arquivo.
 - b. Execute o seguinte comando: `recover-access-points`
 - c. Digite a senha de provisionamento.
 - d. Pare o serviço MI: `service mi stop`
 - e. Pare o serviço Management Application Program Interface (mgmt-api): `service mgmt-api stop`
2. Conclua as seguintes etapas no nó de administração de expansão:
 - a. Efetue login no nó de administração de expansão:
 - i. Digite o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Digite a senha listada no `Passwords.txt` arquivo.
 - iii. Digite o seguinte comando para alternar para root: `su -`

iv. Digite a senha listada no `Passwords.txt` arquivo.

b. Pare o serviço MI: `service mi stop`

c. Pare o serviço mgmt-api: `service mgmt-api stop`

d. Adicione a chave privada SSH ao agente SSH. Digitar: `ssh-add`

e. Digite a senha de acesso SSH listada no `Passwords.txt` arquivo.

f. Copie o banco de dados do nó de administração de origem para o nó de administração de expansão:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Quando solicitado, confirme que deseja substituir o banco de dados MI no nó de administração de expansão.

O banco de dados e seus dados históricos são copiados para o nó de administração de expansão. Quando a operação de cópia é concluída, o script inicia o nó de administração de expansão.

h. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Digitar: `ssh-add -D`

3. Reinicie os serviços no nó de administração principal: `service servermanager start`

Copiar métricas do Prometheus

Depois de adicionar um novo nó de administração, você pode, opcionalmente, copiar as métricas históricas mantidas pelo Prometheus do nó de administração principal para o novo nó de administração. Copiar as métricas garante que as métricas históricas sejam consistentes entre os nós administrativos.

Antes de começar

- O novo nó de administração está instalado e em execução.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

Quando você adiciona um nó de administração, o processo de instalação do software cria um novo banco de dados Prometheus. Você pode manter as métricas históricas consistentes entre os nós copiando o banco de dados Prometheus do nó de administração principal (o *nó de administração de origem*) para o novo nó de administração.



Copiar o banco de dados do Prometheus pode levar uma hora ou mais. Alguns recursos do Grid Manager ficarão indisponíveis enquanto os serviços estiverem interrompidos no nó de administração de origem.

Passos

1. Efetue login no nó de administração de origem:

a. Digite o seguinte comando: `ssh admin@grid_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.
2. No nó de administração de origem, pare o serviço Prometheus: `service prometheus stop`
3. Conclua as seguintes etapas no novo nó de administração:
 - a. Efetue login no novo nó de administração:
 - i. Digite o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Digite a senha listada no `Passwords.txt` arquivo.
 - iii. Digite o seguinte comando para alternar para root: `su -`
 - iv. Digite a senha listada no `Passwords.txt` arquivo.
 - b. Pare o serviço Prometheus: `service prometheus stop`
 - c. Adicione a chave privada SSH ao agente SSH. Digitar: `ssh-add`
 - d. Digite a senha de acesso SSH listada no `Passwords.txt` arquivo.
 - e. Copie o banco de dados Prometheus do nó de administração de origem para o novo nó de administração: `/usr/local/prometheus/bin/prometheus-clone-db.sh`
`Source_Admin_Node_IP`
 - f. Quando solicitado, pressione **Enter** para confirmar que deseja destruir o novo banco de dados Prometheus no novo nó de administração.

O banco de dados original do Prometheus e seus dados históricos são copiados para o novo nó de administração. Quando a operação de cópia estiver concluída, o script iniciará o novo nó de administração. O seguinte status aparece:

```
Database cloned, starting services
```

- a. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Digitar:

```
ssh-add -D
```

4. Reinicie o serviço Prometheus no nó de administração de origem.

```
service prometheus start
```

Copiar logs de auditoria

Quando você adiciona um novo nó de administração por meio de um procedimento de expansão, seu serviço AMS registra apenas eventos e ações que ocorrem depois que ele ingressa no sistema. Conforme necessário, você pode copiar logs de auditoria de um nó de administração instalado anteriormente para o novo nó de administração de expansão para que ele fique sincronizado com o restante do sistema StorageGRID .

Antes de começar

- Você concluiu as etapas de expansão necessárias para adicionar um nó de administração.
- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

Para disponibilizar mensagens de auditoria históricas em um novo nó de administração, você deve copiar os arquivos de log de auditoria manualmente de um nó de administração existente para o nó de administração de expansão.



Por padrão, as informações de auditoria são enviadas para o log de auditoria nos nós de administração. Você pode pular estas etapas se alguma das seguintes situações se aplicar:

- Você configurou um servidor syslog externo e os logs de auditoria agora estão sendo enviados para o servidor syslog em vez de para os nós de administração.
- Você especificou explicitamente que as mensagens de auditoria devem ser salvas somente nos nós locais que as geraram.

Ver ["Configurar mensagens de auditoria e destinos de log"](#) para mais detalhes.

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. Pare o serviço AMS para impedir que ele crie um novo arquivo: `service ams stop`

3. Navegue até o diretório de exportação de auditoria:

```
cd /var/local/log
```

4. Renomear a fonte `audit.log` arquivo para garantir que ele não substitua o arquivo no nó de administração de expansão para o qual você está copiando:

```
ls -l
mv audit.log _new_name_.txt
```

5. Copie todos os arquivos de log de auditoria para o local de destino no nó de administração de expansão:

```
scp -p * IP_address:/var/local/log
```

6. Se for solicitada a senha para `/root/.ssh/id_rsa`, insira a senha de acesso SSH para o nó de administração primário listado em `Passwords.txt` arquivo.

7. Restaurar o original `audit.log` arquivo:

```
mv new_name.txt audit.log
```

8. Inicie o serviço AMS:

```
service ams start
```

9. Sair do servidor:

```
exit
```

10. Efetue login no nó de administração de expansão:

- Digite o seguinte comando: `ssh admin@expansion_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 `#`.

11. Atualize as configurações de usuário e grupo para os arquivos de log de auditoria:

```
cd /var/local/log  
  
chown ams-user:bycast *
```

12. Sair do servidor:

```
exit
```

Rebalancear dados codificados para eliminação após adicionar nós de armazenamento

Depois de adicionar nós de armazenamento, você pode usar o procedimento de rebalanceamento de codificação de eliminação (EC) para redistribuir fragmentos codificados por eliminação entre os nós de armazenamento existentes e novos.

Antes de começar

- Você concluiu as etapas de expansão para adicionar os novos nós de armazenamento.
- Você revisou o ["considerações para rebalanceamento de dados codificados por apagamento"](#).
- Você entende que os dados do objeto replicado não serão movidos por este procedimento e que o procedimento de rebalanceamento do EC não considera o uso de dados replicados em cada nó de armazenamento ao determinar para onde mover os dados codificados para eliminação.
- Você tem o `Passwords.txt` arquivo.

O que acontece quando este procedimento é executado

Antes de iniciar o procedimento, observe o seguinte:

- O procedimento de rebalanceamento do EC não será iniciado se um ou mais volumes estiverem offline (desmontados) ou se estiverem online (montados), mas em estado de erro.
- O procedimento de rebalanceamento da CE reserva temporariamente uma grande quantidade de armazenamento. Alertas de armazenamento podem ser acionados, mas serão resolvidos quando o rebalanceamento for concluído. Se não houver armazenamento suficiente para a reserva, o procedimento de rebalanceamento do EC falhará. As reservas de armazenamento são liberadas quando o procedimento

de rebalanceamento do EC é concluído, independentemente de o procedimento ter falhado ou sido bem-sucedido.

- Se um volume ficar offline enquanto o procedimento de rebalanceamento do EC estiver em andamento, o procedimento de rebalanceamento será encerrado. Todos os fragmentos de dados que já foram movidos permanecerão em seus novos locais e nenhum dado será perdido.

Você pode executar o procedimento novamente depois que todos os volumes estiverem online novamente.

- Quando o procedimento de rebalanceamento do EC estiver em execução, o desempenho das operações do ILM e das operações do cliente S3 poderá ser afetado.



As operações da API S3 para carregar objetos (ou partes de objetos) podem falhar durante o procedimento de rebalanceamento do EC se levarem mais de 24 horas para serem concluídas. As operações PUT de longa duração falharão se a regra ILM aplicável usar posicionamento Balanceado ou Estrito na ingestão. O seguinte erro será relatado: 500 Internal Server Error.

- Durante este procedimento, todos os nós têm um limite de capacidade de armazenamento de 80%. Os nós que excedem esse limite, mas ainda armazenam abaixo da partição de dados de destino, são excluídos de:
 - O valor do desequilíbrio do site
 - Quaisquer condições de conclusão do trabalho



A partição de dados de destino é calculada dividindo o total de dados de um site pelo número de nós.

- **Condições de conclusão do trabalho.** O procedimento de reequilíbrio da CE é considerado completo quando qualquer uma das seguintes situações for verdadeira:
 - Ele não pode mover mais dados codificados para eliminação.
 - Os dados em todos os nós estão dentro de um desvio de 5% da partição de dados de destino.
 - O procedimento está em andamento há 30 dias.

Passos

1. Revise os detalhes atuais do armazenamento de objetos do site que você planeja rebalancear.
 - a. Selecione **NODES**.
 - b. Selecione o primeiro nó de armazenamento no site.
 - c. Selecione a aba **Armazenamento**.
 - d. Posicione o cursor sobre o gráfico Armazenamento usado - Dados do objeto para ver a quantidade atual de dados replicados e dados codificados para eliminação no nó de armazenamento.
 - e. Repita essas etapas para visualizar os outros nós de armazenamento no site.
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. Inicie o procedimento:

```
`rebalance-data start --site "nome-do-site"
```

Para `"site-name"`, especifique o primeiro site onde você adicionou um ou mais novos nós de armazenamento. Incluir `site-name` entre aspas.

O procedimento de rebalanceamento do EC é iniciado e um ID de trabalho é retornado.

4. Copie o ID do trabalho.

5. Monitorar o status do procedimento de rebalanceamento da CE.

- Para visualizar o status de um único procedimento de rebalanceamento de CE:

```
rebalance-data status --job-id job-id
```

Para `job-id`, especifique o ID que foi retornado quando você iniciou o procedimento.

- Para visualizar o status do procedimento atual de rebalanceamento do EC e quaisquer procedimentos concluídos anteriormente:

```
rebalance-data status
```



Para obter ajuda sobre o comando `rebalance-data`:

```
rebalance-data --help
```

6. Execute etapas adicionais com base no status retornado:

- Se `State` é `In progress`, a operação de rebalanceamento da CE ainda está em execução. Você deve monitorar o procedimento periodicamente até que ele seja concluído.

Use o `Site Imbalance` valor para avaliar o quão desequilibrado é o uso de dados do código de eliminação nos nós de armazenamento do site. Esse valor pode variar de 1,0 a 0, com 0 indicando que o uso de dados de codificação de eliminação é completamente equilibrado em todos os nós de armazenamento no site.

O trabalho de rebalanceamento do EC é considerado concluído e será interrompido quando os dados em todos os nós estiverem dentro de um desvio de 5% da partição de dados de destino.

- Se `State` é `Success`, opcionalmente [revisar armazenamento de objetos](#) para ver os detalhes atualizados do site.

Os dados codificados para eliminação agora devem ser mais equilibrados entre os nós de armazenamento no site.

- Se `State` é `Failure`:

i. Confirme se todos os nós de armazenamento no local estão conectados à rede.

- ii. Verifique e resolva quaisquer alertas que possam estar afetando esses nós de armazenamento.
- iii. Reinicie o procedimento de rebalanceamento da CE:

```
rebalance-data start --job-id job-id
```

- iv. [Ver o status](#) do novo procedimento. Se `State` ainda é `Failure`, entre em contato com o suporte técnico.

7. Se o procedimento de rebalanceamento do EC estiver gerando muita carga (por exemplo, operações de ingestão afetadas), pause o procedimento.

```
rebalance-data pause --job-id job-id
```

8. Se você precisar encerrar o procedimento de rebalanceamento do EC (por exemplo, para poder executar uma atualização do software StorageGRID), insira o seguinte:

```
rebalance-data terminate --job-id job-id
```



Quando você encerra um procedimento de rebalanceamento de EC, todos os fragmentos de dados que já foram movidos permanecem em seus novos locais. Os dados não são movidos de volta para o local original.

9. Se você estiver usando codificação de eliminação em mais de um site, execute este procedimento para todos os outros sites afetados.

Solucionar problemas de expansão

Se você encontrar erros durante o processo de expansão da grade que não consiga resolver, ou se uma tarefa da grade falhar, colete os arquivos de log e entre em contato com o suporte técnico.

Antes de entrar em contato com o suporte técnico, colete os arquivos de log necessários para ajudar na solução de problemas.

Passos

1. Conecte-se ao nó de expansão que apresentou falhas:

- a. Digite o seguinte comando: `ssh -p 8022 admin@grid_node_IP`



A porta 8022 é a porta SSH do sistema operacional base, enquanto a porta 22 é a porta SSH do mecanismo de contêiner que executa o StorageGRID.

- 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.

Depois de efetuar login como root, o prompt muda de `$` para `#`.

2. Dependendo do estágio em que a instalação chegou, recupere qualquer um dos seguintes logs que estão disponíveis no nó da grade:

Plataforma	Registros
VMware	• /var/log/daemon.log • /var/log/storagegrid/daemon.log • /var/log/storagegrid/nodes/<node-name>.log
Linux	• /var/log/storagegrid/daemon.log • /etc/storagegrid/nodes/<node-name>.conf(para cada nó com falha) • /var/log/storagegrid/nodes/<node-name>.log(para cada nó com falha; pode não existir)

Manter um sistema StorageGRID

Manutenção da rede

As tarefas de manutenção da rede incluem o descomissionamento de um nó ou local, a renomeação de uma rede, nó ou local e a manutenção de redes. Você também pode executar procedimentos de host e middleware, bem como procedimentos de nó de grade.



Nestas instruções, "Linux" refere-se a uma implantação do Red Hat® Enterprise Linux®, Ubuntu® ou Debian®. Para obter uma lista de versões suportadas, consulte o ["Ferramenta de Matriz de Interoperabilidade da NetApp"](#).

Antes de começar

- Você tem um amplo conhecimento do sistema StorageGRID.
- Você revisou a topologia do seu sistema StorageGRID e entende a configuração da grade.
- Você entende que deve seguir todas as instruções exatamente e prestar atenção a todos os avisos.
- Você entende que procedimentos de manutenção não descritos não são suportados ou exigem uma contratação de serviços.

Procedimentos de manutenção para aparelhos

Para procedimentos de hardware, consulte o ["instruções de manutenção para seu dispositivo StorageGRID"](#).

Baixar pacote de recuperação

O arquivo Recovery Package permite restaurar o sistema StorageGRID caso ocorra uma falha.

Antes de começar

- No nó de administração principal, você é conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem a senha de provisionamento.
- Você tem ["permissões de acesso específicas"](#).

Baixe o arquivo do pacote de recuperação atual antes de fazer alterações na topologia da grade no sistema StorageGRID ou antes de atualizar o software. Em seguida, baixe uma nova cópia do Pacote de Recuperação após fazer alterações na topologia da rede ou após atualizar o software.

Passos

1. Selecione **MANUTENÇÃO > Sistema > Pacote de recuperação**.
2. Digite a senha de provisionamento e selecione **Iniciar download**.

O download começa imediatamente.

3. Quando o download for concluído, abra o `.zip` arquivo e confirme que você pode acessar o conteúdo,

incluindo o `Passwords.txt` arquivo.

4. Copie o arquivo do pacote de recuperação baixado(`.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 .

Descomissionar nós ou site

Desativar nó ou local

Você pode executar um procedimento de descomissionamento para remover permanentemente nós de grade ou um site inteiro do sistema StorageGRID .

Para remover um nó de grade ou um site, execute um dos seguintes procedimentos de desativação:

- Executar um "[descomissionamento de nós de rede](#)" para remover um ou mais nós, que podem estar em um ou mais sites. Os nós que você remove podem estar online e conectados ao sistema StorageGRID , ou podem estar offline e desconectados.
- Executar um "[descomissionamento do local](#)" para remover um site. Você executa um **descomissionamento de site conectado** se todos os nós estiverem conectados ao StorageGRID. Você executa um **descomissionamento de site desconectado** se todos os nós estiverem desconectados do StorageGRID. Se o site contiver uma mistura de nós conectados e desconectados, você deverá colocar todos os nós offline novamente online.



Antes de executar o descomissionamento de um site desconectado, entre em contato com seu representante de conta NetApp . A NetApp analisará seus requisitos antes de habilitar todas as etapas do assistente de descomissionamento do site. Você não deve tentar desativar um site desconectado se acreditar que é possível recuperar o site ou recuperar dados de objetos do site.

Descomissionar nós

Desativação do nó da rede

Você pode usar o procedimento de descomissionamento de nós para remover um ou mais nós de grade em um ou mais sites. Não é possível desativar o nó de administração principal.

Quando desativar um nó

Use o procedimento de descomissionamento do nó quando qualquer uma das seguintes condições for verdadeira:

- Você adicionou um nó de armazenamento maior em uma expansão e deseja remover um ou mais nós de armazenamento menores, preservando ao mesmo tempo os objetos.



Se você deseja substituir um aparelho antigo por um mais novo, considere ["clonando o nó do aparelho"](#) em vez de adicionar um novo aparelho em uma expansão e depois desativar o antigo.

- Você precisa de menos armazenamento total.
- Você não precisa mais de um nó de gateway.
- Você não precisa mais de um nó de administração não primário.
- Sua rede inclui um nó desconectado que você não pode recuperar ou colocar online novamente.
- Sua grade inclui um nó de arquivo.

Como descomissionar um nó

Você pode desativar nós de rede conectados ou desconectados.

Desativar nós conectados

Em geral, você deve desativar os nós da grade somente quando eles estiverem conectados ao sistema StorageGRID e somente quando todos os nós estiverem em funcionamento normal (com ícones verdes nas páginas **NÓS** e na página **Desativar nós**).

Para obter instruções, consulte ["Descomissionar nós de rede conectados"](#).

Desativar nós desconectados

Em alguns casos, pode ser necessário desativar um nó de grade que não esteja conectado à grade no momento (um cuja integridade seja Desconhecida ou Administrativamente Inativo).

Para obter instruções, consulte ["Descomissionar nós de rede desconectados"](#).

O que considerar antes de desativar um nó

Antes de executar qualquer procedimento, revise as considerações para cada tipo de nó:

- ["Considerações sobre a desativação do nó de administração ou gateway"](#)
- ["Considerações sobre a desativação do nó de armazenamento"](#)

Considerações para descomissionamento de nós de administração ou gateway

Revise as considerações para descomissionar um nó de administração ou um nó de gateway.

Considerações para o nó de administração

- Não é possível desativar o nó de administração principal.
- Não é possível desativar um nó de administração se uma de suas interfaces de rede fizer parte de um grupo de alta disponibilidade (HA). Primeiro, você deve remover as interfaces de rede do grupo HA. Veja as instruções para ["gerenciando grupos HA"](#).
- Conforme necessário, você pode alterar com segurança as políticas do ILM ao desativar um nó de administração.
- Se você desativar um nó de administração e o logon único (SSO) estiver habilitado para seu sistema StorageGRID, lembre-se de remover a parte confiável do nó dos Serviços de Federação do Active Directory (AD FS).

- Se você usar "[federação de grade](#)" , certifique-se de que o endereço IP do nó que você está descomissionando não foi especificado para uma conexão de federação de rede.
- Ao desativar um nó de administração desconectado, você perderá os logs de auditoria desse nó; no entanto, esses logs também devem existir no nó de administração principal.

Considerações para o nó de gateway

- Não é possível desativar um nó de gateway se uma de suas interfaces de rede fizer parte de um grupo de alta disponibilidade (HA). Primeiro, você deve remover as interfaces de rede do grupo HA. Veja as instruções para "[gerenciando grupos HA](#)" .
- Conforme necessário, você pode alterar com segurança as políticas do ILM ao desativar um nó de gateway.
- Se você usar "[federação de grade](#)" , certifique-se de que o endereço IP do nó que você está descomissionando não foi especificado para uma conexão de federação de rede.
- Você pode desativar com segurança um nó de gateway enquanto ele estiver desconectado.

Considerações sobre nós de armazenamento

Considerações para descomissionamento de nós de armazenamento

Antes de desativar um nó de armazenamento, considere se você pode cloná-lo. Então, se você decidir desativar o nó, revise como o StorageGRID gerencia objetos e metadados durante o procedimento de desativação.

Quando clonar um nó em vez de desativá-lo

Se você quiser substituir um nó de armazenamento de dispositivo mais antigo por um dispositivo mais novo ou maior, considere clonar o nó do dispositivo em vez de adicionar um novo dispositivo em uma expansão e, em seguida, desativar o dispositivo antigo.

A clonagem de nós de dispositivos permite que você substitua facilmente um nó de dispositivo existente por um dispositivo compatível no mesmo site do StorageGRID . O processo de clonagem transfere todos os dados para o novo dispositivo, coloca o novo dispositivo em serviço e deixa o antigo em um estado de pré-instalação.

Você pode clonar um nó do dispositivo se precisar:

- Substitua um aparelho que esteja chegando ao fim de sua vida útil.
- Atualize um nó existente para aproveitar a tecnologia aprimorada do dispositivo.
- Aumente a capacidade de armazenamento da grade sem alterar o número de nós de armazenamento no seu sistema StorageGRID .
- Melhore a eficiência do armazenamento, alterando, por exemplo, o modo RAID.

Ver "[Clonagem de nó de dispositivo](#)" para mais detalhes.

Considerações para nós de armazenamento conectados

Revise as considerações para descomissionar um nó de armazenamento conectado.

- Você não deve desativar mais de 10 nós de armazenamento em um único procedimento de desativação de nó.

- O sistema deve, em todos os momentos, incluir Nós de Armazenamento suficientes para satisfazer os requisitos operacionais, incluindo o ["Quórum do ADC"](#) e o ativo ["Política de ILM"](#) . Para satisfazer essa restrição, talvez seja necessário adicionar um novo nó de armazenamento em uma operação de expansão antes de desativar um nó de armazenamento existente.

Tenha cuidado ao desativar nós de armazenamento em uma grade contendo nós somente de metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Ver ["Tipos de nós de armazenamento"](#) para obter mais informações sobre nós de armazenamento somente de metadados.

- Quando você remove um nó de armazenamento, grandes volumes de dados de objetos são transferidos pela rede. Embora essas transferências não devam afetar as operações normais do sistema, elas podem afetar a quantidade total de largura de banda de rede consumida pelo sistema StorageGRID .
- As tarefas associadas ao descomissionamento do nó de armazenamento recebem uma prioridade menor do que as tarefas associadas às operações normais do sistema. Isso significa que o descomissionamento não interfere nas operações normais do sistema StorageGRID e não precisa ser agendado para um período de inatividade do sistema. Como o descomissionamento é realizado em segundo plano, é difícil estimar quanto tempo o processo levará para ser concluído. Em geral, o descomissionamento termina mais rapidamente quando o sistema está silencioso ou se apenas um nó de armazenamento estiver sendo removido por vez.
- Pode levar dias ou semanas para desativar um nó de armazenamento. Planeje esse procedimento adequadamente. Embora o processo de descomissionamento seja projetado para não afetar as operações do sistema, ele pode limitar outros procedimentos. Em geral, você deve executar quaisquer atualizações ou expansões planejadas do sistema antes de remover os nós da grade.
- Se você precisar executar outro procedimento de manutenção enquanto os nós de armazenamento estiverem sendo removidos, você pode ["suspender o procedimento de descomissionamento"](#) e retome-o após a conclusão do outro procedimento.



O botão **Pausar** é habilitado somente quando os estágios de avaliação do ILM ou de descomissionamento de dados codificados por eliminação são atingidos; no entanto, a avaliação do ILM (migração de dados) continuará sendo executada em segundo plano.

- Não é possível executar operações de reparo de dados em nenhum nó de grade quando uma tarefa de desativação estiver em execução.
- Você não deve fazer nenhuma alteração em uma política de ILM enquanto um nó de armazenamento estiver sendo desativado.
- Para remover dados de forma permanente e segura, você deve limpar as unidades do nó de armazenamento após a conclusão do procedimento de desativação.

Considerações para nós de armazenamento desconectados

Revise as considerações para descomissionar um nó de armazenamento desconectado.

- Nunca desative um nó desconectado a menos que tenha certeza de que ele não pode ser colocado on-line ou recuperado.



Não execute este procedimento se você acredita que é possível recuperar dados de objeto do nó. Em vez disso, entre em contato com o suporte técnico para determinar se a recuperação do nó é possível.

- Quando você desativa um nó de armazenamento desconectado, o StorageGRID usa dados de outros nós

de armazenamento para reconstruir os dados do objeto e metadados que estavam no nó desconectado.

- Pode ocorrer perda de dados se você desativar mais de um nó de armazenamento desconectado. O sistema pode não conseguir reconstruir dados se não houver cópias de objetos, fragmentos codificados por eliminação ou metadados de objetos suficientes disponíveis. Ao desativar nós de armazenamento em uma grade com nós somente de metadados baseados em software, desativar todos os nós configurados para armazenar objetos e metadados remove todo o armazenamento de objetos da grade. Ver "[Tipos de nós de armazenamento](#)" para obter mais informações sobre nós de armazenamento somente de metadados.



Se você tiver mais de um nó de armazenamento desconectado que não consegue recuperar, entre em contato com o suporte técnico para determinar o melhor curso de ação.

- Quando você desativa um nó de armazenamento desconectado, o StorageGRID inicia trabalhos de reparo de dados no final do processo de desativação. Esses trabalhos tentam reconstruir os dados e metadados do objeto que foram armazenados no nó desconectado.
- Quando você descomissiona um nó de armazenamento desconectado, o procedimento de descomissionamento é concluído relativamente rápido. No entanto, os trabalhos de reparo de dados podem levar dias ou semanas para serem executados e não são monitorados pelo procedimento de desativação. Você deve monitorar manualmente esses trabalhos e reiniciá-los conforme necessário. Ver "[Verifique os trabalhos de reparo de dados](#)".
- Se você desativar um nó de armazenamento desconectado que contém a única cópia de um objeto, o objeto será perdido. Os trabalhos de reparo de dados só podem reconstruir e recuperar objetos se houver pelo menos uma cópia replicada ou fragmentos codificados para eliminação suficientes nos Nós de Armazenamento que estão conectados no momento.

Qual é o quórum do ADC?

Talvez você não consiga desativar determinados nós de armazenamento em um site se poucos serviços de Controlador de Domínio Administrativo (ADC) permanecerem após o descomissionamento.

O serviço ADC, encontrado em alguns nós de armazenamento, mantém informações de topologia de grade e fornece serviços de configuração para a grade. O sistema StorageGRID exige que um quorum de serviços ADC esteja disponível em cada site e o tempo todo.

Você não pode desativar um nó de armazenamento se a remoção do nó fizer com que o quórum do ADC não seja mais atendido. Para satisfazer o quórum do ADC durante um descomissionamento, no mínimo três nós de armazenamento em cada local devem ter o serviço ADC. Se um site tiver mais de três nós de armazenamento com o serviço ADC, a maioria simples desses nós deverá permanecer disponível após o descomissionamento: $((0.5 * \text{Storage Nodes with ADC}) + 1)$



Tenha cuidado ao desativar nós de armazenamento em uma grade contendo nós somente de metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Ver "[Tipos de nós de armazenamento](#)" para obter mais informações sobre nós de armazenamento somente de metadados.

Por exemplo, suponha que um site atualmente inclui seis nós de armazenamento com serviços ADC e você deseja desativar três nós de armazenamento. Devido ao requisito de quórum do ADC, você deve concluir dois procedimentos de desativação, conforme a seguir:

- No primeiro procedimento de descomissionamento, você deve garantir que quatro nós de armazenamento com serviços ADC permaneçam disponíveis: $((0.5 * 6) + 1)$. Isso significa que você só pode desativar dois nós de armazenamento inicialmente.
- No segundo procedimento de descomissionamento, você pode remover o terceiro nó de armazenamento porque o quorum do ADC agora requer apenas três serviços do ADC para permanecer disponível: $((0.5 * 4) + 1)$.

Se você precisar desativar um nó de armazenamento, mas não puder devido ao requisito de quorum do ADC, adicione um novo nó de armazenamento em um "expansão" e especifique que ele deve ter um serviço ADC. Em seguida, descomissione o nó de armazenamento existente.

Revisar a política do ILM e a configuração de armazenamento

Se você planeja desativar um nó de armazenamento, revise a política de ILM do seu sistema StorageGRID antes de iniciar o processo de desativação.

Durante o descomissionamento, todos os dados do objeto são migrados do nó de armazenamento desativado para outros nós de armazenamento.



A política de ILM que você tiver *durante* a desativação será a mesma usada *após* a desativação. Você deve garantir que esta política atenda aos seus requisitos de dados antes de iniciar a desativação e depois que ela for concluída.

Você deve revisar as regras em cada "política ILM ativa" para garantir que o sistema StorageGRID continuará a ter capacidade suficiente do tipo correto e nos locais corretos para acomodar o descomissionamento de um nó de armazenamento.

Considere o seguinte:

- Será possível que os serviços de avaliação do ILM copiem dados de objetos de forma que as regras do ILM sejam atendidas?
- O que acontece se um site ficar temporariamente indisponível enquanto o descomissionamento estiver em andamento? Cópias adicionais podem ser feitas em um local alternativo?
- Como o processo de desativação afetará a distribuição final do conteúdo? Conforme descrito em "Consolidar nós de armazenamento", você deve "adicionar novos nós de armazenamento" antes de descomissionar os antigos. Se você adicionar um nó de armazenamento de substituição maior após desativar um nó de armazenamento menor, os nós de armazenamento antigos poderão estar próximos da capacidade máxima e o novo nó de armazenamento poderá não ter quase nenhum conteúdo. A maioria das operações de gravação de novos dados de objeto seriam direcionadas ao novo Nó de Armazenamento, reduzindo a eficiência geral das operações do sistema.
- O sistema incluirá, em todos os momentos, nós de armazenamento suficientes para satisfazer as políticas de ILM ativas?



Uma política de ILM que não pode ser atendida levará a atrasos e alertas, e pode interromper a operação do sistema StorageGRID.

Verifique se a topologia proposta que resultará do processo de descomissionamento atende à política do ILM avaliando as áreas listadas na tabela.

Área a ser avaliada	O que considerar
Capacidade disponível	Haverá capacidade de armazenamento suficiente para acomodar todos os dados de objetos armazenados no sistema StorageGRID , incluindo as cópias permanentes dos dados de objetos atualmente armazenados no nó de armazenamento a ser desativado? Haverá capacidade suficiente para lidar com o crescimento previsto nos dados de objetos armazenados por um intervalo de tempo razoável após a conclusão do descomissionamento?
Localização do armazenamento	Se houver capacidade suficiente no sistema StorageGRID como um todo, a capacidade estará nos locais corretos para satisfazer as regras de negócios do sistema StorageGRID ?
Tipo de armazenamento	Haverá armazenamento suficiente do tipo apropriado após a conclusão do descomissionamento? Por exemplo, as regras de ILM podem mover conteúdo de um tipo de armazenamento para outro à medida que o conteúdo envelhece. Nesse caso, você deve garantir que haja armazenamento suficiente do tipo apropriado disponível na configuração final do sistema StorageGRID .

Consolidar nós de armazenamento

Você pode consolidar nós de armazenamento para reduzir a contagem de nós de armazenamento para um site ou implantação e, ao mesmo tempo, aumentar a capacidade de armazenamento.

Ao consolidar nós de armazenamento, você ["expandir o sistema StorageGRID"](#) adicionando novos nós de armazenamento de maior capacidade e, em seguida, descomissionando os antigos nós de armazenamento de menor capacidade. Durante o procedimento de desativação, os objetos são migrados dos antigos nós de armazenamento para os novos nós de armazenamento.



Se você estiver consolidando aparelhos mais antigos e menores com novos modelos ou aparelhos de maior capacidade, considere ["clonando o nó do aparelho"](#) (ou use a clonagem de nó do dispositivo e o procedimento de descomissionamento se você não estiver fazendo uma substituição um-para-um).

Por exemplo, você pode adicionar dois novos nós de armazenamento com maior capacidade para substituir três nós de armazenamento mais antigos. Primeiro, você usaria o procedimento de expansão para adicionar os dois novos nós de armazenamento maiores e, em seguida, usaria o procedimento de descomissionamento para remover os três antigos nós de armazenamento de menor capacidade.

Ao adicionar nova capacidade antes de remover os nós de armazenamento existentes, você garante uma distribuição mais equilibrada de dados no sistema StorageGRID . Você também reduz a possibilidade de um nó de armazenamento existente ser empurrado além do nível de marca d'água de armazenamento.

Descomissionar vários nós de armazenamento

Se precisar remover mais de um nó de armazenamento, você poderá desativá-los

sequencialmente ou em paralelo.



Tenha cuidado ao desativar nós de armazenamento em uma grade contendo nós somente de metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Ver "[Tipos de nós de armazenamento](#)" para obter mais informações sobre nós de armazenamento somente de metadados.

- Se você desativar os Nós de Armazenamento sequencialmente, deverá aguardar a conclusão do primeiro Nó de Armazenamento antes de iniciar a desativação do próximo Nó de Armazenamento.
- Se você desativar os Nós de Armazenamento em paralelo, os Nós de Armazenamento processarão simultaneamente as tarefas de desativação para todos os Nós de Armazenamento que estão sendo desativados. Isso pode resultar em uma situação em que todas as cópias permanentes de um arquivo são marcadas como "somente leitura", desabilitando temporariamente a exclusão em grades onde essa funcionalidade está habilitada.

Verifique os trabalhos de reparo de dados

Antes de desativar um nó de grade, você deve confirmar se não há trabalhos de reparo de dados ativos. Se algum reparo falhar, você deve reiniciá-lo e esperar que ele seja concluído antes de executar o procedimento de descomissionamento.

Sobre esta tarefa

Se precisar desativar um nó de armazenamento desconectado, você também deverá concluir estas etapas após a conclusão do procedimento de desativação para garantir que o trabalho de reparo de dados tenha sido concluído com sucesso. Você deve garantir que todos os fragmentos codificados para eliminação que estavam no nó removido tenham sido restaurados com sucesso.

Essas etapas se aplicam somente a sistemas que possuem objetos codificados para eliminação.

Passos

1. Efetue login no nó de administração principal:
 - a. Digite o seguinte comando: `ssh admin@grid_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. Verifique se há reparos em execução: `repair-data show-ec-repair-status`

- Se você nunca executou um trabalho de reparo de dados, a saída é `No job found`. Você não precisa reiniciar nenhum trabalho de reparo.
- Se o trabalho de reparo de dados foi executado anteriormente ou está em execução no momento, a saída listará informações para o reparo. Cada reparo tem um ID de reparo exclusivo.

Repair ID	Affected Nodes / Volumes	Start Time	End Time	State	Estimated Bytes Affected	Bytes Repaired	Percentage
4216507958013005550	DC1-S1-0-182 (Volumes: 2)	2022-08-17T21:37:30.051543	2022-08-17T21:37:37.320998	Completed	1015788876	0	0
18214680851049518682	DC1-S1-0-182 (Volumes: 1)	2022-08-17T20:37:58.869362	2022-08-17T20:38:45.299688	Completed	0	0	100
7962734388032289010	DC1-S1-0-182 (Volumes: 0)	2022-08-17T20:42:29.578740		Stopped			Unknown



Opcionalmente, você pode usar o Grid Manager para monitorar processos de restauração em andamento e exibir um histórico de restauração. Ver ["Restaurar dados de objetos usando o Grid Manager"](#).

3. Se o Estado para todos os reparos for `Completed`, você não precisa reiniciar nenhum trabalho de reparo.
4. Se o Estado para qualquer reparação for `Stopped`, você deve reiniciar esse reparo.

- a. Obtenha o ID do reparo com falha na saída.
- b. Execute o `repair-data start-ec-node-repair` comando.

Use o `--repair-id` opção para especificar o ID do reparo. Por exemplo, se você quiser tentar novamente um reparo com ID de reparo 949292, execute este comando: `repair-data start-ec-node-repair --repair-id 949292`

- c. Continue a acompanhar o status dos reparos de dados da CE até que o Estado para todos os reparos seja `Completed`.

Reúna os materiais necessários

Antes de executar a desativação de um nó de rede, você deve obter as seguintes informações.

Item	Notas
Pacote de Recuperação .zip arquivo	Você deve "baixe o pacote de recuperação mais recente" .zip arquivo(<code>sgws-recovery-package-id-revision.zip</code>). Você pode usar o arquivo do Pacote de Recuperação para restaurar o sistema caso ocorra uma falha.
`Passwords.txt` arquivo	Este arquivo contém as senhas necessárias para acessar os nós da grade na linha de comando e está incluído no Pacote de Recuperação.
Senha de provisionamento	A senha é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está no <code>Passwords.txt</code> arquivo.
Descrição da topologia do sistema StorageGRID antes do descomissionamento	Se disponível, obtenha qualquer documentação que descreva a topologia atual do sistema.

Informações relacionadas

["Requisitos do navegador da Web"](#)

Acesse a página de nós de descomissionamento

Ao acessar a página Desativar nós no Grid Manager, você pode ver rapidamente quais nós podem ser desativados.

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"](#) .



Tenha cuidado ao desativar nós de armazenamento em uma grade contendo nós somente de metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Ver ["Tipos de nós de armazenamento"](#) para obter mais informações sobre nós de armazenamento somente de metadados.

Passos

1. Selecione **MANUTENÇÃO > Tarefas > Desativação**.
2. Selecione **Desativar nós**.

A página Descomissionar nós é exibida. Nesta página, você pode:

- Determine quais nós da rede podem ser desativados atualmente.
- Veja a saúde de todos os nós da grade
- Classifique a lista em ordem crescente ou decrescente por **Nome**, **Site**, **Tipo** ou **Possui ADC**.
- Insira termos de pesquisa para encontrar rapidamente nós específicos.

Neste exemplo, a coluna Possível descomissionamento indica que você pode descomissionar o nó de gateway e um dos quatro nós de armazenamento.

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-		No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-ARC1	Data Center 1	Archive Node	-		No, you can't decommission an Archive Node unless the node is disconnected.
☐ DC1-G1	Data Center 1	API Gateway Node	-		
DC1-S1	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
☐ DC1-S4	Data Center 1	Storage Node	No		

3. Revise a coluna **Desativação possível** para cada nó que você deseja desativar.

Se um nó de grade puder ser desativado, esta coluna incluirá uma marca de seleção verde e a coluna da esquerda incluirá uma caixa de seleção. Se um nó não puder ser desativado, esta coluna descreve o problema. Se houver mais de um motivo pelo qual um nó não pode ser desativado, o motivo mais crítico será mostrado.

Descomissionamento Possível razão	Descrição	Etapas para resolver
Não, o descomissionamento do <i>tipo de nó</i> não é suportado.	Não é possível desativar o nó de administração principal.	Nenhum.

Descomissionamento Possível razão	Descrição	Etapas para resolver
Não, pelo menos um nó da rede está desconectado. Observação: esta mensagem é exibida somente para nós de grade conectados.	Não é possível desativar um nó de rede conectado se algum nó de rede estiver desconectado. A coluna Saúde inclui um destes ícones para nós de grade que estão desconectados:  (cinza): Administrativamente inativo  (azul): Desconhecido	Você deve colocar todos os nós desconectados novamente online ou "descomissionar todos os nós desconectados" antes de poder remover um nó conectado. Observação: se sua rede contiver vários nós desconectados, o software exigirá que você os desative todos ao mesmo tempo, o que aumenta o potencial de resultados inesperados.
Não, um ou mais nós necessários estão desconectados no momento e precisam ser recuperados. Observação: Esta mensagem é exibida somente para nós de rede desconectados.	Não é possível desativar um nó de rede desconectado se um ou mais nós necessários também estiverem desconectados (por exemplo, um nó de armazenamento necessário para o quorum do ADC).	- Revise as mensagens de Possível Desativação para todos os nós desconectados. - Determine quais nós não podem ser desativados porque são necessários. - Se a integridade de um nó necessário estiver administrativamente inativa, coloque o nó novamente online. - Se a integridade de um nó necessário for desconhecida, execute um procedimento de recuperação de nó para recuperá-lo.
Não, membro do(s) grupo(s) HA: <i>nome do grupo</i>. Antes de desativar este nó, você deve removê-lo de todos os grupos de HA.	Não é possível desativar um nó de administração ou um nó de gateway se uma interface de nó pertencer a um grupo de alta disponibilidade (HA).	Edite o grupo HA para remover a interface do nó ou remover todo o grupo HA. Ver "Configurar grupos de alta disponibilidade".
Não, o site x requer um mínimo de <i>n</i> nós de armazenamento com serviços ADC.	Somente nós de armazenamento. Não é possível desativar um nó de armazenamento se não houver nós suficientes no local para dar suporte aos requisitos de quórum do ADC.	Executar uma expansão. Adicione um novo nó de armazenamento ao site e especifique que ele deve ter um serviço ADC. Veja informações sobre o "Quórum do ADC".

Descomissionamento Possível razão	Descrição	Etapas para resolver
Não, um ou mais perfis de codificação de eliminação precisam de pelo menos n nós de armazenamento. Se o perfil não for usado em uma regra ILM, você poderá desativá-lo.	Somente nós de armazenamento. Não é possível desativar um nó de armazenamento a menos que haja nós suficientes para os perfis de codificação de eliminação existentes. Por exemplo, se existir um perfil de codificação de eliminação para codificação de eliminação 4+2, pelo menos 6 nós de armazenamento devem permanecer.	Para cada perfil de codificação de eliminação afetado, execute uma das seguintes etapas, com base em como o perfil está sendo usado: • Usado em políticas ILM ativas: Executar uma expansão. Adicione novos nós de armazenamento suficientes para permitir que a codificação de eliminação continue. Veja as instruções para "expandindo sua grade". • Usado em uma regra de ILM, mas não em políticas de ILM ativas: edite ou exclua a regra e desative o perfil de codificação de eliminação. • Não usado em nenhuma regra do ILM: Desative o perfil de codificação de eliminação. Observação: Uma mensagem de erro será exibida se você tentar desativar um perfil de codificação de eliminação e os dados do objeto ainda estiverem associados ao perfil. Pode ser necessário esperar várias semanas antes de tentar o processo de desativação novamente. Aprenda sobre "desativando um perfil de codificação de eliminação".
Não, você não pode desativar um nó de arquivo a menos que o nó esteja desconectado.	Se um nó de arquivo ainda estiver conectado, você não poderá removê-lo.	Observação: O suporte para nós de arquivo foi removido. Se você precisar desativar um nó de arquivo, consulte "Descomissionamento de nós de grade (site de documentação do StorageGRID 11.8)"

Descomissionar nós de rede desconectados

Pode ser necessário desativar um nó que não esteja conectado à rede no momento (um nó cuja integridade seja desconhecida ou administrativamente inativo).

Antes de começar

- Você entende as considerações para o descomissionamento "[Nós de administração e gateway](#)" e as considerações para o descomissionamento "[Nós de armazenamento](#)".
- Você obteve todos os itens pré-requisitos.
- Você garantiu que nenhum trabalho de reparo de dados esteja ativo. Ver "[Verifique os trabalhos de reparo de dados](#)".
- Você confirmou que a recuperação do nó de armazenamento não está em andamento em nenhum lugar da grade. Se for o caso, você deve esperar até que qualquer reconstrução do Cassandra realizada como parte da recuperação seja concluída. Você pode então prosseguir com o descomissionamento.
- Você garantiu que outros procedimentos de manutenção não serão executados enquanto o procedimento de desativação do nó estiver em execução, a menos que o procedimento de desativação do nó esteja pausado.
- A coluna **Desativação possível** para o nó ou nós desconectados que você deseja desativar inclui uma marca de seleção verde.
- Você tem a senha de provisionamento.

Sobre esta tarefa

Você pode identificar nós desconectados procurando pelo ícone azul Desconhecido  ou o ícone cinza de administração inativa  na coluna **Saúde**.

Antes de desativar qualquer nó desconectado, observe o seguinte:

- Este procedimento destina-se principalmente à remoção de um único nó desconectado. Se sua rede contiver vários nós desconectados, o software exigirá que você os desative todos ao mesmo tempo, o que aumenta o potencial de resultados inesperados.



Pode ocorrer perda de dados se você desativar mais de um nó de armazenamento desconectado por vez. Ver "[Considerações para nós de armazenamento desconectados](#)".



Tenha cuidado ao desativar nós de armazenamento em uma grade contendo nós somente de metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Ver "[Tipos de nós de armazenamento](#)" para obter mais informações sobre nós de armazenamento somente de metadados.

- Se um nó desconectado não puder ser removido (por exemplo, um nó de armazenamento necessário para o quorum do ADC), nenhum outro nó desconectado poderá ser removido.

Passos

1. A menos que você esteja desativando um nó de arquivo (que deve ser desconectado), tente colocar todos os nós de grade desconectados novamente online ou recuperá-los.

Ver "[Procedimentos de recuperação de nós de grade](#)" para obter instruções.

2. Se você não conseguir recuperar um nó de rede desconectado e quiser desativá-lo enquanto estiver desconectado, marque a caixa de seleção desse nó.



Se sua rede contiver vários nós desconectados, o software exigirá que você os desative todos ao mesmo tempo, o que aumenta o potencial de resultados inesperados.



Tenha cuidado ao optar por desativar mais de um nó de rede desconectado por vez, especialmente se estiver selecionando vários nós de armazenamento desconectados. Se você tiver mais de um nó de armazenamento desconectado que não consegue recuperar, entre em contato com o suporte técnico para determinar o melhor curso de ação.

3. Digite a senha de provisionamento.

O botão **Iniciar descomissionamento** está habilitado.

4. Clique em **Iniciar descomissionamento**.

Um aviso é exibido, indicando que você selecionou um nó desconectado e que os dados do objeto serão perdidos se o nó tiver a única cópia de um objeto.

5. Revise a lista de nós e clique em **OK**.

O procedimento de descomissionamento é iniciado e o progresso é exibido para cada nó. Durante o procedimento, um novo Pacote de Recuperação é gerado contendo a alteração da configuração da grade.

6. Assim que o novo Pacote de Recuperação estiver disponível, clique no link ou selecione **MANUTENÇÃO > Sistema > Pacote de recuperação** para acessar a página Pacote de recuperação. Em seguida, baixe o .zip arquivo.

Veja as instruções para "[baixando o pacote de recuperação](#)".



Baixe o Pacote de Recuperação o mais rápido possível para garantir que você possa recuperar sua rede se algo der errado durante o procedimento de desativação.



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.

7. Monitore periodicamente a página Desativação para garantir que todos os nós selecionados sejam desativados com sucesso.

Os nós de armazenamento podem levar dias ou semanas para serem desativados. Quando todas as tarefas estiverem concluídas, a lista de seleção de nós será exibida novamente com uma mensagem de sucesso. Se você descomissionou um nó de armazenamento desconectado, uma mensagem informativa indica que os trabalhos de reparo foram iniciados.

8. Depois que os nós forem desligados automaticamente como parte do procedimento de desativação, remova quaisquer máquinas virtuais restantes ou outros recursos associados ao nó desativado.



Não execute esta etapa até que os nós sejam desligados automaticamente.

9. Se você estiver desativando um nó de armazenamento, monitore o status dos trabalhos de reparo de **dados replicados e dados codificados para eliminação (EC)** que são iniciados automaticamente

durante o processo de desativação.

Dados replicados

- Para obter uma porcentagem estimada de conclusão do reparo replicado, adicione o `show-replicated-repair-status` opção para o comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Para determinar se os reparos foram concluídos:
 - a. Selecione **NÓS > Nó de armazenamento sendo reparado > ILM**.
 - b. Revise os atributos na seção Avaliação. Quando os reparos estiverem concluídos, o atributo **Aguardando - Todos** indica 0 objetos.
- Para monitorar o reparo com mais detalhes:
 - a. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
 - b. Selecione **grid > Nó de armazenamento sendo reparado > LDR > Armazenamento de dados**.
 - c. Use uma combinação dos seguintes atributos para determinar, da melhor forma possível, se os reparos replicados estão completos.



Inconsistências no Cassandra podem estar presentes, e reparos com falha não são rastreados.

- **Reparos Tentados (XRPA)**: Use este atributo para rastrear o progresso de reparos replicados. Este atributo aumenta cada vez que um nó de armazenamento tenta reparar um objeto de alto risco. Quando esse atributo não aumenta por um período maior que o período de verificação atual (fornecido pelo atributo **Período de verificação — Estimado**), significa que a verificação do ILM não encontrou objetos de alto risco que precisem ser reparados em nenhum nó.



Objetos de alto risco são objetos que correm o risco de serem completamente perdidos. Isso não inclui objetos que não satisfazem sua configuração de ILM.

- **Período de verificação — estimado (XSCM)**: use este atributo para estimar quando uma alteração de política será aplicada a objetos ingeridos anteriormente. Se o atributo **Reparos Tentados** não aumentar por um período maior que o período de verificação atual, é provável que reparos replicados sejam feitos. Observe que o período de verificação pode mudar. O atributo **Período de varredura — Estimado (XSCM)** se aplica a toda a grade e é o máximo de todos os períodos de varredura de nós. Você pode consultar o histórico do atributo **Período de verificação — Estimado** da grade para determinar um período de tempo apropriado.

Dados codificados por apagamento (EC)

Para monitorar o reparo de dados codificados para eliminação e tentar novamente quaisquer solicitações que possam ter falhado:

1. Determinar o status dos reparos de dados codificados por eliminação:
 - Selecione **SUPORTE > Ferramentas > Métricas** para visualizar o tempo estimado para conclusão e a porcentagem de conclusão do trabalho atual. Em seguida, selecione **Visão geral do EC** na seção Grafana. Veja os painéis **Tempo estimado para conclusão do trabalho do Grid EC** e **Porcentagem concluída do trabalho do Grid EC**.

- Use este comando para ver o status de um determinado `repair-data` operação:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Use este comando para listar todos os reparos:

```
repair-data show-ec-repair-status
```

A saída lista informações, incluindo `repair ID`, para todos os reparos anteriores e atuais.

2. Se a saída mostrar que a operação de reparo falhou, use o `--repair-id` opção de tentar o reparo novamente.

Este comando tenta novamente um reparo de nó com falha, usando o ID de reparo 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando tenta novamente um reparo de volume com falha, usando o ID de reparo 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Depois que você terminar

Assim que os nós desconectados forem desativados e todos os trabalhos de reparo de dados forem concluídos, você poderá desativar quaisquer nós de grade conectados, conforme necessário.

Em seguida, conclua estas etapas após concluir o procedimento de desativação:

- Certifique-se de que as unidades do nó de rede desativado sejam limpas. Use uma ferramenta ou serviço de limpeza de dados disponível comercialmente para remover dados das unidades de forma permanente e segura.
- Se você descomissionou um nó do dispositivo e os dados no dispositivo foram protegidos usando criptografia de nó, use o StorageGRID Appliance Installer para limpar a configuração do servidor de gerenciamento de chaves (Limpar KMS). Você deve limpar a configuração do KMS se quiser adicionar o dispositivo a outra grade. Para obter instruções, consulte "[Monitorar a criptografia do nó no modo de manutenção](#)".

Descomissionar nós de rede conectados

Você pode desativar e remover permanentemente nós que estão conectados à rede.

Antes de começar

- Você entende as considerações para o descomissionamento "[Nós de administração e gateway](#)" e as considerações para o descomissionamento "[Nós de armazenamento](#)".
- Você reuniu todos os materiais necessários.
- Você garantiu que nenhum trabalho de reparo de dados esteja ativo.
- Você confirmou que a recuperação do nó de armazenamento não está em andamento em nenhum lugar da grade. Se for o caso, aguarde até que qualquer reconstrução do Cassandra realizada como parte da recuperação seja concluída. Você pode então prosseguir com o descomissionamento.

- Você garantiu que outros procedimentos de manutenção não serão executados enquanto o procedimento de desativação do nó estiver em execução, a menos que o procedimento de desativação do nó esteja pausado.
- Você tem a senha de provisionamento.
- Os nós da grade estão conectados.
- A coluna **Desativação possível** para o nó ou nós que você deseja desativar inclui uma marca de seleção verde.



A desativação não será iniciada se um ou mais volumes estiverem offline (desmontados) ou se estiverem online (montados), mas em estado de erro.



Se um ou mais volumes ficarem offline enquanto uma desativação estiver em andamento, o processo de desativação será concluído depois que esses volumes voltarem a ficar online.

- Todos os nós da grade têm saúde normal (verde)  . Se você vir um desses ícones na coluna **Saúde**, tente resolver o problema:

Ícone	Cor	Gravidade
	Amarelo	Perceber
	Laranja claro	Menor
	Laranja escuro	Principal
	Vermelho	Crítico

- Se você descomissionou anteriormente um nó de armazenamento desconectado, todos os trabalhos de reparo de dados foram concluídos com sucesso. Ver "[Verifique os trabalhos de reparo de dados](#)".



Não remova a máquina virtual de um nó de grade ou outros recursos até que seja instruído a fazê-lo neste procedimento.



Tenha cuidado ao desativar nós de armazenamento em uma grade contendo nós somente de metadados baseados em software. Se você desativar todos os nós configurados para armazenar *tanto* objetos quanto metadados, a capacidade de armazenar objetos será removida da grade. Ver "[Tipos de nós de armazenamento](#)" para obter mais informações sobre nós de armazenamento somente de metadados.

Sobre esta tarefa

Quando um nó é desativado, seus serviços são desabilitados e o nó é desligado automaticamente.

Passos

1. Na página Desativar nós, marque a caixa de seleção para cada nó de grade que você deseja desativar.
2. Digite a senha de provisionamento.

O botão **Iniciar descomissionamento** está habilitado.

3. Selecione **Iniciar descomissionamento**.
4. Revise a lista de nós na caixa de diálogo de confirmação e selecione **OK**.

O procedimento de descomissionamento do nó é iniciado e o progresso é exibido para cada nó.



Não coloque um nó de armazenamento offline após o início do procedimento de desativação. Alterar o estado pode fazer com que alguns conteúdos não sejam copiados para outros locais.

5. Assim que o novo Pacote de Recuperação estiver disponível, selecione o link Pacote de Recuperação no banner ou selecione **MANUTENÇÃO > Sistema > Pacote de Recuperação** para acessar a página Pacote de Recuperação. Em seguida, baixe o .zip arquivo.

Ver "[baixando o pacote de recuperação](#)".



Baixe o Pacote de Recuperação o mais rápido possível para garantir que você possa recuperar sua rede se algo der errado durante o procedimento de desativação.

6. Monitore periodicamente a página Nós de Desativação para garantir que todos os nós selecionados sejam desativados com sucesso.



Os nós de armazenamento podem levar dias ou semanas para serem desativados.

Quando todas as tarefas estiverem concluídas, a lista de seleção de nós será exibida novamente com uma mensagem de sucesso.

Depois que você terminar

Conclua estas etapas depois de concluir o procedimento de desativação do nó:

1. Siga o passo apropriado para sua plataforma. Por exemplo:
 - **Linux:** Talvez você queira desanexar os volumes e excluir os arquivos de configuração do nó que você criou durante a instalação. Ver "[Instalar o StorageGRID no Red Hat Enterprise Linux](#)" e "[Instalar o StorageGRID no Ubuntu ou Debian](#)".
 - **VMware:** Talvez você queira usar a opção "Excluir do disco" do vCenter para excluir a máquina virtual. Talvez você também precise excluir quaisquer discos de dados que sejam independentes da máquina virtual.
 - *** Dispositivo StorageGRID *:** O nó do dispositivo reverte automaticamente para um estado não implantado, onde você pode acessar o instalador do dispositivo StorageGRID. Você pode desligar o dispositivo ou adicioná-lo a outro sistema StorageGRID.
2. Certifique-se de que as unidades do nó de rede desativado sejam limpas. Use uma ferramenta ou serviço de limpeza de dados disponível comercialmente para remover dados das unidades de forma permanente e segura.
3. Se você descomissionou um nó do dispositivo e os dados no dispositivo foram protegidos usando criptografia de nó, use o StorageGRID Appliance Installer para limpar a configuração do servidor de gerenciamento de chaves (Limpar KMS). Você deve limpar a configuração do KMS se quiser adicionar o dispositivo a outra grade. Para obter instruções, consulte "[Monitorar a criptografia do nó no modo de manutenção](#)".

Parar e retomar o processo de descomissionamento de nós de armazenamento

Se precisar executar um segundo procedimento de manutenção, você poderá pausar o procedimento de desativação de um nó de armazenamento durante determinados estágios. Após a conclusão do outro procedimento, você pode retomar o descomissionamento.



O botão **Parar** é habilitado somente quando os estágios de avaliação do ILM ou de descomissionamento de dados codificados por eliminação são atingidos; no entanto, a avaliação do ILM (migração de dados) continuará sendo executada em segundo plano.

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" .

Passos

1. Selecione **MANUTENÇÃO > Tarefas > Desativação**.

A página Desativação é exibida.

2. Selecione **Desativar nós**.

A página Descomissionar nós é exibida. Quando o procedimento de desativação atinge qualquer um dos seguintes estágios, o botão **Parar** é habilitado.

- Avaliando o ILM
- Desativação de dados codificados por apagamento

3. Selecione **Parar** para suspender o procedimento.

O estágio atual é pausado e o botão **Continuar** é habilitado.

Decommission Nodes

A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.

Decommissioning procedure has been paused. Click 'Resume' to resume the procedure.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Decommission Nodes					Search
Name	Type	Progress	Stage		
DC1-S5	Storage Node		Evaluating ILM		

Pause Resume

4. Após a conclusão do outro procedimento de manutenção, selecione **Retomar** para prosseguir com a desativação.

Local de descomissionamento

Considerações para remover um site

Antes de usar o procedimento de descomissionamento do site para remover um site, você deve revisar as considerações.

O que acontece quando você desativa um site

Quando você desativa um site, o StorageGRID remove permanentemente todos os nós do site e o próprio site do sistema StorageGRID .

Quando o procedimento de descomissionamento do site estiver concluído:

- Você não pode mais usar o StorageGRID para visualizar ou acessar o site ou qualquer um dos nós do site.
- Você não pode mais usar nenhum pool de armazenamento ou perfil de codificação de eliminação que faça referência ao site. Quando o StorageGRID desativa um site, ele remove automaticamente esses pools de armazenamento e desativa esses perfis de codificação de eliminação.

Diferenças entre procedimentos de descomissionamento de sites conectados e desconectados

Você pode usar o procedimento de desativação do site para remover um site no qual todos os nós estão conectados ao StorageGRID (chamado de desativação do site conectado) ou para remover um site no qual todos os nós estão desconectados do StorageGRID (chamado de desativação do site desconectado). Antes de começar, você precisa entender as diferenças entre esses procedimentos.



Se um site contém uma mistura de (✓) e nós desconectados (☾ ou ⚙), você deve colocar todos os nós offline novamente online.

- A desativação de um site conectado permite que você remova um site operacional do sistema StorageGRID . Por exemplo, você pode executar uma desativação de site conectado para remover um site que está funcional, mas não é mais necessário.
- Quando o StorageGRID remove um site conectado, ele usa o ILM para gerenciar os dados do objeto no site. Antes de iniciar a desativação de um site conectado, você deve remover o site de todas as regras do ILM e ativar uma nova política do ILM. Os processos do ILM para migrar dados de objetos e os processos internos para remover um site podem ocorrer ao mesmo tempo, mas a prática recomendada é permitir que as etapas do ILM sejam concluídas antes de iniciar o procedimento de desativação real.
- A desativação de um site desconectado permite que você remova um site com falha do sistema StorageGRID . Por exemplo, você pode executar uma desativação de site desconectado para remover um site que foi destruído por um incêndio ou inundação.

Quando o StorageGRID remove um site desconectado, ele considera todos os nós irrecuperáveis e não faz nenhuma tentativa de preservar os dados. No entanto, antes de iniciar a desativação de um site desconectado, você deve remover o site de todas as regras do ILM e ativar uma nova política do ILM.



Antes de executar um procedimento de desativação de site desconectado, você deve entrar em contato com seu representante de conta NetApp . A NetApp analisará seus requisitos antes de habilitar todas as etapas do assistente de descomissionamento do site. Você não deve tentar desativar um site desconectado se acreditar que é possível recuperar o site ou recuperar dados de objetos do site.

Requisitos gerais para remover um site conectado ou desconectado

Antes de remover um site conectado ou desconectado, você deve estar ciente dos seguintes requisitos:

- Não é possível desativar um site que inclua o nó de administração principal.
- Não é possível desativar um site se algum dos nós tiver uma interface que pertença a um grupo de alta disponibilidade (HA). Você deve editar o grupo HA para remover a interface do nó ou remover o grupo HA inteiro.
- Você não pode desativar um site se ele contiver uma mistura de () e desconectado ( ou ) nós.
- Você não pode desativar um site se qualquer nó em qualquer outro site estiver desconectado ( ou ).
- Não é possível iniciar o procedimento de desativação do site se uma operação ec-node-repair estiver em andamento. Ver "[Verifique os trabalhos de reparo de dados](#)" para rastrear reparos de dados codificados para eliminação.
- Enquanto o procedimento de descomissionamento do site estiver em andamento:
 - Você não pode criar regras de ILM que façam referência ao site que está sendo desativado. Você também não pode editar uma regra ILM existente para fazer referência ao site.
 - Você não pode executar outros procedimentos de manutenção, como expansão ou atualização.



Se você precisar executar outro procedimento de manutenção durante a desativação de um site conectado, você pode "[pausar o procedimento enquanto os nós de armazenamento estão sendo removidos](#)". O botão **Pausar** é habilitado somente quando os estágios de avaliação do ILM ou de descomissionamento de dados codificados por eliminação são atingidos; no entanto, a avaliação do ILM (migração de dados) continuará sendo executada em segundo plano. Após a conclusão do segundo procedimento de manutenção, você poderá retomar o descomissionamento.

- Se precisar recuperar qualquer nó após iniciar o procedimento de desativação do site, entre em contato com o suporte.
- Você não pode desativar mais de um site por vez.
- Se o site incluir um ou mais nós de administração e o logon único (SSO) estiver habilitado para seu sistema StorageGRID, você deverá remover todos os trusts de terceiros confiáveis do site dos Serviços de Federação do Active Directory (AD FS).

Requisitos para gerenciamento do ciclo de vida da informação (ILM)

Como parte da remoção de um site, você deve atualizar sua configuração do ILM. O assistente do Site de Desativação orienta você por uma série de etapas pré-requisitos para garantir o seguinte:

- O site não é mencionado por nenhuma política do ILM. Se for o caso, você deve editar as políticas ou criar e ativar políticas com novas regras de ILM.
- Nenhuma regra do ILM se refere ao site, mesmo que essas regras não sejam usadas em nenhuma política. Você deve excluir ou editar todas as regras que se referem ao site.

Quando o StorageGRID desativa o site, ele desativa automaticamente todos os perfis de codificação de eliminação não utilizados que fazem referência ao site e exclui automaticamente todos os pools de armazenamento não utilizados que fazem referência ao site. Se o pool de armazenamento All Storage Nodes existir (StorageGRID 11.6 e anteriores), ele será removido porque usa todos os sites.



Antes de remover um site, talvez seja necessário criar novas regras de ILM e ativar uma nova política de ILM. Estas instruções pressupõem que você tenha um bom entendimento de como o ILM funciona e que esteja familiarizado com a criação de pools de armazenamento, perfis de codificação de eliminação, regras de ILM e simulação e ativação de uma política de ILM. Ver ["Gerenciar objetos com ILM"](#).

Considerações sobre os dados do objeto em um site conectado

Se estiver executando uma desativação de site conectado, você deverá decidir o que fazer com os dados de objeto existentes no site ao criar novas regras de ILM e uma nova política de ILM. Você pode fazer uma ou ambas as seguintes ações:

- Mova dados de objetos do site selecionado para um ou mais outros sites na sua grade.

Exemplo de movimentação de dados: Suponha que você queira desativar um site em Raleigh porque adicionou um novo site em Sunnyvale. Neste exemplo, você deseja mover todos os dados do objeto do site antigo para o novo. Antes de atualizar suas regras e políticas de ILM, você deve revisar a capacidade em ambos os sites. Você deve garantir que o site Sunnyvale tenha capacidade suficiente para acomodar os dados de objetos do site Raleigh e que capacidade adequada permanecerá em Sunnyvale para crescimento futuro.



Para garantir que haja capacidade adequada disponível, pode ser necessário ["expandir uma grade"](#) adicionando volumes de armazenamento ou nós de armazenamento a um site existente ou adicionando um novo site antes de executar este procedimento.

- Excluir cópias de objetos do site selecionado.

Exemplo de exclusão de dados: Suponha que você use atualmente uma regra ILM de 3 cópias para replicar dados de objetos em três sites. Antes de desativar um site, você pode criar uma regra ILM equivalente de 2 cópias para armazenar dados em apenas dois sites. Quando você ativa uma nova política de ILM que usa a regra de 2 cópias, o StorageGRID exclui as cópias do terceiro site porque elas não atendem mais aos requisitos de ILM. No entanto, os dados do objeto ainda serão protegidos e a capacidade dos dois sites restantes permanecerá a mesma.



Nunca crie uma regra ILM de cópia única para acomodar a remoção de um site. 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.

Requisitos adicionais para a desativação de um site conectado

Antes que o StorageGRID possa remover um site conectado, você deve garantir o seguinte:

- Todos os nós no seu sistema StorageGRID devem ter um estado de conexão de **Conectado** (); no entanto, os nós podem ter alertas ativos.



Você pode concluir as etapas 1 a 4 do assistente de descomissionamento do site se um ou mais nós estiverem desconectados. No entanto, você não poderá concluir a Etapa 5 do assistente, que inicia o processo de desativação, a menos que todos os nós estejam conectados.

- Se o site que você planeja remover contiver um nó de gateway ou um nó de administração usado para balanceamento de carga, talvez seja necessário ["expandir uma grade"](#) para adicionar um novo nó equivalente em outro site. Certifique-se de que os clientes possam se conectar ao nó de substituição antes de iniciar o procedimento de desativação do site.
- Se o site que você planeja remover contiver algum nó de gateway ou nós de administração que estejam em um grupo de alta disponibilidade (HA), você poderá concluir as etapas 1 a 4 do assistente de descomissionamento do site. No entanto, você não poderá concluir a Etapa 5 do assistente, que inicia o processo de desativação, até remover esses nós de todos os grupos de HA. Se clientes existentes se conectarem a um grupo de HA que inclui nós do site, você deve garantir que eles possam continuar a se conectar ao StorageGRID após a remoção do site.
- Se os clientes se conectarem diretamente aos Nós de Armazenamento no site que você está planejando remover, você deve garantir que eles possam se conectar aos Nós de Armazenamento em outros sites antes de iniciar o procedimento de desativação do site.
- Você deve fornecer espaço suficiente nos sites restantes para acomodar quaisquer dados de objeto que serão movidos devido a alterações em qualquer política de ILM ativa. Em alguns casos, você pode precisar ["expandir uma grade"](#) adicionando nós de armazenamento, volumes de armazenamento ou novos sites antes de concluir a desativação de um site conectado.
- Você deve reservar tempo suficiente para que o procedimento de descomissionamento seja concluído. Os processos do StorageGRID ILM podem levar dias, semanas ou até meses para mover ou excluir dados de objetos do site antes que ele possa ser desativado.



Mover ou excluir dados de objetos de um site pode levar dias, semanas ou até meses, dependendo da quantidade de dados no site, da carga no sistema, das latências da rede e da natureza das alterações necessárias no ILM.

- Sempre que possível, você deve concluir as etapas 1 a 4 do assistente de descomissionamento do site o mais cedo possível. O procedimento de desativação será concluído mais rapidamente e com menos interrupções e impactos no desempenho se você permitir que os dados sejam movidos do site antes de iniciar o procedimento de desativação real (selecionando **Iniciar desativação** na Etapa 5 do assistente).

Requisitos adicionais para a desativação de um site desconectado

Antes que o StorageGRID possa remover um site desconectado, você deve garantir o seguinte:

- Você entrou em contato com seu representante de conta da NetApp . A NetApp analisará seus requisitos antes de habilitar todas as etapas do assistente de descomissionamento do site.



Você não deve tentar desativar um site desconectado se acreditar que é possível recuperar o site ou recuperar quaisquer dados de objeto do site. Ver ["Como o suporte técnico recupera um site"](#) .

- Todos os nós no site devem ter um estado de conexão de um dos seguintes:
 - **Desconhecido** (🌀): Por um motivo desconhecido, um nó é desconectado ou os serviços no nó ficam inesperadamente inativos. Por exemplo, um serviço no nó pode ser interrompido, ou o nó pode ter perdido sua conexão de rede devido a uma falha de energia ou interrupção inesperada.
 - **Administrativamente inativo** (🌑): O nó não está conectado à rede por um motivo esperado. Por exemplo, o nó ou os serviços no nó foram desligados normalmente.
- Todos os nós em todos os outros sites devem ter um estado de conexão de **Conectado** (✅); no

entanto, esses outros nós podem ter alertas ativos.

- Você deve entender que não poderá mais usar o StorageGRID para visualizar ou recuperar quaisquer dados de objeto armazenados no site. Quando o StorageGRID executa esse procedimento, ele não faz nenhuma tentativa de preservar nenhum dado do site desconectado.



Se suas regras e políticas de ILM foram projetadas para proteger contra a perda de um único site, cópias de seus objetos ainda existirão nos sites restantes.

- Você deve entender que se o site contiver a única cópia de um objeto, o objeto será perdido e não poderá ser recuperado.

Considerações sobre consistência ao remover um site

A consistência de um bucket S3 determina se o StorageGRID replica completamente os metadados do objeto para todos os nós e sites antes de informar ao cliente que a ingestão do objeto foi bem-sucedida. A consistência fornece um equilíbrio entre a disponibilidade dos objetos e a consistência desses objetos em diferentes nós de armazenamento e sites.

Quando o StorageGRID remove um site, ele precisa garantir que nenhum dado seja gravado no site que está sendo removido. Como resultado, ele substitui temporariamente a consistência de cada bucket ou contêiner. Após iniciar o processo de desativação do site, o StorageGRID usa temporariamente a consistência forte do site para impedir que metadados do objeto sejam gravados no site que está sendo removido.

Como resultado dessa substituição temporária, esteja ciente de que qualquer operação de gravação, atualização e exclusão do cliente que ocorrer durante a desativação de um site poderá falhar se vários nós ficarem indisponíveis nos sites restantes.

Reúna os materiais necessários

Antes de desativar um site, você deve obter os seguintes materiais.

Item	Notas
Pacote de Recuperação .zip arquivo	Você deve baixar o pacote de recuperação mais recente .zip arquivo(sgws-recovery-package-id-revision.zip). Você pode usar o arquivo do Pacote de Recuperação para restaurar o sistema caso ocorra uma falha. "Baixe o pacote de recuperação"
`Passwords.txt`arquivo	Este arquivo contém as senhas necessárias para acessar os nós da grade na linha de comando e está incluído no Pacote de Recuperação.
Senha de provisionamento	A senha é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está no Passwords.txt arquivo.
Descrição da topologia do sistema StorageGRID antes do descomissionamento	Se disponível, obtenha qualquer documentação que descreva a topologia atual do sistema.

Informações relacionadas

["Requisitos do navegador da Web"](#)

Etapa 1: Selecione o site

Para determinar se um site pode ser desativado, comece acessando o assistente de descomissionamento de site.

Antes de começar

- Você obteve todos os materiais necessários.
- Você revisou as considerações para remover um site.
- Você está conectado ao Grid Manager usando um ["navegador da web compatível"](#).
- Você tem o ["Permissão de acesso root ou permissões de manutenção e ILM"](#).

Passos

1. Selecione **MANUTENÇÃO > Tarefas > Desativação**.
2. Selecione **Local de descomissionamento**.

A Etapa 1 (Selecionar Site) do assistente de Desativação de Site é exibida. Esta etapa inclui uma lista alfabética dos sites no seu sistema StorageGRID.

Decommission Site

1

2

3

4

5

6

Select SiteView DetailsRevise ILM PolicyRemove ILM ReferencesResolve Node ConflictsMonitor Decommission

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity ?	Decommission Possible
☐	Raleigh	3.93 MB	✓
☐	Sunnyvale	3.97 MB	✓
	Vancouver	3.90 MB	No. This site contains the primary Admin Node.

Next

3. Visualize os valores na coluna **Capacidade de armazenamento usada** para determinar quanto armazenamento está sendo usado atualmente para dados de objeto em cada site.

A Capacidade de Armazenamento Utilizada é uma estimativa. Se os nós estiverem offline, a Capacidade de Armazenamento Usada será o último valor conhecido do site.

- Para a desativação de um site conectado, esse valor representa a quantidade de dados de objeto que

precisarão ser movidos para outros sites ou excluídos pelo ILM antes que você possa desativar esse site com segurança.

- Para a desativação de um site desconectado, esse valor representa a quantidade de armazenamento de dados do seu sistema que ficará inacessível quando você desativar esse site.



Se sua política de ILM foi projetada para proteger contra a perda de um único site, cópias dos dados do seu objeto ainda deverão existir nos sites restantes.

4. Revise os motivos na coluna **Desativação possível** para determinar quais sites podem ser desativados atualmente.



Se houver mais de um motivo pelo qual um site não pode ser desativado, o motivo mais crítico será exibido.

Descomissionamento Possível razão	Descrição	Próximo passo
Marca de verificação verde (✓)	Você pode desativar este site.	Vá para o próximo passo .
Não. Este site contém o nó de administração principal.	Não é possível desativar um site que contém o nó de administração principal.	Nenhum. Você não pode executar este procedimento.
Não. Este site contém um ou mais nós de arquivo.	Não é possível desativar um site que contém um nó de arquivo.	Nenhum. Você não pode executar este procedimento.
Não. Todos os nós neste site estão desconectados. Entre em contato com seu representante de conta da NetApp.	Você não pode executar o descomissionamento de um site conectado a menos que todos os nós no site estejam conectados (✓).	Se você quiser executar uma desativação de site desconectado, entre em contato com seu representante de conta da NetApp, que analisará seus requisitos e habilitará o restante do assistente de desativação de site. IMPORTANTE: Nunca coloque nós on-line off-line para poder remover um site. Você perderá dados.

O exemplo mostra um sistema StorageGRID com três sites. A marca de verificação verde (✓) para os locais de Raleigh e Sunnyvale indica que você pode desativar esses locais. No entanto, você não pode desativar o site de Vancouver porque ele contém o nó de administração principal.

1. Se a desativação for possível, selecione o botão de opção do site.

O botão **Avançar** está habilitado.

2. Selecione **Avançar**.

A etapa 2 (Exibir detalhes) é exibida.

Etapa 2: Exibir detalhes

Na Etapa 2 (Exibir detalhes) do assistente de descomissionamento do site, você pode revisar quais nós estão incluídos no site, ver quanto espaço foi usado em cada nó de armazenamento e avaliar quanto espaço livre está disponível nos outros sites da sua grade.

Antes de começar

Antes de desativar um site, você deve revisar a quantidade de dados de objetos existentes no site.

- Se você estiver executando uma desativação de site conectado, deverá entender quantos dados de objeto existem atualmente no site antes de atualizar o ILM. Com base nas capacidades do site e nas suas necessidades de proteção de dados, você pode criar novas regras de ILM para mover dados para outros sites ou excluir dados de objetos do site.
- Execute todas as expansões necessárias do nó de armazenamento antes de iniciar o procedimento de desativação, se possível.
- Se você estiver realizando uma desativação de site desconectado, deverá entender quantos dados de objeto ficarão permanentemente inacessíveis quando você remover o site.

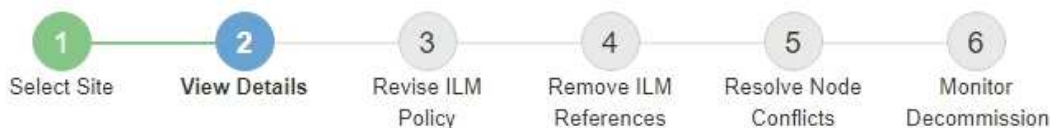


Se você estiver executando uma desativação de site desconectado, o ILM não poderá mover ou excluir dados de objeto. Todos os dados que permanecerem no site serão perdidos. No entanto, se sua política de ILM foi projetada para proteger contra a perda de um único site, cópias dos dados do seu objeto ainda existirão nos sites restantes. Ver "[Habilitar proteção contra perda de site](#)".

Passos

1. Na Etapa 2 (Exibir detalhes), revise todos os avisos relacionados ao site que você selecionou para remover.

Decommission Site



Data Center 2 Details

⚠ This site includes a Gateway Node. If clients are currently connecting to this node, you must configure an equivalent node at another site. Be sure clients can connect to the replacement node before starting the decommission procedure.

⚠ This site contains a mixture of connected and disconnected nodes. Before you can remove this site, you must bring all offline (blue or gray) nodes back online. Contact technical support if you need assistance.

Um aviso aparece nestes casos:

- O site inclui um nó de gateway. Se os clientes S3 estiverem se conectando a este nó, você deverá configurar um nó equivalente em outro site. Certifique-se de que os clientes possam se conectar ao nó de substituição antes de continuar com o procedimento de desativação.
- O site contém uma mistura de (✓) e nós desconectados (☾ ou ⚙). Antes de remover este site, você deve colocar todos os nós offline novamente online.

2. Revise os detalhes sobre o site que você selecionou para remover.

Decommission Site



Raleigh Details

Number of Nodes: 3 Free Space: 475.38 GB
 Used Space: 3.93 MB Site Capacity: 475.38 GB

Node Name	Node Type	Connection State	Details
RAL-S1-101-196	Storage Node	✓	1.30 MB used space
RAL-S2-101-197	Storage Node	✓	1.30 MB used space
RAL-S3-101-198	Storage Node	✓	1.34 MB used space

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB
 Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space ?	Used Space ?	Site Capacity ?
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Previous

Next

As seguintes informações estão incluídas para o site selecionado:

- Número de nós
- O espaço total utilizado, o espaço livre e a capacidade de todos os nós de armazenamento no site.
 - Para a desativação de um site conectado, o valor **Espaço Usado** representa a quantidade de dados de objeto que deve ser movida para outros sites ou excluída com o ILM.
 - Para uma desativação de site desconectado, o valor **Espaço Usado** indica quantos dados de objeto ficarão inacessíveis quando você remover o site.
- Nomes de nós, tipos e estados de conexão:
 -

✓ (Conectado)

• ☾ (Administrativamente inativo)

• 🌐 (Desconhecido)

◦ Detalhes sobre cada nó:

- Para cada nó de armazenamento, a quantidade de espaço que foi usada para dados de objeto.
- Para nós de administração e nós de gateway, se o nó está sendo usado atualmente em um grupo de alta disponibilidade (HA). Não é possível desativar um nó de administração ou um nó de gateway que seja usado em um grupo de alta disponibilidade. Antes de iniciar a desativação, edite os grupos de HA para remover todos os nós do site ou remova o grupo de HA se ele incluir apenas nós deste site. Para obter instruções, consulte ["Gerenciar grupos de alta disponibilidade \(HA\)"](#).

3. Na seção Detalhes de outros sites da página, avalie quanto espaço está disponível nos outros sites da sua grade.

Details for Other Sites

Total Free Space for Other Sites: 950.76 GB

Total Capacity for Other Sites: 950.77 GB

Site Name	Free Space ?	Used Space ?	Site Capacity ?
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Se você estiver executando o descomissionamento de um site conectado e planeja usar o ILM para mover dados de objeto do site selecionado (em vez de apenas excluí-lo), você deve garantir que os outros sites tenham capacidade suficiente para acomodar os dados movidos e que haja capacidade adequada para crescimento futuro.



Um aviso será exibido se o **Espaço Usado** do site que você deseja remover for maior que o **Espaço Livre Total para Outros Sites**. Para garantir que haja capacidade de armazenamento adequada disponível após a remoção do site, talvez seja necessário realizar uma expansão antes de executar este procedimento.

4. Selecione **Avançar**.

A etapa 3 (Revisar política do ILM) é exibida.

Etapa 3: Revisar as políticas do ILM

Na Etapa 3 (Revisar políticas do ILM) do assistente de descomissionamento do site, você pode determinar se o site é referenciado por alguma política do ILM.

Antes de começar

Você tem um bom entendimento de como ["gerenciar objetos com ILM"](#). Você está familiarizado com a criação de pools de armazenamento e regras de ILM e com a simulação e ativação de uma política de ILM.

Sobre esta tarefa

O StorageGRID não pode desativar um site se qualquer regra do ILM em qualquer política (ativa ou inativa) fizer referência a esse site.

Se alguma política do ILM fizer referência ao site que você deseja desativar, você deverá remover essas políticas ou editá-las para que atendam a estes requisitos:

- Proteja totalmente todos os dados do objeto.
- Não faça referência ao local que você está desativando.
- Não use pools de armazenamento que se refiram ao site ou use a opção Todos os sites.
- Não use perfis de codificação de eliminação que façam referência ao site.
- Não use a regra Fazer 2 cópias do StorageGRID 11.6 ou instalações anteriores.



Nunca crie uma regra ILM de cópia única para acomodar a remoção de um site. 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 estiver executando uma *desativação de site conectado*, deverá considerar como o StorageGRID deve gerenciar os dados do objeto atualmente no site que você deseja remover. Dependendo dos seus requisitos de proteção de dados, novas regras podem mover dados de objetos existentes para sites diferentes ou podem excluir quaisquer cópias extras de objetos que não sejam mais necessárias.

Entre em contato com o suporte técnico se precisar de assistência para criar uma nova política.

Passos

1. Na Etapa 3 (Revisar políticas do ILM), determine se alguma política do ILM se refere ao site que você selecionou para descomissionar.
2. Se nenhuma política estiver listada, selecione **Avançar** para ir para ["Etapa 4: Remover referências ILM"](#).
3. Se uma ou mais políticas ILM *ativas* estiverem listadas, clone cada política existente ou crie novas políticas que não façam referência ao site que está sendo desativado:
 - a. Selecione o link para a política na coluna Nome da política.

A página de detalhes da política do ILM aparece em uma nova guia do navegador. A página do Site de Desativação permanecerá aberta na outra aba.

- b. Siga estas diretrizes e instruções conforme necessário:

- Trabalhar com regras ILM:
 - ["Crie um ou mais pools de armazenamento"](#) que não se referem ao site.
 - ["Editar ou substituir regras"](#) que se referem ao site.



Não selecione a regra **Fazer 2 cópias** porque ela usa o pool de armazenamento **Todos os nós de armazenamento**, o que não é permitido.

- Trabalhar com políticas de ILM:
 - ["Clonar uma política de ILM existente"](#) ou ["criar uma nova política de ILM"](#) .
 - Certifique-se de que a regra padrão e outras regras não se refiram ao site.



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.

c. Ingrida objetos de teste e simule a política para garantir que as regras corretas sejam aplicadas.



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.

d. Ative as novas políticas e garanta que as antigas estejam inativas.

Se você deseja ativar várias políticas, ["siga as etapas para criar tags de política do ILM"](#) .

Se você estiver executando o descomissionamento de um site conectado, o StorageGRID começará a remover dados de objeto do site selecionado assim que você ativar a nova política de ILM. Mover ou excluir todas as cópias de objetos pode levar semanas. Embora você possa iniciar com segurança a desativação de um site enquanto os dados do objeto ainda estiverem no site, o procedimento de desativação será concluído mais rapidamente e com menos interrupções e impactos no desempenho se você permitir que os dados sejam movidos do site antes de iniciar o procedimento de desativação real (selecionando **Iniciar desativação** na Etapa 5 do assistente).

4. Para cada política *inativa*, edite-a ou remova-a selecionando primeiro o link para cada política, conforme descrito nas etapas anteriores.
 - ["Editar a política"](#) portanto não se refere ao local a ser desativado.
 - ["Remover uma política"](#) .
5. Quando você terminar de fazer alterações nas regras e políticas do ILM, não deverá haver mais políticas listadas na Etapa 3 (Revisar políticas do ILM). Selecione **Avançar**.

A etapa 4 (Remover referências ILM) é exibida.

Etapas 4: Remover referências ILM

Na Etapa 4 (Remover referências de ILM) do assistente de descomissionamento do site, você deve excluir ou editar quaisquer regras de ILM não utilizadas que façam referência ao site, mesmo que as regras não sejam usadas em nenhuma política de ILM.

Passos

1. Determine se alguma regra ILM não utilizada se refere ao site.

Se alguma regra do ILM for listada, ela ainda se refere ao site, mas não é usada em nenhuma política.



Quando o StorageGRID desativa o site, ele desativa automaticamente todos os perfis de codificação de eliminação não utilizados que fazem referência ao site e exclui automaticamente todos os pools de armazenamento não utilizados que fazem referência ao site. O pool de armazenamento All Storage Nodes (StorageGRID 11.6 e anteriores) foi removido porque usa o site All Sites.

2. Edite ou exclua cada regra não utilizada:

- Para editar uma regra, acesse a página de regras do ILM e atualize todos os posicionamentos que usam um perfil de codificação de eliminação ou pool de armazenamento que se refere ao site. Em seguida, retorne para a **Etapa 4 (Remover referências ILM)**.
- Para excluir uma regra, selecione o ícone da lixeira  e selecione **OK**.



Você deve excluir a regra **Fazer 2 cópias** antes de poder desativar um site.

3. Confirme se nenhuma regra ILM não utilizada faz referência ao site e se o botão **Avançar** está habilitado.

4. Selecione **Avançar**.



Todos os pools de armazenamento restantes e perfis de codificação de eliminação que se referem ao site se tornarão inválidos quando o site for removido. Quando o StorageGRID desativa o site, ele desativa automaticamente todos os perfis de codificação de eliminação não utilizados que fazem referência ao site e exclui automaticamente todos os pools de armazenamento não utilizados que fazem referência ao site. O pool de armazenamento All Storage Nodes (StorageGRID 11.6 e anteriores) foi removido porque usa o site All Sites.

A etapa 5 (Resolver conflitos de nós) é exibida.

Etapa 5: resolver conflitos de nós (e iniciar a desativação)

Na Etapa 5 (Resolver conflitos de nós) do assistente de descomissionamento do site, você pode determinar se algum nó no seu sistema StorageGRID está desconectado ou se algum nó no site selecionado pertence a um grupo de alta disponibilidade (HA). Depois que quaisquer conflitos de nós forem resolvidos, você inicia o procedimento de descomissionamento nesta página.

Antes de começar

Você deve garantir que todos os nós no seu sistema StorageGRID estejam no estado correto, da seguinte forma:

- Todos os nós no seu sistema StorageGRID devem estar conectados ().



Se você estiver executando uma desativação de site desconectado, todos os nós no site que você está removendo devem ser desconectados, e todos os nós em todos os outros sites devem ser conectados.



A desativação não será iniciada se um ou mais volumes estiverem offline (desmontados) ou se estiverem online (montados), mas em estado de erro.



Se um ou mais volumes ficarem offline enquanto uma desativação estiver em andamento, o processo de desativação será concluído depois que esses volumes voltarem a ficar online.

- Nenhum nó no site que você está removendo pode ter uma interface que pertença a um grupo de alta disponibilidade (HA).

Sobre esta tarefa

Se algum nó estiver listado para a Etapa 5 (Resolver conflitos de nós), você deverá corrigir o problema antes de iniciar a desativação.

Antes de iniciar o procedimento de desativação do site nesta página, revise as seguintes considerações:

- Você deve reservar tempo suficiente para que o procedimento de descomissionamento seja concluído.



Mover ou excluir dados de objetos de um site pode levar dias, semanas ou até meses, dependendo da quantidade de dados no site, da carga no sistema, das latências da rede e da natureza das alterações necessárias no ILM.

- Enquanto o procedimento de descomissionamento do site estiver em andamento:
 - Você não pode criar regras de ILM que façam referência ao site que está sendo desativado. Você também não pode editar uma regra ILM existente para fazer referência ao site.
 - Você não pode executar outros procedimentos de manutenção, como expansão ou atualização.



Se precisar executar outro procedimento de manutenção durante a desativação de um site conectado, você poderá pausar o procedimento enquanto os nós de armazenamento estiverem sendo removidos. O botão **Pausar** é ativado durante o estágio "Desativação de dados replicados e codificados para eliminação".

- Se precisar recuperar qualquer nó após iniciar o procedimento de desativação do site, entre em contato com o suporte.

Passos

1. Revise a seção de nós desconectados da Etapa 5 (Resolver conflitos de nós) para determinar se algum nó no seu sistema StorageGRID tem um Estado de conexão Desconhecido () ou administrativamente inativo ().

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

1 disconnected node in the grid

The following nodes have a Connection State of Unknown (blue) or Administratively Down (gray). You must bring these disconnected nodes back online.

For help bringing nodes back online, see the instructions for [monitoring and troubleshooting StorageGRID](#) and the [recovery and maintenance](#) instructions.

Node Name	Connection State	Site	Type
DC1-S3-99-193	Administratively Down	Data Center 1	Storage Node

1 node in the selected site belongs to an HA group

Passphrase

Provisioning Passphrase

Previous

Start Decommission

2. Se algum nó estiver desconectado, coloque-o novamente online.

Veja o "[Procedimentos de nó](#)". Entre em contato com o suporte técnico se precisar de assistência.

3. Quando todos os nós desconectados estiverem online novamente, revise a seção Grupos de HA da Etapa 5 (Resolver conflitos de nós).

Esta tabela lista todos os nós no site selecionado que pertencem a um grupo de alta disponibilidade (HA).

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue:

All grid nodes are connected

1 node in the selected site belongs to an HA group

The following nodes in the selected site belong to a high availability (HA) group. You must either edit the HA group to remove the node's interface or remove the entire HA group.

[Go to HA Groups page.](#)

For information about HA groups, see the instructions for [administering StorageGRID](#)

HA Group Name	Node Name	Node Type
HA group	DC1-GW1-99-190	API Gateway Node

Passphrase

Provisioning Passphrase ?

Previous

Start Decommission

4. Se algum nó estiver listado, faça um dos seguintes:

- Edite cada grupo HA afetado para remover a interface do nó.
- Remover um grupo HA que inclui apenas nós deste site. Veja as instruções para administrar o StorageGRID.

Se todos os nós estiverem conectados e nenhum nó no site selecionado for usado em um grupo de HA, o campo **Senha de provisionamento** será habilitado.

5. Digite a senha de provisionamento.

O botão **Iniciar descomissionamento** fica habilitado.

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be offline.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

All grid nodes are connected

No nodes in the selected site belong to an HA group

Passphrase

Provisioning Passphrase ?

.....

Previous

Start Decommission

6. Se você estiver pronto para iniciar o procedimento de desativação do site, selecione **Iniciar desativação**.

Um aviso lista o site e os nós que serão removidos. Lembre-se de que pode levar dias, semanas ou até meses para remover completamente o site.

7. Revise o aviso. Se estiver pronto para começar, selecione **OK**.

Uma mensagem aparece quando a nova configuração de grade é gerada. Esse processo pode levar algum tempo, dependendo do tipo e do número de nós de rede desativados.

Passphrase

Provisioning Passphrase ?

.....

i Generating grid configuration. This may take some time depending on the type and the number of decommissioned grid nodes.

Previous

Start Decommission



Quando a nova configuração de grade for gerada, a Etapa 6 (Monitorar Desativação) será exibida.



O botão **Anterior** permanece desabilitado até que a desativação seja concluída.

Etapa 6: Monitorar o descomissionamento

Na Etapa 6 (Monitorar descomissionamento) do assistente da página Descomissionar site, você pode monitorar o progresso conforme o site é removido.

Sobre esta tarefa

Quando o StorageGRID remove um site conectado, ele remove os nós nesta ordem:

1. Nós de gateway
2. Nós de administração
3. Nós de armazenamento

Quando o StorageGRID remove um site desconectado, ele remove os nós nesta ordem:

1. Nós de gateway
2. Nós de armazenamento
3. Nós de administração

Cada nó de gateway ou nó de administração pode levar apenas alguns minutos ou uma hora para ser removido; no entanto, os nós de armazenamento podem levar dias ou semanas.

Passos

1. Assim que um novo Pacote de Recuperação for gerado, baixe o arquivo.

Decommission Site



 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.



Baixe o Pacote de Recuperação o mais rápido possível para garantir que você possa recuperar sua rede se algo der errado durante o procedimento de desativação.

- a. Selecione o link na mensagem ou selecione **MANUTENÇÃO > Sistema > Pacote de recuperação**.
- b. Baixe o .zip arquivo.

Veja as instruções para ["baixando o pacote de recuperação"](#).



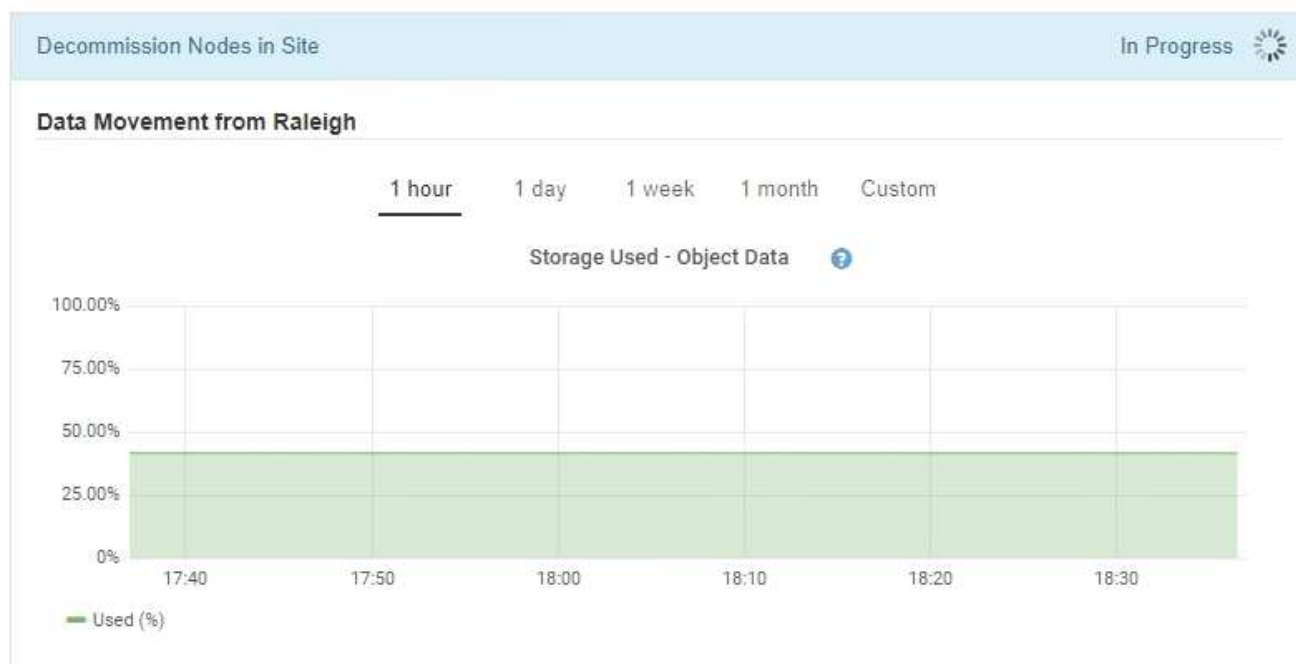
O arquivo do pacote de recuperação deve ser protegido porque contém chaves de criptografia e senhas que podem ser usadas para obter dados do sistema StorageGRID.

2. Usando o gráfico de movimentação de dados, monitore a movimentação de dados de objetos deste site para outros sites.

A movimentação de dados começou quando você ativou a nova política de ILM na Etapa 3 (Revisar

política de ILM). A movimentação de dados ocorrerá durante todo o procedimento de desativação.

Decommission Site Progress



3. Na seção Progresso do nó da página, monitore o progresso do procedimento de desativação à medida que os nós são removidos.

Quando um nó de armazenamento é removido, cada nó passa por uma série de estágios. Embora a maioria dessas etapas ocorra de forma rápida ou até mesmo imperceptível, pode ser necessário esperar dias ou até semanas para que outras etapas sejam concluídas, dependendo da quantidade de dados que precisa ser movida. É necessário tempo adicional para gerenciar dados codificados para eliminação e reavaliar o ILM.

Node Progress

i Depending on the number of objects stored, Storage Nodes might take significantly longer to decommission. Extra time is needed to manage erasure coded data and re-evaluate ILM.

The progress for each node is displayed while the decommission procedure is running. If you need to perform another maintenance procedure, select **Pause** to suspend the decommission (only allowed during certain stages).

Pause

Resume

Search				
Name	Type	Progress	Stage	
RAL-S1-101-196	Storage Node		Decommissioning Replicated and Erasure Coded Data	
RAL-S2-101-197	Storage Node		Decommissioning Replicated and Erasure Coded Data	
RAL-S3-101-198	Storage Node		Decommissioning Replicated and Erasure Coded Data	

Se você estiver monitorando o progresso da desativação de um site conectado, consulte esta tabela para entender os estágios de desativação de um nó de armazenamento:

Estágio	Duração estimada
Pendente	Minuto ou menos
Espere pelas fechaduras	Minutos
Preparar tarefa	Minuto ou menos
Marcação LDR Desativada	Minutos
Desativação de dados replicados e codificados para eliminação	Horas, dias ou semanas com base na quantidade de dados Observação: se você precisar executar outras atividades de manutenção, poderá pausar a desativação do site durante esta etapa.
Estado definido do LDR	Minutos
Filas de auditoria de descarga	Minutos a horas, com base no número de mensagens e na latência da rede.
Completo	Minutos

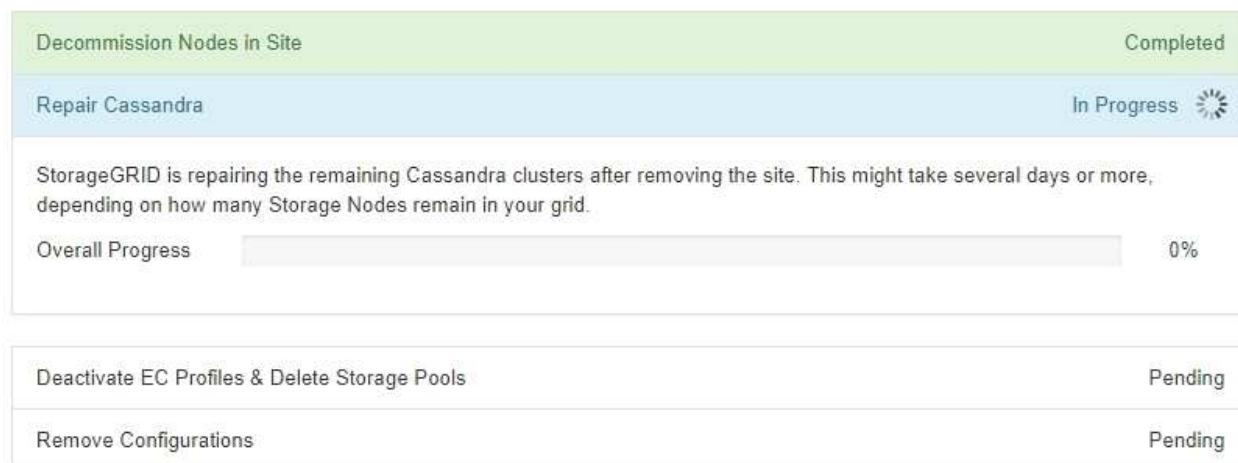
Se você estiver monitorando o progresso da desativação de um site desconectado, consulte esta tabela

para entender os estágios de desativação de um nó de armazenamento:

Estágio	Duração estimada
Pendente	Minuto ou menos
Espere pelas fechaduras	Minutos
Preparar tarefa	Minuto ou menos
Desativar serviços externos	Minutos
Revogação de Certificado	Minutos
Cancelar registro do nó	Minutos
Cancelar registro de nível de armazenamento	Minutos
Remoção do Grupo de Armazenamento	Minutos
Remoção de Entidade	Minutos
Completo	Minutos

4. Depois que todos os nós atingirem o estágio Concluído, aguarde a conclusão das operações restantes de desativação do site.
- Durante a etapa **Reparar Cassandra**, o StorageGRID faz todos os reparos necessários nos clusters Cassandra que permanecem na sua grade. Esses reparos podem levar vários dias ou mais, dependendo de quantos nós de armazenamento restam na sua grade.

Decommission Site Progress



- Durante a etapa **Desativar perfis de EC e excluir pools de armazenamento**, as seguintes alterações no ILM são feitas:

- Todos os perfis de codificação de eliminação que se referiam ao site são desativados.
- Todos os pools de armazenamento que fazem referência ao site são excluídos.



O pool de armazenamento All Storage Nodes (StorageGRID 11.6 e anteriores) também foi removido porque usa o site All Sites.

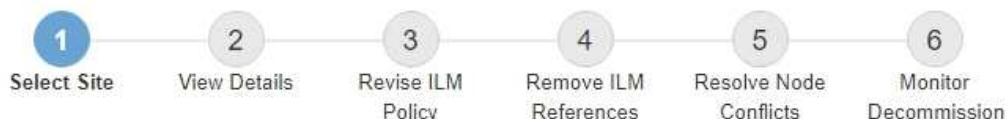
- Por fim, durante a etapa **Remover configuração**, quaisquer referências restantes ao site e seus nós são removidas do restante da grade.

Decommission Site Progress

Decommission Nodes in Site	Completed
Repair Cassandra	Completed
Deactivate EC Profiles & Delete Storage Pools	Completed
Remove Configurations	In Progress
StorageGRID is removing the site and node configurations from the rest of the grid.	

5. Quando o procedimento de desativação for concluído, a página Site de desativação mostrará uma mensagem de sucesso, e o site removido não será mais exibido.

Decommission Site



The previous decommission procedure completed successfully at 2021-01-12 14:28:32 MST.

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity	Decommission Possible
☒	Sunnyvale	4.79 MB	
☐	Vancouver	4.90 MB	No. This site contains the primary Admin Node.

Next

Depois que você terminar

Conclua estas tarefas depois de concluir o procedimento de desativação do site:

- Certifique-se de que as unidades de todos os nós de armazenamento no local desativado sejam limpas. Use uma ferramenta ou serviço de limpeza de dados disponível comercialmente para remover dados das unidades de forma permanente e segura.
- Se o site incluir um ou mais nós de administração e o logon único (SSO) estiver habilitado para seu sistema StorageGRID , remova todos os trusts de terceiros confiáveis do site dos Serviços de Federação do Active Directory (AD FS).
- Depois que os nós forem desligados automaticamente como parte do procedimento de desativação do site conectado, remova as máquinas virtuais associadas.

Renomear grade, site ou nó

Use o procedimento de renomeação

Conforme necessário, você pode alterar os nomes de exibição mostrados no Grid Manager para toda a grade, cada site e cada nó. Você pode atualizar os nomes de exibição com segurança e sempre que precisar.

Qual é o procedimento de renomeação?

Ao instalar o StorageGRID inicialmente, você especifica um nome para a grade, cada site e cada nó. Esses nomes iniciais são conhecidos como *nomes de sistema* e são os nomes mostrados inicialmente em StorageGRID.

Os nomes do sistema são necessários para operações internas do StorageGRID e não podem ser alterados. No entanto, você pode usar o procedimento de renomeação para definir novos *nomes de exibição* para a grade, cada site e cada nó. Esses nomes de exibição aparecem em vários locais do StorageGRID em vez de (ou, em alguns casos, além de) os nomes do sistema subjacente.

Use o procedimento de renomeação para corrigir erros de digitação, implementar uma convenção de nomenclatura diferente ou indicar que um site e todos os seus nós foram realocados. Ao contrário dos nomes do sistema, os nomes de exibição podem ser atualizados sempre que necessário e sem afetar as operações do StorageGRID .

Onde os nomes do sistema e de exibição aparecem?

A tabela a seguir resume onde os nomes do sistema e os nomes de exibição são mostrados na interface do usuário do StorageGRID e nos arquivos do StorageGRID .

Localização	Nome do sistema	Nome de exibição
Páginas do Grid Manager	Exibido a menos que o item seja renomeado	Se um item for renomeado, será exibido em vez do nome do sistema nestes locais: • Pannel • Página de nós • Páginas de configuração para grupos de alta disponibilidade, pontos de extremidade do balanceador de carga, interfaces VLAN, servidores de gerenciamento de chaves, senhas de grade e controle de firewall • Alertas • Definições de pool de armazenamento • Página de consulta de metadados do objeto • Páginas relacionadas a procedimentos de manutenção, incluindo atualização, hotfix, atualização do sistema operacional SANtricity , descomissionamento, expansão, recuperação e verificação de existência de objetos • Páginas de suporte (registros e diagnósticos) • Página de login único, ao lado do nome do host do nó de administração na tabela de detalhes do nó de administração
NÓS > guia Visão geral para um nó	Sempre mostrado	Exibido somente se o item for renomeado
Páginas legadas no Grid Manager (por exemplo, SUPPORT > Grid Topology)	Mostrado	Não mostrado
API node-health	Sempre retornado	Retornado somente se o item for renomeado

Localização	Nome do sistema	Nome de exibição
Prompt ao usar SSH para acessar um nó	Exibido como nome principal, a menos que o item tenha sido renomeado: admin@SYSTEM-NAME: ~ \$ Incluído entre parênteses quando o item é renomeado: admin@DISPLAY-NAME (SYSTEM-NAME) :~ \$	Exibido como nome principal quando o item é renomeado: admin@DISPLAY-NAME (SYSTEM-NAME) :~ \$
`Passwords.txt`arquivo no Pacote de Recuperação	Mostrado como Server Name	Mostrado como Display Name
`/etc/hosts`arquivo em todos os nós Por exemplo: 10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host	Sempre mostrado na segunda coluna	Quando o item é renomeado, mostrado na quarta coluna
topology-display-names.json, incluído com dados do AutoSupport	Não incluído	Vazio, a menos que os itens tenham sido renomeados; caso contrário, mapeia os IDs de grade, site e nó para seus nomes de exibição.

Requisitos de nome de exibição

Antes de usar este procedimento, revise os requisitos para nomes de exibição.

Nomes de exibição para nós

Os nomes de exibição dos nós devem seguir estas regras:

- Deve ser exclusivo em seu sistema StorageGRID .
- Não pode ser o mesmo que o nome do sistema de nenhum outro item no seu sistema StorageGRID .
- Deve conter no mínimo 1 e no máximo 32 caracteres.
- Pode conter números, hifens (-) e letras maiúsculas e minúsculas.
- Pode começar ou terminar com uma letra ou número, mas não pode começar ou terminar com um hífen.
- Não podem ser todos números.
- Não diferenciam maiúsculas de minúsculas. Por exemplo, DC1-ADM e dc1-adm são considerados

duplicados.

Você pode renomear um nó com um nome de exibição que foi usado anteriormente por um nó diferente, desde que a renomeação não resulte em um nome de exibição ou nome do sistema duplicado.

Nomes de exibição para grade e sites

Os nomes de exibição da grade e dos sites seguem as mesmas regras, com estas exceções:

- Pode incluir espaços.
- Pode incluir estes caracteres especiais: = - _ : , . @ !
- Pode começar e terminar com caracteres especiais, incluindo hifens.
- Podem ser todos números ou caracteres especiais.

Melhores práticas para exibir nomes

Se você planeja renomear vários itens, documente seu esquema geral de nomenclatura antes de usar este procedimento. Crie um sistema que garanta que os nomes sejam únicos, consistentes e fáceis de entender rapidamente.

Você pode usar qualquer convenção de nomenclatura que atenda aos requisitos da sua organização. Considere estas sugestões básicas sobre o que incluir:

- **Indicador de site:** Se você tiver vários sites, adicione um código de site ao nome de cada nó.
- **Tipo de nó:** Os nomes dos nós geralmente indicam o tipo do nó. Você pode usar abreviações como `s`, `adm`, e `gw` (Nó de armazenamento, nó de administração e nó de gateway).
- **Número do nó:** Se um site contiver mais de um nó de um tipo específico, adicione um número exclusivo ao nome de cada nó.

Pense duas vezes antes de adicionar detalhes específicos aos nomes que provavelmente mudarão ao longo do tempo. Por exemplo, não inclua endereços IP em nomes de nós porque esses endereços podem ser alterados. Da mesma forma, os locais dos racks ou os números dos modelos dos aparelhos podem mudar se você mover o equipamento ou atualizar o hardware.

Exemplos de nomes de exibição

Suponha que seu sistema StorageGRID tenha três data centers e nós de tipos diferentes em cada data center. Seus nomes de exibição podem ser tão simples quanto estes:

- **Grade:** StorageGRID Deployment
- **Primeiro site:** Data Center 1
 - `dc1-adm1`
 - `dc1-s1`
 - `dc1-s2`
 - `dc1-s3`
 - `dc1-gw1`
- **Segundo local:** Data Center 2

- dc2-adm2
- dc2-s1
- dc2-s2
- dc2-s3

- **Terceiro site:** Data Center 3

- dc3-s1
- dc3-s2
- dc3-s3

Adicionar ou atualizar nomes de exibição

Você pode usar este procedimento para adicionar ou atualizar os nomes de exibição usados para sua grade, sites e nós. Você pode renomear um único item, vários itens ou até mesmo todos os itens ao mesmo tempo. Definir ou atualizar um nome de exibição não afeta as operações do StorageGRID de forma alguma.

Antes de começar

- A partir do **Nó de Administração principal**, você é conectado ao Grid Manager usando um ["navegador da web compatível"](#).



Você pode adicionar ou atualizar nomes de exibição de um nó de administração não primário, mas precisa estar conectado ao nó de administração primário para baixar um pacote de recuperação.

- Você tem o ["Permissão de acesso de manutenção ou root"](#).
- Você tem a senha de provisionamento.
- Você entende os requisitos e as práticas recomendadas para nomes de exibição. Ver ["Renomear grade, sites e nós"](#).

Como renomear grade, sites ou nós

Você pode renomear seu sistema StorageGRID, um ou mais sites ou um ou mais nós.

Você pode usar um nome de exibição que foi usado anteriormente por um nó diferente, desde que a renomeação não resulte em um nome de exibição ou nome do sistema duplicado.

Selecione os itens para renomear

Para começar, selecione os itens que você deseja renomear.

Passos

1. Selecione **MANUTENÇÃO > Tarefas > Renomear grade, sites e nós**.
2. Para a etapa **Selecionar nomes**, selecione os itens que deseja renomear.

Item a ser alterado	Instrução
Nomes de tudo (ou quase tudo) no seu sistema	a. Selecione Selecionar tudo . b. Opcionalmente, limpe todos os itens que você não deseja renomear.
Nome da grade	Selecione a caixa de seleção da grade.
Nome de um site e alguns ou todos os seus nós	a. Marque a caixa de seleção no cabeçalho da tabela do site. b. Opcionalmente, limpe todos os nós que você não deseja renomear.
Nome de um site	Selecione a caixa de seleção do site.
Nome de um nó	Selecione a caixa de seleção do nó.

3. Selecione **Continuar**.

4. Revise a tabela, que inclui os itens que você selecionou.

- A coluna **Nome de exibição** mostra o nome atual de cada item. Se o item nunca tiver sido renomeado, seu nome de exibição será o mesmo que seu nome do sistema.
- A coluna **Nome do sistema** mostra o nome que você inseriu para cada item durante a instalação. Os nomes do sistema são usados para operações internas do StorageGRID e não podem ser alterados. Por exemplo, o nome do sistema de um nó pode ser seu nome de host.
- A coluna **Tipo** indica o tipo do item: Grade, Site ou o tipo específico de nó.

Proponha novos nomes

Para a etapa **Propor novos nomes**, você pode inserir um nome de exibição para cada item individualmente ou pode renomear os itens em massa.

Renomear itens individualmente

Siga estas etapas para inserir um nome de exibição para cada item que você deseja renomear.

Passos

1. No campo **Nome de exibição**, insira um nome de exibição proposto para cada item na lista.

Ver "[Renomear grade, sites e nós](#)" para aprender os requisitos de nomenclatura.

2. Para remover quaisquer itens que você não deseja renomear, selecione  na coluna **Remover da lista**.

Se você não for propor um novo nome para um item, deverá removê-lo da tabela.

3. Quando você tiver proposto novos nomes para todos os itens na tabela, selecione **Renomear**.

Uma mensagem de sucesso é exibida. Os novos nomes de exibição agora são usados em todo o Grid Manager.

Renomear itens em massa

Use a ferramenta de renomeação em massa se os nomes dos itens compartilharem uma sequência de caracteres comum que você deseja substituir por uma sequência de caracteres diferente.

Passos

1. Para a etapa **Propor novos nomes**, selecione **Usar ferramenta de renomeação em massa**.

A **Visualização de renomeação** inclui todos os itens que foram exibidos na etapa **Propor novos nomes**. Você pode usar a visualização para ver como os nomes de exibição ficarão depois de substituir uma string compartilhada.

2. No campo **String existente**, insira a string compartilhada que você deseja substituir. Por exemplo, se a string que você deseja substituir for `Data-Center-1`, digite **Data-Center-1**.

Conforme você digita, seu texto é destacado onde quer que ele seja encontrado nos nomes à esquerda.

3. Selecione  para remover quaisquer itens que você não deseja renomear com esta ferramenta.

Por exemplo, suponha que você queira renomear todos os nós que contêm a string `Data-Center-1`, mas você não quer renomear o `Data-Center-1` site em si. Selecione  para remover o site da visualização de renomeação.

Bulk rename tool

Rename preview

DC1-ADM1

DC1-ARC1

DC1-G1

DC1-S1

DC1-S2

DC1-S3

DC1-S4

Cancel

Add names

Enter the shared string you want to replace. Then, enter a new string to use instead. Optionally, remove any items that you do not want to rename with this tool.

Existing string

Data-Center-1

The string you want to replace. Represented by *italicized text* in the preview section.

New string

DC1

The string you want to use instead. Represented by **bolded text** in the preview section.

- Quando estiver satisfeito com os nomes mostrados na pré-visualização, selecione **Adicionar nomes** para adicionar os nomes à tabela para a etapa **Propor novos nomes**.
- Faça quaisquer alterações adicionais necessárias ou selecione  para remover quaisquer itens que você não deseja renomear.
- Quando estiver pronto para renomear todos os itens na tabela, selecione **Renomear**.

Uma mensagem de sucesso é exibida. Os novos nomes de exibição agora são usados em todo o Grid Manager.

Baixe o pacote de recuperação

Quando terminar de renomear os itens, baixe e salve um novo Pacote de Recuperação. Os novos nomes de exibição para os itens que você renomeou estão incluídos no `Passwords.txt` arquivo.

Passos

1. Digite a senha de provisionamento.
2. Selecione **Baixar pacote de recuperação**.

O download começa imediatamente.

3. Quando o download for concluído, abra o `Passwords.txt` arquivo para ver o nome do servidor para todos os nós e os nomes de exibição para quaisquer nós renomeados.
4. Copie o `sgws-recovery-package-id-revision.zip` archive em 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 .

5. Selecione **Concluir** para retornar ao primeiro passo.

Reverter nomes de exibição para nomes de sistema

Você pode reverter uma grade, site ou nó renomeado de volta ao seu nome original do sistema. Quando você reverte um item para seu nome de sistema, as páginas do Grid Manager e outros locais do StorageGRID não mostram mais um **Nome de exibição** para esse item. Somente o nome do sistema do item é mostrado.

Passos

1. Selecione **MANUTENÇÃO > Tarefas > Renomear grade, sites e nós**.
2. Para a etapa **Selecionar nomes**, selecione todos os itens que você deseja reverter para nomes de sistema.
3. Selecione **Continuar**.
4. Para a etapa **Propor novos nomes**, reverta os nomes de exibição para nomes do sistema individualmente ou em massa.

Reverter para nomes de sistema individualmente

- a. Copie o nome original do sistema de cada item e cole-o no campo **Nome de exibição** ou selecione  para remover quaisquer itens que você não deseja reverter.

Para reverter um nome de exibição, o nome do sistema deve aparecer no campo **Nome de exibição**, mas o nome não diferencia maiúsculas de minúsculas.

- b. Selecione **Renomear**.

Uma mensagem de sucesso é exibida. Os nomes de exibição desses itens não são mais usados.

Reverter para nomes de sistema em massa

- a. Para a etapa **Propor novos nomes**, selecione **Usar ferramenta de renomeação em massa**.
- b. No campo **String existente**, insira a string do nome de exibição que você deseja substituir.
- c. No campo **Nova string**, insira a string do nome do sistema que você deseja usar.
- d. Selecione **Adicionar nomes** para adicionar os nomes à tabela para a etapa **Propor novos nomes**.
- e. Confirme se cada entrada no campo **Nome de exibição** corresponde ao nome no campo **Nome do sistema**. Faça quaisquer alterações ou selecione  para remover quaisquer itens que você não deseja reverter.

Para reverter um nome de exibição, o nome do sistema deve aparecer no campo **Nome de exibição**, mas o nome não diferencia maiúsculas de minúsculas.

- f. Selecione **Renomear**.

Uma mensagem de sucesso é exibida. Os nomes de exibição desses itens não são mais usados.

5. [Baixe e salve um novo pacote de recuperação](#) .

Os nomes de exibição dos itens que você reverteu não estão mais incluídos no `Passwords.txt` arquivo.

Procedimentos de nó

Procedimentos de manutenção de nós

Pode ser necessário executar procedimentos de manutenção relacionados a nós de grade ou serviços de nós específicos.

Procedimentos do Gerenciador de Servidores

O Gerenciador do Servidor é executado em cada nó da grade para supervisionar o início e a interrupção dos serviços e para garantir que os serviços entrem e saiam do sistema StorageGRID sem problemas. O Gerenciador do Servidor também monitora os serviços em cada nó da grade e tentará reiniciar automaticamente quaisquer serviços que relatem falhas.

Para executar procedimentos do Gerenciador do Servidor, normalmente você precisa acessar a linha de comando do nó.



Você deve acessar o Gerenciador do Servidor somente se o suporte técnico tiver instruído você a fazê-lo.



Você deve fechar a sessão atual do shell de comando e fazer logout após terminar de usar o Gerenciador do Servidor. Digitar: `exit`

Procedimentos de reinicialização, desligamento e energia do nó

Use esses procedimentos para reinicializar um ou mais nós, desligar e reiniciar nós ou desligar e ligar novamente os nós.

Procedimentos de remapeamento de portas

Você pode usar os procedimentos de remapeamento de porta para remover os remapeamentos de porta de um nó, por exemplo, se quiser configurar um ponto de extremidade do balanceador de carga usando uma porta que foi remapeada anteriormente.

Procedimentos do Gerenciador de Servidores

Exibir status e versão do Gerenciador de Servidores

Para cada nó de grade, você pode visualizar o status atual e a versão do Gerenciador do Servidor em execução naquele nó de grade. Você também pode obter o status atual de todos os serviços em execução naquele nó de grade.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Passos

1. Efetue login no nó da grade:

- a. Digite o seguinte comando: `ssh admin@grid_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. Veja o status atual do Gerenciador do Servidor em execução no nó da grade: **`service servermanager status`**

O status atual do Gerenciador do Servidor em execução no nó da grade é relatado (em execução ou não). Se o status do Gerenciador do Servidor for `running`, o tempo que ele está em execução desde a última vez que foi iniciado é listado. Por exemplo:

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Veja a versão atual do Gerenciador do Servidor em execução em um nó de grade: **`service servermanager version`**

A versão atual está listada. Por exemplo:

```
11.1.0-20180425.1905.39c9493
```

4. Sair do shell de comando: **`exit`**

Ver o status atual de todos os serviços

Você pode visualizar o status atual de todos os serviços em execução em um nó de grade a qualquer momento.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Passos

1. Efetue login no nó da grade:
 - a. Digite o seguinte comando: `ssh admin@grid_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. Visualize o status de todos os serviços em execução no nó da grade: `storagegrid-status`

Por exemplo, a saída do nó de administração primário mostra o status atual dos serviços AMS, CMN e

NMS como Em execução. Esta saída é atualizada imediatamente se o status de um serviço mudar.

```
Host Name          190-ADM1
IP Address
Operating System Kernel 4.9.0      Verified
Operating System Environment Debian 9.4   Verified
StorageGRID Webscale Release 11.1.0     Verified
Networking          Verified
Storage Subsystem    Verified
Database Engine      5.5.9999+default Running
Network Monitoring    11.1.0     Running
Time Synchronization 1:4.2.8p10+dfsg Running
ams                  11.1.0     Running
cmn                  11.1.0     Running
nms                  11.1.0     Running
ssm                  11.1.0     Running
mi                   11.1.0     Running
dynip                11.1.0     Running
nginx                1.10.3     Running
tomcat               8.5.14     Running
grafana              4.2.0      Running
mgmt api              11.1.0     Running
prometheus           1.5.2+ds   Running
persistence          11.1.0     Running
ade exporter         11.1.0     Running
attrDownPurge        11.1.0     Running
attrDownSamp1        11.1.0     Running
attrDownSamp2        11.1.0     Running
node exporter        0.13.0+ds  Running
```

3. Retorne à linha de comando e pressione **Ctrl+C**.
4. Opcionalmente, visualize um relatório estático para todos os serviços em execução no nó da grade:
`/usr/local/servermanager/reader.rb`

Este relatório inclui as mesmas informações do relatório atualizado continuamente, mas não é atualizado se o status de um serviço mudar.

5. Sair do shell de comando: `exit`

Inicie o Gerenciador do Servidor e todos os serviços

Pode ser necessário iniciar o Gerenciador do Servidor, que também inicia todos os serviços no nó da grade.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

Iniciar o Gerenciador do Servidor em um nó de grade onde ele já está em execução resulta na reinicialização do Gerenciador do Servidor e de todos os serviços no nó de grade.

Passos

1. Efetue login no nó da grade:
 - a. Digite o seguinte comando: `ssh admin@grid_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. Inicie o Gerenciador do Servidor: `service servermanager start`

3. Sair do shell de comando: `exit`

Reinicie o Gerenciador do Servidor e todos os serviços

Pode ser necessário reiniciar o gerenciador do servidor e todos os serviços em execução em um nó de grade.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Passos

1. Efetue login no nó da grade:

a. Digite o seguinte comando: `ssh admin@grid_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. Reinicie o Gerenciador do Servidor e todos os serviços no nó da grade: `service servermanager restart`

O Gerenciador do Servidor e todos os serviços no nó da grade são interrompidos e reiniciados.



Usando o `restart` o comando é o mesmo que usar o `stop` comando seguido pelo `start` comando.

3. Sair do shell de comando: `exit`

Pare o Gerenciador do Servidor e todos os serviços

O Gerenciador do Servidor deve ser executado o tempo todo, mas pode ser necessário interromper o Gerenciador do Servidor e todos os serviços em execução em um nó de grade.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Passos

1. Efetue login no nó da grade:

- a. Digite o seguinte comando: `ssh admin@grid_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. Pare o gerenciador do servidor e todos os serviços em execução no nó da grade: `service servermanager stop`

O Gerenciador do Servidor e todos os serviços em execução no nó da grade são encerrados normalmente. Os serviços podem levar até 15 minutos para serem encerrados.

3. Sair do shell de comando: `exit`

Ver status atual do serviço

Você pode visualizar o status atual de um serviço em execução em um nó de grade a qualquer momento.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Passos

1. Efetue login no nó da grade:
 - a. Digite o seguinte comando: `ssh admin@grid_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. Exibir o status atual de um serviço em execução em um nó de grade: ``service servicename status` O status atual do serviço solicitado em execução no nó de grade é relatado (em execução ou não). Por exemplo:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Sair do shell de comando: **`exit`**

Parar serviço

Alguns procedimentos de manutenção exigem que você interrompa um único serviço enquanto mantém outros serviços no nó da rede em execução. Interrompa serviços individuais somente quando instruído a fazê-lo por um procedimento de manutenção.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

Quando você usa essas etapas para "interromper administrativamente" um serviço, o Gerenciador do Servidor não reiniciará o serviço automaticamente. Você deve iniciar o serviço único manualmente ou reiniciar o Gerenciador do Servidor.

Se você precisar interromper o serviço LDR em um nó de armazenamento, esteja ciente de que pode levar algum tempo para interromper o serviço se houver conexões ativas.

Passos

1. Efetue login no nó da grade:

- a. Digite o seguinte comando: `ssh admin@grid_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. Interrompa um serviço individual: `service servicename stop`

Por exemplo:

```
service ldr stop
```



Os serviços podem levar até 11 minutos para parar.

3. Sair do shell de comando: `exit`

Informações relacionadas

["Forçar o término do serviço"](#)

Forçar o término do serviço

Se você precisar interromper um serviço imediatamente, você pode usar o `force-stop` comando.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Passos

1. Efetue login no nó da grade:

- a. Digite o seguinte comando: `ssh admin@grid_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. Forçar manualmente o encerramento do serviço: `service servicename force-stop`

Por exemplo:

```
service ldr force-stop
```

O sistema aguarda 30 segundos antes de encerrar o serviço.

3. Sair do shell de comando: `exit`

Iniciar ou reiniciar o serviço

Pode ser necessário iniciar um serviço que foi interrompido ou interromper e reiniciar um serviço.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Passos

1. Efetue login no nó da grade:
 - a. Digite o seguinte comando: `ssh admin@grid_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. Decida qual comando emitir, com base no fato de o serviço estar em execução ou parado.
 - Se o serviço estiver parado no momento, use o `start` comando para iniciar o serviço manualmente:
`service servicename start`

Por exemplo:

```
service ldr start
```

- Se o serviço estiver em execução, use o `restart` comando para parar o serviço e reiniciá-lo:
`service servicename restart`

Por exemplo:

```
service ldr restart
```

+



Usando o `restart` o comando é o mesmo que usar o `stop` comando seguido pelo `start` comando. Você pode emitir `restart` mesmo que o serviço esteja atualmente interrompido.

3. Sair do shell de comando: `exit`

Use um arquivo DoNotStart

Se você estiver executando vários procedimentos de manutenção ou configuração sob a direção do suporte técnico, poderá ser solicitado a usar um arquivo DoNotStart para impedir que os serviços sejam iniciados quando o Gerenciador do Servidor for iniciado ou reiniciado.



Você deve adicionar ou remover um arquivo DoNotStart somente se o suporte técnico tiver instruído você a fazer isso.

Para impedir que um serviço seja iniciado, coloque um arquivo DoNotStart no diretório do serviço que você deseja impedir que seja iniciado. Na inicialização, o Gerenciador do Servidor procura o arquivo DoNotStart. Se o arquivo estiver presente, o serviço (e quaisquer serviços dependentes dele) será impedido de iniciar. Quando o arquivo DoNotStart for removido, o serviço interrompido anteriormente será iniciado na próxima inicialização ou reinicialização do Gerenciador do Servidor. Os serviços não são iniciados automaticamente quando o arquivo DoNotStart é removido.

A maneira mais eficiente de impedir que todos os serviços sejam reiniciados é impedir que o serviço NTP seja iniciado. Todos os serviços dependem do serviço NTP e não podem ser executados se o serviço NTP não estiver em execução.

Adicionar arquivo DoNotStart para serviço

Você pode impedir que um serviço individual seja iniciado adicionando um arquivo DoNotStart ao diretório desse serviço em um nó de grade.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Passos

1. Efetue login no nó da grade:

- a. Digite o seguinte comando: `ssh admin@grid_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. Adicione um arquivo DoNotStart: `touch /etc/sv/service/DoNotStart`

onde `service` é o nome do serviço cuja inicialização será impedida. Por exemplo,

```
touch /etc/sv/ldr/DoNotStart
```

Um arquivo DoNotStart é criado. Nenhum conteúdo de arquivo é necessário.

Quando o Gerenciador do Servidor ou o nó da grade é reiniciado, o Gerenciador do Servidor é reiniciado, mas o serviço não.

3. Sair do shell de comando: `exit`

Remover arquivo DoNotStart para serviço

Ao remover um arquivo DoNotStart que está impedindo a inicialização de um serviço, você deve iniciar esse serviço.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Passos

1. Efetue login no nó da grade:

- a. Digite o seguinte comando: `ssh admin@grid_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. Remova o arquivo DoNotStart do diretório de serviço: `rm /etc/sv/service/DoNotStart`

onde `service` é o nome do serviço. Por exemplo,

```
rm /etc/sv/ldr/DoNotStart
```

3. Iniciar o serviço: `service servicename start`

4. Sair do shell de comando: `exit`

Solucionar problemas do Gerenciador do Servidor

Se surgir um problema ao usar o Gerenciador do Servidor, verifique seu arquivo de log.

Mensagens de erro relacionadas ao Gerenciador do Servidor são capturadas no arquivo de log do Gerenciador do Servidor, localizado em: `/var/local/log/servermanager.log`

Verifique este arquivo para mensagens de erro relacionadas a falhas. Encaminhe o problema ao suporte técnico, se necessário. Você pode ser solicitado a encaminhar arquivos de log para o suporte técnico.

Serviço com estado de erro

Se você detectar que um serviço entrou em estado de erro, tente reiniciá-lo.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

O Gerenciador do Servidor monitora serviços e reinicia aqueles que foram interrompidos inesperadamente. Se um serviço falhar, o Gerenciador do Servidor tentará reiniciá-lo. Se houver três tentativas fracassadas de iniciar um serviço em cinco minutos, o serviço entrará em estado de erro. O Gerenciador do Servidor não tenta outra reinicialização.

Passos

1. Efetue login no nó da grade:

- a. Digite o seguinte comando: `ssh admin@grid_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. Confirme o estado de erro do serviço: `service servicename status`

Por exemplo:

```
service ldr status
```

Se o serviço estiver em estado de erro, a seguinte mensagem será retornada: `servicename in error state`. Por exemplo:

```
ldr in error state
```



Se o status do serviço for `disabled`, veja as instruções para ["removendo um arquivo DoNotStart para um serviço"](#).

3. Tente remover o estado de erro reiniciando o serviço: `service servicename restart`

Se o serviço não reiniciar, entre em contato com o suporte técnico.

4. Sair do shell de comando: `exit`

Procedimentos de reinicialização, desligamento e energia

Executar uma reinicialização contínua

Você pode executar uma reinicialização contínua para reinicializar vários nós da grade sem causar interrupção do serviço.

Antes de começar

- Você está conectado ao Grid Manager no nó de administração principal e está usando um ["navegador da web compatível"](#).



Você deve estar conectado ao nó de administração principal para executar este procedimento.

- Você tem o ["Permissão de acesso de manutenção ou root"](#).

Sobre esta tarefa

Use este procedimento se precisar reinicializar vários nós ao mesmo tempo. Por exemplo, você pode usar este procedimento após alterar o modo FIPS para a grade ["Política de segurança TLS e SSH"](#). Quando o modo FIPS muda, você deve reinicializar todos os nós para que a alteração entre em vigor.



Se você precisar reinicializar apenas um nó, você pode ["reinicie o nó na aba Tarefas"](#).

Quando o StorageGRID reinicia os nós da grade, ele emite o `reboot` comando em cada nó, o que faz com que o nó seja desligado e reiniciado. Todos os serviços são reiniciados automaticamente.

- Reinicializar um nó VMware reinicializa a máquina virtual.
- Reinicializar um nó Linux reinicializa o contêiner.
- Reinicializar um nó do StorageGRID Appliance reinicializa o controlador de computação.

O procedimento de reinicialização contínua pode reinicializar vários nós ao mesmo tempo, com estas exceções:

- Dois nós do mesmo tipo não serão reinicializados ao mesmo tempo.
- Os nós de gateway e os nós de administração não serão reinicializados ao mesmo tempo.

Em vez disso, esses nós são reinicializados sequencialmente para garantir que grupos de HA, dados de objetos e serviços de nós críticos permaneçam sempre disponíveis.

Quando você reinicia o nó de administração principal, seu navegador perde temporariamente o acesso ao Grid Manager, então você não pode mais monitorar o procedimento. Por esse motivo, o nó de administração primário é reinicializado por último.

Executar uma reinicialização contínua

Selecione os nós que deseja reinicializar, revise suas seleções, inicie o procedimento de reinicialização e monitore o progresso.

Selecionar nós

Como primeiro passo, acesse a página Reinicialização contínua e selecione os nós que deseja reinicializar.

Passos

1. Selecione **MANUTENÇÃO > Tarefas > Reinicialização contínua**.
2. Revise o estado da conexão e os ícones de alerta na coluna **Nome do nó**.



Não é possível reiniciar um nó se ele estiver desconectado da rede. As caixas de seleção estão desabilitadas para nós com estes ícones:  ou .

3. Se algum nó tiver alertas ativos, revise a lista de alertas na coluna **Resumo do alerta**.



Para ver todos os alertas atuais de um nó, você também pode selecionar o **Nós > guia Visão geral**.

4. Opcionalmente, execute as ações recomendadas para resolver quaisquer alertas atuais.
5. Opcionalmente, se todos os nós estiverem conectados e você quiser reinicializar todos eles, marque a caixa de seleção no cabeçalho da tabela e selecione **Selecionar tudo**. Caso contrário, selecione cada nó que deseja reinicializar.

Você pode usar as opções de filtro da tabela para visualizar subconjuntos de nós. Por exemplo, você pode visualizar e selecionar apenas nós de armazenamento ou todos os nós em um determinado site.

6. Selecione **Revisar seleção**.

Seleção de revisão

Nesta etapa, você pode determinar quanto tempo o procedimento total de reinicialização pode levar e confirmar se selecionou os nós corretos.

1. Na página de seleção Revisar, revise o Resumo, que indica quantos nós serão reinicializados e o tempo total estimado para todos os nós reiniciarem.
2. Opcionalmente, para remover um nó específico da lista de reinicialização, selecione **Remover**.
3. Opcionalmente, para adicionar mais nós, selecione **Etapa anterior**, selecione os nós adicionais e selecione **Revisar seleção**.
4. Quando estiver pronto para iniciar o procedimento de reinicialização contínua para todos os nós selecionados, selecione **Reinicializar nós**.
5. Se você optou por reinicializar o nó de administração principal, leia a mensagem informativa e selecione **Sim**.



O nó de administração principal será o último nó a ser reinicializado. Enquanto este nó estiver reiniciando, a conexão do seu navegador será perdida. Quando o nó de administração principal estiver disponível novamente, você deverá recarregar a página de reinicialização contínua.

Monitorar uma reinicialização contínua

Enquanto o procedimento de reinicialização contínua estiver em execução, você poderá monitorá-lo a partir do nó de administração principal.

Passos

1. Revise o progresso geral da operação, que inclui as seguintes informações:

- Número de nós reinicializados
- Número de nós em processo de reinicialização
- Número de nós que ainda precisam ser reinicializados

2. Revise a tabela para cada tipo de nó.

As tabelas fornecem uma barra de progresso da operação em cada nó e mostram o estágio de reinicialização desse nó, que pode ser um destes:

- Aguardando reinicialização
- Parando serviços
- Reiniciando o sistema
- Iniciando serviços
- Reinicialização concluída

Interrompa o procedimento de reinicialização contínua

Você pode interromper o procedimento de reinicialização contínua no nó de administração principal. Ao interromper o procedimento, todos os nós que tiverem o status "Parando serviços", "Reinicializando o sistema" ou "Iniciando serviços" concluirão a operação de reinicialização. No entanto, esses nós não serão mais rastreados como parte do procedimento.

Passos

1. Selecione **MANUTENÇÃO > Tarefas > Reinicialização contínua**.
2. Na etapa **Monitorar reinicialização**, selecione **Parar procedimento de reinicialização**.

Reiniciar nó de grade na aba Tarefas

Você pode reinicializar um nó de grade individual na guia Tarefas na página Nós.

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.
- Se você estiver reinicializando o nó de administração primário ou qualquer nó de armazenamento, revise as seguintes considerações:
 - Quando você reinicia o nó de administração principal, seu navegador perde temporariamente o acesso ao Grid Manager.
 - Se você reiniciar dois ou mais nós de armazenamento em um determinado site, talvez não consiga acessar determinados objetos durante a reinicialização. Esse problema pode ocorrer se qualquer regra do ILM usar a opção de ingestão **Dual commit** (ou uma regra especificar **Balanced** e não for possível criar imediatamente todas as cópias necessárias). Nesse caso, o StorageGRID enviará os objetos recém-ingeridos para dois nós de armazenamento no mesmo site e avaliará o ILM posteriormente.
 - Para garantir que você possa acessar todos os objetos enquanto um nó de armazenamento estiver sendo reinicializado, interrompa a ingestão de objetos em um site por aproximadamente uma hora antes de reinicializar o nó.

Sobre esta tarefa

Quando o StorageGRID reinicia um nó de grade, ele emite o `reboot` comando no nó, que faz com que o nó seja desligado e reiniciado. Todos os serviços são reiniciados automaticamente.

- Reinicializar um nó VMware reinicializa a máquina virtual.
- Reinicializar um nó Linux reinicializa o contêiner.
- Reinicializar um nó do StorageGRID Appliance reinicializa o controlador de computação.



Se você precisar reinicializar mais de um nó, você pode usar o "[procedimento de reinicialização contínua](#)".

Passos

1. Selecione **NODES**.
2. Selecione o nó da grade que você deseja reinicializar.
3. Selecione a aba **Tarefas**.
4. Selecione **Reiniciar**.

Uma caixa de diálogo de confirmação é exibida. Se você estiver reiniciando o nó de administração principal, a caixa de diálogo de confirmação lembrará que a conexão do seu navegador com o Grid Manager será perdida temporariamente quando os serviços forem interrompidos.

5. Digite a senha de provisionamento e selecione **OK**.
6. Aguarde a reinicialização do nó.

Pode levar algum tempo para que os serviços sejam encerrados.

Quando o nó está sendo reinicializado, o ícone cinza (Administrativamente inativo) aparece para o nó na página Nós. Quando todos os serviços forem reiniciados e o nó estiver conectado com sucesso à rede, a página Nós deverá exibir o status normal (sem ícones à esquerda do nome do nó), indicando que nenhum alerta está ativo e que o nó está conectado à rede.

Reinicializar nó de grade a partir do shell de comando

Se precisar monitorar a operação de reinicialização mais de perto ou se não conseguir acessar o Grid Manager, você pode efetuar login no nó da grade e executar o comando de reinicialização do Server Manager no shell de comando.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Passos

1. Efetue login no nó da grade:
 - a. Digite o seguinte comando: `ssh admin@grid_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. Opcionalmente, pare os serviços: `service servermanager stop`

Interromper serviços é uma etapa opcional, mas recomendada. Os serviços podem levar até 15 minutos para serem desligados, e talvez você queira fazer login no sistema remotamente para monitorar o processo de desligamento antes de reinicializar o nó na próxima etapa.

3. Reinicie o nó da grade: `reboot`
4. Sair do shell de comando: `exit`

Desligar nó da grade

Você pode desligar um nó de grade a partir do shell de comando do nó.

Antes de começar

- Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

Antes de executar este procedimento, revise estas considerações:

- Em geral, você não deve desligar mais de um nó por vez para evitar interrupções.
- Não desligue um nó durante um procedimento de manutenção, a menos que seja explicitamente instruído a fazê-lo pela documentação ou pelo suporte técnico.
- O processo de desligamento é baseado em onde o nó está instalado, da seguinte forma:
 - Desligar um nó VMware desliga a máquina virtual.
 - Desligar um nó Linux desliga o contêiner.
 - Desligar um nó do dispositivo StorageGRID desliga o controlador de computação.
- Se você planeja desligar mais de um nó de armazenamento em um site, interrompa a ingestão de objetos naquele site por aproximadamente uma hora antes de desligar os nós.

Se qualquer regra do ILM usar a opção de ingestão **Dual commit** (ou se uma regra usar a opção **Balanced** e todas as cópias necessárias não puderem ser criadas imediatamente), o StorageGRID imediatamente confirma quaisquer objetos recém-ingeridos em dois nós de armazenamento no mesmo site e avalia o ILM posteriormente. Se mais de um nó de armazenamento em um site for desligado, talvez você não consiga acessar os objetos recém-ingeridos durante o desligamento. As operações de gravação também podem falhar se poucos nós de armazenamento permanecerem disponíveis no site. Ver ["Gerenciar objetos com ILM"](#).

Passos

1. Efetue login no nó da grade:
 - a. Digite o seguinte comando: `ssh admin@grid_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. Pare todos os serviços: `service servermanager stop`

Os serviços podem levar até 15 minutos para serem desligados, e talvez você queira fazer login no sistema remotamente para monitorar o processo de desligamento.

3. Se o nó estiver sendo executado em uma máquina virtual VMware ou for um nó de dispositivo, emita o comando shutdown: `shutdown -h now`

Execute esta etapa independentemente do resultado da `service servermanager stop` comando.



Depois de emitir o `shutdown -h now` comando em um nó do dispositivo, você deve desligar e ligar o dispositivo para reiniciá-lo.

Para o dispositivo, este comando desliga o controlador, mas o dispositivo continua ligado. Você deve concluir a próxima etapa.

4. Se você estiver desligando um nó do dispositivo, siga as etapas para o seu dispositivo.

SG6160

- a. Desligue a energia do controlador de armazenamento SG6100-CN.
- b. Aguarde até que o LED azul de energia no controlador de armazenamento SG6100-CN desligue.

SGF6112

- a. Desligue a energia do aparelho.
- b. Aguarde até que o LED azul de energia desligue.

SG6000

- a. Aguarde até que o LED verde Cache Active na parte traseira dos controladores de armazenamento desligue.

Este LED fica aceso quando dados em cache precisam ser gravados nas unidades. Você deve esperar que este LED desligue antes de desligar a energia.

- b. Desligue o aparelho e aguarde até que o LED azul de energia apague.

SG5800

- a. Aguarde até que o LED verde Cache Active na parte traseira do controlador de armazenamento desligue.

Este LED fica aceso quando dados em cache precisam ser gravados nas unidades. Você deve esperar que este LED desligue antes de desligar a energia.

- b. Na página inicial do SANtricity System Manager, selecione **Exibir operações em andamento**.
- c. Confirme se todas as operações foram concluídas antes de continuar com a próxima etapa.
- d. Desligue os dois interruptores de energia na prateleira do controlador e espere até que todos os LEDs na prateleira do controlador se apaguem.

SG5700

- a. Aguarde até que o LED verde Cache Active na parte traseira do controlador de armazenamento desligue.

Este LED fica aceso quando dados em cache precisam ser gravados nas unidades. Você deve esperar que este LED desligue antes de desligar a energia.

- b. Desligue o aparelho e aguarde até que toda a atividade do LED e do display de sete segmentos pare.

SG100 ou SG1000

- a. Desligue a energia do aparelho.
- b. Aguarde até que o LED azul de energia desligue.

Desligar o host

Antes de desligar um host, você deve interromper os serviços em todos os nós da grade naquele host.

Passos

1. Efetue login no nó da grade:

- a. Digite o seguinte comando: `ssh admin@grid_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. Pare todos os serviços em execução no nó: `service servermanager stop`

Os serviços podem levar até 15 minutos para serem desligados, e talvez você queira fazer login no sistema remotamente para monitorar o processo de desligamento.

3. Repita as etapas 1 e 2 para cada nó no host.

4. Se você tiver um host Linux:

- a. Efetue login no sistema operacional do host.
- b. Pare o nó: `storagegrid node stop`
- c. Desligue o sistema operacional do host.

5. Se o nó estiver sendo executado em uma máquina virtual VMware ou for um nó de dispositivo, emita o comando shutdown: `shutdown -h now`

Execute esta etapa independentemente do resultado da `service servermanager stop` comando.



Depois de emitir o `shutdown -h now` comando em um nó do dispositivo, você deve desligar e ligar o dispositivo para reiniciá-lo.

Para o dispositivo, este comando desliga o controlador, mas o dispositivo continua ligado. Você deve concluir a próxima etapa.

6. Se você estiver desligando um nó do dispositivo, siga as etapas para o seu dispositivo.

SG6160

- a. Desligue a energia do controlador de armazenamento SG6100-CN.
- b. Aguarde até que o LED azul de energia no controlador de armazenamento SG6100-CN desligue.

SGF6112

- a. Desligue a energia do aparelho.
- b. Aguarde até que o LED azul de energia desligue.

SG6000

- a. Aguarde até que o LED verde Cache Active na parte traseira dos controladores de armazenamento desligue.

Este LED fica aceso quando dados em cache precisam ser gravados nas unidades. Você deve esperar que este LED desligue antes de desligar a energia.

- b. Desligue o aparelho e aguarde até que o LED azul de energia apague.

SG5800

- a. Aguarde até que o LED verde Cache Active na parte traseira do controlador de armazenamento desligue.

Este LED fica aceso quando dados em cache precisam ser gravados nas unidades. Você deve esperar que este LED desligue antes de desligar a energia.

- b. Na página inicial do SANtricity System Manager, selecione **Exibir operações em andamento**.
- c. Confirme se todas as operações foram concluídas antes de continuar com a próxima etapa.
- d. Desligue os dois interruptores de energia na prateleira do controlador e espere até que todos os LEDs na prateleira do controlador se apaguem.

SG5700

- a. Aguarde até que o LED verde Cache Active na parte traseira do controlador de armazenamento desligue.

Este LED fica aceso quando dados em cache precisam ser gravados nas unidades. Você deve esperar que este LED desligue antes de desligar a energia.

- b. Desligue o aparelho e aguarde até que toda a atividade do LED e do display de sete segmentos pare.

SG110 ou SG1100

- a. Desligue a energia do aparelho.
- b. Aguarde até que o LED azul de energia desligue.

SG100 ou SG1000

- a. Desligue a energia do aparelho.
- b. Aguarde até que o LED azul de energia desligue.

7. Sair do shell de comando: `exit`

Informações relacionadas

- ["Dispositivos de armazenamento SGF6112 e SG6160"](#)
- ["Dispositivos de armazenamento SG6000"](#)
- ["Dispositivos de armazenamento SG5700"](#)
- ["Dispositivos de armazenamento SG5800"](#)
- ["Aparelhos de serviço SG110 e SG1100"](#)
- ["Aparelhos de serviços SG100 e SG1000"](#)

Desligue e ligue todos os nós da rede

Pode ser necessário desligar todo o sistema StorageGRID , por exemplo, se você estiver movendo um data center. Estas etapas fornecem uma visão geral de alto nível da sequência recomendada para executar um desligamento e inicialização controlados.

Ao desligar todos os nós em um site ou grade, você não poderá acessar os objetos ingeridos enquanto os nós de armazenamento estiverem offline.

Interrompa os serviços e desligue os nós da rede

Antes de desligar um sistema StorageGRID , você deve interromper todos os serviços em execução em cada nó da grade e, em seguida, desligar todas as máquinas virtuais VMware, mecanismos de contêiner e dispositivos StorageGRID .

Sobre esta tarefa

Primeiro, interrompa os serviços nos nós de administração e nos nós de gateway e, depois, interrompa os serviços nos nós de armazenamento.

Essa abordagem permite que você use o nó de administração principal para monitorar o status dos outros nós da grade pelo maior tempo possível.



Se um único host incluir mais de um nó de grade, não desligue o host até ter parado todos os nós nele. Se o host incluir o nó de administração primário, desligue esse host por último.



Se necessário, você pode ["migrar nós de um host Linux para outro"](#) para executar a manutenção do host sem afetar a funcionalidade ou a disponibilidade da sua rede.

Passos

1. Impeça que todos os aplicativos clientes acessem a grade.
2. Faça login em cada nó do Gateway:
 - a. Digite o seguinte comando: `ssh admin@grid_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. Parar todos os serviços em execução no nó: `service servermanager stop`

Os serviços podem levar até 15 minutos para serem desligados, e talvez você queira fazer login no sistema remotamente para monitorar o processo de desligamento.

4. Repita as duas etapas anteriores para interromper os serviços em todos os nós de armazenamento e nós de administração não primários.

Você pode interromper os serviços nesses nós em qualquer ordem.



Se você emitir o `service servermanager stop` comando para interromper os serviços em um nó de armazenamento do dispositivo, você deve desligar e ligar o dispositivo para reiniciar o nó.

5. Para o nó de administração primário, repita as etapas para [fazendo login no nó](#) e [parando todos os serviços no nó](#).
6. Para nós que estão sendo executados em hosts Linux:
 - a. Efetue login no sistema operacional do host.
 - b. Pare o nó: `storagegrid node stop`
 - c. Desligue o sistema operacional do host.
7. Para nós em execução em máquinas virtuais VMware e para nós de armazenamento de dispositivos, emita o comando shutdown: `shutdown -h now`

Execute esta etapa independentemente do resultado da `service servermanager stop` comando.

Para o dispositivo, este comando desliga o controlador de computação, mas o dispositivo ainda fica ligado. Você deve concluir a próxima etapa.

8. Se você tiver nós de dispositivo, siga as etapas para seu dispositivo.

SG110 ou SG1100

- a. Desligue a energia do aparelho.
- b. Aguarde até que o LED azul de energia desligue.

SG100 ou SG1000

- a. Desligue a energia do aparelho.
- b. Aguarde até que o LED azul de energia desligue.

SG6160

- a. Desligue a energia do controlador de armazenamento SG6100-CN.
- b. Aguarde até que o LED azul de energia no controlador de armazenamento SG6100-CN desligue.

SGF6112

- a. Desligue a energia do aparelho.
- b. Aguarde até que o LED azul de energia desligue.

SG6000

- a. Aguarde até que o LED verde Cache Active na parte traseira dos controladores de armazenamento desligue.

Este LED fica aceso quando dados em cache precisam ser gravados nas unidades. Você deve esperar que este LED desligue antes de desligar a energia.

- b. Desligue o aparelho e aguarde até que o LED azul de energia apague.

SG5800

- a. Aguarde até que o LED verde Cache Active na parte traseira do controlador de armazenamento desligue.

Este LED fica aceso quando dados em cache precisam ser gravados nas unidades. Você deve esperar que este LED desligue antes de desligar a energia.

- b. Na página inicial do SANtricity System Manager, selecione **Exibir operações em andamento**.
- c. Confirme se todas as operações foram concluídas antes de continuar com a próxima etapa.
- d. Desligue os dois interruptores de energia na prateleira do controlador e espere até que todos os LEDs na prateleira do controlador se apaguem.

SG5700

- a. Aguarde até que o LED verde Cache Active na parte traseira do controlador de armazenamento desligue.

Este LED fica aceso quando dados em cache precisam ser gravados nas unidades. Você deve esperar que este LED desligue antes de desligar a energia.

- b. Desligue o aparelho e aguarde até que toda a atividade do LED e do display de sete segmentos pare.

9. Se necessário, saia do shell de comando: `exit`

A grade StorageGRID foi desligada.

Iniciar nós de grade



Se toda a rede estiver desligada por mais de 15 dias, você deverá entrar em contato com o suporte técnico antes de iniciar qualquer nó da rede. Não tente os procedimentos de recuperação que reconstroem os dados do Cassandra. Isso pode resultar em perda de dados.

Se possível, ligue os nós da rede nesta ordem:

- Aplique energia primeiro aos nós de administração.
- Aplique energia aos nós de gateway por último.



Se um host incluir vários nós de grade, os nós ficarão online novamente automaticamente quando você ligar o host.

Passos

1. Ligue os hosts do nó de administração primário e de quaisquer nós de administração não primários.



Você não poderá efetuar login nos Nós de Administração até que os Nós de Armazenamento sejam reiniciados.

2. Ligue os hosts para todos os nós de armazenamento.

Você pode ligar esses nós em qualquer ordem.

3. Ligue os hosts para todos os nós de gateway.
4. Sign in no Grid Manager.
5. Selecione **NÓS** e monitore o status dos nós da grade. Verifique se não há ícones de alerta ao lado dos nomes dos nós.

Informações relacionadas

- ["Dispositivos de armazenamento SGF6112 e SG6160"](#)
- ["Aparelhos de serviço SG110 e SG1100"](#)
- ["Aparelhos de serviços SG100 e SG1000"](#)
- ["Dispositivos de armazenamento SG6000"](#)
- ["Dispositivos de armazenamento SG5800"](#)
- ["Dispositivos de armazenamento SG5700"](#)

Procedimentos de remapeamento de portas

Remover remapeamentos de portas

Se você quiser configurar um ponto de extremidade para o serviço Load Balancer e quiser usar uma porta que já foi configurada como a Porta Mapeada para um remapeamento de porta, primeiro você deve remover o remapeamento de porta existente, ou o ponto de extremidade não será efetivo. Você deve executar um script em

cada nó de administração e nó de gateway que tenha portas remapeadas conflitantes para remover todos os remapeamentos de porta do nó.

Sobre esta tarefa

Este procedimento remove todos os remapeamentos de portas. Se você precisar manter alguns dos remapeamentos, entre em contato com o suporte técnico.

Para obter informações sobre como configurar pontos de extremidade do balanceador de carga, consulte ["Configurando endpoints do balanceador de carga"](#).



Se o remapeamento de porta fornecer acesso ao cliente, reconfigure o cliente para usar uma porta diferente como um ponto de extremidade do balanceador de carga para evitar perda de serviço. Caso contrário, a remoção do mapeamento de portas resultará na perda de acesso do cliente e deverá ser agendada adequadamente.



Este procedimento não funciona para um sistema StorageGRID implantado como um contêiner em hosts bare metal. Veja as instruções para ["removendo remapeamentos de portas em hosts bare metal"](#).

Passos

1. Efetue login no nó.

a. Digite o seguinte comando: `ssh -p 8022 admin@node_IP`

A porta 8022 é a porta SSH do sistema operacional base, enquanto a porta 22 é a porta SSH do mecanismo de contêiner que executa o StorageGRID.

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 script: `remove-port-remap.sh`

3. Reinicie o nó: `reboot`

4. Sair do shell de comando: `exit`

5. Repita essas etapas em cada nó de administração e nó de gateway que tenham portas remapeadas conflitantes.

Remover remapeamentos de portas em hosts bare metal

Se você quiser configurar um ponto de extremidade para o serviço Load Balancer e quiser usar uma porta que já foi configurada como a Porta Mapeada para um remapeamento de porta, primeiro você deve remover o remapeamento de porta existente, ou o ponto de extremidade não será efetivo.

Sobre esta tarefa

Se você estiver executando o StorageGRID em hosts bare metal, siga este procedimento em vez do procedimento geral para remover remapeamentos de portas. Você deve editar o arquivo de configuração do

nó para cada nó de administração e nó de gateway que tenha portas remapeadas conflitantes para remover todos os remapeamentos de porta do nó e reiniciá-lo.



Este procedimento remove todos os remapeamentos de portas. Se você precisar manter alguns dos remapeamentos, entre em contato com o suporte técnico.

Para obter informações sobre como configurar pontos de extremidade do balanceador de carga, consulte as instruções para administrar o StorageGRID.



Este procedimento pode resultar em perda temporária de serviço à medida que os nós são reiniciados.

Passos

1. Efetue login no host que dá suporte ao nó. Efetue login como root ou com uma conta que tenha permissão sudo.
2. Execute o seguinte comando para desabilitar temporariamente o nó: `sudo storagegrid node stop node-name`
3. Usando um editor de texto como vim ou pico, edite o arquivo de configuração do nó para o nó.

O arquivo de configuração do nó pode ser encontrado em `/etc/storagegrid/nodes/node-name.conf`.

4. Localize a seção do arquivo de configuração do nó que contém os remapeamentos de porta.

Veja as duas últimas linhas no exemplo a seguir.

```

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443

```

5. Edite as entradas PORT_REMAP e PORT_REMAP_INBOUND para remover remapeamentos de portas.

```

PORT_REMAP =
PORT_REMAP_INBOUND =

```

6. Execute o seguinte comando para validar suas alterações no arquivo de configuração do nó: `sudo storagegrid node validate node-name`

Resolva quaisquer erros ou avisos antes de prosseguir para a próxima etapa.

7. Execute o seguinte comando para reiniciar o nó sem remapeamentos de porta: `sudo storagegrid node start node-name`
8. Efetue login no nó como administrador usando a senha listada em `Passwords.txt` arquivo.
9. Verifique se os serviços iniciam corretamente.
 - a. Veja uma lista dos status de todos os serviços no servidor: `sudo storagegrid-status`

O status é atualizado automaticamente.

b. Aguarde até que todos os serviços tenham o status Em execução ou Verificado.

c. Sair da tela de status:Ctrl+C

10. Repita essas etapas em cada nó de administração e nó de gateway que tenham portas remapeadas conflitantes.

Procedimentos de rede

Atualizar sub-redes para a rede Grid

O StorageGRID mantém uma lista das sub-redes de rede usadas para comunicação entre nós de grade na Rede de Grade (eth0). Essas entradas incluem as sub-redes usadas para a Grid Network por cada site no seu sistema StorageGRID , bem como quaisquer sub-redes usadas para NTP, DNS, LDAP ou outros servidores externos acessados por meio do gateway da Grid Network. Ao adicionar nós de grade ou um novo site em uma expansão, pode ser necessário atualizar ou adicionar sub-redes à Rede de 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.
- Você tem os endereços de rede, em notação CIDR, das sub-redes que deseja configurar.

Sobre esta tarefa

Se você estiver executando uma atividade de expansão que inclua a adição de uma nova sub-rede, adicione uma nova sub-rede à lista de sub-redes da Rede de Grade antes de iniciar o procedimento de expansão. Caso contrário, você terá que cancelar a expansão, adicionar a nova sub-rede e iniciar a expansão novamente.

Não use sub-redes que contenham os seguintes endereços IPv4 para a Rede de Grade, Rede de Administração ou Rede de Cliente de qualquer nó:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Por exemplo, não use os seguintes intervalos de sub-rede para a Rede de Grade, Rede de Administração ou Rede de Cliente de nenhum nó:

- 192.168.130.0/24 porque este intervalo de sub-rede contém os endereços IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 porque este intervalo de sub-rede contém os endereços IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 porque este intervalo de sub-rede contém os endereços IP 198.51.100.2 e 198.51.100.4

Adicionar uma sub-rede

Passos

1. Selecione **MANUTENÇÃO > Rede > Rede de grade**.
2. Selecione **Adicionar outra sub-rede** para adicionar uma nova sub-rede na notação CIDR.

Por exemplo, insira 10.96.104.0/22.
3. Digite a senha de provisionamento e selecione **Salvar**.
4. Aguarde até que as alterações sejam aplicadas e, em seguida, baixe um novo Pacote de Recuperação.
 - a. Selecione **MANUTENÇÃO > Sistema > Pacote de recuperação**.
 - b. Digite a **senha de provisionamento**.



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. Ele também é usado para recuperar o nó de administração primário.

As sub-redes que você especificou são configuradas automaticamente para seu sistema StorageGRID.

Editar uma sub-rede

Passos

1. Selecione **MANUTENÇÃO > Rede > Rede de grade**.
2. Selecione a sub-rede que deseja editar e faça as alterações necessárias.
3. Digite a senha de provisionamento e selecione **Salvar**.
4. Selecione **Sim** na caixa de diálogo de confirmação.

5. Aguarde até que as alterações sejam aplicadas e, em seguida, baixe um novo Pacote de Recuperação.
 - a. Selecione **MANUTENÇÃO > Sistema > Pacote de recuperação**.
 - b. Digite a **senha de provisionamento**.

Excluir uma sub-rede

Passos

1. Selecione **MANUTENÇÃO > Rede > Rede de grade**.
2. Selecione o ícone de exclusão  ao lado da sub-rede.
3. Digite a senha de provisionamento e selecione **Salvar**.
4. Selecione **Sim** na caixa de diálogo de confirmação.
5. Aguarde até que as alterações sejam aplicadas e, em seguida, baixe um novo Pacote de Recuperação.
 - a. Selecione **MANUTENÇÃO > Sistema > Pacote de recuperação**.
 - b. Digite a **senha de provisionamento**.

Configurar endereços IP

Diretrizes de endereço IP

Você pode executar a configuração de rede configurando endereços IP para nós de grade usando a ferramenta Alterar IP.

Você deve usar a ferramenta Alterar IP para fazer a maioria das alterações na configuração de rede que foi definida inicialmente durante a implantação da grade. Alterações manuais usando comandos e arquivos de rede Linux padrão podem não ser propagadas para todos os serviços do StorageGRID e podem não persistir em atualizações, reinicializações ou procedimentos de recuperação de nós.



O procedimento de alteração de IP pode ser um procedimento disruptivo. Partes da grade podem ficar indisponíveis até que a nova configuração seja aplicada.



Se você estiver fazendo alterações apenas na Lista de sub-redes da rede de grade, use o Gerenciador de grade para adicionar ou alterar a configuração da rede. Caso contrário, use a ferramenta Alterar IP se o Grid Manager estiver inacessível devido a um problema de configuração de rede ou se você estiver executando uma alteração de roteamento da Grid Network e outras alterações de rede ao mesmo tempo.



Se você quiser alterar o endereço IP da rede Grid para todos os nós na grade, use o ["procedimento especial para alterações em toda a rede"](#).

Interfaces Ethernet

O endereço IP atribuído a eth0 é sempre o endereço IP da rede do nó da grade. O endereço IP atribuído a eth1 é sempre o endereço IP da rede de administração do nó da grade. O endereço IP atribuído a eth2 é sempre o endereço IP da rede do cliente do nó da grade.

Observe que em algumas plataformas, como dispositivos StorageGRID, eth0, eth1 e eth2 podem ser interfaces agregadas compostas de pontes subordinadas ou ligações de interfaces físicas ou VLAN. Nessas plataformas, a guia **SSM > Recursos** pode mostrar os endereços IP da rede Grid, Admin e Client atribuídos a

outras interfaces além de eth0, eth1 ou eth2.

DHCP

Você só pode configurar o DHCP durante a fase de implantação. Não é possível configurar o DHCP durante a configuração. Você deve usar os procedimentos de alteração de endereço IP se quiser alterar endereços IP, máscaras de sub-rede e gateways padrão para um nó de grade. Usar a ferramenta Alterar IP fará com que os endereços DHCP se tornem estáticos.

Grupos de alta disponibilidade (HA)

- Se uma interface de rede do cliente estiver contida em um grupo HA, você não poderá alterar o endereço IP da rede do cliente para essa interface para um endereço que esteja fora da sub-rede configurada para o grupo HA.
- Não é possível alterar o endereço IP da rede do cliente para o valor de um endereço IP virtual existente atribuído a um grupo de HA configurado na interface da rede do cliente.
- Se uma interface de rede Grid estiver contida em um grupo HA, você não poderá alterar o endereço IP da rede Grid para essa interface para um endereço que esteja fora da sub-rede configurada para o grupo HA.
- Não é possível alterar o endereço IP da Grid Network para o valor de um endereço IP virtual existente atribuído a um grupo HA configurado na interface da Grid Network.

Alterar configuração de rede do nó

Você pode alterar a configuração de rede de um ou mais nós usando a ferramenta Alterar IP. Você pode alterar a configuração da Rede Grid ou adicionar, alterar ou remover as Redes de Administrador ou Cliente.

Antes de começar

Você tem o `Passwords.txt` arquivo.

Sobre esta tarefa

Linux: Se você estiver adicionando um nó de grade à Rede de Administração ou à Rede de Cliente pela primeira vez e não tiver configurado `ADMIN_NETWORK_TARGET` ou `CLIENT_NETWORK_TARGET` anteriormente no arquivo de configuração do nó, deverá fazê-lo agora.

Veja as instruções de instalação do StorageGRID para seu sistema operacional Linux:

- ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
- ["Instalar o StorageGRID no Ubuntu ou Debian"](#)

Dispositivos: Em dispositivos StorageGRID, se a rede do cliente ou do administrador não tiver sido configurada no instalador do dispositivo StorageGRID durante a instalação inicial, a rede não poderá ser adicionada usando apenas a ferramenta Alterar IP. Primeiro, você deve ["coloque o aparelho em modo de manutenção"](#), configure os links, retorne o dispositivo ao modo de operação normal e, em seguida, use a ferramenta Alterar IP para modificar a configuração de rede. Veja o ["procedimento para configuração de links de rede"](#).

Você pode alterar o endereço IP, a máscara de sub-rede, o gateway ou o valor de MTU para um ou mais nós em qualquer rede.

Você também pode adicionar ou remover um nó de uma Rede de Cliente ou de uma Rede de Administração:

- Você pode adicionar um nó a uma rede de cliente ou a uma rede de administrador adicionando um endereço IP/máscara de sub-rede nessa rede ao nó.
- Você pode remover um nó de uma rede de cliente ou de uma rede de administrador excluindo o endereço IP/máscara de sub-rede do nó nessa rede.

Os nós não podem ser removidos da Rede Grid.



Trocas de endereços IP não são permitidas. Se você precisar trocar endereços IP entre nós da grade, deverá usar um endereço IP intermediário temporário.



Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID e você estiver alterando o endereço IP de um nó de administração, esteja ciente de que qualquer confiança de parte confiável que foi configurada usando o endereço IP do nó de administração (em vez de seu nome de domínio totalmente qualificado, conforme recomendado) se tornará inválida. Você não poderá mais fazer login no nó. Imediatamente após alterar o endereço IP, você deve atualizar ou reconfigurar a parte confiável do nó nos Serviços de Federação do Active Directory (AD FS) com o novo endereço IP. Veja as instruções para ["configurando SSO"](#).



Quaisquer alterações feitas na rede usando a ferramenta Alterar IP são propagadas para o firmware do instalador dos dispositivos StorageGRID. Dessa forma, se o software StorageGRID for reinstalado em um dispositivo ou se um dispositivo for colocado em modo de manutenção, a configuração de rede estará correta.

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. Inicie a ferramenta Alterar IP digitando o seguinte comando: `change-ip`

3. Digite a senha de provisionamento no prompt.

O menu principal aparece.

```

Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █

```

4. Opcionalmente, selecione **1** para escolher quais nós atualizar. Em seguida, selecione uma das seguintes opções:

- **1:** Nó único — selecionar por nome
- **2:** Nó único — selecione por site e depois por nome
- **3:** Nó único — selecionar pelo IP atual
- **4:** Todos os nós em um site
- **5:** Todos os nós na grade

Observação: Se você quiser atualizar todos os nós, deixe "todos" selecionado.

Depois de fazer sua seleção, o menu principal aparece, com o campo **Nós selecionados** atualizado para refletir sua escolha. Todas as ações subsequentes são executadas somente nos nós exibidos.

5. No menu principal, selecione a opção **2** para editar informações de IP/máscara, gateway e MTU para os nós selecionados.

a. Selecione a rede onde você deseja fazer alterações:

- **1:** Rede de grade
- **2:** Rede de administração
- **3:** Rede do cliente
- **4:** Todas as redes

Depois de fazer sua seleção, o prompt mostra o nome do nó, o nome da rede (Grid, Admin ou Client), o tipo de dado (IP/máscara, Gateway ou MTU) e o valor atual.

Editar o endereço IP, o comprimento do prefixo, o gateway ou a MTU de uma interface configurada por DHCP mudará a interface para estática. Quando você seleciona alterar uma interface configurada por DHCP, um aviso é exibido para informá-lo de que a interface mudará para estática.

Interfaces configuradas como *fixed* não pode ser editado.

b. Para definir um novo valor, insira-o no formato mostrado para o valor atual.

c. Para deixar o valor atual inalterado, pressione **Enter**.

d. Se o tipo de dados for `IP/mask`, você pode excluir a rede de administração ou cliente do nó digitando **d** ou `0.0.0.0/0`.

e. Depois de editar todos os nós que você deseja alterar, digite **q** para retornar ao menu principal.

Suas alterações serão mantidas até serem limpas ou aplicadas.

6. Revise suas alterações selecionando uma das seguintes opções:

- **5:** Mostra edições na saída que são isoladas para mostrar apenas o item alterado. As alterações são destacadas em verde (adições) ou vermelho (exclusões), conforme mostrado no exemplo de saída:

```
=====
Site: RTP
=====
username-x Grid IP [ 172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Admin IP [ 10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
Press Enter to continue
```

- **6:** Mostra edições na saída que exibem a configuração completa. As alterações são destacadas em verde (adições) ou vermelho (exclusões).



Certas interfaces de linha de comando podem mostrar adições e exclusões usando formatação tachada. A exibição correta depende do seu cliente de terminal suportar as sequências de escape VT100 necessárias.

7. Selecione a opção **7** para validar todas as alterações.

Essa validação garante que as regras para as redes Grid, Admin e Client, como não usar sub-redes sobrepostas, não sejam violadas.

Neste exemplo, a validação retornou erros.

```
Validating new networking configuration... FAILED.

DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

Neste exemplo, a validação foi aprovada.

```
Validating new networking configuration... PASSED.  
Checking for Grid Network IP address swaps... PASSED.  
Press Enter to continue
```

8. Após a validação, escolha uma das seguintes opções:

- **8:** Salvar alterações não aplicadas.

Esta opção permite que você saia da ferramenta Alterar IP e inicie-a novamente mais tarde, sem perder nenhuma alteração não aplicada.

- **10:** Aplique a nova configuração de rede.

9. Se você selecionou a opção **10**, escolha uma das seguintes opções:

- **aplicar:** aplica as alterações imediatamente e reinicia automaticamente cada nó, se necessário.

Se a nova configuração de rede não exigir nenhuma alteração física na rede, você pode selecionar **aplicar** para aplicar as alterações imediatamente. Os nós serão reiniciados automaticamente, se necessário. Os nós que precisam ser reiniciados serão exibidos.

- **estágio:** Aplique as alterações na próxima vez que os nós forem reiniciados manualmente.

Se precisar fazer alterações na configuração de rede física ou virtual para que a nova configuração de rede funcione, você deve usar a opção **stage**, desligar os nós afetados, fazer as alterações de rede física necessárias e reiniciar os nós afetados. Se você selecionar **aplicar** sem primeiro fazer essas alterações de rede, as alterações geralmente falharão.



Se você usar a opção **stage**, deverá reiniciar o nó o mais rápido possível após o preparo para minimizar interrupções.

- **cancelar:** Não faça nenhuma alteração na rede neste momento.

Se você não sabia que as alterações propostas exigem que os nós sejam reiniciados, você pode adiar as alterações para minimizar o impacto ao usuário. Selecionar **cancelar** retorna ao menu principal e preserva suas alterações para que você possa aplicá-las mais tarde.

Quando você seleciona **aplicar** ou **preparar**, um novo arquivo de configuração de rede é gerado, o provisionamento é executado e os nós são atualizados com novas informações de trabalho.

Durante o provisionamento, a saída exibe o status conforme as atualizações são aplicadas.

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

Depois de aplicar ou preparar as alterações, um novo Pacote de Recuperação é gerado como resultado

da alteração na configuração da grade.

10. Se você selecionou **estágio**, siga estas etapas após a conclusão do provisionamento:

- a. Faça as alterações de rede física ou virtual que forem necessárias.

Alterações na rede física: Faça as alterações necessárias na rede física, desligando o nó com segurança, se necessário.

Linux: Se você estiver adicionando o nó a uma rede de administração ou rede de cliente pela primeira vez, certifique-se de ter adicionado a interface conforme descrito em "[Linux: Adicionar interfaces ao nó existente](#)".

- a. Reinicie os nós afetados.

11. Selecione **0** para sair da ferramenta Alterar IP após a conclusão das alterações.

12. Baixe um novo pacote de recuperação do Grid Manager.

- a. Selecione **MANUTENÇÃO > Sistema > Pacote de recuperação**.
- b. Digite a senha de provisionamento.

Adicionar ou alterar listas de sub-redes na rede de administração

Você pode adicionar, excluir ou alterar as sub-redes na Lista de sub-redes da rede de administração de um ou mais nós.

Antes de começar

- Você tem o `Passwords.txt` arquivo.

Você pode adicionar, excluir ou alterar sub-redes para todos os nós na Lista de sub-redes da rede de administração.

Não use sub-redes que contenham os seguintes endereços IPv4 para a Rede de Grade, Rede de Administração ou Rede de Cliente de qualquer nó:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Por exemplo, não use os seguintes intervalos de sub-rede para a Rede de Grade, Rede de Administração ou Rede de Cliente de nenhum nó:

- 192.168.130.0/24 porque este intervalo de sub-rede contém os endereços IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 porque este intervalo de sub-rede contém os endereços IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 porque este intervalo de sub-rede contém os endereços IP 198.51.100.2 e 198.51.100.4

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. Inicie a ferramenta Alterar IP digitando o seguinte comando: `change-ip`

3. Digite a senha de provisionamento no prompt.

O menu principal aparece.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █
```

4. Opcionalmente, limite as redes/nós nos quais as operações são executadas. Escolha uma das seguintes opções:

- Selecione os nós a serem editados escolhendo **1**, se quiser filtrar nós específicos nos quais executar a operação. Selecione uma das seguintes opções:
 - **1:** Nó único (selecionar por nome)
 - **2:** Nó único (selecione por site e depois por nome)
 - **3:** Nó único (selecionar pelo IP atual)
 - **4:** Todos os nós em um site
 - **5:** Todos os nós na grade
 - **0:** Voltar
- Permitir que "todos" permaneça selecionado. Após a seleção ser feita, a tela do menu principal é exibida. O campo Nós selecionados reflete sua nova seleção e agora todas as operações selecionadas serão executadas somente neste item.

5. No menu principal, selecione a opção para editar sub-redes para a Rede de Administração (opção **3**).

6. Escolha uma das seguintes opções:

- Adicione uma sub-rede digitando este comando: `add CIDR`
- Exclua uma sub-rede digitando este comando: `del CIDR`

- Defina a lista de sub-redes inserindo este comando: `set CIDR`



Para todos os comandos, você pode inserir vários endereços usando este formato: `add CIDR, CIDR`

Exemplo: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`



Você pode reduzir a quantidade de digitação necessária usando a "seta para cima" para recuperar valores digitados anteriormente no prompt de entrada atual e editá-los, se necessário.

O exemplo de entrada abaixo mostra a adição de sub-redes à Lista de Sub-redes da Rede de Administração:

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
 10.0.0.0/8
 172.19.0.0/16
 172.21.0.0/16
 172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

- Quando estiver pronto, digite **q** para voltar à tela do menu principal. Suas alterações serão mantidas até serem limpas ou aplicadas.



Se você selecionou qualquer um dos modos de seleção de "todos" nós na etapa 2, pressione **Enter** (sem **q**) para ir para o próximo nó na lista.

- Escolha uma das seguintes opções:

- Selecione a opção **5** para mostrar edições na saída isolada para mostrar apenas o item alterado. As alterações são destacadas em verde (adições) ou vermelho (exclusões), conforme mostrado no exemplo de saída abaixo:

```
=====
Site: Data Center 1
=====
DC1-ADM1-105-154 Admin Subnets
[ 172.14.0.0/16 ]
[ 172.15.0.0/16 ]
[ 172.17.0.0/16 ]
[ 172.19.0.0/16 ]
[ 172.20.0.0/16 ]
[ 172.21.0.0/16 ]
Press Enter to continue
```

- Selecione a opção **6** para mostrar as edições na saída que exibe a configuração completa. As alterações são destacadas em verde (adições) ou vermelho (exclusões). **Observação:** Certos emuladores de terminal podem mostrar adições e exclusões usando a formatação tachada.

Quando você tenta alterar a lista de sub-redes, a seguinte mensagem é exibida:

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that aren't
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
aren't reachable using default StorageGRID routing, but are reachable
using a different interface and gateway. Making and applying changes
to the subnet list will make all automatically applied subnets
persistent. If you don't want that to happen, delete the unwanted
subnets before applying changes. If you know that all /32 subnets in
the list were added intentionally, you can ignore this caution.
```

Se você não atribuiu especificamente as sub-redes do servidor NTP e DNS a uma rede, o StorageGRID cria uma rota de host (/32) para a conexão automaticamente. Se, por exemplo, você preferir ter uma rota /16 ou /24 para conexão de saída para um servidor DNS ou NTP, você deve excluir a rota /32 criada automaticamente e adicionar as rotas desejadas. Se você não excluir a rota de host criada automaticamente, ela será persistida depois que você aplicar quaisquer alterações à lista de sub-redes.



Embora você possa usar essas rotas de host descobertas automaticamente, em geral você deve configurar manualmente as rotas DNS e NTP para garantir a conectividade.

9. Selecione a opção **7** para validar todas as alterações em etapas.

Essa validação garante que as regras para as redes Grid, Admin e Client sejam seguidas, como o uso de sub-redes sobrepostas.

10. Opcionalmente, selecione a opção **8** para salvar todas as alterações preparadas e retornar mais tarde para continuar fazendo alterações.

Esta opção permite que você saia da ferramenta Alterar IP e inicie-a novamente mais tarde, sem perder nenhuma alteração não aplicada.

11. Faça um dos seguintes:

- Selecione a opção **9** se quiser limpar todas as alterações sem salvar ou aplicar a nova configuração de rede.
- Selecione a opção **10** se estiver pronto para aplicar as alterações e provisionar a nova configuração de rede. Durante o provisionamento, a saída exibe o status conforme as atualizações são aplicadas, conforme mostrado no exemplo de saída a seguir:

Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name

12. Baixe um novo pacote de recuperação do Grid Manager.

- a. Selecione **MANUTENÇÃO > Sistema > Pacote de recuperação**.
- b. Digite a senha de provisionamento.

Adicionar ou alterar listas de sub-redes na Grid Network

Você pode usar a ferramenta Alterar IP para adicionar ou alterar sub-redes na Rede de Grade.

Antes de começar

- Você tem o `Passwords.txt` arquivo.

Você pode adicionar, excluir ou alterar sub-redes na Lista de sub-redes da rede de grade. As alterações afetarão o roteamento em todos os nós da grade.



Se você estiver fazendo alterações apenas na Lista de sub-redes da rede de grade, use o Gerenciador de grade para adicionar ou alterar a configuração da rede. Caso contrário, use a ferramenta Alterar IP se o Grid Manager estiver inacessível devido a um problema de configuração de rede ou se você estiver executando uma alteração de roteamento da Grid Network e outras alterações de rede ao mesmo tempo.

Não use sub-redes que contenham os seguintes endereços IPv4 para a Rede de Grade, Rede de Administração ou Rede de Cliente de qualquer nó:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Por exemplo, não use os seguintes intervalos de sub-rede para a Rede de Grade, Rede de Administração ou Rede de Cliente de nenhum nó:

- 192.168.130.0/24 porque este intervalo de sub-rede contém os endereços IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 porque este intervalo de sub-rede contém os endereços IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 porque este intervalo de sub-rede contém os endereços IP 198.51.100.2 e 198.51.100.4

Passos

1. Efetue login no nó de administração principal:

- Digite o seguinte comando: `ssh admin@primary_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. Inicie a ferramenta Alterar IP digitando o seguinte comando: `change-ip`

3. Digite a senha de provisionamento no prompt.

O menu principal aparece.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █
```

4. No menu principal, selecione a opção para editar sub-redes para a Rede Grid (opção 4).



As alterações na Lista de sub-redes da rede de grade são válidas para toda a grade.

5. Escolha uma das seguintes opções:

- Adicione uma sub-rede digitando este comando: `add CIDR`
- Exclua uma sub-rede digitando este comando: `del CIDR`
- Defina a lista de sub-redes inserindo este comando: `set CIDR`



Para todos os comandos, você pode inserir vários endereços usando este formato: `add CIDR, CIDR`

Exemplo: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`



Você pode reduzir a quantidade de digitação necessária usando a "seta para cima" para recuperar valores digitados anteriormente no prompt de entrada atual e editá-los, se necessário.

O exemplo de entrada abaixo mostra a configuração de sub-redes para a Lista de Sub-redes da Rede de

Grade:

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
172.16.0.0/21
172.17.0.0/21
172.18.0.0/21
192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

6. Quando estiver pronto, digite **q** para voltar à tela do menu principal. Suas alterações serão mantidas até serem limpas ou aplicadas.
7. Escolha uma das seguintes opções:
 - Selecione a opção **5** para mostrar edições na saída isolada para mostrar apenas o item alterado. As alterações são destacadas em verde (adições) ou vermelho (exclusões), conforme mostrado no exemplo de saída abaixo:

```
=====
Grid Network Subnet List (GNSL)
=====
add 172.30.0.0/21
add 172.31.0.0/21
del 172.16.0.0/21
del 172.17.0.0/21
del 172.18.0.0/21

[ 172.30.0.0/21 ]
[ 172.31.0.0/21 ]
[ 192.168.0.0/21 ]

Press Enter to continue
```

- Selecione a opção **6** para mostrar as edições na saída que exibe a configuração completa. As alterações são destacadas em verde (adições) ou vermelho (exclusões).



Certas interfaces de linha de comando podem mostrar adições e exclusões usando formatação tachada.

8. Selecione a opção **7** para validar todas as alterações em etapas.

Essa validação garante que as regras para as redes Grid, Admin e Client sejam seguidas, como o uso de sub-redes sobrepostas.

9. Opcionalmente, selecione a opção **8** para salvar todas as alterações preparadas e retornar mais tarde para continuar fazendo alterações.

Esta opção permite que você saia da ferramenta Alterar IP e inicie-a novamente mais tarde, sem perder nenhuma alteração não aplicada.

10. Faça um dos seguintes:

- Selecione a opção **9** se quiser limpar todas as alterações sem salvar ou aplicar a nova configuração de rede.
- Selecione a opção **10** se estiver pronto para aplicar as alterações e provisionar a nova configuração de rede. Durante o provisionamento, a saída exibe o status conforme as atualizações são aplicadas, conforme mostrado no exemplo de saída a seguir:

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

11. Se você selecionou a opção **10** ao fazer alterações na Rede de Grade, selecione uma das seguintes opções:

- **aplicar**: aplica as alterações imediatamente e reinicia automaticamente cada nó, se necessário.

Se a nova configuração de rede funcionar simultaneamente com a configuração de rede antiga sem nenhuma alteração externa, você poderá usar a opção **aplicar** para uma alteração de configuração totalmente automatizada.

- **estágio**: Aplique as alterações na próxima vez que os nós forem reiniciados.

Se precisar fazer alterações na configuração de rede física ou virtual para que a nova configuração de rede funcione, você deve usar a opção **stage**, desligar os nós afetados, fazer as alterações de rede física necessárias e reiniciar os nós afetados.



Se você usar a opção **stage**, reinicie o nó o mais rápido possível após o preparo para minimizar interrupções.

- **cancelar**: Não faça nenhuma alteração na rede neste momento.

Se você não sabia que as alterações propostas exigem que os nós sejam reiniciados, você pode adiar as alterações para minimizar o impacto ao usuário. Selecionar **cancelar** retorna ao menu principal e preserva suas alterações para que você possa aplicá-las mais tarde.

Depois de aplicar ou preparar as alterações, um novo Pacote de Recuperação é gerado como resultado da alteração na configuração da grade.

12. Se a configuração for interrompida devido a erros, as seguintes opções estarão disponíveis:

- Para encerrar o procedimento de alteração de IP e retornar ao menu principal, digite **a**.
- Para tentar novamente a operação que falhou, digite **r**.
- Para continuar para a próxima operação, digite **c**.

A operação com falha pode ser repetida mais tarde selecionando a opção **10** (Aplicar alterações) no menu principal. O procedimento de alteração de IP não estará concluído até que todas as operações sejam concluídas com sucesso.

- Se você tiver que intervir manualmente (para reinicializar um nó, por exemplo) e estiver confiante de

que a ação que a ferramenta considera que falhou foi realmente concluída com sucesso, digite **f** para marcá-la como bem-sucedida e passar para a próxima operação.

13. Baixe um novo pacote de recuperação do Grid Manager.

- a. Selecione **MANUTENÇÃO > Sistema > Pacote de recuperação**.
- b. Digite a senha de provisionamento.



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 .

Alterar endereços IP para todos os nós na grade

Se você precisar alterar o endereço IP da rede Grid para todos os nós na grade, você deve seguir este procedimento especial. Não é possível fazer uma alteração de IP da rede em toda a rede usando o procedimento para alterar nós individuais.

Antes de começar

- Você tem o `Passwords.txt` arquivo.

Para garantir que a grade seja iniciada com sucesso, você deve fazer todas as alterações ao mesmo tempo.



Este procedimento se aplica somente à Rede Grid. Você não pode usar este procedimento para alterar endereços IP nas redes de administrador ou cliente.

Se você quiser alterar os endereços IP e a MTU para os nós em apenas um site, siga as instruções "[Alterar configuração de rede do nó](#)" instruções.

Passos

1. Planeje com antecedência as alterações que você precisa fazer fora da ferramenta Alterar IP, como alterações no DNS ou NTP e alterações na configuração de logon único (SSO), se usada.



Se os servidores NTP existentes não estiverem acessíveis à rede nos novos endereços IP, adicione os novos servidores NTP antes de executar o procedimento de alteração de IP.



Se os servidores DNS existentes não estiverem acessíveis à grade nos novos endereços IP, adicione os novos servidores DNS antes de executar o procedimento de alteração de IP.



Se o SSO estiver habilitado para seu sistema StorageGRID e quaisquer trusts de terceira parte confiável tiverem sido configurados usando endereços IP do nó de administração (em vez de nomes de domínio totalmente qualificados, conforme recomendado), esteja preparado para atualizar ou reconfigurar esses trusts de terceira parte confiável nos Serviços de Federação do Active Directory (AD FS) imediatamente após alterar os endereços IP. Ver "[Configurar logon único](#)".



Se necessário, adicione a nova sub-rede para os novos endereços IP.

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. Inicie a ferramenta Alterar IP digitando o seguinte comando: `change-ip`
4. Digite a senha de provisionamento no prompt.

O menu principal aparece. Por padrão, o `Selected nodes` campo está definido para `all`.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:  SELECT NODES to edit
2:  EDIT IP/mask, gateway and MTU
3:  EDIT admin network subnet lists
4:  EDIT grid network subnet list
5:  SHOW changes
6:  SHOW full configuration, with changes highlighted
7:  VALIDATE changes
8:  SAVE changes, so you can resume later
9:  CLEAR all changes, to start fresh
10: APPLY changes to the grid
0:  Exit

Selection: █
```

5. No menu principal, selecione **2** para editar informações de IP/máscara de sub-rede, gateway e MTU para todos os nós.
 - a. Selecione **1** para fazer alterações na Rede Grid.

Depois de fazer sua seleção, o prompt mostra os nomes dos nós, o nome da rede Grid, o tipo de dados (IP/máscara, Gateway ou MTU) e os valores atuais.

Editar o endereço IP, o comprimento do prefixo, o gateway ou a MTU de uma interface configurada por DHCP mudará a interface para estática. Um aviso é exibido antes de cada interface configurada pelo DHCP.

Interfaces configuradas como `fixed` não pode ser editado.

- a. Para definir um novo valor, insira-o no formato mostrado para o valor atual.
- b. Depois de editar todos os nós que você deseja alterar, digite **q** para retornar ao menu principal.

Suas alterações serão mantidas até serem limpas ou aplicadas.

6. Revise suas alterações selecionando uma das seguintes opções:
 - **5**: Mostra edições na saída que são isoladas para mostrar apenas o item alterado. As alterações são destacadas em verde (adições) ou vermelho (exclusões), conforme mostrado no exemplo de saída:


```

=====
Site: RTP
=====
username-x Grid IP [ 172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Grid MTU [ 1400 ]: 9000
username-x Admin IP [ 10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin IP [ 10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin Gateway [ 10.224.0.1 ]: 0.0.0.0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
username-x Admin MTU [ 1400 ]: 0
Press Enter to continue

```

- 6: Mostra edições na saída que exibem a configuração completa. As alterações são destacadas em verde (adições) ou vermelho (exclusões).



Certas interfaces de linha de comando podem mostrar adições e exclusões usando formatação tachada. A exibição correta depende do seu cliente de terminal suportar as sequências de escape VT100 necessárias.

7. Selecione a opção **7** para validar todas as alterações.

Essa validação garante que as regras da Grid Network, como não usar sub-redes sobrepostas, não sejam violadas.

Neste exemplo, a validação retornou erros.

```

Validating new networking configuration... FAILED.

DK-10-224-S-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
DK-10-224-S-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-S-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

Neste exemplo, a validação foi aprovada.

```

Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

8. Após a validação, selecione **10** para aplicar a nova configuração de rede.
9. Selecione **stage** para aplicar as alterações na próxima vez que os nós forem reiniciados.



Você deve selecionar **estágio**. Não execute uma reinicialização contínua, manualmente ou selecionando **aplicar** em vez de **estágio**; a grade não será iniciada com sucesso.

10. Após concluir as alterações, selecione **0** para sair da ferramenta Alterar IP.
11. Desligue todos os nós simultaneamente.



Toda a rede deve ser desligada para que todos os nós fiquem inativos ao mesmo tempo.

12. Faça as alterações de rede física ou virtual que forem necessárias.
13. Verifique se todos os nós da grade estão inativos.
14. Ligue todos os nós.
15. Após a inicialização bem-sucedida da rede:
 - a. Se você adicionou novos servidores NTP, exclua os valores antigos dos servidores NTP.
 - b. Se você adicionou novos servidores DNS, exclua os valores dos servidores DNS antigos.
16. Baixe o novo pacote de recuperação do Grid Manager.
 - a. Selecione **MANUTENÇÃO > Sistema > Pacote de recuperação**.
 - b. Digite a senha de provisionamento.

Informações relacionadas

- ["Adicionar ou alterar listas de sub-redes na Grid Network"](#)
- ["Desligar nó da grade"](#)

Adicionar interfaces ao nó existente

Linux: Adicionar interfaces de administrador ou cliente a um nó existente

Use estas etapas para adicionar uma interface na Rede de Administração ou na Rede de Cliente a um nó Linux após sua instalação.

Se você não configurou ADMIN_NETWORK_TARGET ou CLIENT_NETWORK_TARGET no arquivo de configuração do nó no host Linux durante a instalação, use este procedimento para adicionar a interface. Para obter mais informações sobre o arquivo de configuração do nó, consulte as instruções para seu sistema operacional Linux:

- ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
- ["Instalar o StorageGRID no Ubuntu ou Debian"](#)

Execute este procedimento no servidor Linux que hospeda o nó que precisa da nova atribuição de rede, não dentro do nó. Este procedimento apenas adiciona a interface ao nó; um erro de validação ocorre se você tentar especificar quaisquer outros parâmetros de rede.

Para fornecer informações de endereçamento, você deve usar a ferramenta Alterar IP. Ver ["Alterar configuração de rede do nó"](#).

Passos

1. Efetue login no servidor Linux que hospeda o nó.
2. Edite o arquivo de configuração do nó: `/etc/storagegrid/nodes/node-name.conf`.



Não especifique nenhum outro parâmetro de rede, ou ocorrerá um erro de validação.

- a. Adicione uma entrada para o novo destino de rede. Por exemplo:

```
CLIENT_NETWORK_TARGET = bond0.3206
```

- b. Opcional: adicione uma entrada para o endereço MAC. Por exemplo:

```
CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
```

3. Execute o comando `node validate`:

```
sudo storagegrid node validate node-name
```

4. Resolva todos os erros de validação.

5. Execute o comando `node reload`:

```
sudo storagegrid node reload node-name
```

Linux: Adicionar interfaces de tronco ou acesso a um nó

Você pode adicionar interfaces de tronco ou acesso extras a um nó Linux depois que ele for instalado. As interfaces adicionadas são exibidas na página de interfaces VLAN e na página de grupos HA.

Antes de começar

- Você tem acesso às instruções para instalar o StorageGRID na sua plataforma Linux.
 - ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
 - ["Instalar o StorageGRID no Ubuntu ou Debian"](#)
- Você tem o `Passwords.txt` arquivo.
- Você tem ["permissões de acesso específicas"](#).



Não tente adicionar interfaces a um nó enquanto uma atualização de software, procedimento de recuperação ou procedimento de expansão estiver ativo.

Sobre esta tarefa

Use estas etapas para adicionar uma ou mais interfaces extras a um nó Linux após o nó ter sido instalado. Por exemplo, você pode querer adicionar uma interface de tronco a um nó de administração ou gateway, para poder usar interfaces de 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).

Se você adicionar uma interface de tronco, deverá configurar uma interface VLAN no StorageGRID. Se você adicionar uma interface de acesso, poderá adicioná-la diretamente a um grupo HA; não precisará configurar uma interface VLAN.

O nó fica indisponível por um breve período quando você adiciona interfaces. Você deve executar este procedimento em um nó por vez.

Passos

1. Efetue login no servidor Linux que hospeda o nó.
2. Usando um editor de texto como vim ou pico, edite o arquivo de configuração do nó:

```
/etc/storagegrid/nodes/node-name.conf
```

3. Adicione uma entrada ao arquivo para especificar o nome e, opcionalmente, a descrição de cada interface extra que você deseja adicionar ao nó. Use este formato.

```
INTERFACE_TARGET_nnnn=value
```

Para *nnnn*, especifique um número exclusivo para cada INTERFACE_TARGET entrada que você está adicionando.

Para *valor*, especifique o nome da interface física no host bare-metal. Em seguida, opcionalmente, adicione uma vírgula e forneça uma descrição da interface, que é exibida na página de interfaces de VLAN e na página de grupos de HA.

Por exemplo:

```
INTERFACE_TARGET_0001=ens256, Trunk
```



Não especifique nenhum outro parâmetro de rede, ou ocorrerá um erro de validação.

4. Execute o seguinte comando para validar suas alterações no arquivo de configuração do nó:

```
sudo storagegrid node validate node-name
```

Resolva quaisquer erros ou avisos antes de prosseguir para a próxima etapa.

5. Execute o seguinte comando para atualizar a configuração do nó:

```
sudo storagegrid node reload node-name
```

Depois que você terminar

- Se você adicionou uma ou mais interfaces de tronco, vá para ["configurar interfaces VLAN"](#) para configurar uma ou mais interfaces VLAN para cada nova interface pai.
- Se você adicionou uma ou mais interfaces de acesso, vá para ["configurar grupos de alta disponibilidade"](#) para adicionar as novas interfaces diretamente aos grupos HA.

VMware: Adicionar interfaces de tronco ou acesso a um nó

Você pode adicionar um tronco ou uma interface de acesso a um nó de VM após o nó ter sido instalado. As interfaces adicionadas são exibidas na página de interfaces VLAN e na página de grupos de HA.

Antes de começar

- Você tem acesso às instruções para ["instalando o StorageGRID na sua plataforma VMware"](#) .

- Você tem máquinas virtuais VMware Admin Node e Gateway Node.
- Você tem uma sub-rede de rede que não está sendo usada como rede de grade, administração ou cliente.
- Você tem o `Passwords.txt` arquivo.
- Você tem "[permissões de acesso específicas](#)".



Não tente adicionar interfaces a um nó enquanto uma atualização de software, procedimento de recuperação ou procedimento de expansão estiver ativo.

Sobre esta tarefa

Use estas etapas para adicionar uma ou mais interfaces extras a um nó VMware após a instalação do nó. Por exemplo, você pode querer adicionar uma interface de tronco a um nó de administração ou gateway, para poder usar interfaces de 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).

Se você adicionar uma interface de tronco, deverá configurar uma interface VLAN no StorageGRID. Se você adicionar uma interface de acesso, poderá adicioná-la diretamente a um grupo HA; não precisará configurar uma interface VLAN.

O nó pode ficar indisponível por um breve período quando você adiciona interfaces.

Passos

1. No vCenter, adicione um novo adaptador de rede (tipo VMXNET3) a uma VM de nó de administração e nó de gateway. Selecione as caixas de seleção **Conectado** e **Conectar ao ligar**.

Network adapter 4 *		CLIENT683_old_vlan	Connected
Status	☒ Connect At Power On		
Adapter Type	VMXNET 3		
DirectPath I/O	☒ Enable		

2. Use SSH para efetuar login no nó de administração ou no nó de gateway.
3. Usar `ip link show` para confirmar que a nova interface de rede `ens256` foi detectada.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

Depois que você terminar

- Se você adicionou uma ou mais interfaces de tronco, vá para ["configurar interfaces VLAN"](#) para configurar uma ou mais interfaces VLAN para cada nova interface pai.
- Se você adicionou uma ou mais interfaces de acesso, vá para ["configurar grupos de alta disponibilidade"](#) para adicionar as novas interfaces diretamente aos grupos HA.

Configurar servidores DNS

Você pode adicionar, atualizar e remover servidores DNS para poder usar nomes de host de nomes de domínio totalmente qualificados (FQDN) em vez de endereços IP.

Para usar nomes de domínio totalmente qualificados (FQDNs) em vez de endereços IP ao especificar nomes de host para destinos externos, especifique o endereço IP de cada servidor DNS que você usará. Essas entradas são usadas para AutoSupport, e-mails de alerta, notificações SNMP, pontos de extremidade de serviços de plataforma, pools de armazenamento em nuvem e muito mais.

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 os endereços IP dos servidores DNS para configurar.

Sobre esta tarefa

Para garantir a operação correta, especifique dois ou três servidores DNS. Se você especificar mais de três, é possível que apenas três sejam usados devido a limitações conhecidas do sistema operacional em algumas plataformas. Se você tiver restrições de roteamento em seu ambiente, você pode ["personalizar a lista de servidores DNS"](#) para nós individuais (normalmente todos os nós em um site) usar um conjunto diferente de até três servidores DNS.

Se possível, use servidores DNS que cada site possa acessar localmente para garantir que um site isolado possa resolver os FQDNs para destinos externos.

Adicionar um servidor DNS

Siga estas etapas para adicionar um servidor DNS.

Passos

1. Selecione **MANUTENÇÃO > Rede > Servidores DNS**.
2. Selecione **Adicionar outro servidor** para adicionar um servidor DNS.
3. Selecione **Salvar**.

Modificar um servidor DNS

Siga estas etapas para modificar um servidor DNS.

Passos

1. Selecione **MANUTENÇÃO > Rede > Servidores DNS**.
2. Selecione o endereço IP do nome do servidor que você deseja editar e faça as alterações necessárias.
3. Selecione **Salvar**.

Excluir um servidor DNS

Siga estas etapas para excluir um endereço IP de um servidor DNS.

Passos

1. Selecione **MANUTENÇÃO > Rede > Servidores DNS**.
2. Selecione o ícone de exclusão  ao lado do endereço IP.
3. Selecione **Salvar**.

Modificar a configuração de DNS para um único nó de grade

Em vez de configurar o DNS globalmente para toda a implantação, você pode executar um script para configurar o DNS de forma diferente para cada nó da grade.

Em geral, você deve usar a opção **MANUTENÇÃO > Rede > Servidores DNS** no Grid Manager para configurar servidores DNS. Use o script a seguir somente se precisar usar servidores DNS diferentes para nós de grade diferentes.

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 `#`.

- e. Adicione a chave privada SSH ao agente SSH. Digitar: `ssh-add`
- f. Digite a senha de acesso SSH listada no `Passwords.txt` arquivo.

2. Faça login no nó que você deseja atualizar com uma configuração DNS personalizada: `ssh node_IP_address`
3. Execute o script de configuração do DNS: `setup_resolv.rb`.

O script responde com a lista de comandos suportados.

```
Tool to modify external name servers

available commands:
  add search <domain>
      add a specified domain to search list
      e.g.> add search netapp.com
  remove search <domain>
      remove a specified domain from list
      e.g.> remove search netapp.com
  add nameserver <ip>
      add a specified IP address to the name server list
      e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
      remove a specified IP address from list
      e.g.> remove nameserver 192.0.2.65
  remove nameserver all
      remove all nameservers from list
  save
      write configuration to disk and quit
  abort
      quit without saving changes
  help
      display this help message

Current list of name servers:
  192.0.2.64
Name servers inherited from global DNS configuration:
  192.0.2.126
  192.0.2.127
Current list of search entries:
  netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
      [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

4. Adicione o endereço IPv4 de um servidor que fornece serviço de nome de domínio para sua rede: `add <nameserver IP_address>`
5. Repita o `add nameserver` comando para adicionar servidores de nomes.
6. Siga as instruções conforme solicitado para outros comandos.

7. Salve suas alterações e saia do aplicativo: `save`
8. Feche o shell de comando no servidor: `exit`
9. Para cada nó da grade, repita as etapas de [fazendo login no nó](#) através [fechando o shell de comando](#).
10. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Digitar: `ssh-add -D`

Gerenciar servidores NTP

Você pode adicionar, atualizar ou remover servidores NTP (Network Time Protocol) para garantir que os dados sejam sincronizados com precisão entre os nós da grade no seu sistema StorageGRID.

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.
- Você tem os endereços IPv4 dos servidores NTP para configurar.

Como o StorageGRID usa o NTP

O sistema StorageGRID usa o Network Time Protocol (NTP) para sincronizar o tempo entre todos os nós da grade.

Em cada site, pelo menos dois nós no sistema StorageGRID recebem a função NTP principal. Eles sincronizam com um mínimo sugerido de quatro e um máximo de seis fontes de tempo externas entre si. Cada nó no sistema StorageGRID que não é um nó NTP primário atua como um cliente NTP e sincroniza com esses nós NTP primários.

Os servidores NTP externos se conectam aos nós aos quais você atribuiu anteriormente funções NTP primárias. Por esse motivo, é recomendável especificar pelo menos dois nós com funções NTP primárias.

Diretrizes do servidor NTP

Siga estas diretrizes para se proteger contra problemas de tempo:

- Os servidores NTP externos se conectam aos nós aos quais você atribuiu anteriormente funções NTP primárias. Por esse motivo, é recomendável especificar pelo menos dois nós com funções NTP primárias.
- Certifique-se de que pelo menos dois nós em cada site possam acessar pelo menos quatro fontes NTP externas. Se apenas um nó em um site puder alcançar as fontes NTP, ocorrerão problemas de tempo se esse nó ficar inativo. Além disso, designar dois nós por site como fontes primárias de NTP garante um tempo preciso se um site estiver isolado do restante da rede.
- Os servidores NTP externos especificados devem usar o protocolo NTP. Você deve especificar referências de servidor NTP do Stratum 3 ou superior para evitar problemas com desvio de tempo.



Ao especificar a origem NTP externa para uma instalação do StorageGRID em nível de produção, não use o serviço Windows Time (W32Time) em uma versão do Windows anterior ao Windows Server 2016. O serviço de tempo em versões anteriores do Windows não é suficientemente preciso e não é suportado pela Microsoft para uso em ambientes de alta precisão, incluindo StorageGRID. Para mais detalhes, veja ["Limite de suporte para configurar o serviço Windows Time para ambientes de alta precisão"](#).

Configurar servidores NTP

Siga estas etapas para adicionar, atualizar ou remover servidores NTP.

Passos

1. Selecione **MANUTENÇÃO > Rede > Servidores NTP**.
2. Na seção Servidores, adicione, atualize ou remova entradas do servidor NTP, conforme necessário.

Você deve incluir pelo menos quatro servidores NTP e pode especificar até seis servidores.

3. Digite a senha de provisionamento do seu sistema StorageGRID e selecione **Salvar**.

A página ficará desativada até que as atualizações de configuração sejam concluídas.



Se todos os seus servidores NTP falharem no teste de conexão depois que você salvar os novos servidores NTP, não prossiga. Entre em contato com o suporte técnico.

Resolver problemas do servidor NTP

Se você encontrar problemas com a estabilidade ou disponibilidade dos servidores NTP especificados originalmente durante a instalação, poderá atualizar a lista de fontes NTP externas que o sistema StorageGRID usa adicionando servidores adicionais ou atualizando ou removendo servidores existentes.

Restaurar a conectividade de rede para nós isolados

Sob certas circunstâncias, um ou mais grupos de nós podem não conseguir entrar em contato com o restante da grade. Por exemplo, alterações de endereço IP em todo o site ou na grade podem resultar em nós isolados.

Sobre esta tarefa

O isolamento do nó é indicado por:

- Alertas, como **Não foi possível comunicar com o nó (Alertas > Atual)**
- Diagnóstico relacionado à conectividade (**SUPORTE > Ferramentas > Diagnóstico**)

Algumas das consequências de ter nós isolados incluem o seguinte:

- Se vários nós estiverem isolados, talvez você não consiga fazer login ou acessar o Grid Manager.
- Se vários nós estiverem isolados, os valores de uso de armazenamento e cota mostrados no painel do Gerenciador de Tenants podem estar desatualizados. Os totais serão atualizados quando a conectividade de rede for restaurada.

Para resolver o problema de isolamento, execute um utilitário de linha de comando em cada nó isolado ou em

um nó em um grupo (todos os nós em uma sub-rede que não contém o nó de administração principal) que esteja isolado da grade. O utilitário fornece aos nós o endereço IP de um nó não isolado na grade, o que permite que o nó isolado ou grupo de nós entre em contato com toda a grade novamente.



Se o sistema de nomes de domínio multicast (mDNS) estiver desabilitado nas redes, talvez seja necessário executar o utilitário de linha de comando em cada nó isolado.

Passos

Este procedimento não se aplica quando apenas alguns serviços estão offline ou relatando erros de comunicação.

1. Acesse o nó e verifique `/var/local/log/dynip.log` para mensagens de isolamento.

Por exemplo:

```
[2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
no contact with other nodes.
If this warning persists, manual action might be required.
```

Se você estiver usando o console do VMware, ele conterá uma mensagem informando que o nó pode estar isolado.

Em implantações Linux, mensagens de isolamento apareceriam em `/var/log/storagegrid/node/<nodename>.log` arquivos.

2. Se as mensagens de isolamento forem recorrentes e persistentes, execute o seguinte comando:

```
add_node_ip.py <address>
```

onde `<address>` é o endereço IP de um nó remoto que está conectado à rede.

```
# /usr/sbin/add_node_ip.py 10.224.4.210

Retrieving local host information
Validating remote node at address 10.224.4.210
Sending node IP hint for 10.224.4.210 to local node
Local node found on remote node. Update complete.
```

3. Verifique o seguinte para cada nó que foi isolado anteriormente:

- Os serviços do nó foram iniciados.
- O status do serviço IP dinâmico é "Em execução" após você executar o `storagegrid-status` comando.
- Na página Nós, o nó não aparece mais desconectado do resto da grade.



Se estiver executando o `add_node_ip.py` o comando não resolver o problema, pode haver outros problemas de rede que precisam ser resolvidos.

Procedimentos de host e middleware

Linux: Migrar nó de grade para novo host

Você pode migrar um ou mais nós do StorageGRID de um host Linux (o *host de origem*) para outro host Linux (o *host de destino*) para executar a manutenção do host sem afetar a funcionalidade ou a disponibilidade da sua grade.

Por exemplo, você pode querer migrar um nó para executar patches no sistema operacional e reinicializar.

Antes de começar

- Você planejou sua implantação do StorageGRID para incluir suporte à migração.
 - ["Requisitos de migração de contêineres de nó para Red Hat Enterprise Linux"](#)
 - ["Requisitos de migração do contêiner Node para Ubuntu ou Debian"](#)
- O host de destino já está preparado para uso do StorageGRID .
- O armazenamento compartilhado é usado para todos os volumes de armazenamento por nó
- As interfaces de rede têm nomes consistentes em todos os hosts.



Em uma implantação de produção, não execute mais de um nó de armazenamento em um único host. Usar um host dedicado para cada nó de armazenamento fornece um domínio de falha isolado.

Outros tipos de nós, como nós de administração ou nós de gateway, podem ser implantados no mesmo host. No entanto, se você tiver vários nós do mesmo tipo (dois nós de gateway, por exemplo), não instale todas as instâncias no mesmo host.

Exportar nó do host de origem

Como primeiro passo, desligue o nó da grade e exporte-o do host Linux de origem.

Execute os seguintes comandos no *host de origem*.

Passos

1. Obtenha o status de todos os nós atualmente em execução no host de origem.

```
sudo storagegrid node status all
```

Exemplo de saída:

```
Name Config-State Run-State
DC1-ADM1 Configured Running
DC1-ARC1 Configured Running
DC1-GW1 Configured Running
DC1-S1 Configured Running
DC1-S2 Configured Running
DC1-S3 Configured Running
```

2. Identifique o nome do nó que você deseja migrar e interrompa-o se seu estado de execução for Em execução.

```
sudo storagegrid node stop DC1-S3
```

Exemplo de saída:

```
Stopping node DC1-S3
Waiting up to 630 seconds for node shutdown
```

3. Exporte o nó do host de origem.

```
sudo storagegrid node export DC1-S3
```

Exemplo de saída:

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you
want to import it again.
```

4. Tome nota do `import` comando sugerido na saída.

Você executará este comando no host de destino na próxima etapa.

Importar nó no host de destino

Depois de exportar o nó do host de origem, você importa e valida o nó no host de destino. A validação confirma que o nó tem acesso aos mesmos dispositivos de armazenamento em bloco e interface de rede que tinha no host de origem.

Execute os seguintes comandos no *host de destino*.

Passos

1. Importe o nó no host de destino.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

Exemplo de saída:

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.
You should run 'storagegrid node validate DC1-S3'
```

2. Valide a configuração do nó no novo host.

```
sudo storagegrid node validate DC1-S3
```

Exemplo de saída:

```
Confirming existence of node DC1-S3... PASSED
Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
DC1-S3... PASSED
Checking for duplication of unique values... PASSED
```

3. Caso ocorra algum erro de validação, resolva-o antes de iniciar o nó migrado.

Para obter informações sobre solução de problemas, consulte as instruções de instalação do StorageGRID para seu sistema operacional Linux.

- ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
- ["Instalar o StorageGRID no Ubuntu ou Debian"](#)

Iniciar nó migrado

Depois de validar o nó migrado, inicie-o executando um comando no *host de destino*.

Passos

1. Inicie o nó no novo host.

```
sudo storagegrid node start DC1-S3
```

2. Sign in no Grid Manager e verifique se o status do nó está verde, sem alerta.



Verificar se o status do nó está verde garante que o nó migrado foi totalmente reiniciado e reingressado na rede. Se o status não estiver verde, não migre nenhum nó adicional para que você não tenha mais de um nó fora de serviço.

3. Se você não conseguir acessar o Grid Manager, aguarde 10 minutos e execute o seguinte comando:

```
sudo storagegrid node status _node-name
```

Confirme se o nó migrado tem um estado de execução em execução.

VMware: Configurar máquina virtual para reinicialização automática

Se a máquina virtual não reiniciar após o VMware vSphere Hypervisor ser reiniciado, talvez seja necessário configurar a máquina virtual para reinicialização automática.

Você deve executar este procedimento se notar que uma máquina virtual não reinicia enquanto você estiver recuperando um nó de grade ou executando outro procedimento de manutenção.

Passos

1. Na árvore do VMware vSphere Client, selecione a máquina virtual que não foi iniciada.
2. Clique com o botão direito do mouse na máquina virtual e selecione **Ligar**.
3. Configure o VMware vSphere Hypervisor para reiniciar a máquina virtual automaticamente no futuro.

Recuperar ou substituir nós

Avisos e considerações para recuperação de nós de rede

Se um nó da grade falhar, você deve recuperá-lo o mais rápido possível. Você deve revisar todos os avisos e considerações para recuperação de nós antes de começar.



StorageGRID é um sistema distribuído composto por vários nós trabalhando em conjunto. Não use snapshots de disco para restaurar nós de grade. Em vez disso, consulte os procedimentos de recuperação e manutenção para cada tipo de nó.



Se um site StorageGRID inteiro falhar, entre em contato com o suporte técnico. O suporte técnico trabalhará com você para desenvolver e executar um plano de recuperação de site que maximize a quantidade de dados recuperados e atenda aos seus objetivos comerciais. Ver ["Como o suporte técnico recupera um site"](#).

Alguns dos motivos para recuperar um nó de rede com falha o mais rápido possível incluem o seguinte:

- Um nó de grade com falha pode reduzir a redundância dos dados do sistema e do objeto, deixando você vulnerável ao risco de perda permanente de dados se outro nó falhar.
- Um nó de rede com falha pode afetar a eficiência das operações diárias.
- Um nó de grade com falha pode reduzir sua capacidade de monitorar as operações do sistema.
- Um nó de grade com falha pode causar um erro interno do servidor 500 se regras rígidas de ILM estiverem em vigor.
- Se um nó da grade não for recuperado prontamente, o tempo de recuperação poderá aumentar. Por exemplo, podem surgir filas que precisam ser limpas antes que a recuperação seja concluída.

Siga sempre o procedimento de recuperação para o tipo específico de nó de grade que você está recuperando. Os procedimentos de recuperação variam para nós de administração primários ou não primários, nós de gateway, nós de dispositivos e nós de armazenamento.

Pré-condições para recuperação de nós de grade

Todas as seguintes condições são assumidas ao recuperar nós de grade:

- O hardware físico ou virtual com falha foi substituído e configurado.
- A versão do instalador do dispositivo StorageGRID no dispositivo de substituição corresponde à versão do software do seu sistema StorageGRID, conforme descrito em ["Verifique e atualize a versão do instalador do StorageGRID Appliance"](#).
- Se você estiver recuperando um nó de grade diferente do nó de administração primário, haverá conectividade entre o nó de grade que está sendo recuperado e o nó de administração primário.
- Se estiver recuperando um nó de armazenamento do dispositivo, você deverá especificar o mesmo tipo de armazenamento do dispositivo original (combinado, somente metadados ou somente dados) durante a instalação do dispositivo. Se você especificar um tipo de armazenamento diferente, a recuperação falhará e exigirá a reinstalação do dispositivo com o tipo de armazenamento correto especificado.

Ordem de recuperação do nó se um servidor que hospeda mais de um nó de grade falhar

Se um servidor que hospeda mais de um nó de grade falhar, você poderá recuperar os nós em qualquer ordem. Entretanto, se o servidor com falha estiver hospedando o nó de administração principal, você deverá recuperar esse nó primeiro. Recuperar primeiro o nó de administração primário evita que outras recuperações de nós sejam interrompidas enquanto aguardam para entrar em contato com o nó de administração primário.

Endereços IP para nós recuperados

Não tente recuperar um nó usando um endereço IP que esteja atualmente atribuído a qualquer outro nó. Ao implantar o novo nó, use o endereço IP atual do nó com falha ou um endereço IP não utilizado.

Se você usar um novo endereço IP para implantar o novo nó e depois recuperá-lo, o novo endereço IP continuará a ser usado para o nó recuperado. Se você quiser reverter para o endereço IP original, use a ferramenta Alterar IP após a conclusão da recuperação.

Reúna os materiais necessários para a recuperação dos nós da grade

Antes de executar procedimentos de manutenção, você deve garantir que possui os materiais necessários para recuperar um nó de rede com falha.

Item	Notas
Arquivo de instalação do StorageGRID	Se você precisar recuperar um nó de grade, você precisa baixe os arquivos de instalação do StorageGRID para sua plataforma. Observação: você não precisa baixar arquivos se estiver recuperando volumes de armazenamento com falha em um nó de armazenamento.
Laptop de serviço	O laptop de serviço deve ter o seguinte: • Porta de rede • Cliente SSH (por exemplo, PuTTY) • "Navegador da Web compatível"

Item	Notas
Pacote de Recuperação .zip arquivo	Obtenha uma cópia do Pacote de Recuperação mais recente .zip arquivo: <code>sgws-recovery-package-id-revision.zip</code> O conteúdo do .zip os arquivos são atualizados sempre que o sistema é modificado. Você será orientado a armazenar a versão mais recente do Pacote de Recuperação em um local seguro após fazer tais alterações. Use a cópia mais recente para se recuperar de falhas na rede. Se o nó de administração principal estiver operando normalmente, você poderá baixar o pacote de recuperação do Grid Manager. Selecione MANUTENÇÃO > Sistema > Pacote de recuperação. Se você não conseguir acessar o Grid Manager, poderá encontrar cópias criptografadas do Pacote de Recuperação em alguns Nós de Armazenamento que contêm o serviço ADC. Em cada nó de armazenamento, examine este local para o pacote de recuperação: <code>/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg</code> Use o Pacote de Recuperação com o maior número de revisão.
`Passwords.txt` arquivo	Contém as senhas necessárias para acessar os nós da grade na linha de comando. Incluído no Pacote de Recuperação.
Senha de provisionamento	A senha é criada e documentada quando o sistema StorageGRID é instalado pela primeira vez. A senha de provisionamento não está no <code>Passwords.txt</code> arquivo.
Documentação atual para sua plataforma	Acesse o site do fornecedor da plataforma para obter a documentação. Para as versões atuais suportadas da sua plataforma, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Baixe e extraia os arquivos de instalação do StorageGRID

Baixe o software e extraia os arquivos, a menos que você esteja ["recuperando volumes de armazenamento com falha em um nó de armazenamento"](#) .

Você deve usar a versão do StorageGRID que está atualmente em execução na grade.

Passos

1. Determine qual versão do software está instalada no momento. Na parte superior do Grid Manager, selecione o ícone de ajuda e selecione **Sobre**.
2. Vá para o ["Página de downloads da NetApp para StorageGRID"](#) .
3. Selecione a versão do StorageGRID que está sendo executada atualmente na grade.

As versões do software StorageGRID têm este formato: 11.x.y .

4. Sign in com o nome de usuário e a senha da sua conta NetApp .
5. Leia o Contrato de Licença do Usuário Final, marque a caixa de seleção e selecione **Aceitar e Continuar**.
6. Na coluna **Instalar StorageGRID** da página de download, selecione o .tgz ou .zip arquivo para sua plataforma.

A versão mostrada no arquivo de instalação deve corresponder à versão do software que está instalado no momento.

Use o .zip arquivo se você estiver executando o Windows.

Plataforma	Arquivo de instalação
Red Hat Enterprise Linux	StorageGRID-WebScale-version-RPM-uniqueID.zip StorageGRID-WebScale-version-RPM-uniqueID.tgz
Ubuntu ou Debian ou Appliances	StorageGRID-WebScale-version-DEB-uniqueID.zip StorageGRID-WebScale-version-DEB-uniqueID.tgz
VMware	StorageGRID-WebScale-version-VMware-uniqueID.zip StorageGRID-WebScale-version-VMware-uniqueID.tgz

7. Baixe e extraia o arquivo compactado.
8. Siga as etapas apropriadas para sua plataforma para escolher os arquivos necessários, com base na sua plataforma e em quais nós de grade você precisa recuperar.

Os caminhos listados na etapa para cada plataforma são relativos ao diretório de nível superior instalado pelo arquivo compactado.

9. Se você estiver recuperando um "[Sistema Red Hat Enterprise Linux](#)", selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID .
	Uma licença gratuita que não fornece nenhum direito de suporte para o produto.
	Pacote RPM para instalar as imagens do nó StorageGRID nos seus hosts RHEL.
	Pacote RPM para instalar o serviço de host StorageGRID em seus hosts RHEL.
Ferramenta de script de implantação	Descrição

Caminho e nome do arquivo	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID .
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID .
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único estiver ativado. Você também pode usar este script para integração do Ping Federate.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> roteiro.
	Exemplo de função e manual do Ansible para configurar hosts RHEL para implantação de contêiner StorageGRID . Você pode personalizar a função ou o manual conforme necessário.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado usando o Active Directory ou o Ping Federate.
	Um script auxiliar chamado pelo companheiro <code>storagegrid-ssoauth-azure.py</code> Script Python para executar interações SSO com o Azure.
	Esquemas de API para StorageGRID. Observação: antes de executar uma atualização, você pode usar esses esquemas para confirmar se qualquer código que você escreveu para usar as APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID , caso você não tenha um ambiente StorageGRID não produtivo para testes de compatibilidade de atualização.

1. Se você estiver recuperando um "[Sistema Ubuntu ou Debian](#)" , selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID .
	Um arquivo de licença NetApp não produtivo que você pode usar para testes e implantações de prova de conceito.
	Pacote DEB para instalar as imagens do nó StorageGRID em hosts Ubuntu ou Debian.
	Soma de verificação MD5 para o arquivo <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Pacote DEB para instalar o serviço de host StorageGRID em hosts Ubuntu ou Debian.
Ferramenta de script de implantação	Descrição
	Um script Python usado para automatizar a configuração de um sistema StorageGRID .
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID .
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único estiver ativado. Você também pode usar este script para integração do Ping Federate.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> roteiro.
	Exemplo de função e manual do Ansible para configurar hosts Ubuntu ou Debian para implantação de contêiner StorageGRID . Você pode personalizar a função ou o manual conforme necessário.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado usando o Active Directory ou o Ping Federate.

Caminho e nome do arquivo	Descrição
	Um script auxiliar chamado pelo companheiro <code>storagegrid-ssoauth-azure.py</code> Script Python para executar interações SSO com o Azure.
	Esquemas de API para StorageGRID. Observação: antes de executar uma atualização, você pode usar esses esquemas para confirmar se qualquer código que você escreveu para usar as APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID , caso você não tenha um ambiente StorageGRID não produtivo para testes de compatibilidade de atualização.

1. Se você estiver recuperando um "Sistema VMware" , selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Um arquivo de texto que descreve todos os arquivos contidos no arquivo de download do StorageGRID .
	Uma licença gratuita que não fornece nenhum direito de suporte para o produto.
	O arquivo de disco da máquina virtual que é usado como modelo para criar máquinas virtuais de nós de grade.
	O arquivo de modelo do Open Virtualization Format(.ovf) e arquivo de manifesto(.mf) para implantar o nó de administração primário.
	O arquivo de modelo(.ovf) e arquivo de manifesto(.mf) para implantar nós administrativos não primários.
	O arquivo de modelo(.ovf) e arquivo de manifesto(.mf) para implantar nós de gateway.
	O arquivo de modelo(.ovf) e arquivo de manifesto(.mf) para implantar nós de armazenamento baseados em máquina virtual.
Ferramenta de script de implantação	Descrição

Caminho e nome do arquivo	Descrição
	Um script de shell Bash usado para automatizar a implantação de nós de grade virtual.
	Um exemplo de arquivo de configuração para uso com o <code>deploy-vsphere-ovftool.sh</code> roteiro.
	Um script Python usado para automatizar a configuração de um sistema StorageGRID .
	Um script Python usado para automatizar a configuração de dispositivos StorageGRID .
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado. Você também pode usar este script para integração do Ping Federate.
	Um exemplo de arquivo de configuração para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um arquivo de configuração em branco para uso com o <code>configure-storagegrid.py</code> roteiro.
	Um exemplo de script Python que você pode usar para fazer login na API de gerenciamento de grade quando o logon único (SSO) estiver habilitado usando o Active Directory ou o Ping Federate.
	Um script auxiliar chamado pelo companheiro <code>storagegrid-ssoauth-azure.py</code> Script Python para executar interações SSO com o Azure.
	Esquemas de API para StorageGRID. Observação: antes de executar uma atualização, você pode usar esses esquemas para confirmar se qualquer código que você escreveu para usar as APIs de gerenciamento do StorageGRID será compatível com a nova versão do StorageGRID , caso você não tenha um ambiente StorageGRID não produtivo para testes de compatibilidade de atualização.

1. Se você estiver recuperando um sistema baseado em dispositivo StorageGRID , selecione os arquivos apropriados.

Caminho e nome do arquivo	Descrição
	Pacote DEB para instalar as imagens do nó StorageGRID em seus dispositivos.
	Soma de verificação MD5 para o arquivo /debs/storagegridwebscale-images-version-SHA.deb .



Para instalação do dispositivo, esses arquivos só são necessários se você precisar evitar tráfego de rede. O dispositivo pode baixar os arquivos necessários do nó de administração principal.

Selecione o procedimento de recuperação do nó

Você deve selecionar o procedimento de recuperação correto para o tipo de nó que falhou.

Nó de grade	Procedimento de recuperação
Mais de um nó de armazenamento	Entre em contato com o suporte técnico. Se mais de um nó de armazenamento falhar, o suporte técnico deverá auxiliar na recuperação para evitar inconsistências no banco de dados que possam levar à perda de dados. Um procedimento de recuperação do site pode ser necessário. "Como o suporte técnico recupera um site"
Um único nó de armazenamento	O procedimento de recuperação do nó de armazenamento depende do tipo e da duração da falha. "Recuperar de falhas do nó de armazenamento"
Nó de administração	O procedimento do nó administrativo depende se você precisa recuperar o nó administrativo primário ou um nó administrativo não primário. "Recuperar de falhas do nó de administração"
Nó de gateway	"Recuperar de falhas do nó de gateway"
Nó de arquivo	"Recuperar de falhas do nó de arquivamento (site de documentação do StorageGRID 11.8)"



Se um servidor que hospeda mais de um nó de grade falhar, você poderá recuperar os nós em qualquer ordem. Entretanto, se o servidor com falha estiver hospedando o nó de administração principal, você deverá recuperar esse nó primeiro. Recuperar primeiro o nó de administração primário evita que outras recuperações de nós sejam interrompidas enquanto aguardam para entrar em contato com o nó de administração primário.

Recuperar de falhas do nó de armazenamento

Recuperar de falhas do nó de armazenamento

O procedimento para recuperar um nó de armazenamento com falha depende do tipo de falha e do tipo de nó de armazenamento que falhou.

Use esta tabela para selecionar o procedimento de recuperação para um nó de armazenamento com falha.

Emitir	Ação	Notas
- Mais de um nó de armazenamento falhou. - Um segundo nó de armazenamento falhou menos de 15 dias após uma falha ou recuperação do nó de armazenamento. Isso inclui o caso em que um nó de armazenamento falha enquanto a recuperação de outro nó de armazenamento ainda está em andamento.	Entre em contato com o suporte técnico.	Recuperar mais de um nó de armazenamento (ou mais de um nó de armazenamento em 15 dias) pode afetar a integridade do banco de dados Cassandra, o que pode causar perda de dados. O suporte técnico pode determinar quando é seguro iniciar a recuperação de um segundo nó de armazenamento. Observação: se mais de um nó de armazenamento que contém o serviço ADC falhar em um site, você perderá todas as solicitações de serviço de plataforma pendentes para esse site.
Mais de um nó de armazenamento em um site falhou ou um site inteiro falhou.	Entre em contato com o suporte técnico. Pode ser necessário executar um procedimento de recuperação do site.	O suporte técnico avaliará sua situação e desenvolverá um plano de recuperação. Ver "Como o suporte técnico recupera um site" .
Um nó de armazenamento do dispositivo falhou.	"Recuperar nó de armazenamento do dispositivo"	O procedimento de recuperação para nós de armazenamento do dispositivo é o mesmo para todas as falhas.
Um ou mais volumes de armazenamento falharam, mas a unidade do sistema está intacta	"Recuperar de falha de volume de armazenamento onde a unidade do sistema está intacta"	Este procedimento é usado para nós de armazenamento baseados em software.

Emitir	Ação	Notas
A unidade do sistema falhou.	"Recuperar de falha de unidade do sistema"	O procedimento de substituição do nó depende da plataforma de implantação e se algum volume de armazenamento também falhou.



Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. Os reparos ocorrem automaticamente assim que os serviços relacionados ou necessários são iniciados. Você pode notar uma saída de script que menciona "reaper" ou "Cassandra repair". Se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

Recuperar nó de armazenamento do dispositivo

Avisos para recuperação de nós de armazenamento do dispositivo

O procedimento para recuperar um nó de armazenamento do dispositivo StorageGRID com falha é o mesmo, independentemente de você estar se recuperando da perda da unidade do sistema ou da perda apenas de volumes de armazenamento.



Se mais de um nó de armazenamento falhar (ou estiver offline), entre em contato com o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.



Se esta for a segunda falha do nó de armazenamento em menos de 15 dias após uma falha ou recuperação do nó de armazenamento, entre em contato com o suporte técnico. Reconstruir o Cassandra em dois ou mais nós de armazenamento em 15 dias pode resultar em perda de dados.



Se mais de um nó de armazenamento em um site falhar, um procedimento de recuperação do site poderá ser necessário. Ver ["Como o suporte técnico recupera um site"](#).



Se as regras do ILM estiverem configuradas para armazenar apenas uma cópia replicada e a cópia existir em um volume de armazenamento que falhou, você não poderá recuperar o objeto.



Para procedimentos de manutenção de hardware, como instruções para substituir um controlador ou reinstalar o SANtricity OS, consulte o ["instruções de manutenção para seu aparelho de armazenamento"](#).

Preparar o nó de armazenamento do dispositivo para reinstalação

Ao recuperar um nó de armazenamento do dispositivo, você deve primeiro preparar o dispositivo para a reinstalação do software StorageGRID.

Passos

1. Efetue login no nó de armazenamento com falha:
 - a. Digite o seguinte comando: `ssh admin@grid_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. Prepare o nó de armazenamento do dispositivo para a instalação do software StorageGRID .
`sgareinstall`
3. Quando solicitado a continuar, digite: `y`

O dispositivo é reinicializado e sua sessão SSH termina. Geralmente, leva cerca de 5 minutos para que o instalador do StorageGRID Appliance fique disponível, embora em alguns casos você possa precisar esperar até 30 minutos.



Não tente acelerar a reinicialização desligando e ligando novamente ou reiniciando o aparelho de qualquer outra forma. Você pode interromper atualizações automáticas de BIOS, BMC ou outros firmwares.

O nó de armazenamento do dispositivo StorageGRID é redefinido e os dados no nó de armazenamento não ficam mais acessíveis. Os endereços IP configurados durante o processo de instalação original devem permanecer intactos; no entanto, é recomendável que você confirme isso quando o procedimento for concluído.

Após executar o `sgareinstall` comando, todas as contas, senhas e chaves SSH provisionadas StorageGRID são removidas e novas chaves de host são geradas.

Iniciar instalação do dispositivo StorageGRID

Para instalar o StorageGRID em um nó de armazenamento do dispositivo, use o instalador do dispositivo StorageGRID , que está incluído no dispositivo.

Antes de começar

- O dispositivo foi instalado em um rack, conectado às suas redes e ligado.
- Links de rede e endereços IP foram configurados para o dispositivo usando o StorageGRID Appliance Installer.
- Você sabe o endereço IP do nó de administração principal da grade StorageGRID .
- Todas as sub-redes da Rede de Grade listadas na página Configuração de IP do Instalador do Dispositivo StorageGRID foram definidas na Lista de Sub-redes da Rede de Grade no Nó de Administração primário.
- Você concluiu essas tarefas de pré-requisito seguindo as instruções de instalação do seu dispositivo de armazenamento. Ver "[Início rápido para instalação de hardware](#)".
- Você está usando um "[navegador da web compatível](#)".
- Você conhece um dos endereços IP atribuídos ao controlador de computação no dispositivo. Você pode usar o endereço IP da Rede de Administração (porta de gerenciamento 1 no controlador), da Rede de Grade ou da Rede de Cliente.

Sobre esta tarefa

Para instalar o StorageGRID em um nó de armazenamento do dispositivo:

- Especifique ou confirme o endereço IP do nó de administração principal e o nome do host (nome do sistema) do nó.
- Você inicia a instalação e aguarda enquanto os volumes são configurados e o software é instalado.



Ao recuperar um nó de armazenamento do dispositivo, reinstale-o com o mesmo tipo de armazenamento do dispositivo original (combinado, somente metadados ou somente dados). Se você especificar um tipo de armazenamento diferente, a recuperação falhará e exigirá a reinstalação do dispositivo com o tipo de armazenamento correto especificado.

- No meio do processo, a instalação é pausada. Para retomar a instalação, você deve entrar no Grid Manager e configurar o nó de armazenamento pendente como um substituto para o nó com falha.
- Após configurar o nó, o processo de instalação do dispositivo é concluído e o dispositivo é reinicializado.

Passos

1. Abra um navegador e insira um dos endereços IP do controlador de computação no dispositivo.

`https://Controller_IP:8443`

A página inicial do instalador do dispositivo StorageGRID é exibida.

2. Na seção Conexão do nó de administração principal, determine se você precisa especificar o endereço IP para o nó de administração principal.

O instalador do dispositivo StorageGRID pode descobrir esse endereço IP automaticamente, supondo que o nó de administração primário, ou pelo menos um outro nó de grade com ADMIN_IP configurado, esteja presente na mesma sub-rede.

3. Se este endereço IP não for exibido ou você precisar alterá-lo, especifique o endereço:

Opção	Passos
Entrada manual de IP	a. Desmarque a caixa de seleção Habilitar descoberta do nó de administração. b. Digite o endereço IP manualmente. c. Clique em Salvar. d. Aguarde enquanto o estado da conexão para o novo endereço IP se torna "pronto".
Descoberta automática de todos os nós administrativos primários conectados	a. Marque a caixa de seleção Habilitar descoberta do nó de administração. b. Na lista de endereços IP descobertos, selecione o nó de administração principal da grade onde este nó de armazenamento do dispositivo será implantado. c. Clique em Salvar. d. Aguarde enquanto o estado da conexão para o novo endereço IP se torna "pronto".

4. No campo **Nome do nó**, insira o mesmo nome de host (nome do sistema) que foi usado para o nó que você está recuperando e clique em **Salvar**.

5. Na seção Instalação, confirme se o estado atual é "Pronto para iniciar a instalação de *node name* na grade com o nó de administração primário *admin_ip*" e que o botão **Iniciar instalação** esteja habilitado.

Se o botão **Iniciar instalação** não estiver habilitado, talvez seja necessário alterar a configuração de rede ou as configurações de porta. Para obter instruções, consulte as instruções de manutenção do seu aparelho.

6. Na página inicial do StorageGRID Appliance Installer, clique em **Iniciar instalação**.

NetApp® StorageGRID® Appliance Installer

[Home](#)[Configure Networking ▾](#)[Configure Hardware ▾](#)[Monitor Installation](#)[Advanced ▾](#)

Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node discovery☐

Primary Admin Node IP

Connection state

Connection to 172.16.4.210 ready

[Cancel](#)[Save](#)

Node name

Node name

[Cancel](#)[Save](#)

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

[Start Installation](#)

O estado atual muda para "A instalação está em andamento" e a página Instalação do monitor é exibida.



Se precisar acessar a página de instalação do monitor manualmente, clique em **Instalação do monitor** na barra de menu. Ver "[Monitorar a instalação do aparelho](#)".

Monitorar a instalação do dispositivo StorageGRID

O instalador do dispositivo StorageGRID fornece status até que a instalação seja concluída. Quando a instalação do software estiver concluída, o dispositivo será reinicializado.

Passos

1. Para monitorar o progresso da instalação, clique em **Monitorar instalação** na barra de menu.

A página Instalação do Monitor mostra o progresso da instalação.

Monitor Installation

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller		Complete	
Clear existing configuration		Complete	
Configure volumes		Creating volume StorageGRID-obj-00	
Configure host settings		Pending	
2. Install OS			Pending
3. Install StorageGRID			Pending
4. Finalize installation			Pending

A barra de status azul indica qual tarefa está em andamento. Barras de status verdes indicam tarefas que foram concluídas com sucesso.



O instalador garante que as tarefas concluídas em uma instalação anterior não sejam executadas novamente. Se você estiver executando uma instalação novamente, todas as tarefas que não precisam ser executadas novamente serão exibidas com uma barra de status verde e o status "Ignorada".

2. Revise o progresso dos dois primeiros estágios da instalação.

- **1. Configurar armazenamento**

Durante esta etapa, o instalador se conecta ao controlador de armazenamento, limpa qualquer configuração existente, se comunica com o SANtricity OS para configurar volumes e define as configurações do host.

- **2. Instalar SO**

Durante esta etapa, o instalador copia a imagem base do sistema operacional do StorageGRID para o dispositivo.

3. Continue monitorando o progresso da instalação até que o estágio **Instalar StorageGRID** seja pausado e uma mensagem apareça no console incorporado solicitando que você aprove este nó no Nó de administração usando o Grid Manager.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Vá para "[Selecione Iniciar recuperação para configurar o nó de armazenamento do dispositivo](#)".

Selecione Iniciar recuperação para configurar o nó de armazenamento do dispositivo

Você deve selecionar Iniciar recuperação no Grid Manager para configurar um nó de armazenamento do dispositivo como substituto do nó com falha.

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.

- Você implantou um nó de armazenamento do dispositivo de recuperação.
- Você tem a data de início de quaisquer trabalhos de reparo para dados codificados para eliminação.
- Você verificou que o nó de armazenamento não foi reconstruído nos últimos 15 dias.

Passos

1. No Grid Manager, selecione **MANUTENÇÃO > Tarefas > Recuperação**.
2. Selecione o nó da grade que você deseja recuperar na lista Nós Pendentes.

Os nós aparecem na lista depois de falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Digite a **senha de provisionamento**.
4. Clique em **Iniciar recuperação**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search Q				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

Start Recovery

5. Monitore o progresso da recuperação na tabela Nó da grade em recuperação.

Quando o nó da grade atingir o estágio "Aguardando etapas manuais", vá para o próximo tópico e execute as etapas manuais para remontar e reformatar os volumes de armazenamento do dispositivo.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT		Waiting For Manual Steps

Reset



A qualquer momento durante a recuperação, você pode clicar em **Redefinir** para iniciar uma nova recuperação. Uma caixa de diálogo aparece, indicando que o nó ficará em um estado indeterminado se você redefinir o procedimento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se desejar tentar a recuperação novamente após redefinir o procedimento, você deve restaurar o nó do dispositivo para um estado pré-instalado executando `sgareinstall` no nó.

Remonte e reformate os volumes de armazenamento do dispositivo (etapas manuais)

Você deve executar manualmente dois scripts para remontar os volumes de armazenamento preservados e reformatar quaisquer volumes de armazenamento com falha. O primeiro script remonta volumes que estão formatados corretamente como volumes de armazenamento StorageGRID. O segundo script reformata todos os volumes desmontados, reconstrói o banco de dados Cassandra, se necessário, e inicia os serviços.

Antes de começar

- Você já substituiu o hardware de todos os volumes de armazenamento com falha que você sabe que precisam ser substituídos.

Executando o `sn-remount-volumes` O script pode ajudar você a identificar volumes de armazenamento adicionais com falha.

- Você verificou se o descomissionamento do nó de armazenamento não está em andamento ou pausou o procedimento de descomissionamento do nó. (No Grid Manager, selecione **MANUTENÇÃO > Tarefas > Desativação.**)
- Você verificou que não há nenhuma expansão em andamento. (No Grid Manager, selecione **MANUTENÇÃO > Tarefas > Expansão.**)



Entre em contato com o suporte técnico se mais de um nó de armazenamento estiver offline ou se um nó de armazenamento nesta grade tiver sido reconstruído nos últimos 15 dias. Não execute o `sn-recovery-postinstall.sh` roteiro. Reconstruir o Cassandra em dois ou mais nós de armazenamento com intervalo de 15 dias entre eles pode resultar em perda de dados.

Sobre esta tarefa

Para concluir este procedimento, execute estas tarefas de alto nível:

- Efetue login no nó de armazenamento recuperado.
- Execute o `sn-remount-volumes` script para remontar volumes de armazenamento formatados corretamente. Quando esse script é executado, ele faz o seguinte:
 - Monta e desmonta cada volume de armazenamento para reproduzir o diário XFS.
 - Executa uma verificação de consistência do arquivo XFS.
 - Se o sistema de arquivos for consistente, determina se o volume de armazenamento é um volume de armazenamento StorageGRID formatado corretamente.
 - Se o volume de armazenamento estiver formatado corretamente, remonta o volume de armazenamento. Todos os dados existentes no volume permanecem intactos.
- Revise a saída do script e resolva quaisquer problemas.
- Execute o `sn-recovery-postinstall.sh` roteiro. Quando esse script é executado, ele faz o seguinte.



Não reinicie um nó de armazenamento durante a recuperação antes de executar `sn-recovery-postinstall.sh` (etapa 4) para reformatar os volumes de armazenamento com falha e restaurar os metadados do objeto. Reiniciando o nó de armazenamento antes `sn-recovery-postinstall.sh` conclui causa erros nos serviços que tentam iniciar e faz com que os nós do dispositivo StorageGRID saiam do modo de manutenção.

- Reformata quaisquer volumes de armazenamento que o `sn-remount-volumes` o script não pôde ser montado ou foi encontrado com formato incorreto.



Se um volume de armazenamento for reformatado, todos os dados contidos nesse volume serão perdidos. Você deve executar um procedimento adicional para restaurar dados de objetos de outros locais na grade, supondo que as regras do ILM foram configuradas para armazenar mais de uma cópia de objeto.

- Reconstrói o banco de dados Cassandra no nó, se necessário.
- Inicia os serviços no nó de armazenamento.

Passos

1. Efetue login no nó de armazenamento recuperado:

- Digite o seguinte comando: `ssh admin@grid_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 primeiro script para remontar quaisquer volumes de armazenamento formatados corretamente.



Se todos os volumes de armazenamento forem novos e precisarem ser formatados, ou se todos os volumes de armazenamento falharem, você pode pular esta etapa e executar o segundo script para reformatar todos os volumes de armazenamento desmontados.

- Execute o script: `sn-remount-volumes`

Este script pode levar horas para ser executado em volumes de armazenamento que contêm dados.

b. Conforme o script é executado, revise a saída e responda a quaisquer prompts.



Conforme necessário, você pode usar o `tail -f` comando para monitorar o conteúdo do arquivo de log do script(`/var/local/log/sn-remount-volumes.log`). O arquivo de log contém informações mais detalhadas do que a saída da linha de comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

===== Device /dev/sdb =====
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

===== Device /dev/sdc =====
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

===== Device /dev/sdd =====
Mount and unmount device /dev/sdd and checking file system
consistency:
```

```

Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

===== Device /dev/sde =====
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.

```

No exemplo de saída, um volume de armazenamento foi remontado com sucesso e três volumes de armazenamento apresentaram erros.

- `/dev/sdb` passou na verificação de consistência do sistema de arquivos XFS e tinha uma estrutura de volume válida, então foi remontado com sucesso. Os dados em dispositivos remontados pelo script são preservados.
- `/dev/sdc` falhou na verificação de consistência do sistema de arquivos XFS porque o volume de armazenamento era novo ou corrompido.
- `/dev/sdd` não pôde ser montado porque o disco não foi inicializado ou o superbloco do disco estava corrompido. Quando o script não consegue montar um volume de armazenamento, ele pergunta se você deseja executar a verificação de consistência do sistema de arquivos.

- Se o volume de armazenamento estiver anexado a um novo disco, responda **N** ao prompt. Você não precisa verificar o sistema de arquivos em um novo disco.
- Se o volume de armazenamento estiver anexado a um disco existente, responda **S** ao prompt. Você pode usar os resultados da verificação do sistema de arquivos para determinar a origem da corrupção. Os resultados são salvos no `/var/local/log/sn-remount-volumes.log` arquivo de log.
- `/dev/sde` passou na verificação de consistência do sistema de arquivos XFS e tinha uma estrutura de volume válida; no entanto, o ID do nó LDR no ``volID` o arquivo não corresponde ao ID deste nó de armazenamento (o configured LDR `noid` exibido na parte superior). Esta mensagem indica que este volume pertence a outro nó de armazenamento.

3. Revise a saída do script e resolva quaisquer problemas.



Se um volume de armazenamento falhar na verificação de consistência do sistema de arquivos XFS ou não puder ser montado, revise cuidadosamente as mensagens de erro na saída. Você deve entender as implicações de executar o `sn-recovery-postinstall.sh` roteiro nesses volumes.

- Verifique se os resultados incluem uma entrada para todos os volumes esperados. Se algum volume não estiver listado, execute o script novamente.
- Revise as mensagens de todos os dispositivos montados. Certifique-se de que não haja erros indicando que um volume de armazenamento não pertence a este nó de armazenamento.

No exemplo, a saída para `/dev/sde` inclui a seguinte mensagem de erro:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```



Se um volume de armazenamento for relatado como pertencente a outro nó de armazenamento, entre em contato com o suporte técnico. Se você executar o `sn-recovery-postinstall.sh` script, o volume de armazenamento será reformatado, o que pode causar perda de dados.

- Se algum dispositivo de armazenamento não puder ser montado, anote o nome do dispositivo e repare ou substitua-o.



Você deve reparar ou substituir quaisquer dispositivos de armazenamento que não puderam ser montados.

Você usará o nome do dispositivo para consultar o ID do volume, que é uma entrada necessária ao executar o `repair-data` script para restaurar dados do objeto para o volume (o próximo procedimento).

- Após reparar ou substituir todos os dispositivos não montáveis, execute o `sn-remount-volumes` script novamente para confirmar que todos os volumes de armazenamento que podem ser remontados foram remontados.



Se um volume de armazenamento não puder ser montado ou estiver formatado incorretamente e você continuar para a próxima etapa, o volume e todos os dados nele contidos serão excluídos. Se você tiver duas cópias dos dados do objeto, terá apenas uma cópia até concluir o próximo procedimento (restaurar os dados do objeto).



Não execute o `sn-recovery-postinstall.sh` script se você acredita que os dados restantes em um volume de armazenamento com falha não podem ser reconstruídos de outro lugar na grade (por exemplo, se sua política de ILM usa uma regra que faz apenas uma cópia ou se os volumes falharam em vários nós). Em vez disso, entre em contato com o suporte técnico para determinar como recuperar seus dados.

4. Execute o `sn-recovery-postinstall.sh` roteiro: `sn-recovery-postinstall.sh`

Este script reformata todos os volumes de armazenamento que não puderam ser montados ou que foram encontrados formatados incorretamente; reconstrói o banco de dados Cassandra no nó, se necessário; e inicia os serviços no nó de armazenamento.

Esteja ciente do seguinte:

- O script pode levar horas para ser executado.
- Em geral, você deve deixar a sessão SSH em paz enquanto o script estiver em execução.
- Não pressione **Ctrl+C** enquanto a sessão SSH estiver ativa.
- O script será executado em segundo plano se ocorrer uma interrupção na rede e encerrar a sessão SSH, mas você pode visualizar o progresso na página Recuperação.
- Se o nó de armazenamento usar o serviço RSM, o script poderá parecer travar por 5 minutos enquanto os serviços do nó são reiniciados. Esse atraso de 5 minutos é esperado sempre que o serviço RSM é inicializado pela primeira vez.



O serviço RSM está presente em nós de armazenamento que incluem o serviço ADC.



Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. Os reparos ocorrem automaticamente assim que os serviços relacionados ou necessários são iniciados. Você pode notar uma saída de script que menciona "reaper" ou "Cassandra repair". Se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

5. Como o `sn-recovery-postinstall.sh` o script é executado, monitore a página Recuperação no Grid Manager.

A barra de progresso e a coluna Estágio na página Recuperação fornecem um status de alto nível do `sn-recovery-postinstall.sh` roteiro.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
No results found.				

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT		Recovering Cassandra

6. Depois do `sn-recovery-postinstall.sh` o script iniciou serviços no nó, você pode restaurar dados do objeto em qualquer volume de armazenamento que foi formatado pelo script.

O script pergunta se você deseja usar o processo de restauração de volume do Grid Manager.

- Na maioria dos casos, você deve "[restaurar dados de objetos usando o Grid Manager](#)". Responder `y` para usar o Grid Manager.
- Em casos raros, como quando instruído pelo suporte técnico, ou quando você sabe que o nó de substituição tem menos volumes disponíveis para armazenamento de objetos do que o nó original, você deve "[restaurar dados do objeto manualmente](#)" usando o `repair-data` roteiro. Se um desses casos se aplicar, responda `n`.



Se você responder `n` para usar o processo de restauração de volume do Grid Manager (restaurar dados do objeto manualmente):

- Não é possível restaurar dados de objetos usando o Grid Manager.
- Você pode monitorar o progresso dos trabalhos de restauração manual usando o Grid Manager.

Após fazer sua seleção, o script é concluído e as próximas etapas para recuperar os dados do objeto são mostradas. Depois de revisar essas etapas, pressione qualquer tecla para retornar à linha de comando.

Restaurar dados do objeto para o volume de armazenamento do dispositivo

Após recuperar volumes de armazenamento para o nó de armazenamento do dispositivo, você pode restaurar os dados de objeto replicados ou codificados para eliminação que foram perdidos quando o nó de armazenamento falhou.

Qual procedimento devo usar?

Sempre que possível, restaure os dados do objeto usando a página **Restauração de volume** no Grid Manager.

- Se os volumes estiverem listados em **MANUTENÇÃO > Restauração de volume > Nós a serem restaurados**, restaure os dados do objeto usando o "[Página de restauração de volume no Grid Manager](#)".

- Se os volumes não estiverem listados em **MANUTENÇÃO > Restauração de volume > Nós para restaurar**, siga as etapas abaixo para usar o `repair-data` script para restaurar dados do objeto.

Se o nó de armazenamento recuperado contiver menos volumes do que o nó que está substituindo, você deverá usar o `repair-data` roteiro.



O script `repair-data` está obsoleto e será removido em uma versão futura. Quando possível, use o "[Procedimento de restauração de volume no Grid Manager](#)".

Use o `repair-data` script para restaurar dados de objetos

Antes de começar

- Você confirmou que o nó de armazenamento recuperado tem um estado de conexão de **Conectado***  na aba ***NÓS > Visão geral** no Gerenciador de grade.

Sobre esta tarefa

Dados de objetos podem ser restaurados de outros nós de armazenamento ou de um pool de armazenamento em nuvem, supondo que as regras de ILM da grade tenham sido configuradas de forma que cópias de objetos estejam disponíveis.

Observe o seguinte:

- Se uma regra de ILM foi configurada para armazenar apenas uma cópia replicada e essa cópia existia em um volume de armazenamento que falhou, você não poderá recuperar o objeto.
- Se a única cópia restante de um objeto estiver em um Cloud Storage Pool, o StorageGRID deverá emitir várias solicitações ao ponto de extremidade do Cloud Storage Pool para restaurar os dados do objeto. Antes de executar este procedimento, entre em contato com o suporte técnico para obter ajuda na estimativa do tempo de recuperação e dos custos associados.

Sobre o `repair-data` roteiro

Para restaurar dados do objeto, execute o `repair-data` roteiro. Este script inicia o processo de restauração de dados do objeto e trabalha com a varredura do ILM para garantir que as regras do ILM sejam atendidas.

Selecione **Dados replicados** ou **Dados codificados por eliminação (EC)** abaixo para aprender as diferentes opções para `repair-data` script, com base no fato de você estar restaurando dados replicados ou dados codificados para eliminação. Se precisar restaurar ambos os tipos de dados, você deverá executar ambos os conjuntos de comandos.



Para mais informações sobre o `repair-data` script, digite `repair-data --help` da linha de comando do nó de administração primário.



O script `repair-data` está obsoleto e será removido em uma versão futura. Quando possível, use o "[Procedimento de restauração de volume no Grid Manager](#)".

Dados replicados

Dois comandos estão disponíveis para restaurar dados replicados, dependendo se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Você pode rastrear reparos de dados replicados com este comando:

```
repair-data show-replicated-repair-status
```

Dados codificados por apagamento (EC)

Dois comandos estão disponíveis para restaurar dados codificados para eliminação, dependendo se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Você pode rastrear reparos de dados codificados para eliminação com este comando:

```
repair-data show-ec-repair-status
```



Os reparos de dados codificados para eliminação podem começar enquanto alguns nós de armazenamento estão offline. Entretanto, se todos os dados codificados para eliminação não puderem ser contabilizados, o reparo não poderá ser concluído. O reparo será concluído depois que todos os nós estiverem disponíveis.



O trabalho de reparo do EC reserva temporariamente uma grande quantidade de armazenamento. Alertas de armazenamento podem ser acionados, mas serão resolvidos quando o reparo for concluído. Se não houver armazenamento suficiente para a reserva, o trabalho de reparo do EC falhará. As reservas de armazenamento são liberadas quando o trabalho de reparo do EC é concluído, independentemente de o trabalho ter falhado ou sido bem-sucedido.

Encontre o nome do host para o nó de armazenamento

1. Efetue login no nó de administração principal:

- Digite o seguinte comando: `ssh admin@primary_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. Use o `/etc/hosts` arquivo para encontrar o nome do host do nó de armazenamento para os volumes de armazenamento restaurados. Para ver uma lista de todos os nós na grade, digite o seguinte: `cat`

/etc/hosts.

Reparar dados se todos os volumes falharem

Se todos os volumes de armazenamento falharem, repare o nó inteiro. Siga as instruções para **dados replicados**, **dados com codificação de eliminação (EC)** ou ambos, dependendo se você usa dados replicados, dados com codificação de eliminação (EC) ou ambos.

Se apenas alguns volumes falharam, vá para [Reparar dados se apenas alguns volumes falharam](#).



Você não pode correr `repair-data` operações para mais de um nó ao mesmo tempo. Para recuperar vários nós, entre em contato com o suporte técnico.

Dados replicados

Se sua grade incluir dados replicados, use o `repair-data start-replicated-node-repair` comando com o `--nodes` opção, onde `--nodes` é o nome do host (nome do sistema) para reparar todo o nó de armazenamento.

Este comando repara os dados replicados em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Conforme os dados do objeto são restaurados, o alerta **Objetos Perdidos** é acionado se o sistema StorageGRID não conseguir localizar os dados do objeto replicados. Alertas podem ser disparados em nós de armazenamento em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Ver "[Investigar objetos perdidos](#)".

Dados codificados por apagamento (EC)

Se sua grade contiver dados codificados por eliminação, use o `repair-data start-ec-node-repair` comando com o `--nodes` opção, onde `--nodes` é o nome do host (nome do sistema) para reparar todo o nó de armazenamento.

Este comando repara os dados codificados para eliminação em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

A operação retorna um valor único `repair ID` que identifica isso `repair_data` operação. Use isto `repair ID` para acompanhar o progresso e o resultado do `repair_data` operação. Nenhum outro feedback é retornado quando o processo de recuperação é concluído.

Os reparos de dados codificados para eliminação podem começar enquanto alguns nós de armazenamento estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Reparar dados se apenas alguns volumes falharam

Se apenas alguns volumes falharam, repare os volumes afetados. Siga as instruções para **dados replicados**, **dados com codificação de eliminação (EC)** ou ambos, dependendo se você usa dados replicados, dados com codificação de eliminação (EC) ou ambos.

Se todos os volumes falharam, vá para [Reparar dados se todos os volumes falharem](#) .

Insira os IDs de volume em hexadecimal. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. Você pode especificar um volume, um intervalo de volumes ou vários volumes que não estejam em uma sequência.

Todos os volumes devem estar no mesmo nó de armazenamento. Se precisar restaurar volumes para mais de um nó de armazenamento, entre em contato com o suporte técnico.

Dados replicados

Se sua grade contiver dados replicados, use o `start-replicated-volume-repair` comando com o `--nodes` opção para identificar o nó (onde `--nodes` é o nome do host do nó). Em seguida, adicione o `--volumes` ou `--volume-range` opção, conforme mostrado nos exemplos a seguir.

Volume único: Este comando restaura dados replicados para o volume 0002 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervalo de volumes: Este comando restaura dados replicados para todos os volumes no intervalo 0003 para 0009 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Vários volumes não em sequência: Este comando restaura dados replicados para volumes 0001 , 0005 , e 0008 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Conforme os dados do objeto são restaurados, o alerta **Objetos Perdidos** é acionado se o sistema StorageGRID não conseguir localizar os dados do objeto replicados. Alertas podem ser disparados em nós de armazenamento em todo o sistema. Observe a descrição do alerta e as ações recomendadas para determinar a causa da perda e se a recuperação é possível.

Dados codificados por apagamento (EC)

Se sua grade contiver dados codificados por eliminação, use o `start-ec-volume-repair` comando com o `--nodes` opção para identificar o nó (onde `--nodes` é o nome do host do nó). Em seguida, adicione o `--volumes` ou `--volume-range` opção, conforme mostrado nos exemplos a seguir.

Volume único: Este comando restaura dados codificados para eliminação no volume 0007 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervalo de volumes: Este comando restaura dados codificados por eliminação para todos os volumes no intervalo 0004 para 0006 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Vários volumes não em sequência: Este comando restaura dados codificados por eliminação para volumes 000A , 000C , e 000E em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

O `repair-data` operação retorna um único `repair ID` que identifica isso `repair_data` operação. Use isto `repair ID` para acompanhar o progresso e o resultado do `repair_data` operação. Nenhum outro feedback é retornado quando o processo de recuperação é concluído.



Os reparos de dados codificados para eliminação podem começar enquanto alguns nós de armazenamento estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Reparos de monitores

Monitore o status dos trabalhos de reparo, com base no uso de **dados replicados**, **dados codificados para eliminação (EC)** ou ambos.

Você também pode monitorar o status dos trabalhos de restauração de volume em andamento e visualizar um histórico dos trabalhos de restauração concluídos em "[Gerenciador de grade](#)".

Dados replicados

- Para obter uma porcentagem estimada de conclusão do reparo replicado, adicione o `show-replicated-repair-status` opção para o comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Para determinar se os reparos foram concluídos:
 - a. Selecione **NÓS > Nó de armazenamento sendo reparado > ILM**.
 - b. Revise os atributos na seção Avaliação. Quando os reparos estiverem concluídos, o atributo **Aguardando - Todos** indica 0 objetos.
- Para monitorar o reparo com mais detalhes:
 - a. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
 - b. Selecione **grid > Nó de armazenamento sendo reparado > LDR > Armazenamento de dados**.
 - c. Use uma combinação dos seguintes atributos para determinar, da melhor forma possível, se os reparos replicados estão completos.



Inconsistências no Cassandra podem estar presentes, e reparos com falha não são rastreados.

- **Reparos Tentados (XRPA)**: Use este atributo para rastrear o progresso de reparos replicados. Este atributo aumenta cada vez que um nó de armazenamento tenta reparar um objeto de alto risco. Quando esse atributo não aumenta por um período maior que o período de verificação atual (fornecido pelo atributo **Período de verificação — Estimado**), significa que a verificação do ILM não encontrou objetos de alto risco que precisem ser reparados em nenhum nó.



Objetos de alto risco são objetos que correm o risco de serem completamente perdidos. Isso não inclui objetos que não satisfazem sua configuração de ILM.

- **Período de verificação — estimado (XSCM)**: use este atributo para estimar quando uma alteração de política será aplicada a objetos ingeridos anteriormente. Se o atributo **Reparos Tentados** não aumentar por um período maior que o período de verificação atual, é provável que reparos replicados sejam feitos. Observe que o período de verificação pode mudar. O atributo **Período de varredura — Estimado (XSCM)** se aplica a toda a grade e é o máximo de todos os períodos de varredura de nós. Você pode consultar o histórico do atributo **Período de verificação — Estimado** da grade para determinar um período de tempo apropriado.

Dados codificados por apagamento (EC)

Para monitorar o reparo de dados codificados para eliminação e tentar novamente quaisquer solicitações que possam ter falhado:

1. Determinar o status dos reparos de dados codificados por eliminação:
 - Selecione **SUPORTE > Ferramentas > Métricas** para visualizar o tempo estimado para conclusão e a porcentagem de conclusão do trabalho atual. Em seguida, selecione **Visão geral do EC** na seção Grafana. Veja os painéis **Tempo estimado para conclusão do trabalho do Grid EC** e **Porcentagem concluída do trabalho do Grid EC**.

- Use este comando para ver o status de um determinado `repair-data` operação:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Use este comando para listar todos os reparos:

```
repair-data show-ec-repair-status
```

A saída lista informações, incluindo `repair ID`, para todos os reparos anteriores e atuais.

2. Se a saída mostrar que a operação de reparo falhou, use o `--repair-id` opção de tentar o reparo novamente.

Este comando tenta novamente um reparo de nó com falha, usando o ID de reparo 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando tenta novamente um reparo de volume com falha, usando o ID de reparo 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Verifique o estado do armazenamento após recuperar o nó de armazenamento do dispositivo

Após recuperar um nó de armazenamento do dispositivo, você deve verificar se o estado desejado do nó de armazenamento do dispositivo está definido como online e garantir que o estado será online por padrão sempre que o servidor do nó de armazenamento for reiniciado.

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- O nó de armazenamento foi recuperado e a recuperação de dados foi concluída.

Passos

1. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
2. Verifique os valores de **Nó de armazenamento recuperado > LDR > Armazenamento > Estado de armazenamento — Desejado** e **Estado de armazenamento — Atual**.

O valor de ambos os atributos deve ser Online.

3. Se o Estado de armazenamento desejado estiver definido como Somente leitura, conclua as seguintes etapas:
 - a. Clique na aba **Configuração**.
 - b. Na lista suspensa **Estado de armazenamento — Desejado**, selecione **Online**.
 - c. Clique em **Aplicar alterações**.
 - d. Clique na guia **Visão geral** e confirme se os valores de **Estado de armazenamento — Desejado** e **Estado de armazenamento — Atual** estão atualizados para Online.

Recuperar de falha de volume de armazenamento onde a unidade do sistema está intacta

Recuperar de falha de volume de armazenamento onde a unidade do sistema está intacta

Você deve concluir uma série de tarefas para recuperar um nó de armazenamento baseado em software onde um ou mais volumes de armazenamento no nó de armazenamento falharam, mas a unidade do sistema está intacta. Se apenas os volumes de armazenamento falharem, o nó de armazenamento ainda estará disponível para o sistema StorageGRID .



Este procedimento de recuperação se aplica somente a nós de armazenamento baseados em software. Se os volumes de armazenamento falharem em um nó de armazenamento do dispositivo, use o procedimento do dispositivo: "[Recuperar nó de armazenamento do dispositivo](#)".

Este procedimento de recuperação inclui as seguintes tarefas:

- "[Revisar avisos para recuperação de volume de armazenamento](#)"
- "[Identificar e desmontar volumes de armazenamento com falha](#)"
- "[Recuperar os volumes e reconstruir o banco de dados Cassandra](#)"
- "[Restaurar dados do objeto](#)"
- "[Verifique o estado do armazenamento](#)"

Avisos para recuperação de volume de armazenamento

Antes de recuperar volumes de armazenamento com falha para um nó de armazenamento, revise os seguintes avisos.

Os volumes de armazenamento (ou rangedbs) em um nó de armazenamento são identificados por um número hexadecimal, conhecido como ID do volume. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. O primeiro armazenamento de objetos (volume 0) em cada nó de armazenamento usa até 4 TB de espaço para metadados de objetos e operações de banco de dados Cassandra; qualquer espaço restante nesse volume é usado para dados de objetos. Todos os outros volumes de armazenamento são usados exclusivamente para dados de objetos.

Se o volume 0 falhar e precisar ser recuperado, o banco de dados Cassandra poderá ser reconstruído como parte do procedimento de recuperação de volume. Cassandra também pode ser reconstruída nas seguintes circunstâncias:

- Um nó de armazenamento é colocado novamente online após ficar offline por mais de 15 dias.
- A unidade do sistema e um ou mais volumes de armazenamento falham e são recuperados.

Quando o Cassandra é reconstruído, o sistema usa informações de outros nós de armazenamento. Se muitos nós de armazenamento estiverem offline, alguns dados do Cassandra podem não estar disponíveis. Se o Cassandra foi reconstruído recentemente, os dados do Cassandra podem ainda não ser consistentes em toda a grade. Pode ocorrer perda de dados se o Cassandra for reconstruído quando muitos nós de armazenamento estiverem offline ou se dois ou mais nós de armazenamento forem reconstruídos com um intervalo de 15 dias entre si.



Se mais de um nó de armazenamento falhar (ou estiver offline), entre em contato com o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.



Se esta for a segunda falha do nó de armazenamento em menos de 15 dias após uma falha ou recuperação do nó de armazenamento, entre em contato com o suporte técnico. Reconstruir o Cassandra em dois ou mais nós de armazenamento em 15 dias pode resultar em perda de dados.



Se mais de um nó de armazenamento em um site falhar, um procedimento de recuperação do site poderá ser necessário. Ver ["Como o suporte técnico recupera um site"](#).



Se as regras do ILM estiverem configuradas para armazenar apenas uma cópia replicada e a cópia existir em um volume de armazenamento que falhou, você não poderá recuperar o objeto.

Informações relacionadas

["Avisos e considerações para recuperação de nós de rede"](#)

Identificar e desmontar volumes de armazenamento com falha

Ao recuperar um nó de armazenamento com volumes de armazenamento com falha, você deve identificar e desmontar os volumes com falha. Você deve verificar se somente os volumes de armazenamento com falha são reformatados como parte do procedimento de recuperação.

Antes de começar

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

Sobre esta tarefa

Você deve recuperar volumes de armazenamento com falha o mais rápido possível.

A primeira etapa do processo de recuperação é detectar volumes que foram desconectados, precisam ser desmontados ou apresentam erros de E/S. Se volumes com falha ainda estiverem anexados, mas tiverem um sistema de arquivos corrompido aleatoriamente, o sistema poderá não detectar nenhuma corrupção em partes não utilizadas ou não alocadas do disco.



Você deve concluir este procedimento antes de executar etapas manuais para recuperar os volumes, como adicionar ou reconectar os discos, parar o nó, iniciar o nó ou reinicializar. Caso contrário, quando você executar o `reformat_storage_block_devices.rb` script, você pode encontrar um erro no sistema de arquivos que faz com que o script trave ou falhe.



Repare o hardware e conecte os discos corretamente antes de executar o `reboot` comando.



Identifique cuidadosamente os volumes de armazenamento com falha. Você usará essas informações para verificar quais volumes devem ser reformatados. Após um volume ser reformatado, os dados nele contidos não poderão ser recuperados.

Para recuperar corretamente volumes de armazenamento com falha, você precisa saber os nomes dos dispositivos dos volumes de armazenamento com falha e suas IDs de volume.

Na instalação, cada dispositivo de armazenamento recebe um identificador exclusivo universal (UUID) do sistema de arquivos e é montado em um diretório rangedb no nó de armazenamento usando esse UUID do sistema de arquivos atribuído. O UUID do sistema de arquivos e o diretório rangedb estão listados no /etc/fstab arquivo. O nome do dispositivo, o diretório rangedb e o tamanho do volume montado são exibidos no Grid Manager.

No exemplo a seguir, o dispositivo /dev/sdc tem um tamanho de volume de 4 TB, é montado em /var/local/rangedb/0 , usando o nome do dispositivo /dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba no/etc/fstab arquivo:

var

local

rangedb

0

1

2

/dev/sdc

4396 GB

/dev/sdd

4396 GB

/dev/sde

4396 GB

/dev/sdc

/etc/fstab file

ext3

errors=remount-ro,barri

/dev/sdd

/var/local

ext3

errors=remount-ro,barri

/dev/sde

swap

swap

defaults

0

proc

/proc

proc

defaults

0

sysfs

/sys

sysfs

noauto

0

debugfs

/sys/kernel/debug

debugfs

noauto

0

devpts

/dev/pts

devpts

mode=0620,gid=5

0

/dev/fd0

/media/floppy

auto

noauto,user,sync

0

/dev/cdrom

/cdrom iso9660 ro,noauto 0 0

/dev/disk/by-uuid/384c4687-8811-47a7-9700-7b31b495a0b8

/var/local/mysql_1bda

/dev/mapper/fsgvg-fsglv

/fsg xfs daapi,mtpt=/fsg,noalign,nobarrier,ikcep 0 2

/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba

/var/local/rangedb/0

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.53 GB	655,360	559,513	Unknown
/var/local	evlsc	Online	96.6 GB	92.8 GB	94,369,792	94,369,445	Unknown
/var/local/rangedb/0	sdc	Online	4,396 GB	4,375 GB	858,993,408	858,983,455	Unavailable
/var/local/rangedb/1	sdd	Online	4,396 GB	4,362 GB	858,993,408	858,973,530	Unavailable
/var/local/rangedb/2	sde	Online	4,396 GB	4,370 GB	858,993,408	858,982,305	Unavailable

Passos

1. Conclua as seguintes etapas para registrar os volumes de armazenamento com falha e seus nomes de dispositivos:
- a. Selecione **SUPORTE > Ferramentas > Topologia de grade.**

b. Selecione **site > Nó de armazenamento com falha > LDR > Armazenamento > Visão geral > Principal** e procure por armazenamentos de objetos com alarmes.

Object Stores

ID	Total	Available	Stored Data	Stored (%)	Health
0000	96.6 GB	96.6 GB	823 KB	0.001 %	Error
0001	107 GB	107 GB	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 %	No Errors

- c. Selecione **site > Nó de armazenamento com falha > SSM > Recursos > Visão geral > Principal.** Determine o ponto de montagem e o tamanho do volume de cada volume de armazenamento com falha identificado na etapa anterior.

Os armazenamentos de objetos são numerados em notação hexadecimal. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. No exemplo, o armazenamento de objetos com um ID de 0000 corresponde a /var/local/rangedb/0 com nome de dispositivo sdc e tamanho de 107 GB.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

2. Efetue login no nó de armazenamento com falha:

- Digite o seguinte comando: `ssh admin@grid_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 `#`.

3. Execute o seguinte script para desmontar um volume de armazenamento com falha:

```
sn-unmount-volume object_store_ID
```

O `object_store_ID` é o ID do volume de armazenamento com falha. Por exemplo, especifique 0 no comando para um armazenamento de objetos com ID 0000.

4. Se solicitado, pressione **y** para interromper o serviço Cassandra dependendo do volume de armazenamento 0.



Se o serviço Cassandra já estiver interrompido, você não será solicitado. O serviço Cassandra é interrompido apenas para o volume 0.

```
root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
Services depending on storage volume 0 (cassandra) aren't down.
Services depending on storage volume 0 must be stopped before running
this script.
Stop services that require storage volume 0 [y/N]? y
Shutting down services that require storage volume 0.
Services requiring storage volume 0 stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

Em poucos segundos, o volume é desmontado. Aparecem mensagens indicando cada etapa do processo. A mensagem final indica que o volume foi desmontado.

5. Se a desmontagem falhar porque o volume está ocupado, você pode forçar uma desmontagem usando o `--use-umountof` opção:



Forçando uma desmontagem usando o `--use-umountof` opção pode fazer com que processos ou serviços que usam o volume se comportem de forma inesperada ou travem.

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

Recuperar volumes de armazenamento com falha e reconstruir o banco de dados Cassandra

Você deve executar um script que reformate e remonte o armazenamento em volumes de armazenamento com falha e reconstrua o banco de dados Cassandra no nó de armazenamento se o sistema determinar que isso é necessário.

Antes de começar

- Você tem o `Passwords.txt` arquivo.
- As unidades do sistema no servidor estão intactas.
- A causa da falha foi identificada e, se necessário, hardware de armazenamento de substituição já foi adquirido.
- O tamanho total do armazenamento de substituição é o mesmo do original.
- Você verificou se o descomissionamento do nó de armazenamento não está em andamento ou pausou o procedimento de descomissionamento do nó. (No Grid Manager, selecione **MANUTENÇÃO > Tarefas > Desativação.**)
- Você verificou que não há nenhuma expansão em andamento. (No Grid Manager, selecione **MANUTENÇÃO > Tarefas > Expansão.**)
- Você tem "[revisou os avisos sobre recuperação de volume de armazenamento](#)".

Passos

1. Conforme necessário, substitua o armazenamento físico ou virtual com falha associado aos volumes de armazenamento com falha que você identificou e desmontou anteriormente.

Não remonte os volumes nesta etapa. O armazenamento é remontado e adicionado a `/etc/fstab` em uma etapa posterior.

2. No Grid Manager, vá para **NODES > appliance Storage Node > Hardware**. Na seção StorageGRID Appliance da página, verifique se o modo Storage RAID está íntegro.
3. Efetue login no nó de armazenamento com falha:
 - a. Digite o seguinte comando: `ssh admin@grid_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 `#`.

4. Use um editor de texto (vi ou vim) para excluir volumes com falha do `/etc/fstab` arquivo e depois salve-o.



Comentando um volume com falha no `/etc/fstab` arquivo é insuficiente. O volume deve ser excluído de `fstab` à medida que o processo de recuperação verifica se todas as linhas no `fstab` arquivo corresponde aos sistemas de arquivos montados.

5. Reformat todos os volumes de armazenamento com falha e reconstrua o banco de dados Cassandra, se necessário. Digitar: `reformat_storage_block_devices.rb`

- Quando o volume de armazenamento 0 for desmontado, prompts e mensagens indicarão que o serviço Cassandra está sendo interrompido.
- Você será solicitado a reconstruir o banco de dados do Cassandra, se necessário.
 - Revise os avisos. Se nenhuma delas se aplicar, reconstrua o banco de dados do Cassandra. Digite: **y**
 - Se mais de um nó de armazenamento estiver offline ou se outro nó de armazenamento tiver sido reconstruído nos últimos 15 dias. Digite: **n**

O script sairá sem reconstruir Cassandra. Entre em contato com o suporte técnico.

- Para cada unidade `rangedb` no nó de armazenamento, quando for perguntado: `Reformat the rangedb drive <name> (device <major number>:<minor number>) ? [y/n] ?`, insira uma das seguintes respostas:
 - **y** para reformatar uma unidade que continha erros. Isso reformatar o volume de armazenamento e adiciona o volume de armazenamento reformatado ao `/etc/fstab` arquivo.
 - **n** se a unidade não contiver erros e você não quiser reformatá-la.



Selecionar **n** sai do script. Monte a unidade (se você acha que os dados na unidade devem ser mantidos e a unidade foi desmontada por engano) ou remova a unidade. Em seguida, execute o `reformat_storage_block_devices.rb` comando novamente.



Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. Os reparos ocorrem automaticamente assim que os serviços relacionados ou necessários são iniciados. Você pode notar uma saída de script que menciona "reaper" ou "Cassandra repair". Se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

No exemplo de saída a seguir, a unidade `/dev/sdf` deve ser reformatado, e Cassandra não precisou ser reconstruída:

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? y
Successfully formatted /dev/sdf with UUID b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done. Now do manual steps to
restore copies of data.
```

Depois que os volumes de armazenamento forem reformatados e remontados e as operações necessárias do Cassandra forem concluídas, você poderá [restaurar dados de objetos usando o Grid Manager](#) .

Restaurar dados do objeto para o volume de armazenamento onde a unidade do sistema está intacta

Após recuperar um volume de armazenamento em um nó de armazenamento onde a unidade do sistema está intacta, você pode restaurar os dados de objeto replicados ou codificados para eliminação que foram perdidos quando o volume de armazenamento falhou.

Qual procedimento devo usar?

Sempre que possível, restaure os dados do objeto usando a página **Restauração de volume** no Grid Manager.

- Se os volumes estiverem listados em **MANUTENÇÃO > Restauração de volume > Nós a serem restaurados**, restaure os dados do objeto usando o ["Página de restauração de volume no Grid Manager"](#) .
- Se os volumes não estiverem listados em **MANUTENÇÃO > Restauração de volume > Nós para restaurar**, siga as etapas abaixo para usar o `repair-data` script para restaurar dados do objeto.

Se o nó de armazenamento recuperado contiver menos volumes do que o nó que está substituindo, você deverá usar o `repair-data` roteiro.



O script `repair-data` está obsoleto e será removido em uma versão futura. Quando possível, use o ["Procedimento de restauração de volume no Grid Manager"](#) .

Use o `repair-data` script para restaurar dados de objetos

Antes de começar

- Você confirmou que o nó de armazenamento recuperado tem um estado de conexão de **Conectado***  na aba ***NÓS > Visão geral** no Gerenciador de grade.

Sobre esta tarefa

Dados de objetos podem ser restaurados de outros nós de armazenamento ou de um pool de armazenamento em nuvem, supondo que as regras de ILM da grade tenham sido configuradas de forma que cópias de objetos estejam disponíveis.

Observe o seguinte:

- Se uma regra de ILM foi configurada para armazenar apenas uma cópia replicada e essa cópia existia em um volume de armazenamento que falhou, você não poderá recuperar o objeto.
- Se a única cópia restante de um objeto estiver em um Cloud Storage Pool, o StorageGRID deverá emitir várias solicitações ao ponto de extremidade do Cloud Storage Pool para restaurar os dados do objeto. Antes de executar este procedimento, entre em contato com o suporte técnico para obter ajuda na estimativa do tempo de recuperação e dos custos associados.

Sobre o `repair-data` roteiro

Para restaurar dados do objeto, execute o `repair-data` roteiro. Este script inicia o processo de restauração de dados do objeto e trabalha com a varredura do ILM para garantir que as regras do ILM sejam atendidas.

Selecione **Dados replicados** ou **Dados codificados por eliminação (EC)** abaixo para aprender as diferentes opções para `repair-data` script, com base no fato de você estar restaurando dados replicados ou dados codificados para eliminação. Se precisar restaurar ambos os tipos de dados, você deverá executar ambos os conjuntos de comandos.



Para mais informações sobre o `repair-data` script, digite `repair-data --help` da linha de comando do nó de administração primário.



O script `repair-data` está obsoleto e será removido em uma versão futura. Quando possível, use o ["Procedimento de restauração de volume no Grid Manager"](#).

Dados replicados

Dois comandos estão disponíveis para restaurar dados replicados, dependendo se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Você pode rastrear reparos de dados replicados com este comando:

```
repair-data show-replicated-repair-status
```

Dados codificados por apagamento (EC)

Dois comandos estão disponíveis para restaurar dados codificados para eliminação, dependendo se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Você pode rastrear reparos de dados codificados para eliminação com este comando:

```
repair-data show-ec-repair-status
```



Os reparos de dados codificados para eliminação podem começar enquanto alguns nós de armazenamento estão offline. Entretanto, se todos os dados codificados para eliminação não puderem ser contabilizados, o reparo não poderá ser concluído. O reparo será concluído depois que todos os nós estiverem disponíveis.



O trabalho de reparo do EC reserva temporariamente uma grande quantidade de armazenamento. Alertas de armazenamento podem ser acionados, mas serão resolvidos quando o reparo for concluído. Se não houver armazenamento suficiente para a reserva, o trabalho de reparo do EC falhará. As reservas de armazenamento são liberadas quando o trabalho de reparo do EC é concluído, independentemente de o trabalho ter falhado ou sido bem-sucedido.

Encontre o nome do host para o nó de armazenamento

1. Efetue login no nó de administração principal:

- Digite o seguinte comando: `ssh admin@primary_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. Use o `/etc/hosts` arquivo para encontrar o nome do host do nó de armazenamento para os volumes de armazenamento restaurados. Para ver uma lista de todos os nós na grade, digite o seguinte: `cat`

/etc/hosts .

Reparar dados se todos os volumes falharem

Se todos os volumes de armazenamento falharem, repare o nó inteiro. Siga as instruções para **dados replicados**, **dados com codificação de eliminação (EC)** ou ambos, dependendo se você usa dados replicados, dados com codificação de eliminação (EC) ou ambos.

Se apenas alguns volumes falharam, vá para [Reparar dados se apenas alguns volumes falharam](#) .



Você não pode correr `repair-data` operações para mais de um nó ao mesmo tempo. Para recuperar vários nós, entre em contato com o suporte técnico.

Dados replicados

Se sua grade incluir dados replicados, use o `repair-data start-replicated-node-repair` comando com o `--nodes` opção, onde `--nodes` é o nome do host (nome do sistema) para reparar todo o nó de armazenamento.

Este comando repara os dados replicados em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Conforme os dados do objeto são restaurados, o alerta **Objetos Perdidos** é acionado se o sistema StorageGRID não conseguir localizar os dados do objeto replicados. Alertas podem ser disparados em nós de armazenamento em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Ver "[Investigar objetos perdidos](#)".

Dados codificados por apagamento (EC)

Se sua grade contiver dados codificados por eliminação, use o `repair-data start-ec-node-repair` comando com o `--nodes` opção, onde `--nodes` é o nome do host (nome do sistema) para reparar todo o nó de armazenamento.

Este comando repara os dados codificados para eliminação em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

A operação retorna um valor único `repair ID` que identifica isso `repair_data` operação. Use isto `repair ID` para acompanhar o progresso e o resultado do `repair_data` operação. Nenhum outro feedback é retornado quando o processo de recuperação é concluído.

Os reparos de dados codificados para eliminação podem começar enquanto alguns nós de armazenamento estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Reparar dados se apenas alguns volumes falharam

Se apenas alguns volumes falharam, repare os volumes afetados. Siga as instruções para **dados replicados**, **dados com codificação de eliminação (EC)** ou ambos, dependendo se você usa dados replicados, dados com codificação de eliminação (EC) ou ambos.

Se todos os volumes falharam, vá para [Reparar dados se todos os volumes falharem](#) .

Insira os IDs de volume em hexadecimal. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. Você pode especificar um volume, um intervalo de volumes ou vários volumes que não estejam em uma sequência.

Todos os volumes devem estar no mesmo nó de armazenamento. Se precisar restaurar volumes para mais de um nó de armazenamento, entre em contato com o suporte técnico.

Dados replicados

Se sua grade contiver dados replicados, use o `start-replicated-volume-repair` comando com o `--nodes` opção para identificar o nó (onde `--nodes` é o nome do host do nó). Em seguida, adicione o `--volumes` ou `--volume-range` opção, conforme mostrado nos exemplos a seguir.

Volume único: Este comando restaura dados replicados para o volume 0002 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervalo de volumes: Este comando restaura dados replicados para todos os volumes no intervalo 0003 para 0009 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Vários volumes não em sequência: Este comando restaura dados replicados para volumes 0001 , 0005 , e 0008 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Conforme os dados do objeto são restaurados, o alerta **Objetos Perdidos** é acionado se o sistema StorageGRID não conseguir localizar os dados do objeto replicados. Alertas podem ser disparados em nós de armazenamento em todo o sistema. Observe a descrição do alerta e as ações recomendadas para determinar a causa da perda e se a recuperação é possível.

Dados codificados por apagamento (EC)

Se sua grade contiver dados codificados por eliminação, use o `start-ec-volume-repair` comando com o `--nodes` opção para identificar o nó (onde `--nodes` é o nome do host do nó). Em seguida, adicione o `--volumes` ou `--volume-range` opção, conforme mostrado nos exemplos a seguir.

Volume único: Este comando restaura dados codificados para eliminação no volume 0007 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervalo de volumes: Este comando restaura dados codificados por eliminação para todos os volumes no intervalo 0004 para 0006 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Vários volumes não em sequência: Este comando restaura dados codificados por eliminação para volumes 000A , 000C , e 000E em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

O `repair-data` operação retorna um único `repair ID` que identifica isso `repair_data` operação. Use isto `repair ID` para acompanhar o progresso e o resultado do `repair_data` operação. Nenhum outro feedback é retornado quando o processo de recuperação é concluído.



Os reparos de dados codificados para eliminação podem começar enquanto alguns nós de armazenamento estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Reparos de monitores

Monitore o status dos trabalhos de reparo, com base no uso de **dados replicados**, **dados codificados para eliminação (EC)** ou ambos.

Você também pode monitorar o status dos trabalhos de restauração de volume em andamento e visualizar um histórico dos trabalhos de restauração concluídos em "[Gerenciador de grade](#)".

Dados replicados

- Para obter uma porcentagem estimada de conclusão do reparo replicado, adicione o `show-replicated-repair-status` opção para o comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Para determinar se os reparos foram concluídos:
 - a. Selecione **NÓS > Nó de armazenamento sendo reparado > ILM**.
 - b. Revise os atributos na seção Avaliação. Quando os reparos estiverem concluídos, o atributo **Aguardando - Todos** indica 0 objetos.
- Para monitorar o reparo com mais detalhes:
 - a. Selecione **SUORTE > Ferramentas > Topologia de grade**.
 - b. Selecione **grid > Nó de armazenamento sendo reparado > LDR > Armazenamento de dados**.
 - c. Use uma combinação dos seguintes atributos para determinar, da melhor forma possível, se os reparos replicados estão completos.



Inconsistências no Cassandra podem estar presentes, e reparos com falha não são rastreados.

- **Reparos Tentados (XRPA)**: Use este atributo para rastrear o progresso de reparos replicados. Este atributo aumenta cada vez que um nó de armazenamento tenta reparar um objeto de alto risco. Quando esse atributo não aumenta por um período maior que o período de verificação atual (fornecido pelo atributo **Período de verificação — Estimado**), significa que a verificação do ILM não encontrou objetos de alto risco que precisem ser reparados em nenhum nó.



Objetos de alto risco são objetos que correm o risco de serem completamente perdidos. Isso não inclui objetos que não satisfazem sua configuração de ILM.

- **Período de verificação — estimado (XSCM)**: use este atributo para estimar quando uma alteração de política será aplicada a objetos ingeridos anteriormente. Se o atributo **Reparos Tentados** não aumentar por um período maior que o período de verificação atual, é provável que reparos replicados sejam feitos. Observe que o período de verificação pode mudar. O atributo **Período de varredura — Estimado (XSCM)** se aplica a toda a grade e é o máximo de todos os períodos de varredura de nós. Você pode consultar o histórico do atributo **Período de verificação — Estimado** da grade para determinar um período de tempo apropriado.

Dados codificados por apagamento (EC)

Para monitorar o reparo de dados codificados para eliminação e tentar novamente quaisquer solicitações que possam ter falhado:

1. Determinar o status dos reparos de dados codificados por eliminação:
 - Selecione **SUORTE > Ferramentas > Métricas** para visualizar o tempo estimado para conclusão e a porcentagem de conclusão do trabalho atual. Em seguida, selecione **Visão geral do EC** na seção Grafana. Veja os painéis **Tempo estimado para conclusão do trabalho do Grid EC** e **Porcentagem concluída do trabalho do Grid EC**.

- Use este comando para ver o status de um determinado `repair-data` operação:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Use este comando para listar todos os reparos:

```
repair-data show-ec-repair-status
```

A saída lista informações, incluindo `repair ID`, para todos os reparos anteriores e atuais.

2. Se a saída mostrar que a operação de reparo falhou, use o `--repair-id` opção de tentar o reparo novamente.

Este comando tenta novamente um reparo de nó com falha, usando o ID de reparo 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando tenta novamente um reparo de volume com falha, usando o ID de reparo 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Verifique o estado do armazenamento após recuperar volumes de armazenamento

Após recuperar os volumes de armazenamento, você deve verificar se o estado desejado do Nó de Armazenamento está definido como online e garantir que o estado será online por padrão sempre que o servidor do Nó de Armazenamento for reiniciado.

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- O nó de armazenamento foi recuperado e a recuperação de dados foi concluída.

Passos

1. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
2. Verifique os valores de **Nó de armazenamento recuperado > LDR > Armazenamento > Estado de armazenamento — Desejado** e **Estado de armazenamento — Atual**.

O valor de ambos os atributos deve ser Online.

3. Se o Estado de armazenamento desejado estiver definido como Somente leitura, conclua as seguintes etapas:
 - a. Clique na aba **Configuração**.
 - b. Na lista suspensa **Estado de armazenamento — Desejado**, selecione **Online**.
 - c. Clique em **Aplicar alterações**.
 - d. Clique na guia **Visão geral** e confirme se os valores de **Estado de armazenamento — Desejado** e **Estado de armazenamento — Atual** estão atualizados para Online.

Recuperar de falha de unidade do sistema

Avisos para recuperação de unidade do sistema do nó de armazenamento

Antes de recuperar uma unidade de sistema com falha de um nó de armazenamento, revise as informações gerais "[avisos e considerações para recuperação de nós de rede](#)" e os seguintes avisos específicos.

Os nós de armazenamento têm um banco de dados Cassandra que inclui metadados de objetos. O banco de dados Cassandra pode ser reconstruído nas seguintes circunstâncias:

- Um nó de armazenamento é colocado novamente online após ficar offline por mais de 15 dias.
- Um volume de armazenamento falhou e foi recuperado.
- A unidade do sistema e um ou mais volumes de armazenamento falham e são recuperados.

Quando o Cassandra é reconstruído, o sistema usa informações de outros nós de armazenamento. Se muitos nós de armazenamento estiverem offline, alguns dados do Cassandra podem não estar disponíveis. Se o Cassandra foi reconstruído recentemente, os dados do Cassandra podem ainda não ser consistentes em toda a grade. Pode ocorrer perda de dados se o Cassandra for reconstruído quando muitos nós de armazenamento estiverem offline ou se dois ou mais nós de armazenamento forem reconstruídos com um intervalo de 15 dias entre si.



Se mais de um nó de armazenamento falhar (ou estiver offline), entre em contato com o suporte técnico. Não execute o seguinte procedimento de recuperação. Pode ocorrer perda de dados.



Se esta for a segunda falha do nó de armazenamento em menos de 15 dias após uma falha ou recuperação do nó de armazenamento, entre em contato com o suporte técnico. Reconstruir o Cassandra em dois ou mais nós de armazenamento em 15 dias pode resultar em perda de dados.



Se mais de um nó de armazenamento em um site falhar, um procedimento de recuperação do site poderá ser necessário. Ver "[Como o suporte técnico recupera um site](#)".



Se este nó de armazenamento estiver no modo de manutenção somente leitura para permitir a recuperação de objetos por outro nó de armazenamento com volumes de armazenamento com falha, recupere os volumes no nó de armazenamento com volumes de armazenamento com falha antes de recuperar este nó de armazenamento com falha. Veja as instruções para "[recuperar de falha de volume de armazenamento onde a unidade do sistema está intacta](#)".



Se as regras do ILM estiverem configuradas para armazenar apenas uma cópia replicada e a cópia existir em um volume de armazenamento que falhou, você não poderá recuperar o objeto.

Substituir o nó de armazenamento

Se a unidade do sistema falhar, você deverá primeiro substituir o nó de armazenamento.

Você deve selecionar o procedimento de substituição de nó para sua plataforma. As etapas para substituir um nó são as mesmas para todos os tipos de nós de grade.



Este procedimento se aplica somente a nós de armazenamento baseados em software. Você deve seguir um procedimento diferente para "[recuperar um nó de armazenamento do aparelho](#)".

Linux: Se você não tiver certeza se a unidade do sistema falhou, siga as instruções para substituir o nó e determinar quais etapas de recuperação são necessárias.

Plataforma	Procedimento
VMware	"Substituir um nó VMware"
Linux	"Substituir um nó Linux"
OpenStack	Os arquivos de disco de máquina virtual e scripts fornecidos pela NetApp para OpenStack não são mais suportados para operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação do OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para " substituindo um nó Linux ".

Selecione Iniciar recuperação para configurar o nó de armazenamento

Após substituir um nó de armazenamento, você deve selecionar Iniciar recuperação no Grid Manager para configurar o novo nó como um substituto para o nó com falha.

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.
- Você implantou e configurou o nó de substituição.
- Você tem a data de início de quaisquer trabalhos de reparo para dados codificados para eliminação.
- Você verificou que o nó de armazenamento não foi reconstruído nos últimos 15 dias.

Sobre esta tarefa

Se o nó de armazenamento estiver instalado como um contêiner em um host Linux, você deverá executar esta etapa somente se uma destas condições for verdadeira:

- Você teve que usar o `--force` sinalizador para importar o nó ou você emitiu `storagegrid node force-recovery node-name`
- Você teve que fazer uma reinstalação completa do nó ou precisou restaurar `/var/local`.

Passos

1. No Grid Manager, selecione **MANUTENÇÃO > Tarefas > Recuperação**.
2. Selecione o nó da grade que você deseja recuperar na lista Nós Pendentes.

Os nós aparecem na lista depois de falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Digite a **senha de provisionamento**.
4. Clique em **Iniciar recuperação**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
104-217-S1	10.96.104.217	Unknown	✓	

Passphrase

Provisioning Passphrase

.....

Start Recovery

5. Monitore o progresso da recuperação na tabela Nó da grade em recuperação.



Enquanto o procedimento de recuperação estiver em execução, você pode clicar em **Redefinir** para iniciar uma nova recuperação. Uma caixa de diálogo aparece, indicando que o nó ficará em um estado indeterminado se você redefinir o procedimento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se você quiser tentar a recuperação novamente após redefinir o procedimento, deverá restaurar o nó para um estado pré-instalado, da seguinte maneira:

- **VMware:** Exclua o nó de grade virtual implantado. Então, quando estiver pronto para reiniciar a recuperação, reimplante o nó.
- **Linux:** Reinicie o nó executando este comando no host Linux: `storagegrid node force-recovery node-name`

6. Quando o nó de armazenamento atingir o estágio "Aguardando etapas manuais", vá para ["Remontar e reformatar volumes de armazenamento \(etapas manuais\)"](#) .

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT		Waiting For Manual Steps

Reset

Remontar e reformatar volumes de armazenamento (etapas manuais)

Você deve executar manualmente dois scripts para remontar os volumes de armazenamento preservados e reformatar quaisquer volumes de armazenamento com falha. O primeiro script remonta volumes que estão formatados corretamente como volumes de armazenamento StorageGRID . O segundo script reformata todos os volumes desmontados, reconstrói o Cassandra, se necessário, e inicia os serviços.

Antes de começar

- Você já substituiu o hardware de todos os volumes de armazenamento com falha que você sabe que precisam ser substituídos.

Executando o `sn-remount-volumes` O script pode ajudar você a identificar volumes de armazenamento adicionais com falha.

- Você verificou se o descomissionamento do nó de armazenamento não está em andamento ou pausou o procedimento de descomissionamento do nó. (No Grid Manager, selecione **MANUTENÇÃO > Tarefas > Desativação.**)
- Você verificou que não há nenhuma expansão em andamento. (No Grid Manager, selecione **MANUTENÇÃO > Tarefas > Expansão.**)
- Você tem ["revisou os avisos para recuperação de unidade do sistema do nó de armazenamento"](#) .



Entre em contato com o suporte técnico se mais de um nó de armazenamento estiver offline ou se um nó de armazenamento nesta grade tiver sido reconstruído nos últimos 15 dias. Não execute o `sn-recovery-postinstall.sh` roteiro. Reconstruir o Cassandra em dois ou mais nós de armazenamento com intervalo de 15 dias entre eles pode resultar em perda de dados.

Sobre esta tarefa

Para concluir este procedimento, execute estas tarefas de alto nível:

- Efetue login no nó de armazenamento recuperado.
- Execute o `sn-remount-volumes` script para remontar volumes de armazenamento formatados corretamente. Quando esse script é executado, ele faz o seguinte:
 - Monta e desmonta cada volume de armazenamento para reproduzir o diário XFS.
 - Executa uma verificação de consistência do arquivo XFS.

- Se o sistema de arquivos for consistente, determina se o volume de armazenamento é um volume de armazenamento StorageGRID formatado corretamente.
- Se o volume de armazenamento estiver formatado corretamente, remonta o volume de armazenamento. Todos os dados existentes no volume permanecem intactos.
- Revise a saída do script e resolva quaisquer problemas.
- Execute o `sn-recovery-postinstall.sh` roteiro. Quando esse script é executado, ele faz o seguinte.



Não reinicie um nó de armazenamento durante a recuperação antes de executar `sn-recovery-postinstall.sh` para reformatar os volumes de armazenamento com falha e restaurar os metadados do objeto. Reiniciando o nó de armazenamento antes `sn-recovery-postinstall.sh` conclui causa erros nos serviços que tentam iniciar e faz com que os nós do dispositivo StorageGRID saiam do modo de manutenção. Veja o passo [para script de pós-instalação](#).

- Reformata quaisquer volumes de armazenamento que o `sn-remount-volumes` o script não pôde ser montado ou foi encontrado com formato incorreto.



Se um volume de armazenamento for reformatado, todos os dados contidos nesse volume serão perdidos. Você deve executar um procedimento adicional para restaurar dados de objetos de outros locais na grade, supondo que as regras do ILM foram configuradas para armazenar mais de uma cópia de objeto.

- Reconstrói o banco de dados Cassandra no nó, se necessário.
- Inicia os serviços no nó de armazenamento.

Passos

1. Efetue login no nó de armazenamento recuperado:

- Digite o seguinte comando: `ssh admin@grid_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 primeiro script para remontar quaisquer volumes de armazenamento formatados corretamente.



Se todos os volumes de armazenamento forem novos e precisarem ser formatados, ou se todos os volumes de armazenamento falharem, você pode pular esta etapa e executar o segundo script para reformatar todos os volumes de armazenamento desmontados.

- Execute o script: `sn-remount-volumes`

Este script pode levar horas para ser executado em volumes de armazenamento que contêm dados.

- Conforme o script é executado, revise a saída e responda a quaisquer prompts.



Conforme necessário, você pode usar o `tail -f` comando para monitorar o conteúdo do arquivo de log do script(`/var/local/log/sn-remount-volumes.log`). O arquivo de log contém informações mais detalhadas do que a saída da linha de comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

===== Device /dev/sdb =====
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

===== Device /dev/sdc =====
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.
```

```

===== Device /dev/sdd =====
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

===== Device /dev/sde =====
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.

```

No exemplo de saída, um volume de armazenamento foi remontado com sucesso e três volumes de armazenamento apresentaram erros.

- `/dev/sdb` passou na verificação de consistência do sistema de arquivos XFS e tinha uma estrutura de volume válida, então foi remontado com sucesso. Os dados em dispositivos remontados pelo script são preservados.
- `/dev/sdc` falhou na verificação de consistência do sistema de arquivos XFS porque o volume de armazenamento era novo ou corrompido.
- `/dev/sdd` não pôde ser montado porque o disco não foi inicializado ou o superbloco do disco estava corrompido. Quando o script não consegue montar um volume de armazenamento, ele pergunta se você deseja executar a verificação de consistência do sistema de arquivos.
 - Se o volume de armazenamento estiver anexado a um novo disco, responda **N** ao prompt. Você não precisa verificar o sistema de arquivos em um novo disco.
 - Se o volume de armazenamento estiver anexado a um disco existente, responda **S** ao prompt. Você pode usar os resultados da verificação do sistema de arquivos para determinar a origem da corrupção. Os resultados são salvos no `/var/local/log/sn-remount-volumes.log` arquivo de log.
- `/dev/sde` passou na verificação de consistência do sistema de arquivos XFS e tinha uma estrutura de volume válida; no entanto, o ID do nó LDR no arquivo `volID` não correspondia ao ID deste nó de armazenamento (o `configured LDR noid` exibido na parte superior). Esta mensagem indica que este volume pertence a outro nó de armazenamento.

3. Revise a saída do script e resolva quaisquer problemas.



Se um volume de armazenamento falhar na verificação de consistência do sistema de arquivos XFS ou não puder ser montado, revise cuidadosamente as mensagens de erro na saída. Você deve entender as implicações de executar o `sn-recovery-postinstall.sh` roteiro nesses volumes.

- Verifique se os resultados incluem uma entrada para todos os volumes esperados. Se algum volume não estiver listado, execute o script novamente.
- Revise as mensagens de todos os dispositivos montados. Certifique-se de que não haja erros indicando que um volume de armazenamento não pertence a este nó de armazenamento.

No exemplo, a saída para `/dev/sde` inclui a seguinte mensagem de erro:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```



Se um volume de armazenamento for relatado como pertencente a outro nó de armazenamento, entre em contato com o suporte técnico. Se você executar o `sn-recovery-postinstall.sh` script, o volume de armazenamento será reformatado, o que pode causar perda de dados.

- Se algum dispositivo de armazenamento não puder ser montado, anote o nome do dispositivo e repare ou substitua-o.



Você deve reparar ou substituir quaisquer dispositivos de armazenamento que não puderam ser montados.

Você usará o nome do dispositivo para consultar o ID do volume, que é uma entrada necessária ao executar o `repair-data` script para restaurar dados do objeto para o volume (o próximo procedimento).

- d. Após reparar ou substituir todos os dispositivos não montáveis, execute o `sn-remount-volumes` script novamente para confirmar que todos os volumes de armazenamento que podem ser remontados foram remontados.



Se um volume de armazenamento não puder ser montado ou estiver formatado incorretamente e você continuar para a próxima etapa, o volume e todos os dados nele contidos serão excluídos. Se você tiver duas cópias dos dados do objeto, terá apenas uma cópia até concluir o próximo procedimento (restaurar os dados do objeto).



Não execute o `sn-recovery-postinstall.sh` script se você acredita que os dados restantes em um volume de armazenamento com falha não podem ser reconstruídos de outro lugar na grade (por exemplo, se sua política de ILM usa uma regra que faz apenas uma cópia ou se os volumes falharam em vários nós). Em vez disso, entre em contato com o suporte técnico para determinar como recuperar seus dados.

4. Execute o `sn-recovery-postinstall.sh` roteiro: `sn-recovery-postinstall.sh`

Este script reformata todos os volumes de armazenamento que não puderam ser montados ou que foram encontrados formatados incorretamente; reconstrói o banco de dados Cassandra no nó, se necessário; e inicia os serviços no nó de armazenamento.

Esteja ciente do seguinte:

- O script pode levar horas para ser executado.
- Em geral, você deve deixar a sessão SSH em paz enquanto o script estiver em execução.
- Não pressione **Ctrl+C** enquanto a sessão SSH estiver ativa.
- O script será executado em segundo plano se ocorrer uma interrupção na rede e encerrar a sessão SSH, mas você pode visualizar o progresso na página Recuperação.
- Se o nó de armazenamento usar o serviço RSM, o script poderá parecer travar por 5 minutos enquanto os serviços do nó são reiniciados. Esse atraso de 5 minutos é esperado sempre que o serviço RSM é inicializado pela primeira vez.



O serviço RSM está presente em nós de armazenamento que incluem o serviço ADC.



Alguns procedimentos de recuperação do StorageGRID usam o Reaper para lidar com reparos do Cassandra. Os reparos ocorrem automaticamente assim que os serviços relacionados ou necessários são iniciados. Você pode notar uma saída de script que menciona "reaper" ou "Cassandra repair". Se você vir uma mensagem de erro indicando que o reparo falhou, execute o comando indicado na mensagem de erro.

5. Como o `sn-recovery-postinstall.sh` o script é executado, monitore a página Recuperação no Grid Manager.

A barra de progresso e a coluna Estágio na página Recuperação fornecem um status de alto nível do `sn-recovery-postinstall.sh` roteiro.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
No results found.				

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT		Recovering Cassandra

6. Depois do `sn-recovery-postinstall.sh` o script iniciou serviços no nó, você pode restaurar dados do objeto em qualquer volume de armazenamento que foi formatado pelo script.

O script pergunta se você deseja usar o processo de restauração de volume do Grid Manager.

- Na maioria dos casos, você deve "[restaurar dados de objetos usando o Grid Manager](#)". Responder `y` para usar o Grid Manager.
- Em casos raros, como quando instruído pelo suporte técnico, ou quando você sabe que o nó de substituição tem menos volumes disponíveis para armazenamento de objetos do que o nó original, você deve "[restaurar dados do objeto manualmente](#)" usando o `repair-data` roteiro. Se um desses casos se aplicar, responda `n`.



Se você responder `n` para usar o processo de restauração de volume do Grid Manager (restaurar dados do objeto manualmente):

- Não é possível restaurar dados de objetos usando o Grid Manager.
- Você pode monitorar o progresso dos trabalhos de restauração manual usando o Grid Manager.

Após fazer sua seleção, o script é concluído e as próximas etapas para recuperar os dados do objeto são mostradas. Depois de revisar essas etapas, pressione qualquer tecla para retornar à linha de comando.

Restaurar dados do objeto para o volume de armazenamento (falha da unidade do sistema)

Após recuperar volumes de armazenamento para um nó de armazenamento que não seja um dispositivo, você pode restaurar os dados de objeto replicados ou codificados para eliminação que foram perdidos quando o nó de armazenamento falhou.

Qual procedimento devo usar?

Sempre que possível, restaure os dados do objeto usando a página **Restauração de volume** no Grid Manager.

- Se os volumes estiverem listados em **MANUTENÇÃO > Restauração de volume > Nós a serem restaurados**, restaure os dados do objeto usando o "[Página de restauração de volume no Grid Manager](#)".

- Se os volumes não estiverem listados em **MANUTENÇÃO > Restauração de volume > Nós para restaurar**, siga as etapas abaixo para usar o `repair-data` script para restaurar dados do objeto.

Se o nó de armazenamento recuperado contiver menos volumes do que o nó que está substituindo, você deverá usar o `repair-data` roteiro.



O script `repair-data` está obsoleto e será removido em uma versão futura. Quando possível, use o ["Procedimento de restauração de volume no Grid Manager"](#).

Use o `repair-data` script para restaurar dados de objetos

Antes de começar

- Você confirmou que o nó de armazenamento recuperado tem um estado de conexão de **Conectado***  na aba ***NÓS > Visão geral** no Gerenciador de grade.

Sobre esta tarefa

Dados de objetos podem ser restaurados de outros nós de armazenamento ou de um pool de armazenamento em nuvem, supondo que as regras de ILM da grade tenham sido configuradas de forma que cópias de objetos estejam disponíveis.

Observe o seguinte:

- Se uma regra de ILM foi configurada para armazenar apenas uma cópia replicada e essa cópia existia em um volume de armazenamento que falhou, você não poderá recuperar o objeto.
- Se a única cópia restante de um objeto estiver em um Cloud Storage Pool, o StorageGRID deverá emitir várias solicitações ao ponto de extremidade do Cloud Storage Pool para restaurar os dados do objeto. Antes de executar este procedimento, entre em contato com o suporte técnico para obter ajuda na estimativa do tempo de recuperação e dos custos associados.

Sobre o `repair-data` roteiro

Para restaurar dados do objeto, execute o `repair-data` roteiro. Este script inicia o processo de restauração de dados do objeto e trabalha com a varredura do ILM para garantir que as regras do ILM sejam atendidas.

Selecione **Dados replicados** ou **Dados codificados por eliminação (EC)** abaixo para aprender as diferentes opções para `repair-data` script, com base no fato de você estar restaurando dados replicados ou dados codificados para eliminação. Se precisar restaurar ambos os tipos de dados, você deverá executar ambos os conjuntos de comandos.



Para mais informações sobre o `repair-data` script, digite `repair-data --help` da linha de comando do nó de administração primário.



O script `repair-data` está obsoleto e será removido em uma versão futura. Quando possível, use o ["Procedimento de restauração de volume no Grid Manager"](#).

Dados replicados

Dois comandos estão disponíveis para restaurar dados replicados, dependendo se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Você pode rastrear reparos de dados replicados com este comando:

```
repair-data show-replicated-repair-status
```

Dados codificados por apagamento (EC)

Dois comandos estão disponíveis para restaurar dados codificados para eliminação, dependendo se você precisa reparar o nó inteiro ou apenas determinados volumes no nó:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Você pode rastrear reparos de dados codificados para eliminação com este comando:

```
repair-data show-ec-repair-status
```



Os reparos de dados codificados para eliminação podem começar enquanto alguns nós de armazenamento estão offline. Entretanto, se todos os dados codificados para eliminação não puderem ser contabilizados, o reparo não poderá ser concluído. O reparo será concluído depois que todos os nós estiverem disponíveis.



O trabalho de reparo do EC reserva temporariamente uma grande quantidade de armazenamento. Alertas de armazenamento podem ser acionados, mas serão resolvidos quando o reparo for concluído. Se não houver armazenamento suficiente para a reserva, o trabalho de reparo do EC falhará. As reservas de armazenamento são liberadas quando o trabalho de reparo do EC é concluído, independentemente de o trabalho ter falhado ou sido bem-sucedido.

Encontre o nome do host para o nó de armazenamento

1. Efetue login no nó de administração principal:

- Digite o seguinte comando: `ssh admin@primary_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. Use o `/etc/hosts` arquivo para encontrar o nome do host do nó de armazenamento para os volumes de armazenamento restaurados. Para ver uma lista de todos os nós na grade, digite o seguinte: `cat`

/etc/hosts.

Reparar dados se todos os volumes falharem

Se todos os volumes de armazenamento falharem, repare o nó inteiro. Siga as instruções para **dados replicados**, **dados com codificação de eliminação (EC)** ou ambos, dependendo se você usa dados replicados, dados com codificação de eliminação (EC) ou ambos.

Se apenas alguns volumes falharam, vá para [Reparar dados se apenas alguns volumes falharam](#).



Você não pode correr `repair-data` operações para mais de um nó ao mesmo tempo. Para recuperar vários nós, entre em contato com o suporte técnico.

Dados replicados

Se sua grade incluir dados replicados, use o `repair-data start-replicated-node-repair` comando com o `--nodes` opção, onde `--nodes` é o nome do host (nome do sistema) para reparar todo o nó de armazenamento.

Este comando repara os dados replicados em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



Conforme os dados do objeto são restaurados, o alerta **Objetos Perdidos** é acionado se o sistema StorageGRID não conseguir localizar os dados do objeto replicados. Alertas podem ser disparados em nós de armazenamento em todo o sistema. Você deve determinar a causa da perda e se a recuperação é possível. Ver "[Investigar objetos perdidos](#)".

Dados codificados por apagamento (EC)

Se sua grade contiver dados codificados por eliminação, use o `repair-data start-ec-node-repair` comando com o `--nodes` opção, onde `--nodes` é o nome do host (nome do sistema) para reparar todo o nó de armazenamento.

Este comando repara os dados codificados para eliminação em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

A operação retorna um valor único `repair ID` que identifica isso `repair_data` operação. Use isto `repair ID` para acompanhar o progresso e o resultado do `repair_data` operação. Nenhum outro feedback é retornado quando o processo de recuperação é concluído.

Os reparos de dados codificados para eliminação podem começar enquanto alguns nós de armazenamento estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Reparar dados se apenas alguns volumes falharam

Se apenas alguns volumes falharam, repare os volumes afetados. Siga as instruções para **dados replicados**, **dados com codificação de eliminação (EC)** ou ambos, dependendo se você usa dados replicados, dados com codificação de eliminação (EC) ou ambos.

Se todos os volumes falharam, vá para [Reparar dados se todos os volumes falharem](#) .

Insira os IDs de volume em hexadecimal. Por exemplo, 0000 é o primeiro volume e 000F é o décimo sexto volume. Você pode especificar um volume, um intervalo de volumes ou vários volumes que não estejam em uma sequência.

Todos os volumes devem estar no mesmo nó de armazenamento. Se precisar restaurar volumes para mais de um nó de armazenamento, entre em contato com o suporte técnico.

Dados replicados

Se sua grade contiver dados replicados, use o `start-replicated-volume-repair` comando com o `--nodes` opção para identificar o nó (onde `--nodes` é o nome do host do nó). Em seguida, adicione o `--volumes` ou `--volume-range` opção, conforme mostrado nos exemplos a seguir.

Volume único: Este comando restaura dados replicados para o volume 0002 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervalo de volumes: Este comando restaura dados replicados para todos os volumes no intervalo 0003 para 0009 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Vários volumes não em sequência: Este comando restaura dados replicados para volumes 0001 , 0005 , e 0008 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



Conforme os dados do objeto são restaurados, o alerta **Objetos Perdidos** é acionado se o sistema StorageGRID não conseguir localizar os dados do objeto replicados. Alertas podem ser disparados em nós de armazenamento em todo o sistema. Observe a descrição do alerta e as ações recomendadas para determinar a causa da perda e se a recuperação é possível.

Dados codificados por apagamento (EC)

Se sua grade contiver dados codificados por eliminação, use o `start-ec-volume-repair` comando com o `--nodes` opção para identificar o nó (onde `--nodes` é o nome do host do nó). Em seguida, adicione o `--volumes` ou `--volume-range` opção, conforme mostrado nos exemplos a seguir.

Volume único: Este comando restaura dados codificados para eliminação no volume 0007 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervalo de volumes: Este comando restaura dados codificados por eliminação para todos os volumes no intervalo 0004 para 0006 em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Vários volumes não em sequência: Este comando restaura dados codificados por eliminação para volumes 000A , 000C , e 000E em um nó de armazenamento chamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

O `repair-data` operação retorna um único `repair ID` que identifica isso `repair_data` operação. Use isto `repair ID` para acompanhar o progresso e o resultado do `repair_data` operação. Nenhum outro feedback é retornado quando o processo de recuperação é concluído.



Os reparos de dados codificados para eliminação podem começar enquanto alguns nós de armazenamento estão offline. O reparo será concluído depois que todos os nós estiverem disponíveis.

Reparos de monitores

Monitore o status dos trabalhos de reparo, com base no uso de **dados replicados**, **dados codificados para eliminação (EC)** ou ambos.

Você também pode monitorar o status dos trabalhos de restauração de volume em andamento e visualizar um histórico dos trabalhos de restauração concluídos em "[Gerenciador de grade](#)".

Dados replicados

- Para obter uma porcentagem estimada de conclusão do reparo replicado, adicione o `show-replicated-repair-status` opção para o comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Para determinar se os reparos foram concluídos:
 - a. Selecione **NÓS > Nó de armazenamento sendo reparado > ILM**.
 - b. Revise os atributos na seção Avaliação. Quando os reparos estiverem concluídos, o atributo **Aguardando - Todos** indica 0 objetos.
- Para monitorar o reparo com mais detalhes:
 - a. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
 - b. Selecione **grid > Nó de armazenamento sendo reparado > LDR > Armazenamento de dados**.
 - c. Use uma combinação dos seguintes atributos para determinar, da melhor forma possível, se os reparos replicados estão completos.



Inconsistências no Cassandra podem estar presentes, e reparos com falha não são rastreados.

- **Reparos Tentados (XRPA)**: Use este atributo para rastrear o progresso de reparos replicados. Este atributo aumenta cada vez que um nó de armazenamento tenta reparar um objeto de alto risco. Quando esse atributo não aumenta por um período maior que o período de verificação atual (fornecido pelo atributo **Período de verificação — Estimado**), significa que a verificação do ILM não encontrou objetos de alto risco que precisem ser reparados em nenhum nó.



Objetos de alto risco são objetos que correm o risco de serem completamente perdidos. Isso não inclui objetos que não satisfazem sua configuração de ILM.

- **Período de verificação — estimado (XSCM)**: use este atributo para estimar quando uma alteração de política será aplicada a objetos ingeridos anteriormente. Se o atributo **Reparos Tentados** não aumentar por um período maior que o período de verificação atual, é provável que reparos replicados sejam feitos. Observe que o período de verificação pode mudar. O atributo **Período de varredura — Estimado (XSCM)** se aplica a toda a grade e é o máximo de todos os períodos de varredura de nós. Você pode consultar o histórico do atributo **Período de verificação — Estimado** da grade para determinar um período de tempo apropriado.

Dados codificados por apagamento (EC)

Para monitorar o reparo de dados codificados para eliminação e tentar novamente quaisquer solicitações que possam ter falhado:

1. Determinar o status dos reparos de dados codificados por eliminação:
 - Selecione **SUPORTE > Ferramentas > Métricas** para visualizar o tempo estimado para conclusão e a porcentagem de conclusão do trabalho atual. Em seguida, selecione **Visão geral do EC** na seção Grafana. Veja os painéis **Tempo estimado para conclusão do trabalho do Grid EC** e **Porcentagem concluída do trabalho do Grid EC**.

- Use este comando para ver o status de um determinado `repair-data` operação:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Use este comando para listar todos os reparos:

```
repair-data show-ec-repair-status
```

A saída lista informações, incluindo `repair ID`, para todos os reparos anteriores e atuais.

2. Se a saída mostrar que a operação de reparo falhou, use o `--repair-id` opção de tentar o reparo novamente.

Este comando tenta novamente um reparo de nó com falha, usando o ID de reparo 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando tenta novamente um reparo de volume com falha, usando o ID de reparo 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Verifique o estado do armazenamento após recuperar a unidade do sistema do nó de armazenamento

Após recuperar a unidade do sistema para um Nó de Armazenamento, você deve verificar se o estado desejado do Nó de Armazenamento está definido como online e garantir que o estado será online por padrão sempre que o servidor do Nó de Armazenamento for reiniciado.

Antes de começar

- Você está conectado ao Grid Manager usando um "[navegador da web compatível](#)".
- O nó de armazenamento foi recuperado e a recuperação de dados foi concluída.

Passos

1. Selecione **SUORTE > Ferramentas > Topologia de grade**.
2. Verifique os valores de **Nó de armazenamento recuperado > LDR > Armazenamento > Estado de armazenamento — Desejado** e **Estado de armazenamento — Atual**.

O valor de ambos os atributos deve ser Online.

3. Se o Estado de armazenamento desejado estiver definido como Somente leitura, conclua as seguintes etapas:
 - a. Clique na aba **Configuração**.
 - b. Na lista suspensa **Estado de armazenamento — Desejado**, selecione **Online**.
 - c. Clique em **Aplicar alterações**.
 - d. Clique na guia **Visão geral** e confirme se os valores de **Estado de armazenamento — Desejado** e **Estado de armazenamento — Atual** estão atualizados para Online.

Restaurar dados de objetos usando o Grid Manager

Você pode restaurar dados de objeto para um volume de armazenamento ou nó de armazenamento com falha usando o Grid Manager. Você também pode usar o Grid Manager para monitorar processos de restauração em andamento e exibir um histórico de restauração.

Antes de começar

- Você concluiu um destes procedimentos para formatar volumes com falha:
 - ["Remonte e reformate os volumes de armazenamento do dispositivo \(etapas manuais\)"](#)
 - ["Remontar e reformatar volumes de armazenamento \(etapas manuais\)"](#)
- Você confirmou que o nó de armazenamento onde você está restaurando objetos tem um estado de conexão de **Conectado***  na aba ***NÓS > Visão geral** no Gerenciador de grade.
- Você confirmou o seguinte:
 - Uma expansão de grade para adicionar um nó de armazenamento não está em andamento.
 - A desativação de um nó de armazenamento não está em andamento ou falhou.
 - A recuperação de um volume de armazenamento com falha não está em andamento.
 - A recuperação de um nó de armazenamento com uma unidade de sistema com falha não está em andamento.
 - Um trabalho de rebalanceamento de EC não está em andamento.
 - A clonagem do nó do dispositivo não está em andamento.

Sobre esta tarefa

Depois de substituir as unidades e executar as etapas manuais para formatar os volumes, o Grid Manager exibe os volumes como candidatos para restauração na guia **MANUTENÇÃO > Restauração de volume > Nós para restaurar**.

Sempre que possível, restaure os dados do objeto usando a página Restauração de volume no Grid Manager. Você pode [habilitar modo de restauração automática](#) para iniciar automaticamente a restauração do volume quando os volumes estiverem prontos para serem restaurados ou [executar manualmente a restauração do volume](#). Siga estas diretrizes:

- Se os volumes estiverem listados em **MANUTENÇÃO > Restauração de volume > Nós a serem restaurados**, restaure os dados do objeto conforme descrito nas etapas abaixo. Os volumes serão listados se:
 - Alguns, mas não todos, volumes de armazenamento em um nó falharam
 - Todos os volumes de armazenamento em um nó falharam e estão sendo substituídos pelo mesmo número de volumes ou mais volumes

A página Restauração de volume no Grid Manager também permite que você [monitorar o processo de restauração de volume](#) e [ver histórico de restauração](#).

- Se os volumes não estiverem listados no Grid Manager como candidatos para restauração, siga as etapas apropriadas para usar o `repair-data` script para restaurar dados do objeto:
 - ["Restaurando dados do objeto para o volume de armazenamento \(falha da unidade do sistema\)"](#)
 - ["Restaurar dados do objeto para o volume de armazenamento onde a unidade do sistema está intacta"](#)

- "Restaurar dados do objeto para o volume de armazenamento do dispositivo"



O script repair-data está obsoleto e será removido em uma versão futura.

Se o nó de armazenamento recuperado contiver menos volumes do que o nó que está substituindo, você deverá usar o `repair-data` roteiro.

Você pode restaurar dois tipos de dados de objeto:

- Objetos de dados replicados são restaurados de outros locais, supondo que as regras de ILM da grade foram configuradas para disponibilizar cópias de objetos.
 - Se uma regra de ILM foi configurada para armazenar apenas uma cópia replicada e essa cópia existia em um volume de armazenamento que falhou, você não poderá recuperar o objeto.
 - Se a única cópia restante de um objeto estiver em um Cloud Storage Pool, o StorageGRID deverá emitir várias solicitações ao ponto de extremidade do Cloud Storage Pool para restaurar os dados do objeto.
- Objetos de dados codificados por eliminação (EC) são restaurados pela remontagem dos fragmentos armazenados. Fragmentos corrompidos ou perdidos são recriados pelo algoritmo de codificação de eliminação a partir dos dados restantes e fragmentos de paridade.

Os reparos de dados codificados para eliminação podem começar enquanto alguns nós de armazenamento estão offline. Entretanto, se todos os dados codificados para eliminação não puderem ser contabilizados, o reparo não poderá ser concluído. O reparo será concluído depois que todos os nós estiverem disponíveis.



A restauração de volume depende da disponibilidade de recursos onde as cópias de objetos são armazenadas. O progresso da restauração do volume não é linear e pode levar dias ou semanas para ser concluído.

Habilitar modo de restauração automática

Quando você ativa o modo de restauração automática, a restauração do volume inicia automaticamente quando os volumes estão prontos para serem restaurados.

Passos

1. No Grid Manager, vá para **MANUTENÇÃO > Restauração de volume**.
2. Selecione a aba **Nós para restaurar** e deslize o botão de alternância do **Modo de restauração automática** para a posição habilitado.
3. Quando a caixa de diálogo de confirmação aparecer, revise os detalhes.



- Você não poderá iniciar trabalhos de restauração de volume manualmente em nenhum nó.
- As restaurações de volume começarão automaticamente somente quando nenhum outro procedimento de manutenção estiver em andamento.
- Você pode monitorar o status do trabalho na página de monitoramento de progresso.
- O StorageGRID tenta automaticamente restaurações de volumes que não iniciam.

4. Quando você entender os resultados da ativação do modo de restauração automática, selecione **Sim** na

caixa de diálogo de confirmação.

Você pode desativar o modo de restauração automática a qualquer momento.

Restaurar manualmente o volume ou nó com falha

Siga estas etapas para restaurar um volume ou nó com falha.

Passos

1. No Grid Manager, vá para **MANUTENÇÃO > Restauração de volume**.
2. Selecione a aba **Nós para restaurar** e deslize o botão de alternância do **Modo de restauração automática** para a posição desativado.

O número na guia indica o número de nós com volumes que requerem restauração.

3. Expanda cada nó para ver os volumes que precisam de restauração e seu status.
4. Corrija quaisquer problemas que impeçam a restauração de cada volume. Os problemas serão indicados quando você selecionar **Aguardando etapas manuais**, se for exibido como status do volume.
5. Selecione um nó para restaurar onde todos os volumes indiquem o status Pronto para restauração.

Você só pode restaurar os volumes de um nó por vez.

Cada volume no nó deve indicar que está pronto para restauração.

6. Selecione **Iniciar restauração**.
7. Resolva quaisquer avisos que possam aparecer ou selecione **Iniciar mesmo assim** para ignorar os avisos e iniciar a restauração.

Os nós são movidos da guia **Nós a serem restaurados** para a guia **Progresso da restauração** quando a restauração começa.

Se uma restauração de volume não puder ser iniciada, o nó retornará para a guia **Nós para restaurar**.

Ver o progresso da restauração

A guia **Progresso da restauração** mostra o status do processo de restauração do volume e informações sobre os volumes de um nó que está sendo restaurado.

As taxas de reparo de dados para objetos replicados e codificados por apagamento em todos os volumes são médias que resumem todas as restaurações em andamento, incluindo aquelas iniciadas usando o `repair-data` roteiro. A porcentagem de objetos nesses volumes que estão intactos e não requerem restauração também é indicada.



A restauração de dados replicados depende da disponibilidade de recursos onde as cópias replicadas são armazenadas. O progresso da restauração de dados replicados não é linear e pode levar dias ou semanas para ser concluído.

A seção Tarefas de restauração exibe informações sobre restaurações de volume iniciadas no Grid Manager.

- O número no título da seção Tarefas de restauração indica o número de volumes que estão sendo restaurados ou na fila para restauração.

- A tabela exibe informações sobre cada volume em um nó que está sendo restaurado e seu progresso.
 - O progresso de cada nó exibe a porcentagem de cada trabalho.
 - Expanda a coluna Detalhes para exibir a hora de início da restauração e o ID do trabalho.
- Se uma restauração de volume falhar:
 - A coluna Status indica `failed (attempting retry)` , e será repetido automaticamente.
 - Se vários trabalhos de restauração falharem, o trabalho mais recente será repetido automaticamente primeiro.
 - O alerta **Falha no reparo do EC** é acionado se as tentativas continuarem falhando. Siga as etapas do alerta para resolver o problema.

Ver histórico de restauração

A guia **Histórico de restauração** mostra informações sobre todas as restaurações de volume que foram concluídas com sucesso.



Os tamanhos não são aplicáveis a objetos replicados e aparecem somente para restaurações que contêm objetos de dados codificados por eliminação (EC).

Monitorar trabalhos de reparo de dados

Você pode monitorar o status dos trabalhos de reparo usando o `repair-data` script da linha de comando.

Isso inclui trabalhos que você iniciou manualmente ou trabalhos que o StorageGRID iniciou automaticamente como parte de um procedimento de desativação.



Se você estiver executando trabalhos de restauração de volume, "[monitorar o progresso e visualizar um histórico desses trabalhos no Grid Manager](#)" em vez de.

Monitorar o status de `repair-data` trabalhos com base no uso de **dados replicados**, **dados codificados para eliminação (EC)** ou ambos.

Dados replicados

- Para obter uma porcentagem estimada de conclusão do reparo replicado, adicione o `show-replicated-repair-status` opção para o comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Para determinar se os reparos foram concluídos:
 - a. Selecione **NÓS > Nó de armazenamento sendo reparado > ILM**.
 - b. Revise os atributos na seção Avaliação. Quando os reparos estiverem concluídos, o atributo **Aguardando - Todos** indica 0 objetos.
- Para monitorar o reparo com mais detalhes:
 - a. Selecione **SUPORTE > Ferramentas > Topologia de grade**.
 - b. Selecione **grid > Nó de armazenamento sendo reparado > LDR > Armazenamento de dados**.
 - c. Use uma combinação dos seguintes atributos para determinar, da melhor forma possível, se os reparos replicados estão completos.



Inconsistências no Cassandra podem estar presentes, e reparos com falha não são rastreados.

- **Reparos Tentados (XRPA)**: Use este atributo para rastrear o progresso de reparos replicados. Este atributo aumenta cada vez que um nó de armazenamento tenta reparar um objeto de alto risco. Quando esse atributo não aumenta por um período maior que o período de verificação atual (fornecido pelo atributo **Período de verificação — Estimado**), significa que a verificação do ILM não encontrou objetos de alto risco que precisem ser reparados em nenhum nó.



Objetos de alto risco são objetos que correm o risco de serem completamente perdidos. Isso não inclui objetos que não satisfazem sua configuração de ILM.

- **Período de verificação — estimado (XSCM)**: use este atributo para estimar quando uma alteração de política será aplicada a objetos ingeridos anteriormente. Se o atributo **Reparos Tentados** não aumentar por um período maior que o período de verificação atual, é provável que reparos replicados sejam feitos. Observe que o período de verificação pode mudar. O atributo **Período de varredura — Estimado (XSCM)** se aplica a toda a grade e é o máximo de todos os períodos de varredura de nós. Você pode consultar o histórico do atributo **Período de verificação — Estimado** da grade para determinar um período de tempo apropriado.

Dados codificados por apagamento (EC)

Para monitorar o reparo de dados codificados para eliminação e tentar novamente quaisquer solicitações que possam ter falhado:

1. Determinar o status dos reparos de dados codificados por eliminação:
 - Selecione **SUPORTE > Ferramentas > Métricas** para visualizar o tempo estimado para conclusão e a porcentagem de conclusão do trabalho atual. Em seguida, selecione **Visão geral do EC** na seção Grafana. Veja os painéis **Tempo estimado para conclusão do trabalho do Grid EC** e **Porcentagem concluída do trabalho do Grid EC**.

- Use este comando para ver o status de um determinado `repair-data` operação:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Use este comando para listar todos os reparos:

```
repair-data show-ec-repair-status
```

A saída lista informações, incluindo `repair ID`, para todos os reparos anteriores e atuais.

2. Se a saída mostrar que a operação de reparo falhou, use o `--repair-id` opção de tentar o reparo novamente.

Este comando tenta novamente um reparo de nó com falha, usando o ID de reparo 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando tenta novamente um reparo de volume com falha, usando o ID de reparo 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Recuperar de falhas do nó de administração

Recuperação do nó de administração primário ou não primário

O processo de recuperação de um nó administrativo depende se ele é o nó administrativo principal ou um nó administrativo não principal.

As etapas de alto nível para recuperar um nó administrativo primário ou não primário são as mesmas, embora os detalhes das etapas sejam diferentes.

Sempre siga o procedimento de recuperação correto para o nó de administração que você está recuperando. Os procedimentos parecem os mesmos em alto nível, mas diferem nos detalhes.

Escolhas

- ["Recuperar de falhas do nó de administração primário"](#)
- ["Recuperar de falhas de nó de administração não primário"](#)

Recuperar de falhas do nó de administração primário

Recuperar de falhas do nó de administração primário

Você deve concluir um conjunto específico de tarefas para se recuperar de uma falha do nó de administração primário. O nó de administração principal hospeda o serviço do nó de gerenciamento de configuração (CMN) para a grade.



Você deve reparar ou substituir um nó administrativo primário com falha imediatamente ou a grade poderá perder a capacidade de ingerir novos objetos. O período exato depende da sua taxa de ingestão de objetos: se precisar de uma avaliação mais precisa do período da sua grade, entre em contato com o suporte técnico.

O serviço Nó de Gerenciamento de Configuração (CMN) no Nó de Administração primário é responsável por emitir blocos de identificadores de objetos para a grade. Esses identificadores são atribuídos aos objetos à medida que são ingeridos. Novos objetos não podem ser ingeridos a menos que haja identificadores disponíveis. A ingestão de objetos pode continuar enquanto o CMN estiver indisponível porque aproximadamente um mês de fornecimento de identificadores é armazenado em cache na grade. Entretanto, depois que os identificadores armazenados em cache forem esgotados, nenhum novo objeto poderá ser adicionado.

Siga estas etapas de alto nível para recuperar um nó de administração primário:

1. ["Copiar logs de auditoria do nó de administração primário com falha"](#)
2. ["Substituir o nó de administração primário"](#)
3. ["Configurar o nó de administração primário de substituição"](#)
4. ["Determinar se há um requisito de hotfix para o nó de administração primário recuperado"](#)
5. ["Restaurar o log de auditoria no nó de administração primário recuperado"](#)
6. ["Restaurar o banco de dados do nó de administração ao recuperar um nó de administração primário"](#)
7. ["Restaurar métricas do Prometheus ao recuperar um nó de administração primário"](#)

Copiar logs de auditoria do nó de administração primário com falha

Se você conseguir copiar os logs de auditoria do nó de administração primário com falha, deverá preservá-los para manter o registro da atividade e do uso do sistema na grade. Você pode restaurar os logs de auditoria preservados para o nó de administração primário recuperado depois que ele estiver instalado e funcionando.

Sobre esta tarefa

Este procedimento copia os arquivos de log de auditoria do nó administrativo com falha para um local temporário em um nó de grade separado. Esses logs de auditoria preservados podem então ser copiados para o nó de administração de substituição. Os logs de auditoria não são copiados automaticamente para o novo nó de administração.

Dependendo do tipo de falha, talvez você não consiga copiar logs de auditoria de um nó de administração com falha. Se a implantação tiver apenas um nó administrativo, o nó administrativo recuperado começará a registrar eventos no log de auditoria em um novo arquivo vazio e os dados registrados anteriormente serão perdidos. Se a implantação incluir mais de um nó de administração, você poderá recuperar os logs de auditoria de outro nó de administração.



Se os logs de auditoria não estiverem acessíveis no nó de administração com falha agora, você poderá acessá-los mais tarde, por exemplo, após a recuperação do host.

Passos

1. Se possível, faça login no nó de administração com falha. Caso contrário, efetue login no nó de administração principal ou em outro nó de administração, se disponível.
 - a. Digite o seguinte comando: `ssh admin@grid_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. Pare o serviço AMS para evitar que ele crie um novo arquivo de log: `service ams stop`
3. Navegue até o diretório de exportação de auditoria:

```
cd /var/local/log
```

4. Renomear a fonte `audit.log` arquivo para um nome de arquivo numerado exclusivo. Por exemplo, renomeie o arquivo `audit.log` para `2023-10-25.txt.1`.

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. Reinicie o serviço AMS: `service ams start`
6. Crie o diretório para copiar todos os arquivos de log de auditoria para um local temporário em um nó de grade separado: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando solicitado, digite a senha do administrador.

7. Copie todos os arquivos de log de auditoria para o local temporário: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando solicitado, digite a senha do administrador.

8. Sair como root: `exit`

Substituir nó de administração primário

Para recuperar um nó de administração primário, você deve primeiro substituir o hardware físico ou virtual.

Você pode substituir um nó de administração primário com falha por um nó de administração primário em execução na mesma plataforma ou pode substituir um nó de administração primário em execução no VMware ou em um host Linux por um nó de administração primário hospedado em um dispositivo de serviços.

Use o procedimento que corresponde à plataforma de substituição selecionada para o nó. Depois de concluir o procedimento de substituição do nó (que é adequado para todos os tipos de nó), esse procedimento o direcionará para a próxima etapa para recuperação do nó de administração primário.

Plataforma de substituição	Procedimento
VMware	"Substituir um nó VMware"
Linux	"Substituir um nó Linux"

Plataforma de substituição	Procedimento
Aparelhos de serviços	"Substituir um aparelho de serviços"
OpenStack	Os arquivos de disco de máquina virtual e scripts fornecidos pela NetApp para OpenStack não são mais suportados para operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação do OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para "substituindo um nó Linux" .

Configurar nó de administração primário de substituição

O nó de substituição deve ser configurado como o nó de administração principal do seu sistema StorageGRID .

Antes de começar

- Para nós de administração primários hospedados em máquinas virtuais, a máquina virtual foi implantada, ligada e inicializada.
- Para nós de administração primários hospedados em um dispositivo de serviços, você substituiu o dispositivo e instalou o software. Veja o ["instruções de instalação para seu aparelho"](#) .
- Você tem o backup mais recente do arquivo do pacote de recuperação(`sgws-recovery-package-id-revision.zip`).
- Você tem a senha de provisionamento.

Passos

1. Abra seu navegador da web e navegue até `https://primary_admin_node_ip` .
2. Gerencie uma senha temporária do instalador conforme necessário:
 - Se uma senha já tiver sido definida usando um desses métodos, digite a senha para prosseguir.
 - Um usuário definiu a senha ao acessar o instalador anteriormente
 - Para sistemas bare metal, a senha foi importada automaticamente do arquivo de configuração do nó em `/etc/storagegrid/nodes/<node_name>.conf`
 - Para VMs, a senha SSH/console foi importada automaticamente das propriedades do OVF
 - Se uma senha não tiver sido definida, opcionalmente defina uma senha para proteger o instalador do StorageGRID .
3. Clique em **Recuperar um nó de administração primário com falha**.

Welcome

Use this page to install a new StorageGRID system, or recover a failed primary Admin Node for an existing system.

Note: You must have access to a StorageGRID license, network configuration and grid topology information, and NTP settings to complete the installation. You must have the latest version of the Recovery Package file to complete a primary Admin Node recovery.



Install a StorageGRID system



Recover a failed primary Admin
Node

4. Carregue o backup mais recente do Pacote de Recuperação:
 - a. Clique em **Navegar**.
 - b. Localize o arquivo do pacote de recuperação mais recente para o seu sistema StorageGRID e clique em **Abrir**.
5. Digite a senha de provisionamento.
6. Clique em **Iniciar recuperação**.

O processo de recuperação começa. O Grid Manager pode ficar indisponível por alguns minutos enquanto os serviços necessários são iniciados. Quando a recuperação estiver concluída, a página de login será exibida.

7. Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID e a confiança da parte confiável para o nó de administração que você recuperou foi configurada para usar o certificado de interface de gerenciamento padrão, atualize (ou exclua e recrie) a confiança da parte confiável do nó nos Serviços de Federação do Active Directory (AD FS). Use o novo certificado de servidor padrão gerado durante o processo de recuperação do nó de administração.



Para configurar uma confiança de terceira parte confiável, consulte "[Configurar logon único](#)". Para acessar o certificado do servidor padrão, efetue login no shell de comando do nó de administração. Vá para o `/var/local/mgmt-api` diretório e selecione o `server.crt` arquivo.



Após recuperar um nó de administração primário, "[determinar se você precisa aplicar um hotfix](#)".

Determinar o requisito de hotfix para o nó de administração primário

Após recuperar um nó de administração primário, determine se você precisa aplicar um hotfix.

Antes de começar

A recuperação do nó de administração primário foi concluída.

Passos

1. Sign in no Grid Manager usando um ["navegador da web compatível"](#).
2. Selecione **NODES**.
3. Na lista à esquerda, selecione o nó de administração principal.
4. Na guia Visão geral, observe a versão exibida no campo **Versão do software**.
5. Selecione qualquer outro nó da grade.
6. Na guia Visão geral, observe a versão exibida no campo **Versão do software**.
 - Se as versões exibidas nos campos **Versão do software** forem as mesmas, não será necessário aplicar um hotfix.
 - Se as versões exibidas nos campos **Versão do software** forem diferentes, você deve ["aplicar um hotfix"](#) para atualizar o nó de administração primário recuperado para a mesma versão.

Restaurar log de auditoria no nó de administração primário recuperado

Se você conseguiu preservar o log de auditoria do nó de administração primário com falha, poderá copiá-lo para o nó de administração primário que está recuperando.

Antes de começar

- O nó de administração recuperado está instalado e em execução.
- Você copiou os logs de auditoria para outro local após a falha do nó de administração original.

Sobre esta tarefa

Se um nó administrativo falhar, os logs de auditoria salvos nesse nó administrativo serão potencialmente perdidos. Pode ser possível preservar dados contra perda copiando logs de auditoria do nó administrativo com falha e restaurando esses logs de auditoria para o nó administrativo recuperado. Dependendo da falha, pode não ser possível copiar logs de auditoria do nó de administração com falha. Nesse caso, se a implantação tiver mais de um nó administrativo, você poderá recuperar logs de auditoria de outro nó administrativo, pois os logs de auditoria são replicados para todos os nós administrativos.

Se houver apenas um nó de administração e o log de auditoria não puder ser copiado do nó com falha, o nó de administração recuperado começará a registrar eventos no log de auditoria como se a instalação fosse nova.

Você deve recuperar um nó de administração o mais rápido possível para restaurar a funcionalidade de registro.

Por padrão, as informações de auditoria são enviadas para o log de auditoria nos nós de administração. Você pode pular estas etapas se alguma das seguintes situações se aplicar:



- Você configurou um servidor syslog externo e os logs de auditoria agora estão sendo enviados para o servidor syslog em vez de para os nós de administração.
- Você especificou explicitamente que as mensagens de auditoria devem ser salvas somente nos nós locais que as geraram.

Ver "[Configurar mensagens de auditoria e destinos de log](#)" para mais detalhes.

Passos

1. Efetue login no nó de administração recuperado:

- a. Digite o seguinte comando: `ssh admin@recovery_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.

Depois de efetuar login como root, o prompt muda de `$` para `#`.

2. Verifique quais arquivos de auditoria foram preservados: `cd /var/local/log`

3. Copie os arquivos de log de auditoria preservados para o nó de administração recuperado: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Quando solicitado, digite a senha do administrador.

4. Por segurança, exclua os logs de auditoria do nó de grade com falha após verificar se eles foram copiados com sucesso para o nó de administração recuperado.

5. Atualize as configurações de usuário e grupo dos arquivos de log de auditoria no nó de administração recuperado: `chown ams-user: bycast *`

6. Sair como root: `exit`

Restaurar o banco de dados do nó de administração ao recuperar o nó de administração primário

Se quiser manter as informações históricas sobre atributos e alertas em um nó administrativo primário que falhou, você pode restaurar o banco de dados do nó administrativo. Você só poderá restaurar este banco de dados se o seu sistema StorageGRID incluir outro nó de administração.

Antes de começar

- O nó de administração recuperado está instalado e em execução.
- O sistema StorageGRID inclui pelo menos dois nós de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

Se um nó administrativo falhar, as informações históricas armazenadas no banco de dados do nó

administrativo serão perdidas. Este banco de dados inclui as seguintes informações:

- Histórico de alertas
- Dados de atributos históricos, que são usados em gráficos de estilo legado na página Nós

Quando você recupera um nó de administração, o processo de instalação do software cria um banco de dados de nó de administração vazio no nó recuperado. No entanto, o novo banco de dados inclui apenas informações de servidores e serviços que atualmente fazem parte do sistema ou foram adicionados posteriormente.

Se você restaurou um nó de administração primário e seu sistema StorageGRID tiver outro nó de administração, você poderá restaurar as informações históricas copiando o banco de dados do nó de administração de um nó de administração não primário (o *nó de administração de origem*) para o nó de administração primário recuperado. Se o seu sistema tiver apenas um nó de administração primário, você não poderá restaurar o banco de dados do nó de administração.



Copiar o banco de dados do nó de administração pode levar várias horas. Alguns recursos do Grid Manager ficarão indisponíveis enquanto os serviços estiverem interrompidos no nó de administração de origem.

Passos

1. Efetue login no nó de administração de origem:
 - a. Digite o seguinte comando: `ssh admin@grid_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.
2. No nó de administração de origem, pare o serviço MI: `service mi stop`
3. No nó de administração de origem, pare o serviço Management Application Program Interface (mgmt-api):
`service mgmt-api stop`
4. Conclua as seguintes etapas no nó de administração recuperado:
 - a. Efetue login no nó de administração recuperado:
 - i. Digite o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Digite a senha listada no `Passwords.txt` arquivo.
 - iii. Digite o seguinte comando para alternar para root: `su -`
 - iv. Digite a senha listada no `Passwords.txt` arquivo.
 - b. Pare o serviço MI: `service mi stop`
 - c. Pare o serviço mgmt-api: `service mgmt-api stop`
 - d. Adicione a chave privada SSH ao agente SSH. Digitar: `ssh-add`
 - e. Digite a senha de acesso SSH listada no `Passwords.txt` arquivo.
 - f. Copie o banco de dados do nó de administração de origem para o nó de administração recuperado:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
 - g. Quando solicitado, confirme que deseja substituir o banco de dados MI no nó de administração recuperado.

O banco de dados e seus dados históricos são copiados para o nó de administração recuperado. Quando a operação de cópia estiver concluída, o script inicia o nó de administração recuperado.

- h. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Digitar: `ssh-add -D`

5. Reinicie os serviços no nó de administração de origem: `service servermanager start`

Restaurar métricas do Prometheus ao recuperar o nó de administração primário

Opcionalmente, você pode manter as métricas históricas mantidas pelo Prometheus em um nó de administração primário que falhou. As métricas do Prometheus só poderão ser restauradas se o seu sistema StorageGRID incluir outro nó de administração.

Antes de começar

- O nó de administração recuperado está instalado e em execução.
- O sistema StorageGRID inclui pelo menos dois nós de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

Se um nó administrativo falhar, as métricas mantidas no banco de dados Prometheus no nó administrativo serão perdidas. Quando você recupera o nó de administração, o processo de instalação do software cria um novo banco de dados Prometheus. Depois que o nó de administração recuperado é iniciado, ele registra métricas como se você tivesse executado uma nova instalação do sistema StorageGRID.

Se você restaurou um nó de administração primário e seu sistema StorageGRID tiver outro nó de administração, você poderá restaurar as métricas históricas copiando o banco de dados Prometheus de um nó de administração não primário (o *nó de administração de origem*) para o nó de administração primário recuperado. Se o seu sistema tiver apenas um nó de administração primário, você não poderá restaurar o banco de dados do Prometheus.



Copiar o banco de dados do Prometheus pode levar uma hora ou mais. Alguns recursos do Grid Manager ficarão indisponíveis enquanto os serviços estiverem interrompidos no nó de administração de origem.

Passos

1. Efetue login no nó de administração de origem:
 - a. Digite o seguinte comando: `ssh admin@grid_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.
2. No nó de administração de origem, pare o serviço Prometheus: `service prometheus stop`
3. Conclua as seguintes etapas no nó de administração recuperado:
 - a. Efetue login no nó de administração recuperado:
 - i. Digite o seguinte comando: `ssh admin@grid_node_IP`

- ii. Digite a senha listada no `Passwords.txt` arquivo.
- iii. Digite o seguinte comando para alternar para root: `su -`
- iv. Digite a senha listada no `Passwords.txt` arquivo.
- b. Pare o serviço Prometheus: `service prometheus stop`
- c. Adicione a chave privada SSH ao agente SSH. Digitar: `ssh-add`
- d. Digite a senha de acesso SSH listada no `Passwords.txt` arquivo.
- e. Copie o banco de dados Prometheus do nó de administração de origem para o nó de administração recuperado: `/usr/local/prometheus/bin/prometheus-clone-db.sh`
`Source_Admin_Node_IP`
- f. Quando solicitado, pressione **Enter** para confirmar que deseja destruir o novo banco de dados Prometheus no nó de administração recuperado.

O banco de dados original do Prometheus e seus dados históricos são copiados para o nó de administração recuperado. Quando a operação de cópia estiver concluída, o script inicia o nó de administração recuperado. O seguinte status aparece:

Banco de dados clonado, iniciando serviços

- a. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Digitar: `ssh-add -D`
- 4. Reinicie o serviço Prometheus no nó de administração de origem. `service prometheus start`

Recuperar de falhas de nó de administração não primário

Recuperar de falhas de nó de administração não primário

Você deve concluir as seguintes tarefas para se recuperar de uma falha do nó administrativo não primário. Um nó de administração hospeda o serviço Nó de gerenciamento de configuração (CMN) e é conhecido como o nó de administração principal. Embora você possa ter vários nós de administração, cada sistema StorageGRID inclui apenas um nó de administração principal. Todos os outros nós administrativos são nós administrativos não primários.

Siga estas etapas de alto nível para recuperar um nó de administração não primário:

1. ["Copiar logs de auditoria do nó administrativo não primário com falha"](#)
2. ["Substituir o nó de administração não primário"](#)
3. ["Selecione Iniciar recuperação para configurar o nó de administração não primário"](#)
4. ["Restaurar o log de auditoria em um nó administrativo não primário recuperado"](#)
5. ["Restaurar o banco de dados do nó de administração ao recuperar um nó de administração não primário"](#)
6. ["Restaurar métricas do Prometheus ao recuperar um nó administrativo não primário"](#)

Copiar logs de auditoria do nó administrativo não primário com falha

Se você conseguir copiar os logs de auditoria do nó de administração com falha, deverá

preservá-los para manter o registro da atividade e do uso do sistema na grade. Você pode restaurar os logs de auditoria preservados para o nó administrativo não primário recuperado depois que ele estiver instalado e funcionando.

Este procedimento copia os arquivos de log de auditoria do nó administrativo com falha para um local temporário em um nó de grade separado. Esses logs de auditoria preservados podem então ser copiados para o nó de administração de substituição. Os logs de auditoria não são copiados automaticamente para o novo nó de administração.

Dependendo do tipo de falha, talvez você não consiga copiar logs de auditoria de um nó de administração com falha. Se a implantação tiver apenas um nó administrativo, o nó administrativo recuperado começará a registrar eventos no log de auditoria em um novo arquivo vazio e os dados registrados anteriormente serão perdidos. Se a implantação incluir mais de um nó de administração, você poderá recuperar os logs de auditoria de outro nó de administração.



Se os logs de auditoria não estiverem acessíveis no nó de administração com falha agora, você poderá acessá-los mais tarde, por exemplo, após a recuperação do host.

1. Se possível, faça login no nó de administração com falha. Caso contrário, efetue login no nó de administração principal ou em outro nó de administração, se disponível.

- a. Digite o seguinte comando: `ssh admin@grid_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. Pare o serviço AMS para evitar que ele crie um novo arquivo de log: `service ams stop`
3. Navegue até o diretório de exportação de auditoria:

```
cd /var/local/log
```

4. Renomeie o arquivo `audit.log` de origem para um nome de arquivo numerado exclusivo. Por exemplo, renomeie o arquivo `audit.log` para `2023-10-25.txt.1`.

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. Reinicie o serviço AMS: `service ams start`
6. Crie o diretório para copiar todos os arquivos de log de auditoria para um local temporário em um nó de grade separado: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando solicitado, digite a senha do administrador.

7. Copie todos os arquivos de log de auditoria para o local temporário: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando solicitado, digite a senha do administrador.

8. Sair como root: `exit`

Substituir nó de administração não primário

Para recuperar um nó de administração não primário, primeiro você deve substituir o hardware físico ou virtual.

Você pode substituir um nó administrativo não primário com falha por um nó administrativo não primário em execução na mesma plataforma ou pode substituir um nó administrativo não primário em execução no VMware ou em um host Linux por um nó administrativo não primário hospedado em um dispositivo de serviços.

Use o procedimento que corresponde à plataforma de substituição selecionada para o nó. Depois de concluir o procedimento de substituição do nó (que é adequado para todos os tipos de nó), esse procedimento o direcionará para a próxima etapa para recuperação do nó administrativo não primário.

Plataforma de substituição	Procedimento
VMware	"Substituir um nó VMware"
Linux	"Substituir um nó Linux"
Aparelhos de serviços	"Substituir um aparelho de serviços"
OpenStack	Os arquivos de disco de máquina virtual e scripts fornecidos pela NetApp para OpenStack não são mais suportados para operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação do OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para "substituindo um nó Linux" .

Selecione Iniciar recuperação para configurar o nó de administração não primário

Após substituir um nó administrativo não primário, você deve selecionar Iniciar recuperação no Grid Manager para configurar o novo nó como um substituto para o nó com falha.

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.
- Você implantou e configurou o nó de substituição.

Passos

1. No Grid Manager, selecione **MANUTENÇÃO > Tarefas > Recuperação**.
2. Selecione o nó da grade que você deseja recuperar na lista Nós Pendentes.

Os nós aparecem na lista depois de falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Digite a **senha de provisionamento**.
4. Clique em **Iniciar recuperação**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

.....

Start Recovery

5. Monitore o progresso da recuperação na tabela Nó da grade em recuperação.



Enquanto o procedimento de recuperação estiver em execução, você pode clicar em **Redefinir** para iniciar uma nova recuperação. Uma caixa de diálogo aparece, indicando que o nó ficará em um estado indeterminado se você redefinir o procedimento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se você quiser tentar a recuperação novamente após redefinir o procedimento, deverá restaurar o nó para um estado pré-instalado, da seguinte maneira:

- **VMware:** Exclua o nó de grade virtual implantado. Então, quando estiver pronto para reiniciar a recuperação, reimplante o nó.
- **Linux:** Reinicie o nó executando este comando no host Linux: `storagegrid node force-recovery node-name`

- **Dispositivo:** Se você quiser tentar a recuperação novamente após redefinir o procedimento, deverá restaurar o nó do dispositivo para um estado pré-instalado executando `sgareinstall` no nó. Ver ["Preparar o aparelho para reinstalação \(somente substituição da plataforma\)"](#).

6. Se o logon único (SSO) estiver habilitado para seu sistema StorageGRID e a confiança da parte confiável para o nó de administração que você recuperou foi configurada para usar o certificado de interface de gerenciamento padrão, atualize (ou exclua e recrie) a confiança da parte confiável do nó nos Serviços de Federação do Active Directory (AD FS). Use o novo certificado de servidor padrão gerado durante o processo de recuperação do nó de administração.



Para configurar uma confiança de terceira parte confiável, consulte ["Configurar logon único"](#). Para acessar o certificado do servidor padrão, efetue login no shell de comando do nó de administração. Vá para o `/var/local/mgmt-api` diretório e selecione o `server.crt` arquivo.

Restaurar log de auditoria no nó de administração não primário recuperado

Se você conseguiu preservar o log de auditoria do nó administrativo não primário com falha, para que as informações históricas do log de auditoria sejam retidas, você pode copiá-lo para o nó administrativo não primário que está recuperando.

Antes de começar

- O nó de administração recuperado está instalado e em execução.
- Você copiou os logs de auditoria para outro local após a falha do nó de administração original.

Sobre esta tarefa

Se um nó administrativo falhar, os logs de auditoria salvos nesse nó administrativo serão potencialmente perdidos. Pode ser possível preservar dados contra perda copiando logs de auditoria do nó administrativo com falha e restaurando esses logs de auditoria para o nó administrativo recuperado. Dependendo da falha, pode não ser possível copiar logs de auditoria do nó de administração com falha. Nesse caso, se a implantação tiver mais de um nó administrativo, você poderá recuperar logs de auditoria de outro nó administrativo, pois os logs de auditoria são replicados para todos os nós administrativos.

Se houver apenas um nó de administração e o log de auditoria não puder ser copiado do nó com falha, o nó de administração recuperado começará a registrar eventos no log de auditoria como se a instalação fosse nova.

Você deve recuperar um nó de administração o mais rápido possível para restaurar a funcionalidade de registro.

Por padrão, as informações de auditoria são enviadas para o log de auditoria nos nós de administração. Você pode pular estas etapas se alguma das seguintes situações se aplicar:



- Você configurou um servidor syslog externo e os logs de auditoria agora estão sendo enviados para o servidor syslog em vez de para os nós de administração.
- Você especificou explicitamente que as mensagens de auditoria devem ser salvas somente nos nós locais que as geraram.

Ver ["Configurar mensagens de auditoria e destinos de log"](#) para mais detalhes.

Passos

1. Efetue login no nó de administração recuperado:

a. Digite o seguinte comando:

```
ssh admin@recovery_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.

Depois de efetuar login como root, o prompt muda de `$` para `#`.

2. Verifique quais arquivos de auditoria foram preservados:

```
cd /var/local/log
```

3. Copie os arquivos de log de auditoria preservados para o nó de administração recuperado:

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

Quando solicitado, digite a senha do administrador.

4. Por segurança, exclua os logs de auditoria do nó de grade com falha após verificar se eles foram copiados com sucesso para o nó de administração recuperado.

5. Atualize as configurações de usuário e grupo dos arquivos de log de auditoria no nó de administração recuperado:

```
chown ams-user:bycast *
```

6. Sair como root: `exit`

Restaurar o banco de dados do nó de administração ao recuperar o nó de administração não primário

Se quiser manter as informações históricas sobre atributos e alertas em um nó administrativo não primário que falhou, você pode restaurar o banco de dados do nó administrativo a partir do nó administrativo primário.

Antes de começar

- O nó de administração recuperado está instalado e em execução.
- O sistema StorageGRID inclui pelo menos dois nós de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

Se um nó administrativo falhar, as informações históricas armazenadas no banco de dados do nó administrativo serão perdidas. Este banco de dados inclui as seguintes informações:

- Histórico de alertas
- Dados de atributos históricos, que são usados em gráficos de estilo legado na página Nós

Quando você recupera um nó de administração, o processo de instalação do software cria um banco de

dados de nó de administração vazio no nó recuperado. No entanto, o novo banco de dados inclui apenas informações de servidores e serviços que atualmente fazem parte do sistema ou foram adicionados posteriormente.

Se você restaurou um nó administrativo não primário, poderá restaurar as informações históricas copiando o banco de dados do nó administrativo do nó administrativo primário (o *nó administrativo de origem*) para o nó recuperado.



Copiar o banco de dados do nó de administração pode levar várias horas. Alguns recursos do Grid Manager ficarão indisponíveis enquanto os serviços estiverem interrompidos no nó de origem.

Passos

1. Efetue login no nó de administração de origem:
 - a. Digite o seguinte comando: `ssh admin@grid_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.
2. Execute o seguinte comando no nó de administração de origem. Em seguida, insira a senha de provisionamento, se solicitado. `recover-access-points`
3. No nó de administração de origem, pare o serviço MI: `service mi stop`
4. No nó de administração de origem, pare o serviço Management Application Program Interface (mgmt-api): `service mgmt-api stop`
5. Conclua as seguintes etapas no nó de administração recuperado:
 - a. Efetue login no nó de administração recuperado:
 - i. Digite o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Digite a senha listada no `Passwords.txt` arquivo.
 - iii. Digite o seguinte comando para alternar para root: `su -`
 - iv. Digite a senha listada no `Passwords.txt` arquivo.
 - b. Pare o serviço MI: `service mi stop`
 - c. Pare o serviço mgmt-api: `service mgmt-api stop`
 - d. Adicione a chave privada SSH ao agente SSH. Digitar: `ssh-add`
 - e. Digite a senha de acesso SSH listada no `Passwords.txt` arquivo.
 - f. Copie o banco de dados do nó de administração de origem para o nó de administração recuperado: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
 - g. Quando solicitado, confirme que deseja substituir o banco de dados MI no nó de administração recuperado.

O banco de dados e seus dados históricos são copiados para o nó de administração recuperado. Quando a operação de cópia estiver concluída, o script inicia o nó de administração recuperado.
 - h. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Digitar: `ssh-add -D`

6. Reinicie os serviços no nó de administração de origem: `service servermanager start`

Restaurar métricas do Prometheus ao recuperar nó de administração não primário

Opcionalmente, você pode manter as métricas históricas mantidas pelo Prometheus em um nó administrativo não primário que falhou.

Antes de começar

- O nó de administração recuperado está instalado e em execução.
- O sistema StorageGRID inclui pelo menos dois nós de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

Se um nó administrativo falhar, as métricas mantidas no banco de dados Prometheus no nó administrativo serão perdidas. Quando você recupera o nó de administração, o processo de instalação do software cria um novo banco de dados Prometheus. Depois que o nó de administração recuperado é iniciado, ele registra métricas como se você tivesse executado uma nova instalação do sistema StorageGRID .

Se você restaurou um nó administrativo não primário, poderá restaurar as métricas históricas copiando o banco de dados Prometheus do nó administrativo primário (o *nó administrativo de origem*) para o nó administrativo recuperado.



Copiar o banco de dados do Prometheus pode levar uma hora ou mais. Alguns recursos do Grid Manager ficarão indisponíveis enquanto os serviços estiverem interrompidos no nó de administração de origem.

Passos

1. Efetue login no nó de administração de origem:
 - a. Digite o seguinte comando: `ssh admin@grid_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.
2. No nó de administração de origem, pare o serviço Prometheus: `service prometheus stop`
3. Conclua as seguintes etapas no nó de administração recuperado:
 - a. Efetue login no nó de administração recuperado:
 - i. Digite o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Digite a senha listada no `Passwords.txt` arquivo.
 - iii. Digite o seguinte comando para alternar para root: `su -`
 - iv. Digite a senha listada no `Passwords.txt` arquivo.
 - b. Pare o serviço Prometheus: `service prometheus stop`
 - c. Adicione a chave privada SSH ao agente SSH. Digitar: `ssh-add`

- d. Digite a senha de acesso SSH listada no `Passwords.txt` arquivo.
- e. Copie o banco de dados Prometheus do nó de administração de origem para o nó de administração recuperado: `/usr/local/prometheus/bin/prometheus-clone-db.sh`
`Source_Admin_Node_IP`
- f. Quando solicitado, pressione **Enter** para confirmar que deseja destruir o novo banco de dados Prometheus no nó de administração recuperado.

O banco de dados original do Prometheus e seus dados históricos são copiados para o nó de administração recuperado. Quando a operação de cópia estiver concluída, o script inicia o nó de administração recuperado. O seguinte status aparece:

Banco de dados clonado, iniciando serviços

- a. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Digitar: `ssh-add -D`

4. Reinicie o serviço Prometheus no nó de administração de origem. `service prometheus start`

Recuperar de falhas do nó de gateway

Substituir nó de gateway

Você pode substituir um nó de gateway com falha por um nó de gateway em execução no mesmo hardware físico ou virtual, ou pode substituir um nó de gateway em execução no VMware ou em um host Linux por um nó de gateway hospedado em um dispositivo de serviços.

O procedimento de substituição de nó que você deve seguir depende de qual plataforma será usada pelo nó de substituição. Depois de concluir o procedimento de substituição do nó (que é adequado para todos os tipos de nó), esse procedimento o direcionará para a próxima etapa de recuperação do nó do gateway.

Plataforma de substituição	Procedimento
VMware	"Substituir um nó VMware"
Linux	"Substituir um nó Linux"
Aparelhos de serviços	"Substituir um aparelho de serviços"
OpenStack	Os arquivos de disco de máquina virtual e scripts fornecidos pela NetApp para OpenStack não são mais suportados para operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação do OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para "substituindo um nó Linux" .

Selecione Iniciar recuperação para configurar o nó do gateway

Após substituir um nó de gateway, você deve selecionar Iniciar recuperação no Grid

Manager para configurar o novo nó como um substituto para o nó com falha.

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.
- Você implantou e configurou o nó de substituição.

Passos

1. No Grid Manager, selecione **MANUTENÇÃO > Tarefas > Recuperação**.
2. Selecione o nó da grade que você deseja recuperar na lista Nós Pendentes.

Os nós aparecem na lista depois de falharem, mas você não pode selecionar um nó até que ele tenha sido reinstalado e esteja pronto para recuperação.

3. Digite a **senha de provisionamento**.
4. Clique em **Iniciar recuperação**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
104-217-S1	10.96.104.217	Unknown	✓	

Passphrase

Provisioning Passphrase

Start Recovery

5. Monitore o progresso da recuperação na tabela Nó da grade em recuperação.



Enquanto o procedimento de recuperação estiver em execução, você pode clicar em **Redefinir** para iniciar uma nova recuperação. Uma caixa de diálogo aparece, indicando que o nó ficará em um estado indeterminado se você redefinir o procedimento.

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Se você quiser tentar a recuperação novamente após redefinir o procedimento, deverá restaurar o nó para um estado pré-instalado, da seguinte maneira:

- **VMware:** Exclua o nó de grade virtual implantado. Então, quando estiver pronto para reiniciar a recuperação, reimplante o nó.
- **Linux:** Reinicie o nó executando este comando no host Linux: `storagegrid node force-recovery node-name`
- **Dispositivo:** Se você quiser tentar a recuperação novamente após redefinir o procedimento, deverá restaurar o nó do dispositivo para um estado pré-instalado executando `sgareinstall` no nó. Ver ["Preparar o aparelho para reinstalação \(somente substituição da plataforma\)"](#).

Recuperar de falhas do nó de arquivo

Recuperar de falhas do nó de arquivo

O suporte para nós de arquivo foi removido.

Para obter informações sobre como recuperar nós de arquivo, consulte ["Recuperar de falhas do nó de arquivamento \(site de documentação do StorageGRID 11.8\)"](#).

Substituir nó Linux

Substituir nó Linux

Se uma falha exigir que você implante um ou mais novos hosts físicos ou virtuais ou reinstale o Linux em um host existente, implante e configure o host de substituição antes de poder recuperar o nó da grade. Este procedimento é uma etapa do processo de recuperação de nós de grade para todos os tipos de nós de grade.

"Linux" refere-se a uma implantação do Red Hat® Enterprise Linux®, Ubuntu® ou Debian®. Para obter uma lista de versões suportadas, consulte o ["Ferramenta de Matriz de Interoperabilidade NetApp \(IMT\)"](#).

Este procedimento é executado apenas como uma etapa no processo de recuperação de nós de

armazenamento baseados em software, nós de administração primários ou não primários ou nós de gateway. As etapas são idênticas, independentemente do tipo de nó de grade que você está recuperando.

Se mais de um nó de grade estiver hospedado em um host Linux físico ou virtual, você poderá recuperar os nós de grade em qualquer ordem. No entanto, recuperar primeiro um nó administrativo primário, se presente, evita que a recuperação de outros nós da grade seja interrompida enquanto tentam entrar em contato com o nó administrativo primário para se registrar para recuperação.

Implantar novos hosts Linux

Com algumas exceções, você prepara os novos hosts como fez durante o processo de instalação inicial.

Para implantar hosts Linux físicos ou virtuais novos ou reinstalados, siga o procedimento para preparar os hosts nas instruções de instalação do StorageGRID para seu sistema operacional Linux:

- ["Instalar Linux \(Red Hat Enterprise Linux\)"](#)
- ["Instalar Linux \(Ubuntu ou Debian\)"](#)

Este procedimento inclui etapas para realizar as seguintes tarefas:

1. Instale o Linux.
2. Configurar a rede do host.
3. Configurar armazenamento do host.
4. Instale o mecanismo do contêiner.
5. Instale o serviço de host StorageGRID .



Pare após concluir a tarefa "Instalar serviço de host StorageGRID " nas instruções de instalação. Não inicie a tarefa "Implantando nós de grade".

Ao executar essas etapas, observe as seguintes diretrizes importantes:

- Certifique-se de usar os mesmos nomes de interface de host que você usou no host original.
- Se você usar armazenamento compartilhado para dar suporte aos seus nós StorageGRID ou tiver movido algumas ou todas as unidades ou SSDs dos nós com falha para os nós de substituição, será necessário restabelecer os mesmos mapeamentos de armazenamento que estavam presentes no host original. Por exemplo, se você usou WWIDs e aliases em `/etc/multipath.conf` conforme recomendado nas instruções de instalação, certifique-se de usar os mesmos pares de alias/WWID em `/etc/multipath.conf` no host de substituição.
- Se o nó StorageGRID usar armazenamento atribuído de um sistema NetApp ONTAP , confirme se o volume não tem 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.

Restaurar nós de grade para o host

Para restaurar um nó de grade com falha em um novo host Linux, execute estas etapas para restaurar o arquivo de configuração do nó.

1. [Restaurar e validar o nó](#) restaurando o arquivo de configuração do nó. Para uma nova instalação, crie um arquivo de configuração de nó para cada nó de grade a ser instalado em um host. Ao restaurar um nó de grade para um host de substituição, você restaura ou substitui o arquivo de configuração do nó para quaisquer nós de grade com falha.
2. [Inicie o serviço do host StorageGRID](#) .
3. Conforme necessário, [recuperar todos os nós que não iniciam](#) .

Se algum volume de armazenamento em bloco foi preservado do host anterior, talvez seja necessário executar procedimentos de recuperação adicionais. Os comandos nesta seção ajudam a determinar quais procedimentos adicionais são necessários.

Restaurar e validar nós de grade

Você deve restaurar os arquivos de configuração da grade para quaisquer nós de grade com falha e, em seguida, validar os arquivos de configuração da grade e resolver quaisquer erros.

Sobre esta tarefa

Você pode importar qualquer nó de grade que deva estar presente no host, desde que seja `/var/local` o volume não foi perdido como resultado da falha do host anterior. Por exemplo, o `/var/local` o volume ainda pode existir se você usou armazenamento compartilhado para volumes de dados do sistema StorageGRID , conforme descrito nas instruções de instalação do StorageGRID para seu sistema operacional Linux. A importação do nó restaura seu arquivo de configuração do nó no host.

Se não for possível importar os nós ausentes, você deverá recriar os arquivos de configuração da grade.

Você deve então validar o arquivo de configuração da grade e resolver quaisquer problemas de rede ou armazenamento que possam ocorrer antes de reiniciar o StorageGRID. Ao recriar o arquivo de configuração para um nó, você deve usar o mesmo nome para o nó de substituição que foi usado para o nó que você está recuperando.

Consulte as instruções de instalação para obter mais informações sobre a localização do `/var/local` volume para um nó.

- ["Instalar o StorageGRID no Red Hat Enterprise Linux"](#)
- ["Instalar o StorageGRID no Ubuntu ou Debian"](#)

Passos

1. Na linha de comando do host recuperado, liste todos os nós StorageGRID configurados atualmente: `sudo storagegrid node list`

Se nenhum nó de grade estiver configurado, não haverá saída. Se alguns nós de grade estiverem configurados, espere uma saída no seguinte formato:

Name	Metadata-Volume
=====	=====
dc1-adm1	/dev/mapper/sgws-adm1-var-local
dc1-gw1	/dev/mapper/sgws-gw1-var-local
dc1-sn1	/dev/mapper/sgws-sn1-var-local
dc1-arc1	/dev/mapper/sgws-arc1-var-local

Se alguns ou todos os nós de grade que devem ser configurados no host não estiverem listados, você precisará restaurar os nós de grade ausentes.

2. Para importar nós de grade que tenham um /var/local volume:

- a. Execute o seguinte comando para cada nó que você deseja importar: `sudo storagegrid node import node-var-local-volume-path`

O `storagegrid node import` O comando será bem-sucedido somente se o nó de destino tiver sido desligado corretamente no host em que foi executado pela última vez. Se esse não for o caso, você observará um erro semelhante ao seguinte:

```
This node (node-name) appears to be owned by another host (UUID host-uuid).
```

Use the `--force` flag if you are sure import is safe.

- a. Se você vir o erro sobre o nó pertencer a outro host, execute o comando novamente com o `--force` sinalizador para concluir a importação: `sudo storagegrid --force node import node-var-local-volume-path`



Todos os nós importados com o `--force` a bandeira exigirá etapas adicionais de recuperação antes de poder retornar à rede, conforme descrito em "[Próximo passo: execute etapas adicionais de recuperação, se necessário](#)".

3. Para nós de grade que não têm um /var/local volume, recrie o arquivo de configuração do nó para restaurá-lo no host. Para obter instruções, consulte:

- "[Criar arquivos de configuração de nó para o Red Hat Enterprise Linux](#)"
- "[Crie arquivos de configuração de nó para Ubuntu ou Debian](#)"



Ao recriar o arquivo de configuração para um nó, você deve usar o mesmo nome para o nó de substituição que foi usado para o nó que você está recuperando. Para implantações do Linux, certifique-se de que o nome do arquivo de configuração contenha o nome do nó. Você deve usar as mesmas interfaces de rede, mapeamentos de dispositivos de bloco e endereços IP sempre que possível. Essa prática minimiza a quantidade de dados que precisam ser copiados para o nó durante a recuperação, o que pode tornar a recuperação significativamente mais rápida (em alguns casos, minutos em vez de semanas).



Se você usar quaisquer novos dispositivos de bloco (dispositivos que o nó StorageGRID não usou anteriormente) como valores para qualquer uma das variáveis de configuração que começam com `BLOCK_DEVICE_` ao recriar o arquivo de configuração para um nó, siga as diretrizes em [Corrigir erros de dispositivos de bloco ausentes](#) .

4. Execute o seguinte comando no host recuperado para listar todos os nós do StorageGRID .

```
sudo storagegrid node list
```

5. Valide o arquivo de configuração do nó para cada nó da grade cujo nome foi mostrado na saída da lista de nós do storagegrid:

```
sudo storagegrid node validate node-name
```

Você deve corrigir quaisquer erros ou avisos antes de iniciar o serviço de host do StorageGRID . As seções a seguir fornecem mais detalhes sobre erros que podem ter significado especial durante a recuperação.

Corrigir erros de interface de rede ausentes

Se a rede do host não estiver configurada corretamente ou um nome estiver escrito incorretamente, ocorrerá um erro quando o StorageGRID verificar o mapeamento especificado no `/etc/storagegrid/nodes/node-name.conf` arquivo.

Você pode ver um erro ou aviso correspondente a este padrão:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
      <node-name>: Interface <host-interface-name>' does not exist
```

O erro pode ser relatado para a Rede Grid, a Rede Admin ou a Rede Cliente. Este erro significa que o `/etc/storagegrid/nodes/node-name.conf` arquivo mapeia a rede StorageGRID indicada para a interface do host chamada `host-interface-name` , mas não há nenhuma interface com esse nome no host atual.

Se você receber esse erro, verifique se concluiu as etapas em ["Implantar novos hosts Linux"](#) . Use os mesmos nomes para todas as interfaces de host que foram usados no host original.

Se você não conseguir nomear as interfaces do host para corresponder ao arquivo de configuração do nó, poderá editar o arquivo de configuração do nó e alterar o valor de `GRID_NETWORK_TARGET`, `ADMIN_NETWORK_TARGET` ou `CLIENT_NETWORK_TARGET` para corresponder a uma interface do host existente.

Certifique-se de que a interface do host forneça acesso à porta de rede física ou VLAN apropriada e que a interface não faça referência direta a um dispositivo de ligação ou ponte. Você deve configurar uma VLAN (ou outra interface virtual) sobre o dispositivo de ligação no host ou usar um par de ponte e Ethernet virtual (veth).

Corrigir erros de dispositivos de bloco ausentes

O sistema verifica se cada nó recuperado mapeia para um arquivo especial de dispositivo de bloco válido ou

um softlink válido para um arquivo especial de dispositivo de bloco. Se o StorageGRID encontrar um mapeamento inválido no `/etc/storagegrid/nodes/node-name.conf` arquivo, um erro de dispositivo de bloco ausente é exibido.

Se você observar um erro que corresponde a este padrão:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

Isso significa que `/etc/storagegrid/nodes/node-name.conf` mapeia o dispositivo de bloco usado por *node-name* para `PURPOSE` para o caminho fornecido no sistema de arquivos Linux, mas não há um arquivo especial de dispositivo de bloco válido, ou link simbólico para um arquivo especial de dispositivo de bloco, naquele local.

Verifique se você concluiu as etapas em ["Implantar novos hosts Linux"](#). Use os mesmos nomes de dispositivos persistentes para todos os dispositivos de bloco que foram usados no host original.

Se você não conseguir restaurar ou recriar o arquivo especial do dispositivo de bloco ausente, poderá alocar um novo dispositivo de bloco do tamanho e categoria de armazenamento apropriados e editar o arquivo de configuração do nó para alterar o valor de `BLOCK_DEVICE_PURPOSE` para apontar para o novo arquivo especial do dispositivo de bloco.

Determine o tamanho e a categoria de armazenamento apropriados usando as tabelas para seu sistema operacional Linux:

- ["Requisitos de armazenamento e desempenho para o Red Hat Enterprise Linux"](#)
- ["Requisitos de armazenamento e desempenho para Ubuntu ou Debian"](#)

Revise as recomendações para configurar o armazenamento do host antes de prosseguir com a substituição do dispositivo de bloco:

- ["Configurar armazenamento de host para Red Hat Enterprise Linux"](#)
- ["Configurar armazenamento de host para Ubuntu ou Debian"](#)



Se você precisar fornecer um novo dispositivo de armazenamento em bloco para qualquer uma das variáveis do arquivo de configuração começando com `BLOCK_DEVICE_` como o dispositivo de bloco original foi perdido com o host com falha, certifique-se de que o novo dispositivo de bloco não esteja formatado antes de tentar procedimentos de recuperação adicionais. O novo dispositivo de bloco não será formatado se você estiver usando armazenamento compartilhado e tiver criado um novo volume. Se não tiver certeza, execute o seguinte comando em qualquer novo arquivo especial do dispositivo de armazenamento em bloco.



Execute o seguinte comando somente para novos dispositivos de armazenamento em bloco. Não execute este comando se você acredita que o armazenamento em bloco ainda contém dados válidos para o nó que está sendo recuperado, pois todos os dados no dispositivo serão perdidos.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

Iniciar serviço de host StorageGRID

Para iniciar seus nós StorageGRID e garantir que eles reiniciem após uma reinicialização do host, você deve habilitar e iniciar o serviço do host StorageGRID .

Passos

1. Execute os seguintes comandos em cada host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Execute o seguinte comando para garantir que a implantação esteja em andamento:

```
sudo storagegrid node status node-name
```

3. Se algum nó retornar o status "Não em execução" ou "Parado", execute o seguinte comando:

```
sudo storagegrid node start node-name
```

4. Se você habilitou e iniciou o serviço de host StorageGRID anteriormente (ou se não tiver certeza se o serviço foi habilitado e iniciado), execute também o seguinte comando:

```
sudo systemctl reload-or-restart storagegrid
```

Recuperar nós que não iniciam normalmente

Se um nó StorageGRID não se juntar novamente à grade normalmente e não aparecer como recuperável, ele pode estar corrompido. Você pode forçar o nó a entrar no modo de recuperação.

Passos

1. Confirme se a configuração de rede do nó está correta.

O nó pode não ter conseguido se reintegrar à rede devido a mapeamentos incorretos da interface de rede ou a um endereço IP ou gateway incorreto da rede de rede.

2. Se a configuração da rede estiver correta, emita o `force-recovery` comando:

```
sudo storagegrid node force-recovery node-name
```

3. Execute as etapas adicionais de recuperação para o nó. Ver ["Próximo passo: execute etapas adicionais de recuperação, se necessário"](#) .

Próximo passo: execute etapas adicionais de recuperação, se necessário

Dependendo das ações específicas que você tomou para colocar os nós do StorageGRID em execução no host de substituição, pode ser necessário executar

etapas de recuperação adicionais para cada nó.

A recuperação do nó estará concluída se você não precisar tomar nenhuma ação corretiva enquanto substitui o host Linux ou restaura o nó de grade com falha no novo host.

Ações corretivas e próximos passos

Durante a substituição do nó, pode ser necessário tomar uma destas ações corretivas:

- Você teve que usar o `--force` sinalizador para importar o nó.
- Para qualquer `<PURPOSE>`, o valor do `BLOCK_DEVICE_<PURPOSE>` A variável do arquivo de configuração se refere a um dispositivo de bloco que não contém os mesmos dados que continha antes da falha do host.
- Você emitiu `storagegrid node force-recovery node-name` para o nó.
- Você adicionou um novo dispositivo de bloco.

Se você tomou **qualquer** dessas ações corretivas, você deve executar etapas adicionais de recuperação.

Tipo de recuperação	Próximo passo
Nó de administração primário	"Configurar nó de administração primário de substituição"
Nó de administração não primário	"Selecione Iniciar recuperação para configurar o nó de administração não primário"
Nó de gateway	"Selecione Iniciar recuperação para configurar o nó do gateway"
Nó de armazenamento (baseado em software): • Se você tivesse que usar o <code>--force</code> sinalizador para importar o nó ou você emitiu <code>storagegrid node force-recovery node-name</code> • Se você tivesse que fazer uma reinstalação completa do nó ou precisasse restaurar <code>/var/local</code>	"Selecione Iniciar recuperação para configurar o nó de armazenamento"
Nó de armazenamento (baseado em software): • Se você adicionou um novo dispositivo de bloco. • Se, por qualquer <code><PURPOSE></code>, o valor do <code>BLOCK_DEVICE_<PURPOSE></code> A variável do arquivo de configuração se refere a um dispositivo de bloco que não contém os mesmos dados que continha antes da falha do host.	"Recuperar de falha de volume de armazenamento onde a unidade do sistema está intacta"

Substituir nó VMware

Ao recuperar um nó StorageGRID com falha que estava hospedado no VMware, você remove o nó com falha e implanta um nó de recuperação.

Antes de começar

Você determinou que a máquina virtual não pode ser restaurada e deve ser substituída.

Sobre esta tarefa

Use o VMware vSphere Web Client para primeiro remover a máquina virtual associada ao nó de grade com falha. Depois, você pode implantar uma nova máquina virtual.

Este procedimento é apenas uma etapa no processo de recuperação do nó da rede. O procedimento de remoção e implantação de nós é o mesmo para todos os nós VMware, incluindo nós de administração, nós de armazenamento e nós de gateway.

Passos

1. Efetue login no VMware vSphere Web Client.
2. Navegue até a máquina virtual do nó de grade com falha.
3. Anote todas as informações necessárias para implantar o nó de recuperação.
 - a. Clique com o botão direito do mouse na máquina virtual, selecione a aba **Editar configurações** e anote as configurações em uso.
 - b. Selecione a aba **Opções do vApp** para visualizar e registrar as configurações de rede do nó da grade.
4. Se o nó de grade com falha for um nó de armazenamento, determine se algum dos discos rígidos virtuais usados para armazenamento de dados está intacto e preserve-os para reconexão ao nó de grade recuperado.
5. Desligue a máquina virtual.
6. Selecione **Ações > Todas as ações do vCenter > Excluir do disco** para excluir a máquina virtual.
7. Implante uma nova máquina virtual para ser o nó de substituição e conecte-a a uma ou mais redes StorageGRID . Para obter instruções, consulte ["Implantando um nó StorageGRID como uma máquina virtual"](#) .

Ao implantar o nó, você pode, opcionalmente, remapear as portas do nó ou aumentar as configurações de CPU ou memória.



Após implantar o novo nó, você pode adicionar novos discos virtuais de acordo com seus requisitos de armazenamento, reconectar quaisquer discos rígidos virtuais preservados do nó de grade com falha removido anteriormente, ou ambos.

8. Conclua o procedimento de recuperação do nó, com base no tipo de nó que você está recuperando.

Tipo de nó	Vá para
Nó de administração primário	"Configurar nó de administração primário de substituição"
Nó de administração não primário	"Selecione Iniciar recuperação para configurar o nó de administração não primário"

Tipo de nó	Vá para
Nó de gateway	"Selecione Iniciar recuperação para configurar o nó do gateway"
Nó de armazenamento	"Selecione Iniciar recuperação para configurar o nó de armazenamento"

Substituir nó com falha por dispositivo de serviços

Substituir nó com falha por dispositivo de serviços

Você pode usar um dispositivo de serviços para recuperar um nó de gateway com falha, um nó de administração não primário com falha ou um nó de administração primário com falha que estava hospedado no VMware, em um host Linux ou em um dispositivo de serviços. Este procedimento é uma etapa do procedimento de recuperação do nó da grade.

Antes de começar

- Você determinou que uma das seguintes situações é verdadeira:
 - A máquina virtual que hospeda o nó não pode ser restaurada.
 - O host Linux físico ou virtual para o nó da grade falhou e deve ser substituído.
 - O dispositivo de serviços que hospeda o nó da rede deve ser substituído.
- Você confirmou que a versão do instalador do StorageGRID Appliance no appliance de serviços corresponde à versão do software do seu sistema StorageGRID . Ver ["Verifique e atualize a versão do instalador do StorageGRID Appliance"](#) .



Não implante um dispositivo de serviços SG110 e um SG1100 ou um dispositivo de serviços SG100 e um SG1000 no mesmo site. Pode resultar em desempenho imprevisível.

Sobre esta tarefa

Você pode usar um dispositivo de serviços para recuperar um nó de grade com falha nos seguintes casos:

- O nó com falha foi hospedado no VMware ou Linux (["mudança de plataforma"](#))
- O nó com falha foi hospedado em um dispositivo de serviços (["substituição de plataforma"](#))

Instalar serviço de appliance (somente mudança de plataforma)

Ao recuperar um nó de grade com falha que estava hospedado no VMware ou em um host Linux e estiver usando um dispositivo de serviços para o nó de substituição, você deve primeiro instalar o novo hardware do dispositivo usando o mesmo nome de nó (nome do sistema) do nó com falha.

Antes de começar

Você tem as seguintes informações sobre o nó com falha:

- **Nome do nó:** você deve instalar o dispositivo de serviços usando o mesmo nome de nó do nó com falha.

O nome do nó é o nome do host (nome do sistema).

- **Endereços IP:** Você pode atribuir ao dispositivo de serviços os mesmos endereços IP do nó com falha, que é a opção preferencial, ou pode selecionar um novo endereço IP não utilizado em cada rede.

Sobre esta tarefa

Execute este procedimento somente se estiver recuperando um nó com falha que estava hospedado no VMware ou Linux e o estiver substituindo por um nó hospedado em um dispositivo de serviços.

Passos

1. Siga as instruções para instalar um novo dispositivo de serviços. Ver "[Início rápido para instalação de hardware](#)".
2. Quando solicitado um nome de nó, use o nome do nó com falha.

Preparar o aparelho para reinstalação (somente substituição da plataforma)

Ao recuperar um nó de grade que estava hospedado em um dispositivo de serviços, você deve primeiro preparar o dispositivo para a reinstalação do software StorageGRID .

Execute este procedimento somente se estiver substituindo um nó com falha que estava hospedado em um dispositivo de serviços. Não siga estas etapas se o nó com falha foi originalmente hospedado no VMware ou em um host Linux.

Passos

1. Efetue login no nó de grade com falha:
 - a. Digite o seguinte comando: `ssh admin@grid_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. Prepare o dispositivo para a instalação do software StorageGRID . Digitar: `sgareinstall`
3. Quando solicitado a continuar, digite: `y`

O dispositivo é reinicializado e sua sessão SSH termina. Geralmente, leva cerca de 5 minutos para que o instalador do StorageGRID Appliance fique disponível, embora em alguns casos você possa precisar esperar até 30 minutos.

O dispositivo de serviços é reiniciado e os dados no nó da grade não ficam mais acessíveis. Os endereços IP configurados durante o processo de instalação original devem permanecer intactos; no entanto, é recomendável que você confirme isso quando o procedimento for concluído.

Após executar o `sgareinstall` comando, todas as contas, senhas e chaves SSH provisionadas StorageGRID são removidas e novas chaves de host são geradas.

Iniciar instalação de software no dispositivo de serviços

Para instalar um nó de gateway ou um nó de administração em um dispositivo de

serviços, use o instalador do dispositivo StorageGRID , que está incluído no dispositivo.

Antes de começar

- O dispositivo é instalado em um rack, conectado às suas redes e ligado.
- Os links de rede e endereços IP são configurados para o dispositivo usando o StorageGRID Appliance Installer.
- Se estiver instalando um nó de gateway ou um nó de administração não primário, você saberá o endereço IP do nó de administração primário da grade StorageGRID .
- Todas as sub-redes da Rede de Grade listadas na página Configuração de IP do Instalador do Dispositivo StorageGRID são definidas na Lista de Sub-redes da Rede de Grade no Nó de Administração primário.

Ver "[Início rápido para instalação de hardware](#)" .

- Você está usando um "[navegador da web compatível](#)" .
- Você tem um dos endereços IP atribuídos ao dispositivo. Você pode usar o endereço IP da Rede de Administração, da Rede de Grade ou da Rede de Cliente.
- Se estiver instalando um nó de administração primário, você terá os arquivos de instalação do Ubuntu ou Debian para esta versão do StorageGRID disponíveis.



Uma versão recente do software StorageGRID é pré-carregada no dispositivo de serviços durante a fabricação. Se a versão pré-carregada do software corresponder à versão que está sendo usada na sua implantação do StorageGRID , você não precisará dos arquivos de instalação.

Sobre esta tarefa

Para instalar o software StorageGRID em um dispositivo de serviços:

- Para um nó de administração primário, especifique o nome do nó e carregue os pacotes de software apropriados (se necessário).
- Para um nó de administração não primário ou um nó de gateway, especifique ou confirme o endereço IP do nó de administração primário e o nome do nó.
- Você inicia a instalação e aguarda enquanto os volumes são configurados e o software é instalado.
- No meio do processo, a instalação é pausada. Para retomar a instalação, você deve entrar no Grid Manager e configurar o nó pendente como um substituto para o nó com falha.
- Após configurar o nó, o processo de instalação do dispositivo é concluído e o dispositivo é reinicializado.

Passos

1. Abra um navegador e insira um dos endereços IP do dispositivo de serviços.

```
https://Controller_IP:8443
```

A página inicial do instalador do dispositivo StorageGRID é exibida.

NetApp® StorageGRID® Appliance Installer Help ▾

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Home

This Node

Node type Gateway ▾

Node name NetApp-SGA

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery ☒ Uncheck to manually enter the Primary Admin Node IP

Connection state Admin Node discovery is in progress

Cancel Save

Installation

Current state Unable to start installation. The Admin Node connection is not ready.

Start installation

2. Para instalar um nó de administração primário:

- a. Na seção Este nó, para **Tipo de nó**, selecione **Administrador principal**.
- b. No campo **Nome do nó**, insira o mesmo nome que foi usado para o nó que você está recuperando e clique em **Salvar**.
- c. Na seção Instalação, verifique a versão do software listada em Estado atual

Se a versão do software que está pronta para instalar estiver correta, pule para a próxima etapa. [Etapa de instalação](#) .
- d. Se você precisar carregar uma versão diferente do software, no menu **Avançado**, selecione *Carregar software StorageGRID *.

A página Upload StorageGRID Software é exibida.

NetApp® StorageGRID® Appliance Installer

Help ▾

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Upload StorageGRID Software

If this node is the primary Admin Node of a new deployment, you must use this page to upload the StorageGRID software installation package, unless the version of the software you want to install has already been uploaded. If you are adding this node to an existing deployment, you can avoid network traffic by uploading the installation package that matches the software version running on the existing grid. If you do not upload the correct package, the node obtains the software from the grid's primary Admin Node during installation.

Current StorageGRID Installation Software

Version

None

Package Name

None

Upload StorageGRID Installation Software

Software Package

Browse

Checksum File

Browse

- a. Clique em **Procurar** para carregar o **Pacote de software** e o **Arquivo de soma de verificação** para o software StorageGRID .

Os arquivos são carregados automaticamente após você selecioná-los.

- b. Clique em **Início** para retornar à página inicial do instalador do dispositivo StorageGRID .

3. Para instalar um nó de gateway ou um nó de administração não primário:

- a. Na seção Este nó, para **Tipo de nó**, selecione **Gateway** ou **Administrador não primário**, dependendo do tipo de nó que você está restaurando.
- b. No campo **Nome do nó**, insira o mesmo nome que foi usado para o nó que você está recuperando e clique em **Salvar**.
- c. Na seção Conexão do nó de administração principal, determine se você precisa especificar o endereço IP para o nó de administração principal.

O instalador do dispositivo StorageGRID pode descobrir esse endereço IP automaticamente, supondo que o nó de administração primário, ou pelo menos um outro nó de grade com ADMIN_IP configurado, esteja presente na mesma sub-rede.

- d. Se este endereço IP não for exibido ou você precisar alterá-lo, especifique o endereço:

Opção	Descrição
Entrada manual de IP	a. Desmarque a caixa de seleção Habilitar descoberta do nó de administração. b. Digite o endereço IP manualmente. c. Clique em Salvar. d. Aguarde enquanto o estado da conexão para o novo endereço IP se torna "pronto".

1610

Opção	Descrição
Descoberta automática de todos os nós administrativos primários conectados	a. Marque a caixa de seleção Habilitar descoberta do nó de administração. b. Na lista de endereços IP descobertos, selecione o nó de administração principal da grade onde este dispositivo de serviços será implantado. c. Clique em Salvar. d. Aguarde enquanto o estado da conexão para o novo endereço IP se torna "pronto".

- Na seção Instalação, confirme se o estado atual é Pronto para iniciar a instalação do nome do nó e se o botão **Iniciar instalação** está habilitado.

Se o botão **Iniciar instalação** não estiver habilitado, talvez seja necessário alterar a configuração de rede ou as configurações de porta. Para obter instruções, consulte as instruções de manutenção do seu aparelho.

- Na página inicial do StorageGRID Appliance Installer, clique em **Iniciar instalação**.

O estado atual muda para "A instalação está em andamento" e a página Instalação do monitor é exibida.



Se precisar acessar a página de instalação do monitor manualmente, clique em **Instalação do monitor** na barra de menu.

Instalação de aparelhos de serviços de monitoramento

O instalador do dispositivo StorageGRID fornece status até que a instalação seja concluída. Quando a instalação do software estiver concluída, o dispositivo será reinicializado.

Passos

- Para monitorar o progresso da instalação, clique em **Monitorar instalação** na barra de menu.

A página Instalação do Monitor mostra o progresso da instalação.

Monitor Installation

1. Configure storage		Complete
2. Install OS		Running
Step	Progress	Status
Obtain installer binaries		Complete
Configure installer		Complete
Install OS		Installer VM running
3. Install StorageGRID		Pending
4. Finalize installation		Pending

A barra de status azul indica qual tarefa está em andamento. Barras de status verdes indicam tarefas que foram concluídas com sucesso.



O instalador garante que as tarefas concluídas em uma instalação anterior não sejam executadas novamente. Se você estiver executando uma instalação novamente, todas as tarefas que não precisam ser executadas novamente serão exibidas com uma barra de status verde e o status "Ignorada".

2. Revise o progresso dos dois primeiros estágios da instalação.

◦ 1. Configurar armazenamento

Durante esta etapa, o instalador limpa qualquer configuração existente das unidades e define as configurações do host.

◦ 2. Instalar SO

Durante esse estágio, o instalador copia a imagem do sistema operacional base para o StorageGRID do nó de administração principal para o dispositivo ou instala o sistema operacional base do pacote de instalação para o nó de administração principal.

3. Continue monitorando o progresso da instalação até que ocorra uma das seguintes situações:

- Para nós de gateway de dispositivo ou nós de administração de dispositivo não primários, o estágio **Instalar StorageGRID** é pausado e uma mensagem é exibida no console incorporado, solicitando que você aprove esse nó no nó de administração usando o Grid Manager.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Para os nós de administração primários do dispositivo, uma quinta fase (Carregar instalador do StorageGRID) é exibida. Se a quinta fase estiver em andamento por mais de 10 minutos, atualize a página manualmente.

NetApp® StorageGRID® Appliance Installer
Help

Home
Configure Networking
Configure Hardware
Monitor Installation
Advanced

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Complete
4. Finalize installation	Complete
5. Load StorageGRID Installer	Running

Step	Progress	Status
Starting StorageGRID Installer		Do not refresh. You will be redirected when the installer is ready

4. Vá para a próxima etapa do processo de recuperação para o tipo de nó de grade do dispositivo que você está recuperando.

Tipo de recuperação	Referência
Nó de gateway	" Selecione Iniciar recuperação para configurar o nó do gateway "
Nó de administração não primário	" Selecione Iniciar recuperação para configurar o nó de administração não primário "
Nó de administração primário	" Configurar nó de administração primário de substituição "

Como o suporte técnico recupera um site

Se um site StorageGRID inteiro falhar ou se vários nós de armazenamento falharem, você deverá entrar em contato com o suporte técnico. O suporte técnico avaliará sua situação, desenvolverá um plano de recuperação e, em seguida, recuperará os nós ou sites com falha de uma forma que atenda aos seus objetivos de negócios, otimize o tempo de recuperação e evite perdas desnecessárias de dados.



A recuperação do site só pode ser realizada pelo suporte técnico.

Os sistemas StorageGRID são resilientes a uma ampla variedade de falhas, e você pode executar com sucesso muitos procedimentos de recuperação e manutenção sozinho. No entanto, é difícil criar um procedimento de recuperação de site simples e generalizado porque as etapas detalhadas dependem de fatores específicos da sua situação. Por exemplo:

- Seus objetivos de negócios:** Após a perda completa de um site StorageGRID , você deve avaliar a melhor forma de atingir seus objetivos de negócios. Por exemplo, você quer reconstruir o site perdido no local? Você quer substituir o site StorageGRID perdido em um novo local? A situação de cada cliente é diferente, e seu plano de recuperação deve ser elaborado para atender às suas prioridades.
- Natureza exata da falha:** Antes de iniciar a recuperação do site, estabeleça se algum nó no site com falha está intacto ou se algum nó de armazenamento contém objetos recuperáveis. Se você reconstruir nós ou volumes de armazenamento que contenham dados válidos, poderá ocorrer perda desnecessária de

dados.

- **Políticas de ILM ativas:** O número, o tipo e o local das cópias de objetos na sua grade são controlados pelas suas políticas de ILM ativas. As especificidades das suas políticas de ILM podem afetar a quantidade de dados recuperáveis, bem como as técnicas específicas necessárias para recuperação.



Se um site contiver a única cópia de um objeto e o site for perdido, o objeto será perdido.

- **Consistência do bucket (ou contêiner):** A consistência aplicada a um bucket (ou contêiner) afeta se o StorageGRID replica completamente os metadados do objeto para todos os nós e sites antes de informar ao cliente que a ingestão do objeto foi bem-sucedida. Se o valor de consistência permitir consistência eventual, alguns metadados do objeto podem ter sido perdidos na falha do site. Isso pode afetar a quantidade de dados recuperáveis e potencialmente os detalhes do procedimento de recuperação.
- **Histórico de alterações recentes:** Os detalhes do seu procedimento de recuperação podem ser afetados pelo fato de haver procedimentos de manutenção em andamento no momento da falha ou por alterações recentes feitas em suas políticas de ILM. O suporte técnico deve avaliar o histórico recente da sua rede, bem como sua situação atual, antes de iniciar uma recuperação do site.



A recuperação do site só pode ser realizada pelo suporte técnico.

Esta é uma visão geral do processo que o suporte técnico usa para recuperar um site com falha:

1. Suporte técnico:
 - a. Faz uma avaliação detalhada da falha.
 - b. Trabalha com você para revisar seus objetivos de negócios.
 - c. Desenvolve um plano de recuperação adaptado à sua situação.
2. Se o nó de administração primário falhar, o suporte técnico o recuperará.
3. O suporte técnico recupera todos os nós de armazenamento, seguindo este esboço:
 - a. Substitua o hardware do nó de armazenamento ou as máquinas virtuais conforme necessário.
 - b. Restaurar metadados do objeto para o site com falha.
 - c. Restaure dados de objetos para os nós de armazenamento recuperados.



Perda de dados ocorrerá se os procedimentos de recuperação para um único nó de armazenamento com falha forem usados.



Quando um site inteiro falha, o suporte técnico usa comandos especializados para restaurar objetos e metadados de objetos com sucesso.

4. O suporte técnico recupera outros nós com falha.

Após a recuperação dos metadados e dados do objeto, o suporte técnico usa procedimentos padrão para recuperar nós de gateway com falha ou nós de administração não primários.

Informações relacionadas

["Desativação do local"](#)

Como habilitar o StorageGRID em seu ambiente

Vá para "[Como habilitar o StorageGRID](#)" para aprender como testar e habilitar aplicativos em seu ambiente StorageGRID .

Como gerenciar o StorageGRID usando o NetApp Console

Vá para ["Gerenciamento do StorageGRID usando o NetApp Console"](#) para aprender como gerenciar seus sistemas StorageGRID no NetApp Console usando o Grid Manager e usar os serviços de dados do NetApp Console para backups, armazenamento de dados em camadas e muito mais.

- BlueXP agora é NetApp Console*

O NetApp Console, criado com base na base aprimorada e reestruturada do BlueXP , fornece gerenciamento centralizado do armazenamento NetApp e do NetApp Data Services em ambientes locais e na nuvem em nível empresarial, fornecendo insights em tempo real, fluxos de trabalho mais rápidos e administração simplificada, de forma altamente segura e compatível.

Para obter detalhes sobre o que mudou, consulte o ["Notas de versão do NetApp Console"](#) .

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos autorais

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Política de Privacidade

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais e licenças de terceiros usados no software NetApp .

https://library.netapp.com/ecm/ecm_download_file/ECMLP3330669

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.