aws

Guia do usuário do Lustre

FSx para Lustre

FSx para Lustre: Guia do usuário do Lustre

Table of Contents

O que é o Amazon FSx para Lustre?

O FSx para Lustre torna fácil e econômico iniciar e executar o popular sistema de arquivos de alta performance do Lustre. É possível usar o Lustre para workloads em que a velocidade é importante, como machine learning, computação de alta performance (HPC), processamento de vídeo e modelagem financeira.

O sistema de arquivos de código aberto do Lustre foi projetado para aplicações que exigem armazenamento rápido, em que você deseja que o armazenamento acompanhe a computação. O Lustre foi criado para resolver o problema do processamento rápido e barato dos conjuntos de dados cada vez maiores do mundo. É um sistema de arquivos amplamente usado, projetado para os computadores mais rápidos do mundo. Ele fornece latências inferiores a um milissegundo, até centenas de GBps de throughput e até milhões de IOPS. Para obter mais informações, visite o site do Lustre.

Como um serviço totalmente gerenciado, o Amazon FSx facilita o uso do Lustre para workloads em que a velocidade de armazenamento é importante. O FSx para Lustre elimina a complexidade tradicional de configurar e gerenciar sistemas de arquivos do Lustre, permitindo que você crie e execute em minutos um sistema de arquivos de alta performance e testado na prática. Ele também fornece várias opções de implantação para que você possa otimizar o custo de acordo com suas necessidades.

O FSx para Lustre é compatível com POSIX, de modo que você pode usar suas aplicações atuais baseadas em Linux sem precisar fazer alterações. O FSx para Lustre fornece uma interface nativa de sistema de arquivos e funciona como qualquer sistema de arquivos com o sistema operacional Linux. Ele também fornece read-after-write consistência e suporta o bloqueio de arquivos.

Tópicos

- Preço do Amazon FSx para Lustre
- Fóruns do Amazon FSx para Lustre
- Você é um usuário iniciante do Amazon FSx para Lustre?

Várias opções de implantação

O Amazon FSx para Lustre oferece uma opção de sistemas de arquivos transitórios e permanentes para acomodar diferentes necessidades de processamento de dados. Os sistemas de arquivos transitórios são ideais para armazenamento temporário e para processamento de dados de curto prazo. Os dados não são replicados e não persistem no caso de falha em um servidor de arquivos. Os sistemas de arquivos persistentes são ideais para armazenamento de longo prazo e workloads com foco no throughput. Nos sistemas de arquivos persistentes, os dados são replicados e os servidores de arquivos são substituídos quando apresentam falhas. Para ter mais informações, consulte Opções de implantação para sistemas de arquivos do FSx para Lustre.

Várias opções de armazenamento

O Amazon FSx para Lustre oferece uma opção de tipos de armazenamento em SSD e HDD que são otimizados para diferentes requisitos de processamento de dados:

- Opções de armazenamento SSD: para workloads de baixa latência e uso intenso de IOPS que normalmente têm operações de arquivos pequenas e aleatórias, escolha uma das opções de armazenamento SSD.
- Opções de armazenamento HDD: para workloads com alto throughput que normalmente têm operações de arquivos grandes e sequenciais, escolha uma das opções de armazenamento HDD.

Se você estiver provisionando um sistema de arquivos com a opção de armazenamento HDD, terá a opção de provisionar um cache SSD somente leitura que seja dimensionado para 20% da capacidade do armazenamento HDD. Isso fornece latências inferiores a um milissegundo e IOPS mais altas para arquivos acessados com frequência. Os sistemas de arquivos baseados em SSD e em HDD são provisionados com servidores de metadados baseados em SSD. Como resultado, todas as operações de metadados, que representam a maioria das operações do sistema de arquivos, são fornecidas com latências inferiores a um milissegundo.

Para obter mais informações sobre a performance dessas opções de armazenamento, consulte Performance do Amazon FSx para Lustre.

FSx para Lustre e repositórios de dados

Você pode vincular sistemas de arquivos do FSx para Lustre a repositórios de dados no Amazon S3 ou a armazenamentos de dados on-premises.

Integração do repositório de dados entre FSx para Lustre e S3

O FSx para Lustre se integra ao Amazon S3, facilitando o processamento de conjuntos de dados na nuvem usando o sistema de arquivos de alta performance do Lustre. Quando vinculado a um bucket do Amazon S3, um sistema de arquivos do FSx para Lustre apresenta de forma transparente objetos do S3 como arquivos. O Amazon FSx importa listagens de todos os arquivos existentes no bucket do S3 na criação do sistema de arquivos. O Amazon FSx também pode importar listas de arquivos adicionados ao repositório de dados após a criação do sistema de arquivos. Você pode definir as preferências de importação para atender às suas necessidades de fluxo de trabalho. O sistema de arquivos também possibilita que você grave os dados do sistema de arquivos novamente no S3. As tarefas do repositório de dados simplificam a transferência de dados e metadados entre o sistema de arquivos do FSx para Lustre e seu repositório de dados durável no Amazon S3. Para obter mais informações, consulte Tarefas de repositório de dados e Como usar repositórios de dados com o Amazon FSx para Lustre.

FSx para Lustre e repositórios de dados on-premises

Com o Amazon FSx para Lustre, você pode expandir suas workloads de processamento de dados de on-premises para Nuvem AWS importando dados com o uso de AWS Direct Connect ou AWS VPN Para ter mais informações, consulte Como usar o Amazon FSx com dados on-premises.

Acesso a sistemas de arquivo do FSx para Lustre

Você pode misturar e combinar os tipos de instância de computação e as imagens de máquina da Amazon (AMIs) do Linux que estão conectados a um único sistema de arquivos do FSx para Lustre.

Os sistemas de arquivos do Amazon FSx para Lustre são acessíveis por meio de workloads de computação em execução nas instâncias do Amazon Elastic Compute Cloud (Amazon EC2), nos contêineres do Docker do Amazon Elastic Container Service (Amazon ECS) e nos contêineres em execução no Amazon Elastic Kubernetes Service (Amazon EKS).

- Amazon EC2: você acessa seu sistema de arquivos por meio de suas instâncias de computação do Amazon EC2 usando o cliente Lustre de código aberto. As instâncias do Amazon EC2 podem

acessar seu sistema de arquivo por meio de outras zonas de disponibilidade na mesma Amazon Virtual Private Cloud (Amazon VPC), desde que sua configuração de rede forneça acesso entre sub-redes na VPC. Depois que o sistema de arquivos do Amazon FSx para Lustre estiver montado, você poderá trabalhar com os arquivos e diretórios da mesma forma que trabalha com um sistema de arquivos local.

- Amazon EKS: você acessa o Amazon FSx para Lustre por meio dos contêineres executados no Amazon EKS usando o driver CSI do FSx para Lustre de código aberto, conforme descrito no Guia do usuário do Amazon EKS. Seus contêineres em execução no Amazon EKS podem usar volumes persistentes (PVs) de alta performance com o suporte do Amazon FSx para Lustre.
- Amazon ECS: você acessa o Amazon FSx para Lustre por meio dos contêineres do Docker do Amazon ECS nas instâncias do Amazon EC2. Para ter mais informações, consulte Montagem usando o Amazon Elastic Container Service.

O Amazon FSx para Lustre é compatível com as AMIs baseadas em Linux mais populares, incluindo Amazon Linux 2 e Amazon Linux, Red Hat Enterprise Linux (RHEL), CentOS, Ubuntu e SUSE Linux. O cliente Lustre está incluído no Amazon Linux 2 e no Amazon Linux. Para RHEL, CentOS e Ubuntu, um repositório de clientes Lustre AWS fornece clientes compatíveis com esses sistemas operacionais.

Usando o FSx para Lustre, você pode expandir suas workloads de alta computação de on-premises para a Nuvem AWS importando dados pelo AWS Direct Connect ou pela AWS Virtual Private Network. Você pode acessar o sistema de arquivos do Amazon FSx on-premises, copiar dados para seu sistema de arquivos, conforme necessário, e executar workloads com uso intensivo de computação em instâncias na nuvem.

Para obter mais informações sobre clientes, instâncias de computação e ambientes nos quais você pode acessar os sistemas de arquivos do FSx para Lustre, consulte Acesso a sistemas de arquivos.

Integrações com serviços da AWS

O Amazon FSx for Lustre se integra à SageMaker Amazon como fonte de dados de entrada. Ao usar SageMaker com o FSx for Lustre, seus trabalhos de treinamento de aprendizado de máquina são acelerados com a eliminação da etapa inicial de download do Amazon S3. Além disso, o custo total de propriedade (TCO) é reduzido ao evitar o download repetitivo de objetos comuns para trabalhos repetitivos no mesmo conjunto de dados, uma vez que você economiza nos custos de solicitações do S3. Para obter mais informações, consulte O que é SageMaker? no Amazon SageMaker Developer Guide. Para ver uma explicação sobre como usar o Amazon FSx for Lustre como fonte de dados,

consulte Acelere o treinamento na Amazon usando o Amazon SageMaker FSx SageMaker for Lustre e os sistemas de arquivos Amazon EFS no blog do Machine Learning. AWS

O FSx para Lustre se integra com o AWS Batch usando modelos de inicialização do EC2. O AWS Batch permite que você execute workloads de computação em lote na Nuvem AWS, incluindo computação de alta performance (HPC), machine learning e outras workloads assíncronas. O AWS Batch dimensiona as instâncias de forma automática e dinâmica com base nos requisitos de recursos do trabalho. Para obter mais informações, consulte O que é o AWS Batch? no Guia do usuário do AWS Batch.

O FSx para Lustre se integra com o AWS ParallelCluster. O AWS ParallelCluster é uma ferramenta de gerenciamento de clusters de código aberto que conta com o suporte da AWS usada para implantar e gerenciar clusters de HPC. É capaz de criar automaticamente sistemas de arquivos do FSx para Lustre ou usar sistemas de arquivos existentes durante o processo de criação do cluster.

Segurança e conformidade

Os sistemas de arquivo do FSx para Lustre oferecem suporte à criptografia em repouso e em trânsito. O Amazon FSx criptografa automaticamente os dados em repouso do sistema de arquivos usando chaves gerenciadas no AWS Key Management Service (AWS KMS) Os dados em trânsito também são criptografados automaticamente em determinados sistemas de arquivos Regiões da AWS quando acessados a partir de instâncias compatíveis do Amazon EC2. Para obter mais informações sobre criptografia de dados no FSx for LustreRegiões da AWS, incluindo onde a criptografia de dados em trânsito é suportada, consulte. Criptografia de dados no Amazon FSx para Lustre O Amazon FSx foi avaliado em conformidade com as certificações ISO, PCI-DSS e SOC e está qualificado para a HIPAA. Para ter mais informações, consulte Segurança no FSx para Lustre.

Suposições

Neste guia, fazemos as seguintes suposições:

- Se você usa o Amazon Elastic Compute Cloud (Amazon EC2), presumimos que esteja familiarizado com esse serviço. Consulte a documentação do Amazon EC2 para obter mais informações sobre como utilizá-lo.
- Presumimos que você esteja familiarizado com o uso da Amazon Virtual Private Cloud (Amazon VPC). Para obter mais informações sobre como usar a Amazon VPC, consulte o Guia do usuário da Amazon VPC.

- Presumimos que você não tenha alterado as regras do grupo de segurança padrão da sua VPC com base no serviço da Amazon VPC. Se tiver, certifique-se de adicionar as regras necessárias para permitir o tráfego de rede da sua instância do Amazon EC2 para o sistema de arquivos do Amazon FSx para Lustre. Para obter mais detalhes, consulte Controle de acesso ao sistema de arquivos com a Amazon VPC.

Preço do Amazon FSx para Lustre

Com o Amazon FSx para Lustre, não há custos iniciais de hardware ou software. Você paga somente pelos recursos usados, sem compromissos mínimos, custos de configuração ou taxas adicionais. Para obter informações sobre preços e taxas associados ao serviço, consulte Preços do Amazon FSx para Lustre.

Fóruns do Amazon FSx para Lustre

Se você encontrar problemas ao utilizar o Amazon FSx para Lustre, consulte os fóruns.

Você é um usuário iniciante do Amazon FSx para Lustre?

Se você não estiver familiarizado com o Amazon FSx para Lustre, recomendamos que leia as seções abaixo, nesta ordem:

1. Se estiver pronto para criar seu primeiro sistema de arquivos do Amazon FSx para Lustre, tente Conceitos básicos do Amazon FSx para Lustre
2. Para obter informações sobre performance, consulte Performance do Amazon FSx para Lustre.
3. Para obter informações sobre como vincular seu sistema de arquivos a um repositório de dados de bucket do Amazon S3, consulte Como usar repositórios de dados com o Amazon FSx para Lustre.
4. Para obter detalhes de segurança do Amazon FSx para Lustre, consulte Segurança no FSx para Lustre.
5. Para obter informações sobre os limites de escalabilidade do Amazon FSx para Lustre, incluindo throughput e tamanho do sistema de arquivos, consulte Cotas.
6. Para obter informações sobre a API do Amazon FSx para Lustre, consulte Amazon FSx for Lustre API Reference.

Configuração do Amazon FSx para Lustre

Antes de usar o Amazon FSx para Lustre pela primeira vez, execute as tarefas da seção Cadastre-se na Amazon Web Services. Para concluir o Tutorial de conceitos básicos, certifique-se de que o bucket do Amazon S3 que você vinculará ao seu sistema de arquivos tenha as permissões listadas em Adição de permissões para usar repositórios de dados no Amazon S3.

Tópicos

Cadastre-se na Amazon Web Services

Para configurar para a AWS, execute as tarefas a seguir:

1. Cadastrar-se em uma Conta da AWS
2. Criar um usuário administrativo

Cadastrar-se em uma Conta da AWS

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para se cadastrar em uma Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de aplicação envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se cadastra em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e use somente o usuário raiz para realizar as tarefas que exigem acesso do usuário raiz.

A AWS envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário administrativo

Depois de se inscrever em uma Conta da AWS, proteja seu Usuário raiz da conta da AWS, habilite o AWS IAM Identity Center e crie um usuário administrativo para não usar o usuário raiz em tarefas cotidianas.

Proteger seu Usuário raiz da conta da AWS

1. Faça login no AWS Management Console como o proprietário da conta ao escolher a opção Usuário raiz e inserir o endereço de e-mail da Conta da AWS. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS.
2. Ative a autenticação multifator (MFA) para o usuário raiz.c

   Para obter instruções, consulte Habilitar um dispositivo MFA virtual para o usuário raiz de sua conta da Conta da AWS para seu (console) no Guia do usuário do IAM.

Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Enabling AWS IAM Identity Center no Manual do Usuário do AWS IAM Identity Center.
2. No Centro de Identidade do IAM, conceda acesso administrativo a um usuário administrativo.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configure user access with the default Diretório do Centro de Identidade do IAM no Manual do Usuário do AWS IAM Identity Center.

Login como usuário administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

Para obter ajuda com o login utilizando um usuário do Centro de Identidade do IAM, consulte Fazer login no portal de acesso da AWS, no Guia do usuário do Início de Sessão da AWS.

Adição de permissões para usar repositórios de dados no Amazon S3

O Amazon FSx para Lustre está profundamente integrado ao Amazon S3. Essa integração significa que as aplicações que acessam o sistema de arquivos do FSx para Lustre também podem acessar facilmente os objetos armazenados no bucket vinculado do Amazon S3. Para ter mais informações, consulte Como usar repositórios de dados com o Amazon FSx para Lustre.

Para usar repositórios de dados, primeiro você deve dar ao Amazon FSx para Lustre determinadas permissões do IAM em um perfil associado à conta do usuário administrador.

Para incorporar uma política em linha de um perfil usando o console

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com//iam/.
2. No painel de navegação, escolha Perfis.
3. Na lista, selecione o nome da função para incorporar uma política.
4. Escolha a aba Permissões.
5. Role até o final da página e selecione Add inline policy.

> **Note**
>
> Você não pode incorporar uma política em linha em um perfil vinculado ao serviço no IAM. Como o serviço vinculado determina se as permissões da função podem ou não ser modificadas, você pode adicionar políticas adicionais do console de serviço, da API ou da AWS CLI. Para ver a documentação do perfil vinculado de um serviço, consulte AWSServiços que funcionam com o IAM e escolha Sim na coluna Perfil vinculado ao serviço do seu serviço.

6. Escolha Criação de políticas com o editor visual
7. Adicione a instrução de política de permissões a seguir.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "iam:CreateServiceLinkedRole",
            "iam:AttachRolePolicy",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/*"
    }
}
```

Após a criação de uma política em linha, ela é automaticamente incorporada à sua função. Para obter mais informações sobre funções vinculadas ao serviço, consulte Como usar perfis vinculados a serviço no Amazon FSx.

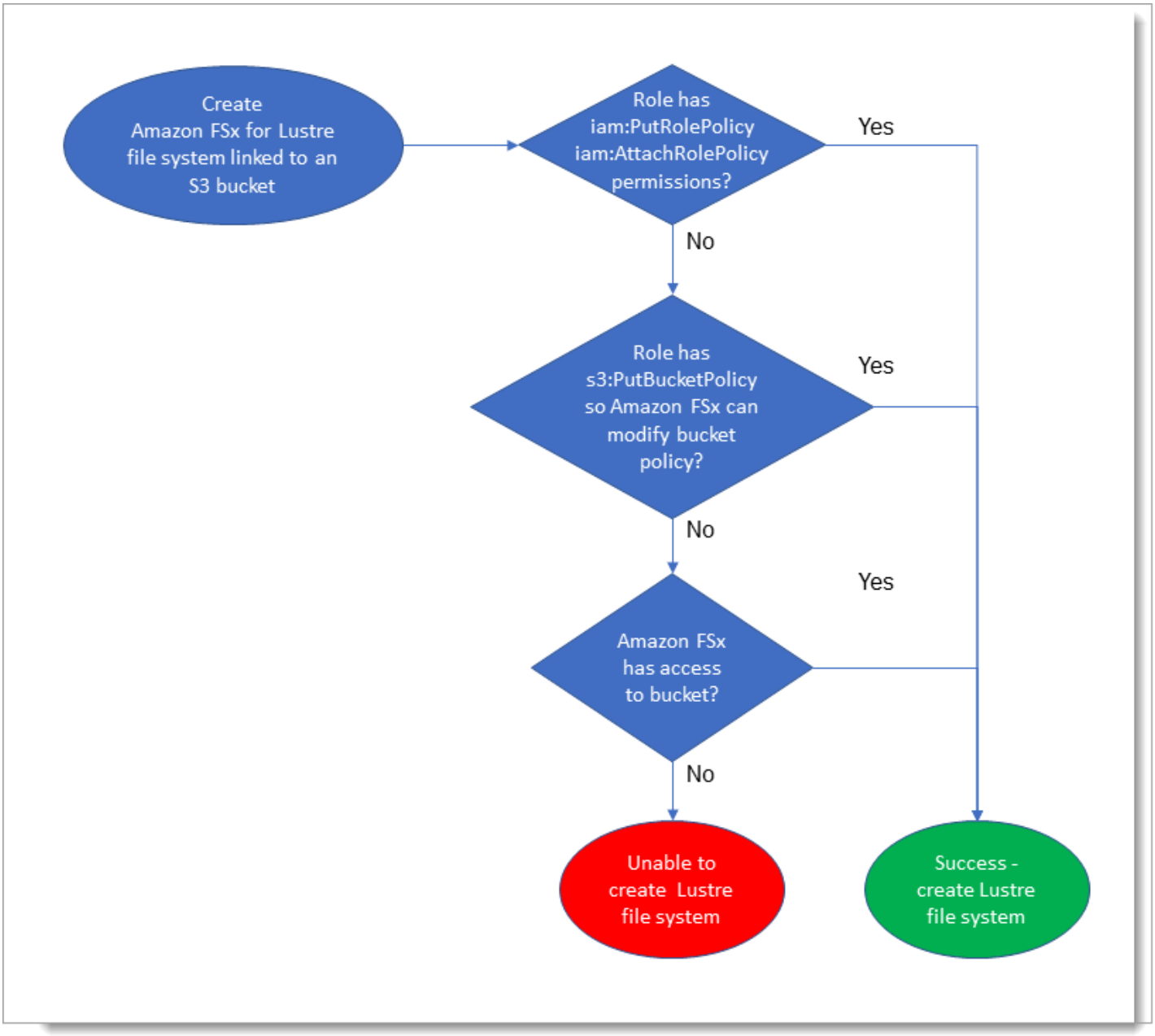
Como o FSx para Lustre verifica o acesso aos buckets do S3 vinculados

Se o perfil do IAM que você usa para criar o sistema de arquivos do FSx para Lustre não tiver as permissões `iam:AttachRolePolicy` e `iam:PutRolePolicy`, o Amazon FSx verificará se pode atualizar a política de bucket do S3. O Amazon FSx poderá atualizar a política de bucket se a permissão `s3:PutBucketPolicy` estiver incluída no perfil do IAM para permitir que o sistema de arquivos do Amazon FSx importe ou exporte dados para o bucket do S3. Se for permitido modificar a política do bucket, o Amazon FSx adicionará as seguintes permissões à política do bucket:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:PutObject`
- `s3:Get*`
- `s3:List*`
- `s3:PutBucketNotification`
- `s3:PutBucketPolicy`
- `s3:DeleteBucketPolicy`

Se o Amazon FSx não puder modificar a política de bucket, ele verificará se a política existente concede a ele acesso ao bucket.

Se todas essas opções falharem, a solicitação para criar o sistema de arquivos falhará. O diagrama a seguir ilustra as verificações que o Amazon FSx segue ao determinar se um sistema de arquivos pode acessar o bucket do S3 ao qual ele será vinculado.



Próxima etapa

Para começar a usar o FSx para ONTAP, consulte Conceitos básicos do Amazon FSx para Lustre para obter instruções de como criar seus recursos do Amazon FSx para Lustre.

Conceitos básicos do Amazon FSx para Lustre

A seguir, você aprenderá como começar a usar o Amazon FSx para Lustre. Estas etapas orientam a criação de um sistema de arquivos do Amazon FSx para Lustre e o acesso a ele usando suas instâncias de computação. Opcionalmente, as etapas mostram como usar o sistema de arquivos do Amazon FSx para Lustre para processar os dados no bucket do Amazon S3 com aplicações baseadas em arquivos.

Este exercício sobre os conceitos básicos inclui as etapas apresentadas a seguir.

Tópicos

Pré-requisitos

Para realizar este exercício sobre os conceitos básicos, você precisará do seguinte:

- Uma AWS conta com as permissões necessárias para criar um sistema de arquivos Amazon FSx for Lustre e uma instância do Amazon EC2. Para ter mais informações, consulte Configuração do Amazon FSx para Lustre.
- Crie um grupo de segurança da Amazon VPC para ser associado ao seu sistema de arquivos FSx for Lustre e não o altere após a criação do sistema de arquivos. Para obter mais informações, consulte Para criar um grupo de segurança para seu sistema de arquivos Amazon FSx.
- Uma instância do Amazon EC2 que executa uma versão com suporte do Linux em sua nuvem privada virtual (VPC) com base no serviço da Amazon VPC. Para este exercício de introdução, recomendamos o uso do Amazon Linux 2023. Você instalará o cliente Lustre nesta instância do EC2 e, em seguida, montará o sistema de arquivos do FSx para Lustre na instância do EC2. Para obter mais informações sobre a criação de uma instância do EC2, consulte Getting started: Launch an instance or Launch your instance no Amazon EC2 User Guide for Linux Instances.

O cliente Lustre é compatível com Amazon Linux; Amazon Linux 2; Amazon Linux 2023; CentOS e Red Hat Enterprise Linux 7.7 a 7.9, 8.2 a 8.9, 9.0 e 9.3; Rocky Linux 8.4 a 8.9, 9.0 e 9.3; SUSE Linux Enterprise Server 12 SP3, SP4 e SP5; e Ubuntu 18.04, 20.04 e 22.04. Para ter mais informações, consulte Compatibilidade do sistema de arquivos Lustre e do kernel do cliente.

Ao criar a instância do Amazon EC2 para este exercício sobre os conceitos básicos, lembre-se do seguinte:

- Recomendamos criar a instância em sua VPC padrão.
- Recomendamos usar o grupo de segurança padrão ao criar sua instância do EC2.

- Cada sistema de arquivos do FSx para Lustre requer um endereço IP para o servidor de metadados (MDS) e um endereço IP para cada servidor de armazenamento (OSS).
  - Os sistemas de arquivos persistentes baseados em SSD são provisionados com 2,4 TiB de armazenamento por OSS.
  - Os sistemas de arquivos persistentes baseados em HDD com 12 MB/s/TiB de capacidade de throughput são provisionados com 6 TiB de armazenamento por OSS.
  - Os sistemas de arquivos persistentes baseados em HDD com 40 MB/s/TiB de capacidade de throughput são provisionados com 1,8 TiB de armazenamento por OSS.
  - Os sistemas de arquivos Scratch_2 são provisionados com 2,4 TiB de armazenamento por OSS.
  - Os sistemas de arquivos Scratch_1 são provisionados com 3,6 TiB de armazenamento por OSS.
- Um bucket do Amazon S3 que armazena os dados a serem processados pela workload. O bucket do S3 corresponderá ao repositório de dados durável vinculado ao seu sistema de arquivos do FSx para Lustre.
- Determinar qual tipo de sistema de arquivos do Amazon FSx para Lustre você deseja criar: transitório ou persistente. Para ter mais informações, consulte Opções de implantação de sistemas de arquivos para o FSx para Lustre .

Crie seu sistema de arquivos FSx for Lustre

A seguir, você criará o sistema de arquivos no console.

Para criar seu sistema de arquivos do

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.

2. No painel, escolha Criar sistema de arquivos para iniciar o assistente de criação de sistemas de arquivos.
3. Escolha FSx para Lustre e, em seguida, selecione Próximo para exibir a página Criar sistema de arquivos.
4. Forneça as informações na seção Detalhes do sistema de arquivos:

   - Em Nome do sistema de arquivos (opcional), forneça um nome para seu sistema de arquivos. É possível usar até 256 letras do Unicode, espaços em branco e números, além dos caracteres especiais + - = . _ : /.
   - Em Tipo de implantação e armazenamento, escolha uma das opções:

     O armazenamento em SSD fornece workloads de baixa latência e uso intensivo de IOPS que, normalmente, têm operações de arquivos pequenas e randômicas. O armazenamento em HDD fornece workloads com alto throughput que, normalmente, têm operações de arquivos grandes e sequenciais.

     Para obter mais informações sobre os tipos de armazenamento, consulte Várias opções de armazenamento.

     Para obter mais informações sobre os tipos de implantação, consulte Opções de implantação para sistemas de arquivos do FSx para Lustre.

     Para obter mais informações sobre Regiões da AWS onde a criptografia de dados em trânsito está disponível, consulteCriptografia de dados em trânsito.

     - Escolha o tipo de implantação Persistent, SSD para o armazenamento de longo prazo e para as workloads sensíveis à latência que requerem os mais altos níveis de IOPS e throughput. Os servidores de arquivos estão altamente disponíveis, os dados são replicados automaticamente na zona de disponibilidade do sistema de arquivos e oferecem suporte à criptografia de dados em trânsito. O tipo de implantação Persistent, SSD usa Persistent 2, a última geração de sistemas de arquivos persistentes.
     - Escolha o tipo de implantação Persistent, HDD para o armazenamento de longo prazo e para as workloads com foco no throughput que não são sensíveis à latência. Os servidores de arquivos estão altamente disponíveis, os dados são replicados automaticamente na zona de disponibilidade do sistema de arquivos e esse tipo oferece suporte à criptografia de dados em trânsito. O tipo de implantação Persistent, HDD usa o tipo de implantação Persistent 1.

Escolha com cache SSD para criar um cache SSD que é dimensionado para 20% da capacidade de armazenamento em HDD com a finalidade de fornecer latências inferiores a um milissegundo e IOPS mais altas para arquivos acessados com frequência.

- Escolha o tipo de implantação Scratch, SSD para o armazenamento temporário e o processamento de dados de curto prazo. O tipo de implantação Scratch, SSD usa sistemas de arquivos Scratch 2 e oferece criptografia de dados em trânsito.

- Escolha a quantidade de Throughput por unidade de armazenamento desejada para o sistema de arquivos. Esta opção é válida somente para tipos de implantação Persistent.

  O Throughput por unidade de armazenamento corresponde à quantidade de throughput de leitura e de gravação para cada 1 tebibyte (TiB) de armazenamento provisionado, em MB/s/TiB. Você paga pela quantidade de throughput que provisiona:

  - Para o armazenamento persistente baseados em SSD, escolha um valor de 125, 250, 500 ou 1.000 MB/s/TiB.
  - Para o armazenamento persistente em HDD, escolha um valor de 12 ou 40 MB/s/TiB.

  É possível aumentar ou diminuir a quantidade de throughput por unidade de armazenamento, conforme necessário, após criar o sistema de arquivos. Para ter mais informações, consulte Como gerenciar a capacidade de throughput.

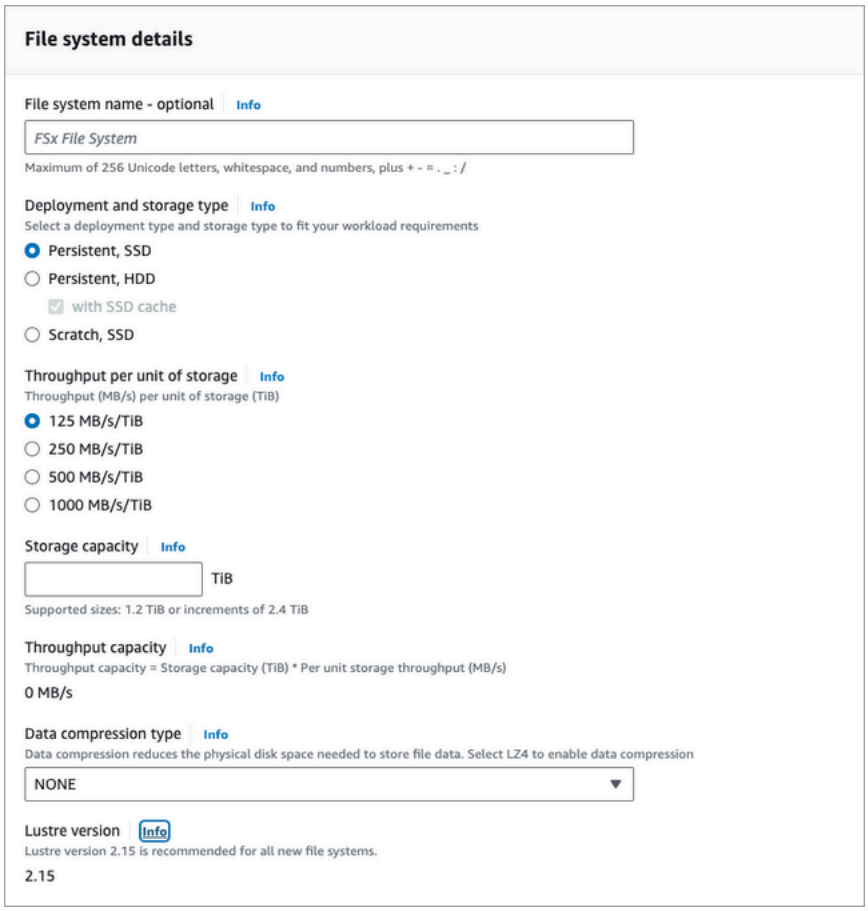
- Em Capacidade de armazenamento, defina a quantidade de capacidade de armazenamento para o sistema de arquivos, em TiB:

  - Para um tipo de implantação Persistent, SSD, defina-a como um valor de 1,2 TiB, 2,4 TiB ou incrementos de 2,4 TiB.
  - Para um tipo de implantação Persistent, HDD, esse valor pode ser definido em incrementos de 6,0 TiB para sistemas de arquivos de 12 MB/s/TiB e em incrementos de 1,8 TiB para sistemas de arquivos de 40 MB/s/TiB.

  Você pode aumentar a quantidade de capacidade de armazenamento, conforme necessário, após criar o sistema de arquivos. Para ter mais informações, consulte Como gerenciar a capacidade de armazenamento.

- Em Tipo de compactação de dados, escolha NENHUM para desativar a compactação de dados ou escolha LZ4 para ativar a compactação de dados com o algoritmo LZ4. Para ter mais informações, consulte Compactação de dados do Lustre.

Todos os sistemas de arquivos do FSx para Lustre são desenvolvidos na versão 2.15 do Lustre quando criados usando o console do Amazon FSx.

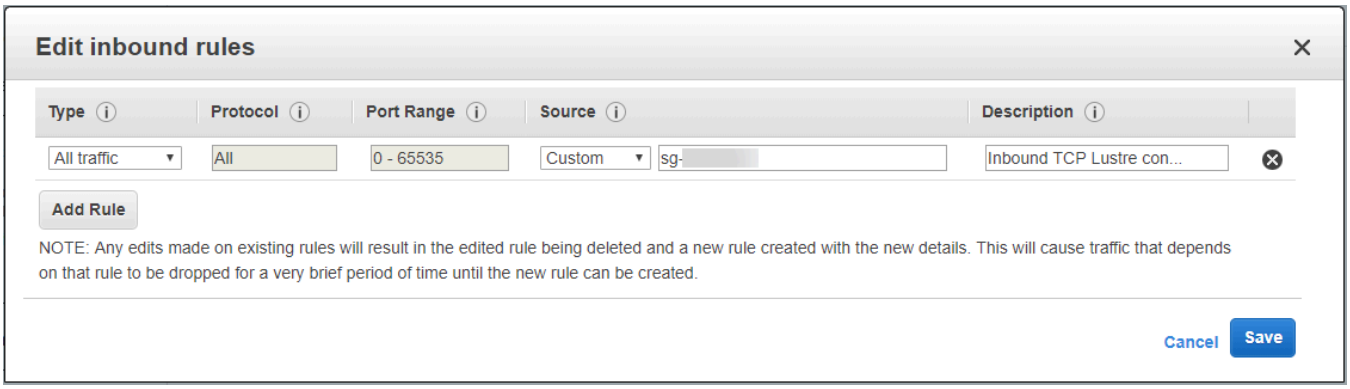


5. Na seção Rede e segurança, forneça as seguintes informações relacionadas à rede e ao grupo de segurança:

   - Em Nuvem privada virtual (VPC), escolha a VPC que você deseja associar ao sistema de arquivos. Para este exercício sobre os conceitos básicos, escolha a mesma VPC escolhida para a instância do Amazon EC2.
   - Em Grupos de segurança de VPC, o ID do grupo de segurança padrão para sua VPC já deve estar adicionado. Se você não estiver usando o grupo de segurança padrão, certifique-se de que a regra de entrada a seguir seja adicionada ao grupo de segurança que você está usando neste exercício sobre os conceitos básicos.

Tipo	Protocolo	Intervalo de portas	Origem	Descrição
Todos os TCP	TCP	0-65535	Personalizado *the_ID_of_this_security_group*	Regra de tráfego de entrada do Lustre

A captura de tela apresentada a seguir mostra um exemplo de edição de regras de entrada.



> **Important**
>
> Certifique-se de que o grupo de segurança que você está usando siga as instruções de configuração fornecidas emControle de acesso ao sistema de arquivos com a Amazon VPC. Você deve configurar o grupo de segurança para permitir o tráfego de entrada nas portas 988 e 1018 a 1023 do próprio grupo de segurança ou do CIDR completo da sub-rede, que é necessário para permitir que os hosts do sistema de arquivos se comuniquem entre si.

- Em Sub-rede, escolha qualquer valor na lista de sub-redes disponíveis.

6. Na seção Criptografia, as opções disponíveis variam com base no tipo de sistema de arquivos que você está criando:

   - Para um sistema de arquivos persistente, você pode escolher uma chave de criptografia AWS Key Management Service (AWS KMS) para criptografar os dados em seu sistema de arquivos em repouso.

- Para um sistema de arquivos temporário, os dados em repouso são criptografados usando chaves gerenciadas por AWS.
- Para sistemas de arquivos transitório 2 e persistente, os dados em trânsito são criptografados automaticamente quando o sistema de arquivos é acessado usando um tipo de instância do Amazon EC2 com suporte. Para ter mais informações, consulte Criptografia de dados em trânsito.

7. Na seção Importação e exportação de repositórios de dados (opcional), a vinculação do sistema de arquivos aos repositórios de dados do Amazon S3 está desabilitado por padrão. Para obter informações sobre como habilitar essa opção e criar uma associação de repositório de dados a um bucket do S3 existente, consulte Para vincular um bucket do S3 ao criar um sistema de arquivos (console).

   > **Important**
   >
   > - Selecionar esta opção também desabilita os backups e você não poderá habilitá-los durante a criação do sistema de arquivos.
   > - Se você vincular um ou mais sistemas de arquivos do Amazon FSx para Lustre a um bucket do Amazon S3, não exclua o bucket do Amazon S3 até que todos os sistemas de arquivos vinculados tenham sido excluídos.

8. Em Registro em log (opcional), o registro em log está habilitado por padrão. Quando ativados, as falhas e os avisos da atividade do repositório de dados em seu sistema de arquivos são registrados no Amazon Logs. CloudWatch Para obter informações sobre como configurar o registro em log, consulte Como gerenciar registros em log.
9. Em Backup e manutenção (opcional), é possível realizar os procedimentos a seguir.

   Para backups automáticos diários:

   - Desabilite o Backup automático diário. Esta opção está habilitada por padrão, a menos que você tenha habilitado Importação e exportação de repositórios de dados.
   - Defina o horário de início para a Janela de backup automático diário.
   - Defina o Período de retenção de backup automático, que pode ter de 1 a 35 dias.

   Para ter mais informações, consulte Trabalhar com backups.

10. Defina o horário de início para a Janela de manutenção semanal ou mantenha-o definido como o padrão Sem preferência.
11. Para Root Squash - opcional, o root squash está desativado por padrão. Para obter informações sobre como habilitar e configurar o root squash, consulte. Para habilitar o root squash ao criar um sistema de arquivos (console)
12. Crie todas as tags que deseja aplicar ao sistema de arquivos.
13. Escolha Próximo para exibir a página Resumo da criação de sistemas de arquivos.
14. Analise as configurações do sistema de arquivos do Amazon FSx para Lustre e, em seguida, escolha Criar sistema de arquivos.

Agora que você criou o sistema de arquivos, anote o nome de domínio totalmente qualificado e o nome da montagem a serem usados em uma etapa posterior. Você pode encontrar o nome de domínio totalmente qualificado e o nome da montagem de um sistema de arquivos ao escolher o nome do sistema de arquivos no painel Caches e, em seguida, ao selecionar Anexar.

Instale e configure o cliente Lustre

Antes de acessar seu sistema de arquivos Amazon FSx for Lustre a partir da sua instância do Amazon EC2, você precisa fazer o seguinte:

- Verifique se sua instância do EC2 atende aos requisitos mínimos do kernel.
- Atualize o kernel, se necessário.
- Baixe e instale o cliente Lustre.

Para verificar a versão do kernel e baixar o cliente Lustre

1. Abra uma janela de terminal na sua instância do EC2.
2. Determine qual kernel está em execução, no momento, na sua instância de computação ao executar o comando apresentado a seguir.

```
uname -r
```

3. Execute um destes procedimentos:

   - Se o comando retornar `6.1.79-99.167.amzn2023.x86_64` para as instâncias do EC2 baseadas em x86 ou `6.1.79-99.167.amzn2023.aarch64` ou valores superiores para as

instâncias do EC2 baseadas no Graviton2, faça download e instale o cliente Lustre com o comando apresentado a seguir.

```
sudo dnf install -y lustre-client
```

- Se o comando retornar um resultado inferior a `6.1.79-99.167.amzn2023.x86_64` para as instâncias do EC2 baseadas em x86 ou inferior a `6.1.79-99.167.amzn2023.aarch64` para as instâncias do EC2 baseadas no Graviton2, atualize o kernel e reinicialize a instância do Amazon EC2 ao executar o comando apresentado a seguir.

  ```
  sudo dnf -y update kernel && sudo reboot
  ```

  Confirme se o kernel foi atualizado usando o comando uname -r. Em seguida, faça download e instale o cliente Lustre conforme descrito acima.

Para obter informações sobre como instalar o cliente Lustre em outras distribuições do Linux, consulte Instalação do cliente Lustre.

Monte o sistema de arquivos

Para montar seu sistema de arquivos, você criará um diretório de montagem ou ponto de montagem e, em seguida, montará o sistema de arquivos no seu cliente e verificará se ele pode acessar o sistema de arquivos.

Como montar o sistema de arquivos

1. Faça um diretório para o ponto de montagem com o comando a seguir.

   ```
   sudo mkdir -p /mnt/fsx
   ```

2. Monte o sistema de arquivos do Amazon FSx para Lustre no diretório que você criou. Use o seguinte comando e substitua os seguintes itens:

   - Substitua *`file_system_dns_name`* pelo nome do Sistema de Nomes de Domínio (DNS) real do sistema de arquivos.
   - *`mountname`*Substitua pelo nome de montagem do sistema de arquivos, que você pode obter executando o describe-file-systems AWS CLI comando ou a operação da DescribeFileSystemsAPI.

```
sudo mount -t lustre -o relatime,flock file_system_dns_name@tcp:/mountname /mnt/fsx
```

Este comando monta o sistema de arquivos com duas opções, `-o relatime` e `flock`:

- `relatime`: embora a opção `atime` mantenha dados de `atime` (horários de acesso de inodes) para cada vez que um arquivo é acessado, a opção `relatime` também mantém dados de `atime`, mas não para cada vez que um arquivo é acessado. Com a opção `relatime` habilitada, os dados de `atime` serão gravados para o disco somente se o arquivo tiver sido modificado desde a última atualização dos dados de `atime` (`mtime`) ou se o arquivo tiver sido acessado pela última vez há mais tempo do que um determinado período (seis horas por padrão). Usar a opção `relatime` ou `atime` otimizará os processos de liberação de arquivos.

  > **Note**
  >
  > Se a workload requerer uma precisão rigorosa quanto ao horário de acesso, você poderá montar com a opção de montagem `atime`. No entanto, isso pode afetar a performance da workload ao aumentar o tráfego de rede necessário para manter valores rigorosos quanto ao horário de acesso.
  > Se a workload não requerer o horário de acesso aos metadados, usar a opção de montagem `noatime` para desabilitar atualizações relacionadas ao horário de acesso poderá proporcionar um ganho de performance. Esteja ciente de que os processos focados na opção `atime`, como a liberação de arquivos ou a liberação da validade de dados, serão imprecisos em suas liberações.

- `flock`: ativa o bloqueio de arquivos para o sistema de arquivos. Se você não desejar que o bloqueio de arquivos seja habilitado, use o comando `mount` sem `flock`.

3. Verifique se o comando mount ocorreu com êxito ao listar o conteúdo do diretório no qual você montou o sistema de arquivos `/mnt/fsx`, usando o comando apresentado a seguir.

```
ls /mnt/fsx
import-path  lustre
$
```

Você também pode usar o comando `df` apresentado a seguir.

```
df
Filesystem                     1K-blocks    Used  Available Use% Mounted on
devtmpf                          1001808       0    1001808   0% /dev
tmpfs                            1019760       0    1019760   0% /dev/shm
tmpfs                            1019760     392    1019368   1% /run
tmpfs                            1019760       0    1019760   0% /sys/fs/cgroup
/dev/xvda1                       8376300 1263180    7113120  16% /
123.456.789.0@tcp:/mountname  3547698816   13824 3547678848   1% /mnt/fsx
tmpfs                             203956       0     203956   0% /run/user/1000
```

Os resultados mostram o sistema de arquivos do Amazon FSx montado em /mnt/fsx.

Executar o fluxo de trabalho

Agora que o sistema de arquivos foi criado e montado em uma instância de computação, é possível usá-lo para executar a workload de computação de alta performance.

Você pode criar uma associação de repositório de dados para vincular o sistema de arquivos a um repositório de dados do Amazon S3. Para obter mais informações, consulte Como vincular o sistema de arquivos a um bucket do S3.

Após vincular o sistema de arquivos a um repositório de dados do Amazon S3, você poderá exportar os dados gravados no sistema de arquivos de volta para o bucket do Amazon S3 a qualquer momento. Em um terminal em uma de suas instâncias de computação, execute o comando apresentado a seguir para exportar um arquivo para o bucket do Amazon S3.

```
sudo lfs hsm_archive file_name
```

Para obter mais informações sobre como executar esse comando em uma pasta ou em uma grande coleção de arquivos com rapidez, consulte Exportação de arquivos usando comandos do HSM.

Limpeza de recursos

Depois de concluir este exercício, você deve seguir estas etapas para limpar seus recursos e proteger sua AWS conta.

Como limpar recursos

1. Se desejar realizar uma exportação final, execute o comando apresentado a seguir.

```
nohup find /mnt/fsx -type f -print0 | xargs -0 -n 1 sudo lfs hsm_archive &
```

2. No console do Amazon EC2, encerre sua instância. Para obter mais informações, consulte Terminar a instância no Guia do usuário do Amazon EC2 para instâncias do Linux.
3. No console do Amazon FSx para Lustre, exclua o sistema de arquivos com o seguinte procedimento:

   a. No painel de navegação, escolha Sistemas de arquivos.

   b. Escolha o sistema de arquivos que você deseja excluir da lista de sistemas de arquivos no painel.

   c. Para Ações, escolha Excluir sistema de arquivos.

   d. Na caixa de diálogo exibida, escolha se deseja fazer um backup final do sistema de arquivos. Em seguida, forneça o ID do sistema de arquivos para confirmar a exclusão. Escolha Excluir sistema de arquivos.
4. Se você criou um bucket do Amazon S3 para este exercício e não deseja preservar os dados exportados, você pode excluí-lo agora. Para obter mais informações, consulte Excluir um bucket no Guia do usuário do Amazon Simple Storage Service.

Opções de implantação para sistemas de arquivos do FSx para Lustre

O FSx para Lustre disponibiliza um sistema de arquivos paralelo de alta performance que armazena dados em diversos servidores de arquivos de rede para maximizar a performance e reduzir os gargalos. Esses servidores têm vários discos. Para distribuir a carga, o Amazon FSx fragmenta os dados do sistema de arquivos em fragmentos menores e os distribui entre discos e servidores usando um processo chamado distribuição. Para obter mais informações sobre a distribuição de dados para o FSx para Lustre, consulte Distribuição de dados no sistema de arquivos.

É uma prática recomendada vincular um repositório de dados de longo prazo e altamente durável residente no Amazon S3 ao sistema de arquivos de alta performance do FSx para Lustre.

Nesse cenário, você armazena os conjuntos de dados no repositório de dados vinculado do Amazon S3. Ao criar o sistema de arquivos do FSx para Lustre, você o vincula ao repositório de dados do S3. Neste ponto, os objetos em seu bucket do S3 são listados como arquivos e diretórios no sistema de arquivos do FSx. Em seguida, o Amazon FSx copia automaticamente o conteúdo do arquivo do S3 para o sistema de arquivos do Lustre quando um arquivo é acessado pela primeira vez no sistema de arquivos do Amazon FSx. Após a execução da workload de computação, ou a qualquer momento, você poderá usar uma tarefa de repositório de dados para exportar as alterações de volta para o S3. Para obter mais informações, consulte Como usar tarefas do repositório de dados para exportar alterações e Como usar repositórios de dados com o Amazon FSx para Lustre.

Opções de implantação de sistemas de arquivos para o FSx para Lustre

O Amazon FSx para Lustre oferece duas opções de implantação para o sistema de arquivos: transitório e persistente.

> **Note**
>
> Ambas as opções de implantação oferecem suporte ao armazenamento em unidade de estado sólido (SSD). No entanto, o suporte para o armazenamento em unidade de disco rígido (HDD) ocorre somente em um dos tipos de implantação persistente.

Você escolhe o tipo de implantação do sistema de arquivos ao criar um novo sistema de arquivos, usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API do Amazon FSx para Lustre. Para obter mais informações, consulte Crie seu sistema de arquivos FSx for Lustre e CreateFileSystemna Referência da API Amazon FSx.

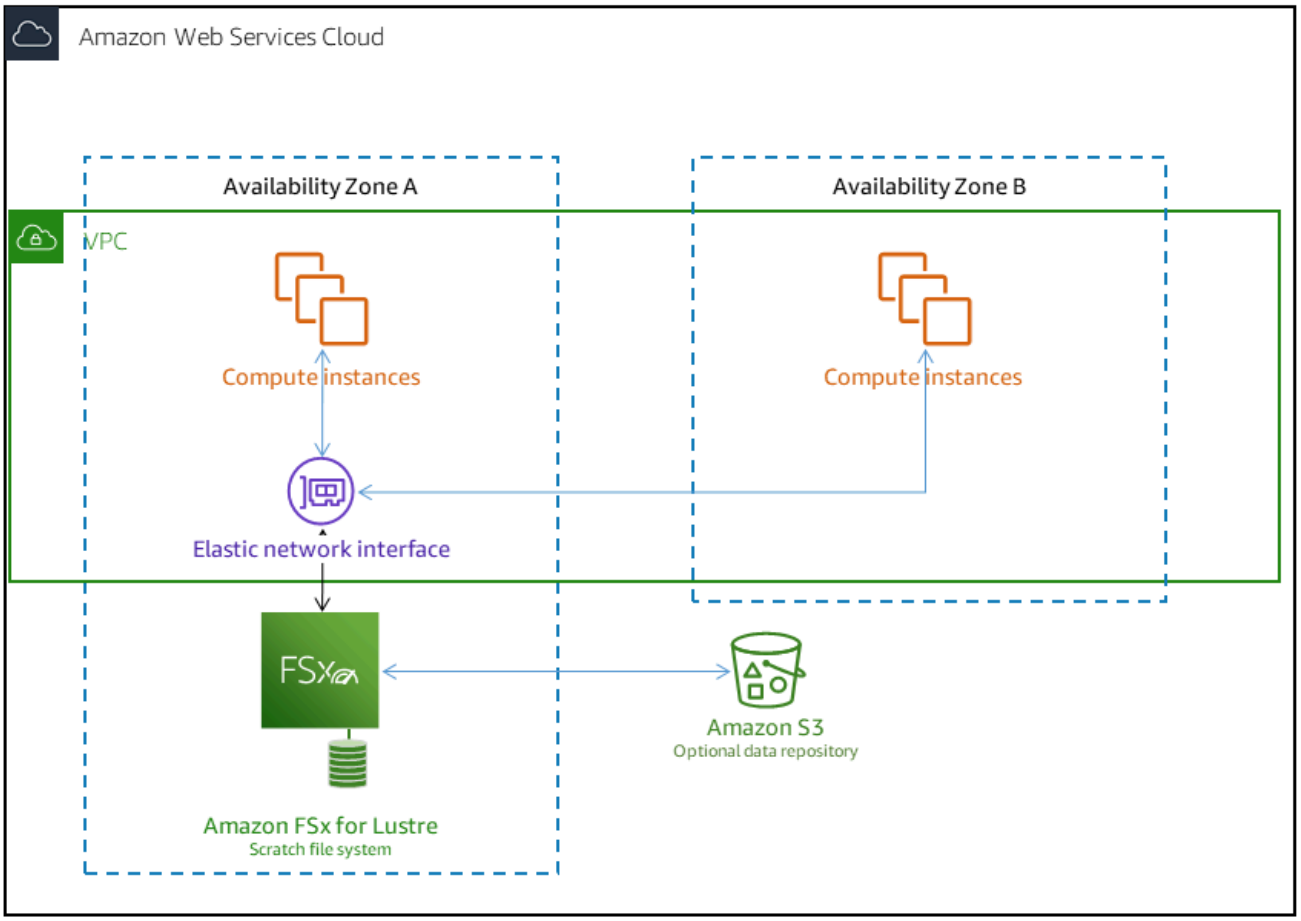
A criptografia de dados em repouso é habilitada automaticamente quando você cria um sistema de arquivos do Amazon FSx para Lustre, independentemente do tipo de implantação usado. Os sistemas de arquivos Scratch 2 e persistent criptografam automaticamente os dados em trânsito quando eles são acessados de instâncias do Amazon EC2 que oferecem suporte à criptografia em trânsito. Para obter mais informações sobre criptografia, consulte Criptografia de dados no Amazon FSx para Lustre.

Sistemas de arquivos transitórios

Os sistemas de arquivos transitórios são projetados para o armazenamento temporário e para o processamento de dados de curto prazo. Os dados não são replicados e não persistem no caso de um servidor de arquivos apresentar falhas. Os sistemas de arquivos transitórios fornecem alto throughput de intermitência com até seis vezes o throughput básico de 200 MBps por TiB de capacidade de armazenamento. Para ter mais informações, consulte Performance agregada do sistema de arquivos.

Use sistemas de arquivos transitórios quando precisar de armazenamento com custo otimizado para workload de curto prazo e com alto processamento.

O diagrama a seguir mostra a arquitetura de um sistema de arquivos transitório do Amazon FSx para Lustre.



Em um sistema de arquivos transitório, os servidores de arquivos não serão substituídos se apresentarem falhas e os dados não forem replicados. Se um servidor de arquivos ou um disco de armazenamento se tornar indisponível em um sistema de arquivos transitório, os arquivos armazenados em outros servidores ainda estarão acessíveis. Se os clientes tentarem acessar dados que estão no servidor ou no disco indisponível, eles receberão um erro de E/S imediato.

A tabela a seguir ilustra a disponibilidade ou a durabilidade para a qual os sistemas de arquivos transitórios com os tamanhos de exemplo foram projetados, ao longo de um dia e de uma semana. Como sistemas de arquivos maiores têm mais servidores de arquivos e mais discos, as probabilidades de falha aumentam.

Tamanho do sistema de arquivos (TiB)	Número de servidores de arquivos	Disponibilidade ou durabilidade ao longo de um dia	Disponibilidade ou durabilidade ao longo de uma semana
1.2	2	99,9%	99,4%
2.4	2	99,9%	99,4%
4.8	3	99,8%	99,2%
9.6	5	99,8%	98,6%
50,4	22	99,1%	93,9%

Sistemas de arquivos persistentes

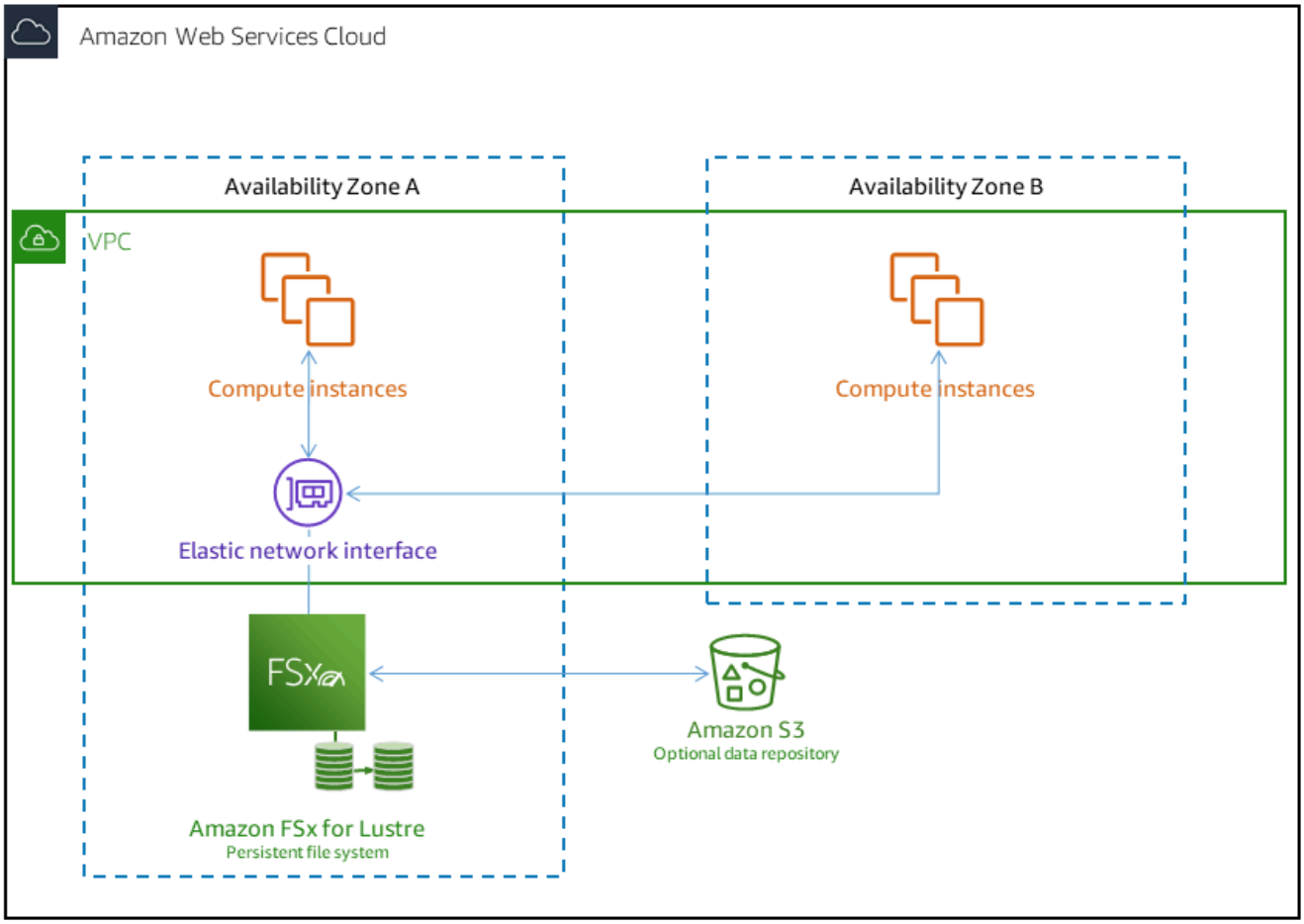
Os sistemas de arquivos persistentes são projetados para armazenamento e workloads de longo prazo. Os servidores de arquivos estão altamente disponíveis e os dados são replicados automaticamente na mesma zona de disponibilidade em que o sistema de arquivos está localizado. Os volumes de dados anexados aos servidores de arquivos são replicados independentemente dos servidores de arquivos aos quais estão anexados.

O Amazon FSx monitora continuamente os sistemas de arquivos persistentes em busca de falhas relacionadas ao hardware e substitui automaticamente os componentes da infraestrutura em caso de falhas. Em um sistema de arquivos persistente, se um servidor de arquivos se tornar indisponível, ele será substituído automaticamente minutos após apresentar falhas. Durante esse período, as solicitações do cliente por dados nesse servidor serão repetidas com transparência e, eventualmente, terão êxito após a substituição do servidor de arquivos. Os dados em sistemas de arquivos persistentes são replicados em discos, e quaisquer discos com falhas são automaticamente substituídos com transparência.

Use sistemas de arquivos persistentes para o armazenamento de longo prazo e para as workloads com foco no throughput que são executadas por períodos prolongados ou indefinidamente e podem ser sensíveis a interrupções na disponibilidade.

O diagrama apresentado a seguir mostra a arquitetura para um sistema de arquivos persistente do Amazon FSx para Lustre, com servidores de arquivos e volumes de dados replicados e altamente disponíveis em uma única zona de disponibilidade.

Os tipos de implantação persistentes criptografam automaticamente os dados em trânsito quando eles são acessados de instâncias do Amazon EC2 que oferecem suporte à criptografia em trânsito.



O Amazon FSx para Lustre oferece suporte a dois tipos de implantação persistentes, Persistent_1 e Persistent_2.

Tipo de implantação Persistent_1

Os tipos de implantação Persistent_1 podem ser desenvolvidos no Lustre 2.10 ou 2.12 e oferecem suporte aos tipos de armazenamento em SSD (unidade de estado sólido) e em HDD (unidade de disco rígido). O tipo de implantação Persistent_1 é adequado para casos de uso que requerem armazenamento de longo prazo e têm workloads com foco no throughput que não são sensíveis à latência.

Para um sistema de arquivos Persistent_1 com armazenamento em SSD, o throughput por unidade de armazenamento corresponde a 50, 100 ou 200 MB/s por tebibyte (TiB). Para armazenamento em

HDD, o throughput do tipo Persistent_1 por unidade de armazenamento corresponde a 12 ou 40 MB/s por TiB.

Você pode criar tipos de implantação Persistent_1 somente ao usar a AWS CLI e a API do Amazon FSx.

Tipo de implantação Persistent_2

O Persistent_2 corresponde à última geração do tipo de implantação persistente e é a melhor opção para casos de uso que requerem armazenamento de longo prazo e têm workloads sensíveis à latência que exigem os mais altos níveis de IOPS e de throughput. Os tipos de implantação Persistent_2 são desenvolvidos no Lustre v2.12 e oferecem suporte ao armazenamento em SSD. Eles oferecem suporte a níveis mais altos de throughput por unidade de armazenamento em comparação com os sistemas de arquivos Persistent_1, com opções de 125, 250, 500 e 1.000 MB/s/TiB.

Você pode criar tipos de implantação Persistent_2 usando o console do Amazon FSx, a AWS Command Line Interface e a API.

Regiões disponíveis

Os tipos de implantação Persistent_1 e Persistent_2 estão disponíveis nas seguintes Regiões da AWS:

Região da AWS	Persistent_1	Persistent_2
Leste dos EUA (Ohio)	✓	✓
Leste dos EUA (N. da Virgínia)	✓	✓
Oeste dos EUA (N. da Califórnia)	✓	
Oeste dos EUA (Los Angeles)	✓	
Oeste dos EUA (Oregon)	✓	✓
África (Cidade do Cabo)	✓	
Ásia-Pacífico (Hong Kong)	✓	✓
Ásia-Pacífico (Hyderabad)	✓	

Região da AWS	Persistent_1	Persistent_2
Ásia-Pacífico (Jacarta)	✓	
Ásia-Pacífico (Melbourne)	✓	
Ásia-Pacífico (Mumbai)	✓	✓
Ásia-Pacífico (Osaka)	✓	
Ásia-Pacífico (Seul)	✓	✓
Ásia-Pacífico (Singapura)	✓	✓
Ásia-Pacífico (Sydney)	✓	✓
Ásia-Pacífico (Tóquio)	✓	✓
Canadá (Central)	✓	✓
Europa (Frankfurt)	✓	✓
Europa (Irlanda)	✓	✓
Europa (Londres)	✓	✓
Europa (Milão)	✓	
Europe (Paris)	✓	
Europa (Espanha)	✓	
Europa (Estocolmo)	✓	✓
Europa (Zurique)	✓	
Israel (Tel Aviv)	✓	
Oriente Médio (Barém)	✓	
Oriente Médio (Emirados Árabes Unidos)	✓	

Região da AWS	Persistent_1	Persistent_2
América do Sul (São Paulo)	✓	
AWS GovCloud (Leste dos EUA)	✓	
AWS GovCloud (Oeste dos EUA)	✓	

Para obter mais informações sobre a performance do FSx para Lustre, consulte Performance agregada do sistema de arquivos.

Como usar repositórios de dados com o Amazon FSx para Lustre

O Amazon FSx para Lustre fornece sistemas de arquivos de alta performance otimizados para processamento rápido da workload. Ele oferece suporte a workloads como machine learning, computação de alta performance (HPC), processamento de vídeo, modelagem financeira e Automação de Design Eletrônico (EDA). Essas workloads geralmente exigem que os dados sejam apresentados usando uma interface de sistema de arquivos escalável e de alta velocidade para acesso aos dados. Muitas vezes, os conjuntos de dados usados para essas workloads são armazenados em repositórios de dados de longo prazo no Amazon S3. O FSx para Lustre é nativamente integrado ao Amazon S3, facilitando o processamento de conjuntos de dados com o sistema de arquivos do Lustre.

> **Note**
>
> Não há suporte para backups do sistema de arquivos naqueles sistemas vinculados a um repositório de dados. Para obter mais informações, consulte Trabalhar com backups.

Tópicos

Visão geral dos repositórios de dados

Ao usar o Amazon FSx para Lustre com repositórios de dados, você pode ingerir e processar grandes volumes de dados de arquivos em um sistema de arquivos de alta performance usando tarefas automáticas de importação e importação de repositórios de dados. Ao mesmo tempo, você pode gravar resultados em seus repositórios de dados usando tarefas automáticas de exportação ou exportação do repositório de dados. Com esses recursos, você pode reiniciar sua workload a qualquer momento usando os dados mais recentes armazenados em seu repositório de dados.

> **Note**
>
> Associações de repositório de dados, exportação automática e suporte para vários repositórios de dados não estão disponíveis nos sistemas de arquivos do FSx para Lustre 2.10 ou nos sistemas de arquivos `Scratch 1`.

O FSx para Lustre está profundamente integrado ao Amazon S3. Essa integração significa que você pode acessar facilmente os objetos armazenados nos buckets do Amazon S3 das aplicações que montam o sistema de arquivos do FSx para Lustre Você também pode executar suas workloads com uso intensivo de computação nas instâncias do Amazon EC2 na Nuvem AWS e exportar os resultados para o seu repositório de dados após a conclusão da workload.

Para acessar objetos no repositório de dados do Amazon S3 como arquivos e diretórios no sistema de arquivos, os metadados de arquivos e diretórios devem ser carregados no sistema de arquivos. Você pode carregar metadados de um repositório de dados vinculado ao criar uma associação de repositório de dados.

Além disso, você pode importar metadados de arquivos e diretórios de seus repositórios de dados vinculados para o sistema de arquivos usando a importação automática ou usando uma tarefa de importação de repositório de dados. Quando você ativa a importação automática para uma associação de repositório de dados, seu sistema de arquivos importa automaticamente os metadados do arquivo à medida que os arquivos são criados, modificados e excluídos no repositório de dados do S3. Como alternativa, você poderá importar metadados de arquivos e diretórios novos ou alterados usando uma tarefa de importação de repositório de dados.

> **Note**
>
> As tarefas de importação automática e de importação do repositório de dados podem ser usadas simultaneamente em um sistema de arquivos.

Você também pode exportar arquivos e seus metadados associados no sistema de arquivos para o repositório de dados usando a exportação automática ou usando uma tarefa de exportação do repositório de dados. Quando você ativa a exportação automática em uma associação de repositório de dados, seu sistema de arquivos exporta automaticamente os dados e metadados do arquivo à medida que os arquivos são criados, modificados ou excluídos. Como alternativa, você pode exportar arquivos ou diretórios usando uma tarefa de exportação do repositório de dados. Quando você usa uma tarefa de exportação do repositório de dados, os dados e metadados do arquivo que foram criados ou modificados desde a última tarefa desse tipo são exportados.

> **Note**
>
> - As tarefas de exportação automática e de exportação do repositório de dados não podem ser usadas simultaneamente em um sistema de arquivos.
> - As associações de repositório de dados só exportam arquivos comuns, links simbólicos e diretórios. Isso significa que todos os outros tipos de arquivos (especial FIFO, especial em bloco, especial de caracteres e soquete) não serão exportados como parte dos processos de exportação, como tarefas de exportação automática e de exportação do repositório de dados.

O FSx para Lustre também oferece suporte a workloads de expansão na nuvem com sistemas de arquivos on-premises, permitindo que você copie dados de clientes on-premises usando AWS Direct Connect ou VPN.

> **Important**
>
> Se você tiver vinculado um ou mais sistemas de arquivos do FSx para Lustre a um repositório de dados no Amazon S3, não exclua o bucket do Amazon S3 até que tenha excluído ou desvinculado todos os sistemas de arquivos vinculados.

Suporte a metadados POSIX para repositórios de dados

O Amazon FSx para Lustre transfere automaticamente metadados da Portable Operating System Interface (POSIX) para arquivos, diretórios e links simbólicos ao importar e exportar dados de e para um repositório de dados vinculado no Amazon S3. Quando você exporta alterações em seu sistema de arquivos para o repositório de dados vinculado, o FSx para Lustre também exporta alterações de metadados POSIX como metadados de objetos do S3. Isso significa que se outro sistema de arquivos do FSx para Lustre importar os mesmos arquivos do S3, os arquivos terão os mesmos metadados POSIX nesse sistema de arquivos, incluindo propriedade e permissões.

O FSx para Lustre só importa objetos do S3 que tenham chaves de objeto compatíveis com POSIX, como as a seguir.

```
mydir/
mydir/myfile1
mydir/mysubdir/
mydir/mysubdir/myfile2.txt
```

O FSx para Lustre armazena diretórios e links simbólicos como objetos distintos no repositório de dados vinculado do S3. Para diretórios, o FSx para Lustre cria um objeto do S3 com um nome de chave que termina com barra (“/”), da seguinte forma:

- A chave de objeto `mydir/` do S3 é mapeada para o diretório `mydir/` do FSx para Lustre.
- A chave de objeto `mydir/mysubdir/` do S3 é mapeada para o diretório `mydir/mysubdir/` do FSx para Lustre.

Para links simbólicos, o FSx para Lustre usa o seguinte esquema do Amazon S3:

- Chave de objeto do S3: o caminho para o link, em relação ao diretório de montagem do FSx para Lustre
- Dados de objeto do S3: o caminho de destino desse link simbólico
- Metadados de objeto do S3: os metadados do link simbólico

O FSx para Lustre armazena metadados POSIX, incluindo propriedade, permissões e timestamps para arquivos, diretórios e links simbólicos, em objetos do S3 da seguinte forma:

- `Content-Type`: o cabeçalho da entidade HTTP usado para indicar o tipo de mídia do recurso para navegadores da web.
- `x-amz-meta-file-permissions`: o tipo de arquivo e as permissões no formato `<octal file type><octal permission mask>`, consistentes com `st_mode` na página de manual stat(2) do Linux.

  > **Note**
  >
  > O FSx para Lustre não importa nem retém informações `setuid`.

- `x-amz-meta-file-owner`: o ID do usuário proprietário (UID) expresso como número inteiro.
- `x-amz-meta-file-group`: o ID do grupo (GID) expresso como número inteiro.
- `x-amz-meta-file-atime`: o tempo do último acesso em nanossegundos desde o início da época do Unix. Termine o valor do tempo com `ns`; caso contrário, o FSx para Lustre interpretará o valor como milissegundos.
- `x-amz-meta-file-mtime`: o tempo da última modificação em nanossegundos desde o início da época do Unix. Termine o valor do tempo com `ns`; caso contrário, o FSx para Lustre interpretará o valor como milissegundos.
- `x-amz-meta-user-agent`: o agente do usuário, ignorado durante a importação do FSx para Lustre. Durante a exportação, o FSx para Lustre define esse valor como `aws-fsx-lustre`.

Ao importar objetos do S3 que não têm permissões POSIX associadas, a permissão POSIX padrão que o FSx para Lustre atribui a um arquivo é `755`. Essa permissão permite acesso de leitura e execução para todos os usuários e acesso de gravação para o proprietário do arquivo.

> **Note**
>
> O FSx para Lustre não retém nenhum metadado personalizado definido pelo usuário em objetos do S3.

Links físicos e exportação para o S3

Se a exportação automática (com políticas NOVAS e ALTERADAS) estiver habilitada em um DRA no seu sistema de arquivos, cada link físico contido no DRA será exportado para o Amazon S3 como objeto do S3 distinto para cada link físico. Se um arquivo com vários links físicos for modificado no

sistema de arquivos, todas as cópias no S3 serão atualizadas, independentemente de qual link físico foi usado ao alterar o arquivo.

Se os links físicos forem exportados para o S3 usando tarefas de repositório de dados (DRTs), cada link físico contido nos caminhos especificados para o DRT será exportado para o S3 como objeto do S3 distinto para cada link físico. Se um arquivo com vários links físicos for modificado no sistema de arquivos, cada cópia no S3 será atualizada no momento em que o respectivo link físico for exportado, independentemente de qual link físico foi usado ao alterar o arquivo.

> **Important**
>
> Quando um novo sistema de arquivos do FSx para Lustre é vinculado a um bucket do S3 para o qual os links físicos foram exportados anteriormente por outro sistema de arquivos do FSx para Lustre, AWS DataSync ou Gateway de Arquivos do Amazon FSx, os links físicos são posteriormente importados como arquivos distintos no novo sistema de arquivos.

Links físicos e arquivos liberados

Um arquivo liberado é aquele cujos metadados estão presentes no sistema de arquivos, mas cujo conteúdo está armazenado apenas no S3. Para obter mais informações sobre arquivos liberados, consulte Liberação de arquivos.

> **Important**
>
> O uso de links físicos em um sistema de arquivos que tem associações de repositório de dados (DRAs) está sujeito às seguintes limitações:
>
> - Excluir e recriar um arquivo liberado com vários links físicos pode fazer com que o conteúdo de todos os links físicos seja sobrescrito.
> - Excluir um arquivo liberado excluirá o conteúdo de todos os links físicos que residem fora de uma associação de repositório de dados.
> - Criar um link físico para um arquivo liberado cujo objeto do S3 correspondente esteja em uma das classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive não criará um novo objeto no S3 para o link físico.

Demonstração: anexar permissões POSIX ao fazer upload de objetos em um bucket do Amazon S3

O procedimento a seguir explica o processo de upload de objetos no Amazon S3 com permissões POSIX. Isso permite que você importe as permissões POSIX ao criar um sistema de arquivos do Amazon FSx vinculado a esse bucket do S3.

Para fazer upload de objetos com permissões POSIX para o Amazon S3

1. Em seu computador ou máquina local, use os comandos de exemplo a seguir para criar um diretório de teste (`s3cptestdir`) e um arquivo (`s3cptest.txt`) que serão carregados via upload no bucket do S3.

   ```
   $ mkdir s3cptestdir
   $ echo "S3cp metadata import test" >> s3cptestdir/s3cptest.txt
   $ ls -ld s3cptestdir/ s3cptestdir/s3cptest.txt
   drwxr-xr-x 3 500 500 96 Jan 8 11:29 s3cptestdir/
   -rw-r--r-- 1 500 500 26 Jan 8 11:29 s3cptestdir/s3cptest.txt
   ```

   O arquivo e o diretório recém-criados têm um ID de usuário (UID) proprietário e um ID de grupo (GID) 500, bem como permissões, conforme mostrado no exemplo anterior.
2. Chame a API do Amazon S3 para criar o diretório `s3cptestdir` com permissões de metadados. Você deve especificar o nome do diretório com uma barra final (`/`). Para obter informações sobre os metadados POSIX com suporte, consulte Suporte a metadados POSIX para repositórios de dados.

   Substitua *`bucket_name`* pelo nome do bucket do S3.

   ```
   $ aws s3api put-object --bucket bucket_name --key s3cptestdir/ --metadata '{"user-
   agent":"aws-fsx-lustre" , \
         "file-atime":"1595002920000000000ns" , "file-owner":"500" , "file-
   permissions":"0100664","file-group":"500" , \
         "file-mtime":"1595002920000000000ns"}'
   ```
3. Verifique se as permissões POSIX estão marcadas com tag nos metadados de objeto do S3.

   ```
   $ aws s3api head-object --bucket bucket_name --key s3cptestdir/
   {
       "AcceptRanges": "bytes",
       "LastModified": "Fri, 08 Jan 2021 17:32:27 GMT",
   ```

```
    "ContentLength": 0,
    "ETag": "\"d41d8cd98f00b204e9800998ecf8427e\"",
    "VersionId": "bAlhCoWq7aIEjc3R6Myc6UOb8sHHtJkR",
    "ContentType": "binary/octet-stream",
    "Metadata": {
        "user-agent": "aws-fsx-lustre",
        "file-atime": "1595002920000000000ns",
        "file-owner": "500",
        "file-permissions": "0100664",
        "file-group": "500",
        "file-mtime": "1595002920000000000ns"
    }
}
```

4. Faça upload do arquivo de teste (criado na etapa 1) do seu computador para o bucket do S3 com permissões de metadados.

```
$ aws s3 cp s3cptestdir/s3cptest.txt s3://bucket_name/s3cptestdir/s3cptest.txt \
      --metadata '{"user-agent":"aws-fsx-lustre" , "file-
atime":"1595002920000000000ns" , \
      "file-owner":"500" , "file-permissions":"0100664","file-group":"500" , "file-
mtime":"1595002920000000000ns"}'
```

5. Verifique se as permissões POSIX estão marcadas com tag nos metadados de objeto do S3.

```
$ aws s3api head-object --bucket bucket_name --key s3cptestdir/s3cptest.txt
{
    "AcceptRanges": "bytes",
    "LastModified": "Fri, 08 Jan 2021 17:33:35 GMT",
    "ContentLength": 26,
    "ETag": "\"eb33f7e1f44a14a8e2f9475ae3fc45d3\"",
    "VersionId": "w9ztRoEhB832m8NC3a_JTlTyIx7Uzql6",
    "ContentType": "text/plain",
    "Metadata": {
        "user-agent": "aws-fsx-lustre",
        "file-atime": "1595002920000000000ns",
        "file-owner": "500",
        "file-permissions": "0100664",
        "file-group": "500",
        "file-mtime": "1595002920000000000ns"
    }
}
```

6. Verifique as permissões no sistema de arquivos do Amazon FSx vinculado ao bucket do S3.

```
$ sudo lfs df -h /fsx
UUID                       bytes        Used   Available Use% Mounted on
3rnxfbmv-MDT0000_UUID       34.4G        6.1M       34.4G   0% /fsx[MDT:0]
3rnxfbmv-OST0000_UUID        1.1T        4.5M        1.1T   0% /fsx[OST:0]

filesystem_summary:          1.1T        4.5M        1.1T   0% /fsx

$ cd /fsx/s3cptestdir/
$ ls -ld s3cptestdir/
drw-rw-r-- 2 500 500 25600 Jan  8 17:33 s3cptestdir/

$ ls -ld s3cptestdir/s3cptest.txt
-rw-rw-r-- 1 500 500 26 Jan 8 17:33 s3cptestdir/s3cptest.txt
```

O diretório `s3cptestdir` e o arquivo `s3cptest.txt` têm permissões POSIX importadas.

Como vincular o sistema de arquivos a um bucket do S3

É possível vincular seu sistema de arquivos do Amazon FSx para Lustre a repositórios de dados no Amazon S3. Você pode criar o link ao criar o sistema de arquivos ou a qualquer momento após a criação do sistema de arquivos.

Um link entre um diretório no sistema de arquivos e um bucket ou prefixo do S3 é chamado de associação de repositório de dados (DRA). Você pode configurar no máximo oito associações de repositório de dados em um sistema de arquivos do FSx para Lustre. No máximo oito solicitações de DRA podem ser enfileiradas, mas apenas uma solicitação pode ser processada por vez no sistema de arquivos. Cada DRA deve ter um diretório exclusivo do sistema de arquivos do FSx para Lustre e um bucket ou prefixo exclusivo do S3 associado a ele.

> **Note**
>
> Associações de repositório de dados, exportação automática e suporte para vários repositórios de dados não estão disponíveis nos sistemas de arquivos do FSx para Lustre 2.10 ou nos sistemas de arquivos `Scratch 1`.

Para acessar objetos no repositório de dados do S3 como arquivos e diretórios no sistema de arquivos, os metadados de arquivos e diretórios devem ser carregados no sistema de arquivos. Você pode carregar metadados de um repositório de dados vinculado ao criar o DRA ou carregar metadados para lotes de arquivos e diretórios que deseja acessar usando o sistema de arquivos do FSx para Lustre posteriormente usando uma tarefa de importação de repositório de dados, ou usar a exportação automática para carregar metadados automaticamente quando objetos forem adicionados, alterados ou excluídos do repositório de dados.

Você pode configurar um DRA somente para importação automática, somente para exportação automática ou ambas. Uma associação de repositório de dados configurada com importação e exportação automáticas propaga os dados em ambas as direções entre o sistema de arquivos e o bucket do S3 vinculado. Conforme você faz alterações nos dados no seu repositório de dados do S3, o FSx para Lustre detecta as alterações e, em seguida, importa automaticamente as alterações para o sistema de arquivos. À medida que você cria, modifica ou exclui arquivos, o FSx para Lustre exporta automaticamente as alterações para o Amazon S3 de forma assíncrona quando sua aplicação termina de modificar o arquivo.

> **Important**
>
> - Se você modificar o mesmo arquivo no sistema de arquivos e no bucket do S3, certifique-se da coordenação no nível da aplicação para evitar conflitos. O FSx para Lustre não evita gravações conflitantes em vários locais.
> - Para arquivos marcados com um atributo imutável, o FSx para Lustre não consegue sincronizar as alterações entre o sistema de arquivos do FSx para Lustre e um bucket do S3 vinculado ao sistema de arquivos. Definir um sinalizador imutável por um longo período de tempo pode diminuir a performance da movimentação de dados entre o Amazon FSx e o S3.

Ao criar uma associação de repositório de dados, você pode configurar as seguintes propriedades:

- Caminho do sistema de arquivos — insira um caminho local no sistema de arquivos que aponte para um diretório (como `/ns1/`) ou subdiretório (como `/ns1/subdir/`) que será mapeado one-to-one com o caminho do repositório de dados especificado abaixo. A barra inicial no nome é obrigatória. Duas associações de repositórios de dados não podem ter caminhos de sistema de arquivos sobrepostos. Por exemplo, se um repositório de dados estiver associado ao caminho do

sistema de arquivos `/ns1`, você não poderá vincular outro repositório de dados ao caminho do sistema de arquivos `/ns1/ns2`.

> **Note**
>
> Se você especificar somente uma barra (`/`) como o caminho do sistema de arquivos, poderá vincular somente um repositório de dados ao sistema de arquivos. Só é possível especificar "/" como o caminho do sistema de arquivos para o primeiro repositório de dados associado a um sistema de arquivos.

- Caminho do repositório de dados: insira um caminho no repositório de dados do S3. O caminho pode ser um bucket ou prefixo do S3 no formato `s3://myBucket/myPrefix/`. Essa propriedade especifica de onde os arquivos do repositório de dados do S3 serão importados ou para onde serão exportados. O FSx para Lustre anexará uma barra "/" final ao caminho do repositório de dados, caso você não forneça uma. Por exemplo, se você fornecer um caminho de repositório de dados `s3://myBucket/myPrefix`, o FSx para Lustre o interpretará como `s3://myBucket/myPrefix/`.

  Duas associações de repositório de dados não podem ter caminhos de repositório de dados sobrepostos. Por exemplo, se um repositório de dados com o caminho `s3://myBucket/myPrefix/` estiver vinculado ao sistema de arquivos, você não poderá criar outra associação de repositório de dados com o caminho `s3://myBucket/myPrefix/mySubPrefix` do repositório de dados.
- Importar metadados do repositório: você pode selecionar essa opção para importar metadados de todo o repositório de dados imediatamente após criar a associação de repositório de dados. Se preferir, você poderá executar uma tarefa de importação do repositório de dados para carregar todos ou um subconjunto dos metadados do repositório de dados vinculado no sistema de arquivos a qualquer momento após a criação da associação de repositório de dados.
- Configurações de importação: escolha uma política de importação que especifique o tipo de objetos atualizados (qualquer combinação de novos, alterados e excluídos) que serão importados automaticamente do bucket do S3 vinculado para o sistema de arquivos. A importação automática (nova, alterada, excluída) é ativada por padrão quando você adiciona um repositório de dados do console, mas é desabilitada por padrão ao usar a AWS CLI ou a API do Amazon FSx.
- Configurações de importação: escolha uma política de importação que especifique o tipo de objetos atualizados (qualquer combinação de novos, alterados e excluídos) que serão exportados automaticamente para o bucket do S3. A exportação automática (nova, alterada, excluída) é

ativada por padrão quando você adiciona um repositório de dados do console, mas é desabilitada por padrão ao usar a AWS CLI ou a API do Amazon FSx.

As configurações Caminho do sistema de arquivos e Caminho do repositório de dados fornecem um mapeamento individual entre caminhos no Amazon FSx e chaves de objeto no S3.

Suporte regional e de conta para buckets do S3 vinculados

Ao criar links para buckets do S3, lembre-se das seguintes limitações de suporte à região e à conta:

- A exportação automática oferece suporte a configurações entre regiões. O sistema de arquivos do Amazon FSx e o bucket do S3 vinculado podem estar localizados na mesma Região da AWS ou em Regiões da AWS diferentes.
- A importação automática não oferece suporte a configurações entre regiões. O sistema de arquivos do Amazon FSx e o bucket do S3 vinculado devem estar localizados na mesma Região da AWS.
- A exportação e a importação automáticas oferecem suporte a configurações entre contas. O sistema de arquivos do Amazon FSx e o bucket do S3 vinculado podem pertencer à mesma Conta da AWS ou a Contas da AWS diferentes.

Como criar um link para um bucket do S3

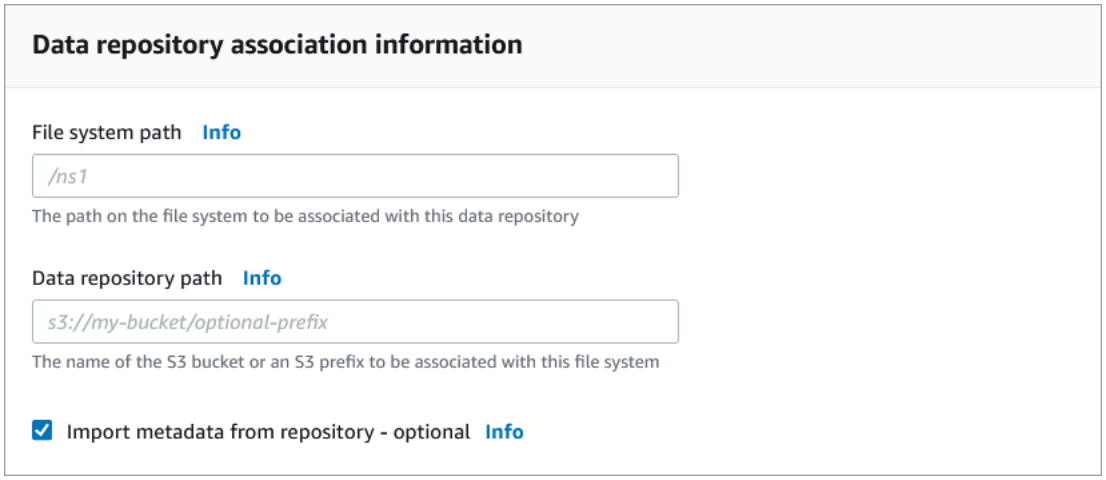
Os procedimentos a seguir orientam você no processo de criação de uma associação de repositório de dados para um sistema de arquivos do FSx para Lustre com um bucket do S3 existente, usando o AWS Management Console e a AWS Command Line Interface (AWS CLI) Para obter informações sobre como adicionar permissões a um bucket do S3 para vinculá-lo ao seu sistema de arquivos, consulteAdição de permissões para usar repositórios de dados no Amazon S3.

> **Note**
>
> Os repositórios de dados não podem ser vinculados a sistemas de arquivos que tenham backups de sistema de arquivos habilitados. Desative os backups antes da vinculação a um repositório de dados.

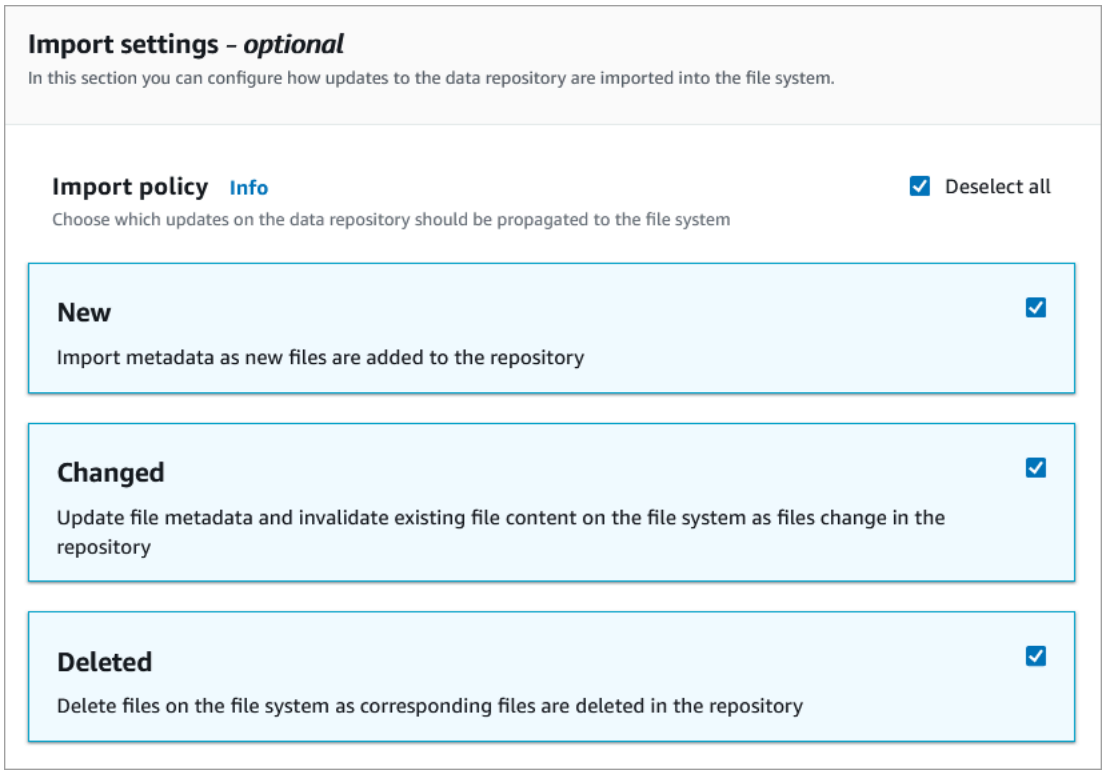
Para vincular um bucket do S3 ao criar um sistema de arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para a criação de um novo sistema de arquivos descrito na Crie seu sistema de arquivos FSx for Lustre na seção de Conceitos básicos.
3. Abra a seção Importação/exportação do repositório de dados: opcional. Por padrão, o recurso está desabilitado:
4. Escolha Importar e exportar dados no S3.
5. Na caixa de diálogo Informações de associação de repositório de dados, forneça informações para os campos a seguir.

   - Caminho do sistema de arquivos: insira o nome de um diretório de alto nível (como `/ns1`) ou subdiretório (como `/ns1/subdir`) dentro do sistema de arquivos do Amazon FSx que será associado ao repositório de dados do S3. A barra inicial no caminho é obrigatória. Duas associações de repositórios de dados não podem ter caminhos de sistema de arquivos sobrepostos. Por exemplo, se um repositório de dados estiver associado ao caminho do sistema de arquivos `/ns1`, você não poderá vincular outro repositório de dados ao caminho do sistema de arquivos `/ns1/ns2`. A configuração Caminho do sistema de arquivos deve ser exclusiva em todas as associações de repositório de dados do sistema de arquivos.
   - Caminho do repositório de dados: insira o caminho de um bucket ou prefixo do S3 existente a ser associado ao sistema de arquivos (por exemplo, `s3://my-bucket/my-prefix/`). Duas associações de repositório de dados não podem ter caminhos de repositório de dados sobrepostos. Por exemplo, se um repositório de dados com o caminho `s3://myBucket/myPrefix/` estiver vinculado ao sistema de arquivos, você não poderá criar outra associação de repositório de dados com o caminho `s3://myBucket/myPrefix/mySubPrefix` do repositório de dados. A configuração Caminho do repositório de dados deve ser exclusiva em todas as associações de repositório de dados do sistema de arquivos.
   - Importar metadados do repositório: selecione essa propriedade para, opcionalmente, executar uma tarefa de importação do repositório de dados para importar metadados imediatamente após a criação do link.

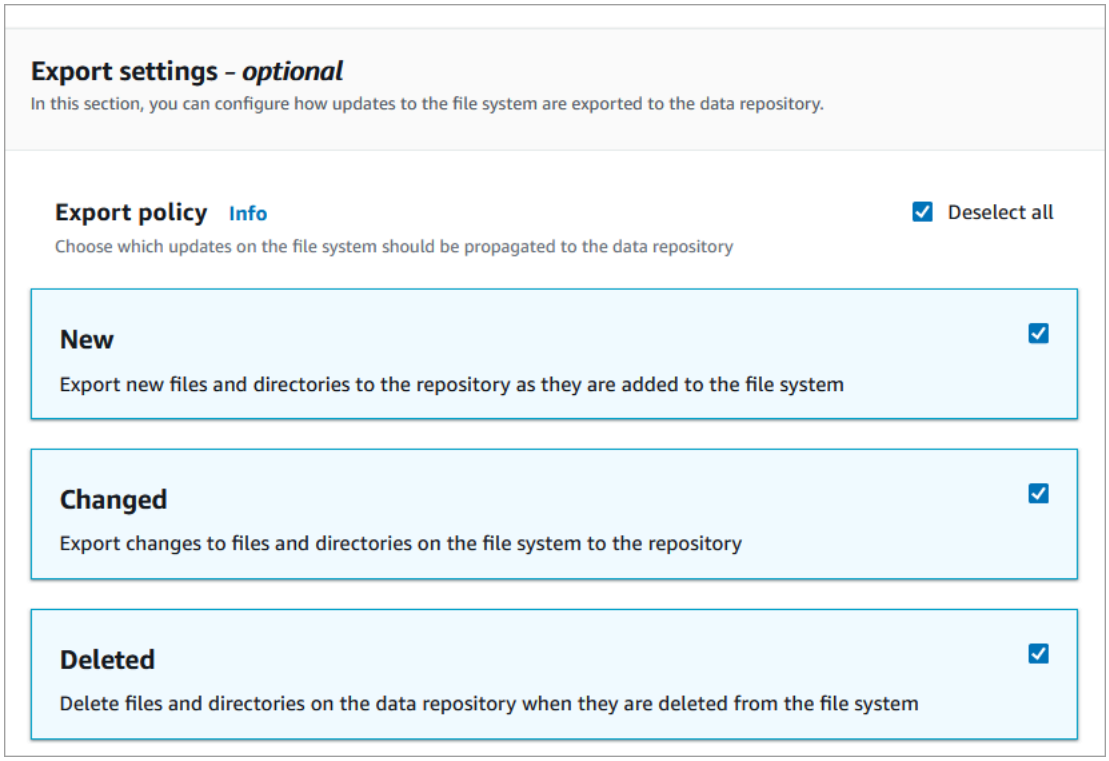


6. Para Configurações de importação: opcional, defina uma Política de importação que determine como suas listagens de arquivos e diretórios são mantidas atualizadas à medida que você adiciona, altera ou exclui objetos em seu bucket do S3. Por exemplo, escolha Novo para importar metadados para seu sistema de arquivos de novos objetos criados no bucket do S3. Para obter mais informações sobre políticas de importação, consulte Importação automática de atualizações do bucket do S3.



7. Em Política de exportação, defina uma política de exportação que determine como seus arquivos são exportados para o bucket do S3 vinculado à medida que você adiciona, altera ou

exclui objetos em seu sistema de arquivos. Por exemplo, escolha Alterado para exportar objetos cujo conteúdo ou metadados foram alterados em seu sistema de arquivos. Para obter mais informações sobre políticas de exportação, consulte Exportação automática de atualizações para o bucket do S3.



8. Prossiga para a próxima seção do assistente de criação do sistema de arquivos.

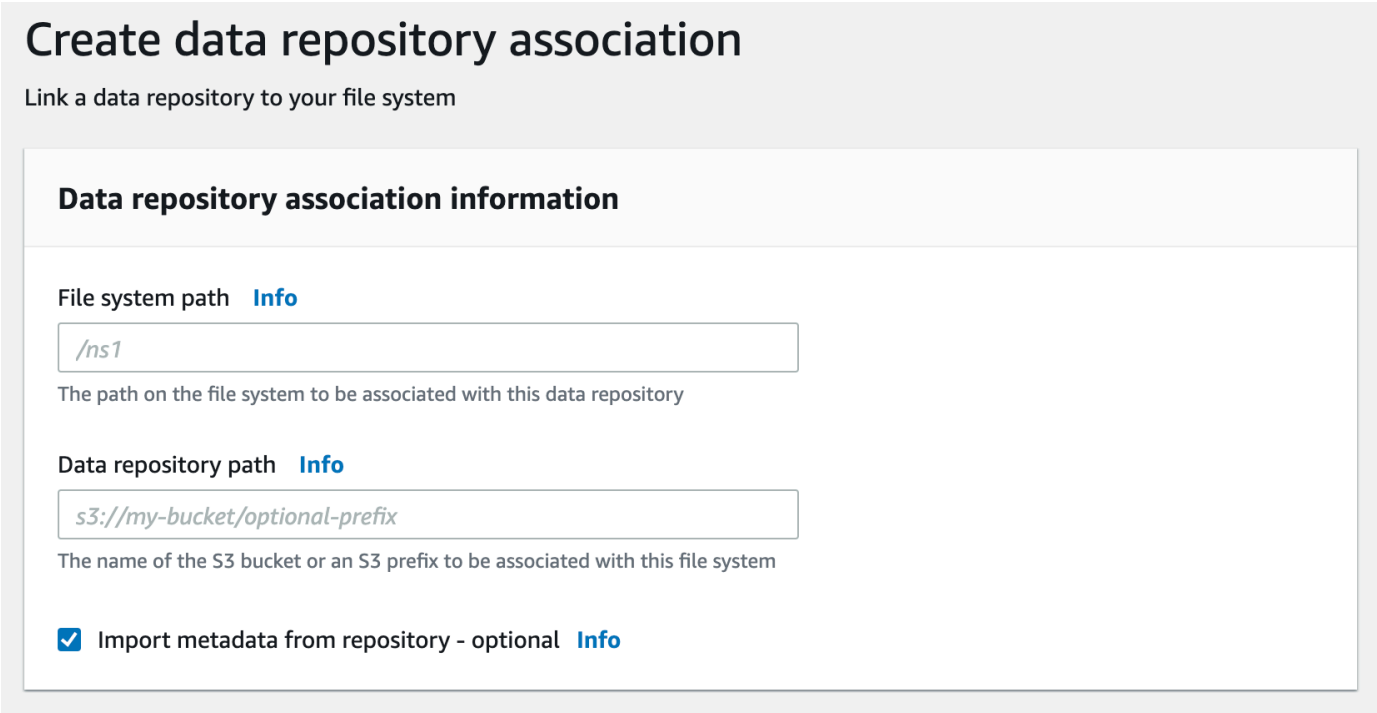
Para vincular um bucket do S3 a um sistema de arquivos existente (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel, escolha Sistemas de arquivos e selecione o sistema de arquivos para o qual você deseja criar uma associação de repositório de dados.
3. Escolha a guia Repositório de dados.
4. No painel Associações de repositório de dados, escolha Criar associação de repositório de dados.
5. Na caixa de diálogo Informações de associação de repositório de dados, forneça informações para os campos a seguir.

   - Caminho do sistema de arquivos: insira o nome de um diretório de alto nível (como `/ns1`) ou subdiretório (como `/ns1/subdir`) dentro do sistema de arquivos do Amazon FSx que será associado ao repositório de dados do S3. A barra inicial no caminho é obrigatória. Duas

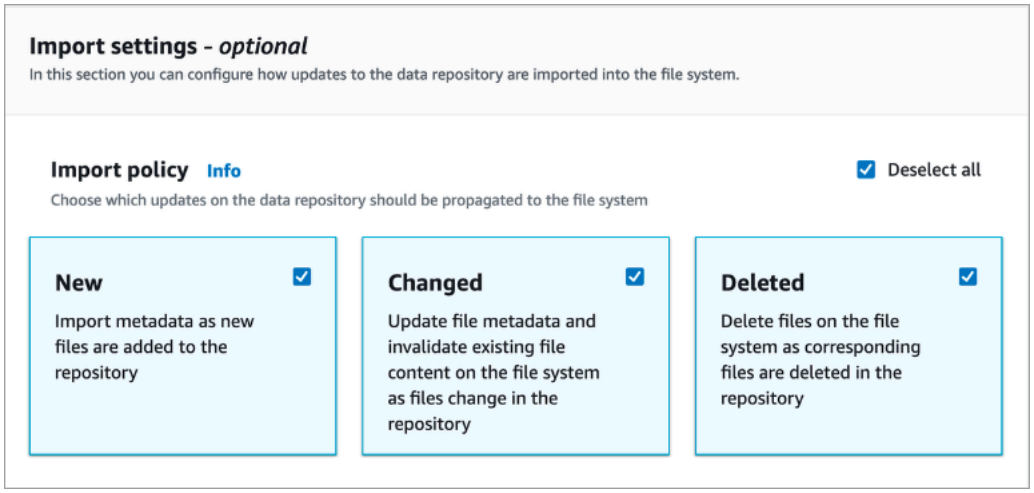
associações de repositórios de dados não podem ter caminhos de sistema de arquivos sobrepostos. Por exemplo, se um repositório de dados estiver associado ao caminho do sistema de arquivos `/ns1`, você não poderá vincular outro repositório de dados ao caminho do sistema de arquivos `/ns1/ns2`. A configuração Caminho do sistema de arquivos deve ser exclusiva em todas as associações de repositório de dados do sistema de arquivos.

- Caminho do repositório de dados: insira o caminho de um bucket ou prefixo do S3 existente a ser associado ao sistema de arquivos (por exemplo, `s3://my-bucket/my-prefix/`). Duas associações de repositório de dados não podem ter caminhos de repositório de dados sobrepostos. Por exemplo, se um repositório de dados com o caminho `s3://myBucket/myPrefix/` estiver vinculado ao sistema de arquivos, você não poderá criar outra associação de repositório de dados com o caminho `s3://myBucket/myPrefix/mySubPrefix` do repositório de dados. A configuração Caminho do repositório de dados deve ser exclusiva em todas as associações de repositório de dados do sistema de arquivos.
- Importar metadados do repositório: selecione essa propriedade para, opcionalmente, executar uma tarefa de importação do repositório de dados para importar metadados imediatamente após a criação do link.

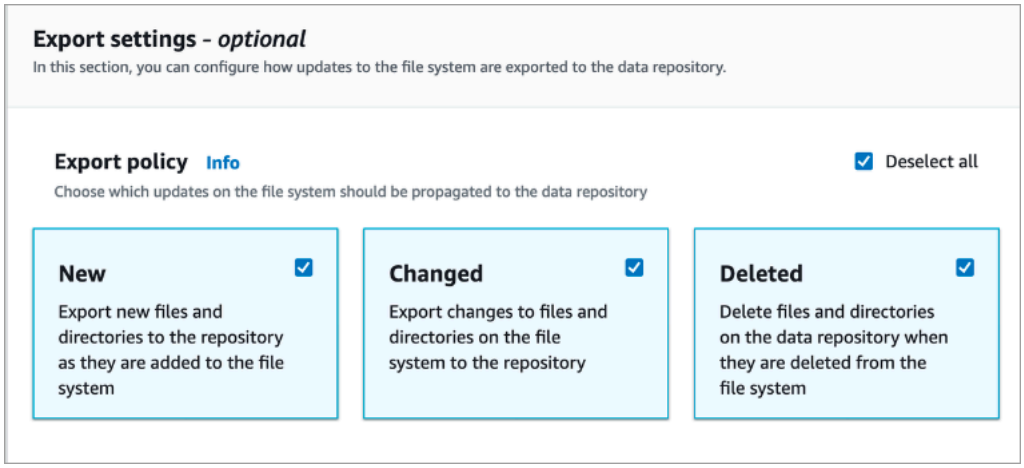


6. Para Configurações de importação: opcional, defina uma Política de importação que determine como suas listagens de arquivos e diretórios são mantidas atualizadas à medida que você adiciona, altera ou exclui objetos em seu bucket do S3. Por exemplo, escolha Novo para

importar metadados para seu sistema de arquivos de novos objetos criados no bucket do S3. Para obter mais informações sobre políticas de importação, consulte Importação automática de atualizações do bucket do S3.



7. Em Política de exportação, defina uma política de exportação que determine como seus arquivos são exportados para o bucket do S3 vinculado à medida que você adiciona, altera ou exclui objetos em seu sistema de arquivos. Por exemplo, escolha Alterado para exportar objetos cujo conteúdo ou metadados foram alterados em seu sistema de arquivos. Para obter mais informações sobre políticas de exportação, consulte Exportação automática de atualizações para o bucket do S3.



8. Escolha Criar.

Vincular um sistema de arquivos a um bucket do S3 (AWS CLI)

O exemplo a seguir cria uma associação de repositório de dados que vincula um sistema de arquivos do Amazon FSx a um bucket do S3, com uma política de importação que importa todos os arquivos

novos ou alterados para o sistema de arquivos e uma política de exportação que exporta arquivos novos, alterados ou excluídos para o bucket do S3 vinculado.

- Para criar uma associação de repositório de dados, use o comando `create-data-repository-association` da CLI do Amazon FSx, conforme mostrado a seguir.

```
$ aws fsx create-data-repository-association \
      --file-system-id fs-0123456789abcdef0 \
      --file-system-path /ns1/path1/ \
      --data-repository-path s3://mybucket/myprefix/ \
      --s3
 "AutoImportPolicy={Events=[NEW,CHANGED,DELETED]},AutoExportPolicy={Events=[NEW,CHANGED,DEL
```

O Amazon FSx retorna imediatamente a descrição JSON do DRA. O DRA é criado de forma assíncrona.

Você pode usar esse comando para criar uma associação de repositório de dados mesmo antes da conclusão da criação do sistema de arquivos. A solicitação será colocada na fila e a associação de repositório de dados será criada após a disponibilidade do sistema de arquivos.

Atualização das configurações de associação de repositório de dados

Você pode atualizar as configurações de uma associação de repositório de dados existente usando o AWS Management Console, a AWS CLI e a API do Amazon FSx, conforme mostrado nos procedimentos a seguir.

> **Note**
>
> Você não pode atualizar o caminho `File system path` ou `Data repository path` de um DRA após a criação. Se quiser alterar o caminho `File system path` ou `Data repository path`, exclua o DRA e crie-o novamente.

Atualizar as configurações de uma associação de repositório de dados existente (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel, escolha Sistemas de arquivos e selecione o sistema de arquivos que você deseja gerenciar.

3. Escolha a guia Repositório de dados.
4. No painel Associações de repositório de dados, escolha a associação de repositório de dados que você deseja alterar.
5. Escolha Atualizar. Uma caixa de diálogo de edição é exibida para a associação de repositório de dados.
6. Para Configurações de importação: opcional, você pode atualizar a Política de importação. Para obter mais informações sobre políticas de importação, consulte Importação automática de atualizações do bucket do S3.
7. Para Configurações de exportação: opcional, você pode atualizar a política de exportação. Para obter mais informações sobre políticas de exportação, consulte Exportação automática de atualizações para o bucket do S3.
8. Escolha Atualizar.

Atualizar as configurações de uma associação de repositório de dados (CLI) existente

- Para atualizar uma associação de repositório de dados, use o comando `update-data-repository-association` da CLI do Amazon FSx, conforme mostrado a seguir.

```
$ aws fsx update-data-repository-association \
      --association-id 'dra-872abab4b4503bfc2' \
      --s3
 "AutoImportPolicy={Events=[NEW,CHANGED,DELETED]},AutoExportPolicy={Events=[NEW,CHANGED,DEL
```

Depois de atualizar com êxito as políticas de importação e exportação da associação de repositório de dados, o Amazon FSx retorna como JSON a descrição da associação de repositório de dados atualizada.

Exclusão de uma associação com um bucket do S3

Os procedimentos a seguir orientam você no processo de exclusão de uma associação de repositório de dados de um sistema de arquivos do Amazon FSx com um bucket do S3 existente, usando o AWS Management Console e a AWS Command Line Interface (AWS CLI) A exclusão da associação de repositório de dados desvincula o sistema de arquivos do bucket do S3.

Excluir um link de um sistema de arquivos para um bucket do S3 (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.

2. No painel, escolha Sistemas de arquivos e selecione o sistema de arquivos do qual você deseja excluir uma associação de repositório de dados.
3. Escolha a guia Repositório de dados.
4. No painel Associações de repositório de dados, escolha a associação que deseja excluir.
5. Em Ações, escolha Excluir associação.
6. (Opcional) Na caixa de diálogo Excluir, você pode escolher Excluir dados no sistema de arquivos para excluir fisicamente os dados no sistema de arquivos que correspondem à associação de repositório de dados.
7. Escolha Excluir para remover a associação de repositório de dados do sistema de arquivos.

Excluir um link de um sistema de arquivos para um bucket do S3 (AWS CLI)

O exemplo a seguir exclui uma associação de repositório de dados que vincula um sistema de arquivos do Amazon FSx a um bucket do S3. O parâmetro `--association-id` especifica o ID da associação de repositório de dados a ser excluída.

- Para excluir uma associação de repositório de dados, use o comando `delete-data-repository-association` da CLI do Amazon FSx, conforme mostrado a seguir.

```
$ aws fsx delete-data-repository-association \
      --association-id dra-872abab4b4503bfc \
      --delete-data-in-file-system false
```

Depois de excluir com êxito a associação de repositório de dados, o Amazon FSx retorna sua descrição como JSON.

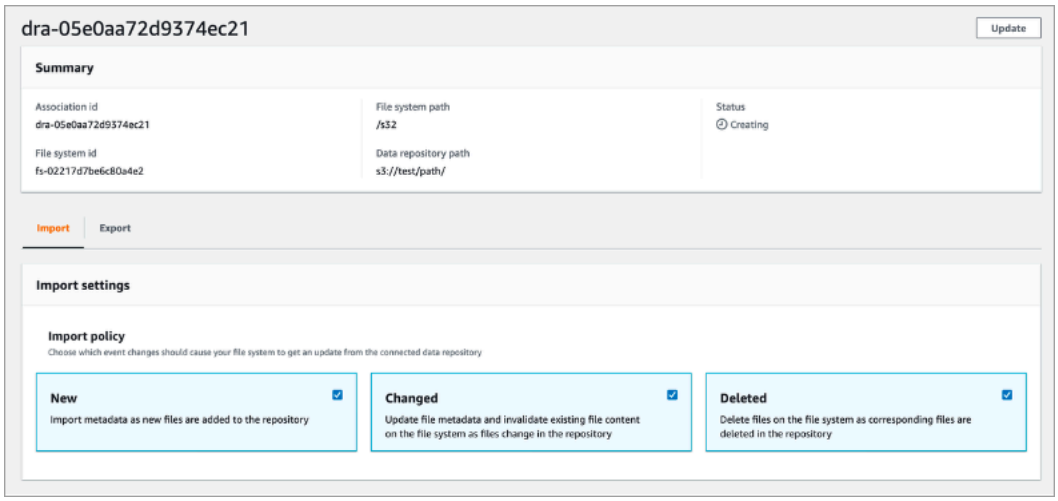
Visualização dos detalhes da associação de repositório de dados

Você pode visualizar os detalhes de uma associação de repositório de dados usando o console do FSx para Lustre, a AWS CLI e a API. Os detalhes incluem o ID de associação do DRA, o caminho do sistema de arquivos, o caminho do repositório de dados, as configurações de importação, as configurações de exportação, o status e o ID do sistema de arquivos associado.

Visualizar detalhes do DRA (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.

2. No painel, escolha Sistemas de arquivos e, em seguida, selecione o sistema de arquivos cujos detalhes de uma associação de repositório de dados você deseja visualizar.
3. Escolha a guia Repositório de dados.
4. No painel Associações de repositório de dados, escolha a associação do repositório de dados que deseja visualizar. A página Resumo é exibida, mostrando os detalhes do DRA.



Visualizar detalhes do DRA (CLI)

- Para visualizar os detalhes de uma associação de repositório de dados específica, use o comando `describe-data-repository-associations` da CLI do Amazon FSx, conforme mostrado a seguir.

```
$ aws fsx describe-data-repository-associations \
      --association-ids dra-872abab4b4503bfc2
```

O Amazon FSx retorna a descrição da associação de repositório de dados como JSON.

Estado do ciclo de vida da associação de repositório de dados

O estado do ciclo de vida da associação de repositório de dados fornece informações de status sobre um DRA específico. Uma associação de repositório de dados pode ter os seguintes Estados do ciclo de vida:

- Criando: o Amazon FSx está criando a associação de repositório de dados entre o sistema de arquivos e o repositório de dados vinculado. O repositório de dados está indisponível.
- Disponível: a associação de repositório de dados está disponível para uso.

- Atualizando: a associação de repositório de dados está passando por uma atualização iniciada pelo cliente que pode afetar a disponibilidade.
- Excluindo: a associação de repositório de dados está passando por uma exclusão iniciada pelo cliente.
- Configuração incorreta: o Amazon FSx não pode importar automaticamente as atualizações do bucket do S3, nem exportá-las, até que a configuração da associação de repositório de dados seja corrigida.
- Falha: a associação de repositório de dados está em um estado terminal que não pode ser recuperado (por exemplo, porque o caminho do sistema de arquivos foi excluído ou o bucket do S3 foi excluído).

Você pode visualizar o estado do ciclo de vida de uma associação de repositório de dados usando o console, a AWS Command Line Interface e a API do Amazon FSx. Para obter mais informações, consulte Visualização dos detalhes da associação de repositório de dados.

Como trabalhar com buckets do Amazon S3 criptografados no lado do servidor

O FSx para Lustre oferece suporte a buckets do Amazon S3 que usam a criptografia no lado do servidor com chaves gerenciadas pelo S3 (SSE-S3) e com AWS KMS keys armazenadas no AWS Key Management Service (SSE-KMS).

Se você quiser que o Amazon FSx criptografe dados ao gravar no bucket do S3, defina a criptografia padrão no bucket do S3 como SSE-S3 ou SSE-KMS. Para obter mais informações, consulte Configuração da criptografia padrão no Guia do usuário do Amazon S3. Ao gravar arquivos no bucket do S3, o Amazon FSx segue a política de criptografia padrão do bucket do S3.

Por padrão, o Amazon FSx oferece suporte a buckets do S3 criptografados com o uso da criptografia SSE-S3. Se você quiser vincular seu sistema de arquivos do Amazon FSx a um bucket do S3 criptografado com o uso da criptografia SSE-KMS, adicione uma declaração à sua política de chave gerenciada pelo cliente que permita que o Amazon FSx criptografe e decriptografe objetos no bucket do S3 usando a chave KMS.

Ado declaração a seguir permite que um sistema de arquivos do Amazon FSx específico criptografe e decriptografe objetos de um bucket S3 específico, *bucket_name*.

```
{
```

```
    "Sid": "Allow access through S3 for the FSx SLR to use the KMS key on the objects
 in the given S3 bucket",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::aws_account_id:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fsx_file_system_id"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "aws_account_id",
            "kms:ViaService": "s3.bucket-region.amazonaws.com"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
        }
    }
}
```

Note

Se você estiver usando um KMS com uma CMK para criptografar seu bucket do S3 com as chaves do bucket do S3 habilitadas, defina `EncryptionContext` como ARN do bucket, não o ARN do objeto, como neste exemplo:

```
"StringLike": {
    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name"
}
```

A declaração de política a seguir permite que todos os sistemas de arquivos do Amazon FSx em sua conta sejam vinculados a um bucket do S3 específico.

```
{
```

```
    "Sid": "Allow access through S3 for the FSx SLR to use the KMS key on the objects
 in the given S3 bucket",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "aws_account_id",
            "kms:ViaService": "s3.bucket-region.amazonaws.com"
        },
        "StringLike": {
            "aws:userid": "*:FSx",
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
        }
    }
}
```

Acesso aos buckets do Amazon S3 criptografados no lado do servidor em uma Conta da AWS diferente

Depois de criar um sistema de arquivos do FSx para Lustre vinculado a um bucket do Amazon S3 criptografado , você deve então conceder ao perfil vinculado ao serviço (SLR) `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`* acesso à chave KMS usada para criptografar o bucket do S3 antes de ler ou gravar dados no bucket do S3 vinculado. Você pode usar um perfil do IAM que já tenha permissões para a chave KMS.

> **Note**
>
> Esse perfil do IAM deve estar na conta na qual o sistema de arquivos do FSx para Lustre foi criado (que é a mesma conta do SLR do S3), não na conta à qual a chave KMS/bucket do S3 pertence.

Você usa o perfil do IAM para chamar a API do AWS KMS a seguir a fim de criar uma concessão para o SLR do S3 de modo que o SLR ganhe permissão para os objetos do S3. Para encontrar o ARN associado ao SLR, pesquise nos perfis do IAM usando o ID do sistema de arquivos como string de pesquisa.

```
$ aws kms create-grant --region fs_account_region \
      --key-id arn:aws:kms:s3_bucket_account_region:s3_bucket_account:key/key_id \
      --grantee-principal arn:aws:iam::fs_account_id:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_file-system-id \
      --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Para obter mais informações sobre funções vinculadas ao serviço, consulte Como usar perfis vinculados a serviço no Amazon FSx.

Importação de alterações do repositório de dados

Você pode importar alterações nos dados e nos metadados POSIX de um repositório de dados vinculado para o seu sistema de arquivos do Amazon FSx. Os metadados POSIX associados incluem propriedade, permissões e timestamps.

Para importar alterações no sistema de arquivos, use um dos métodos a seguir:

- Configure o sistema de arquivos para importar automaticamente arquivos novos, alterados ou excluídos do seu repositório de dados vinculado. Para obter mais informações, consulte Importação automática de atualizações do bucket do S3.
- Selecione a opção para importar metadados ao criar uma associação de repositório de dados. Isso iniciará uma tarefa de importação do repositório de dados imediatamente após a criação da associação de repositório de dados.
- Use uma tarefa de importação de repositório de dados sob demanda. Para obter mais informações, consulte Como usar tarefas do repositório de dados para importar alterações.

As tarefas de importação automática e importação do repositório de dados podem ser executadas ao mesmo tempo.

Quando você ativa a importação automática para uma associação de repositório de dados, seu sistema de arquivos atualiza automaticamente os metadados do arquivo à medida que os

objetos são criados, modificados ou excluídos no S3. Quando você seleciona a opção de importar metadados ao criar uma associação de repositório de dados, seu sistema de arquivos importa metadados para todos os objetos no repositório de dados. Quando você importa usando uma tarefa de importação de repositório de dados, seu sistema de arquivos importa apenas metadados de objetos que foram criados ou modificados desde a última importação.

O FSx para Lustre copia automaticamente o conteúdo de um arquivo do seu repositório de dados e o carrega no sistema de arquivos quando a aplicação acessa pela primeira vez o arquivo no sistema de arquivos. Essa movimentação de dados é gerenciada pelo FSx para Lustre e é transparente para as aplicações. As leituras subsequentes desses arquivos são fornecidas diretamente do sistema de arquivos com latências inferiores a um milissegundo.

Você também pode pré-carregar todo o sistema de arquivos ou um diretório dentro do sistema de arquivos. Para obter mais informações, consulte Pré-carregamento de arquivos no sistema de arquivos. Se você solicitar o pré-carregamento de vários arquivos simultaneamente, o FSx para Lustre carregará os arquivos do repositório de dados do Amazon S3 em paralelo.

O FSx para Lustre só importa objetos do S3 que tenham chaves de objeto compatíveis com POSIX. As tarefas de importação automática e importação do repositório de dados importam metadados POSIX. Para obter mais informações, consulte Suporte a metadados POSIX para repositórios de dados.

> **Note**
>
> O FSx para Lustre não oferece suporte à importação de metadados para links simbólicos das classes de armazenamento S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive. Os metadados de objetos do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive que não são links simbólicos podem ser importados (ou seja, um inode é criado no sistema de arquivos do FSx para Lustre com os metadados corretos). No entanto, para ler esses dados do sistema de arquivos, você deve primeiro restaurar o objeto S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Não há suporte para a importação de dados de arquivos diretamente dos objetos do Amazon S3 na classe de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive no FSx para Lustre.

Importação automática de atualizações do bucket do S3

É possível configurar o FSx para Lustre para atualizar automaticamente metadados no sistema de arquivos conforme os objetos são adicionados, alterados ou excluídos do bucket do S3. O FSx para

Lustre cria, atualiza ou exclui a listagem de arquivos e diretórios, correspondendo à alteração no S3. Se o objeto alterado no bucket do S3 não contiver mais seus metadados, o FSx para Lustre manterá os valores atuais dos metadados do arquivo, incluindo as permissões atuais.

> **Note**
>
> O sistema de arquivos do FSx para Lustre e o bucket do S3 vinculado devem estar localizados na mesma Região da AWS para importar atualizações automaticamente.

Você pode configurar a importação automática ao criar a associação de repositório de dados e pode atualizar as configurações de importação automática a qualquer momento usando o console de gerenciamento do FSx, a AWS CLI, ou a API da AWS..

> **Note**
>
> É possível configurar a importação e a exportação automáticas na mesma associação de repositório de dados. Este tópico descreve apenas o recurso de importação automática.

> **Important**
>
> - Se um objeto for modificado no S3 com todas as políticas de importação automática habilitadas e a exportação automática desabilitada, o conteúdo desse objeto sempre será importado para um arquivo correspondente no sistema de arquivos. Se um arquivo já existir no local de destino, ele será sobrescrito.
> - Se um arquivo for modificado no sistema de arquivos e no S3, com todas as políticas de importação e exportação automáticas habilitadas, o arquivo no sistema de arquivos ou o objeto no S3 poderá ser substituído pelo outro. Não é garantido que uma edição posterior em um local substitua uma edição anterior em outro local. Se você modificar o mesmo arquivo no sistema de arquivos e no bucket do S3, certifique-se da coordenação no nível da aplicação para evitar conflitos. O FSx para Lustre não evita gravações conflitantes em vários locais.

A política de importação especifica como você deseja que o FSx para Lustre atualize seu sistema de arquivos à medida que o conteúdo muda no bucket do S3 vinculado. Uma associação de repositório de dados pode ter uma das seguintes políticas de importação:

- Novo: o FSx para Lustre atualiza automaticamente os metadados de arquivos e diretórios somente quando novos objetos são adicionados ao repositório de dados do S3 vinculado.
- Alterado: o FSx para Lustre atualiza automaticamente os metadados de arquivos e diretórios somente quando um objeto existente no repositório de dados é alterado.
- Excluído: o FSx para Lustre atualiza automaticamente os metadados de arquivos e diretórios somente quando um objeto no repositório de dados é excluído.
- Qualquer combinação de novo, alterado e excluído: o FSx para Lustre atualiza automaticamente os metadados de arquivos e diretórios quando qualquer uma das ações especificadas ocorre no repositório de dados do S3. Por exemplo, você pode especificar para que o sistema de arquivos seja atualizado quando um objeto for adicionado (Novo) ou removido (Excluído) no repositório do S3, mas não seja atualizado quando um objeto for alterado.
- Nenhuma política configurada: o FSx para Lustre não atualiza os metadados de arquivos e diretórios no sistema de arquivos quando objetos são adicionados, alterados ou excluídos no repositório de dados do S3. Se você não configurar uma política de importação, a importação automática será desabilitada para a associação de repositório de dados. Você ainda pode importar manualmente as alterações de metadados usando uma tarefa de importação de repositório de dados, conforme descrito em Como usar tarefas do repositório de dados para importar alterações.

> **Important**
>
> A importação automática não sincronizará as seguintes ações do S3 com o sistema de arquivos do FSx para Lustre vinculado:
>
> - Exclusão de um objeto usando as expirações do ciclo de vida do objeto do S3
> - Exclusão permanente da versão atual do objeto em um bucket habilitado para versionamento
> - Cancelamento da exclusão de um objeto em um bucket com versionamento habilitado

Na maioria dos casos de uso, recomendamos que você configure uma política de importação de objeto Novo, Alterado e Excluído. Essa política garante que todas as atualizações feitas no

repositório de dados vinculado do S3 sejam importadas automaticamente para o sistema de arquivos.

Quando você define uma política de importação para atualizar metadados de arquivos e diretórios do sistema de arquivos com base nas alterações ocorridas no repositório de dados do S3 vinculado, o FSx para Lustre cria uma configuração de notificação de evento no bucket do S3 vinculado. A configuração de notificação de evento é chamada de `FSx`. Não modifique nem exclua a configuração de notificação de evento `FSx` no bucket do S3. Isso evitará a importação automática de metadados de arquivos e diretórios atualizados para seu sistema de arquivos.

Quando o FSx para Lustre atualiza uma listagem de arquivos que foi alterada no repositório de dados do S3 vinculado, ele substitui o arquivo local pela versão atualizada, mesmo que o arquivo esteja bloqueado para gravação.

O FSx para Lustre faz de tudo para atualizar o sistema de arquivos. O FSx para Lustre não consegue atualizar o sistema de arquivos nas seguintes situações:

- Se FSx para Lustre não tiver permissão para abrir o objeto do S3 novo ou alterado. Nesse caso, o FSx para Lustre ignora o objeto e continua. O estado do ciclo de vida do DRA não é afetado.
- Se o FSx para Lustre não tiver permissões no nível do bucket, como para `GetBucketAcl`. Isso fará com que o estado do ciclo de vida do repositório de dados fique com uma Configuração incorreta. Para obter mais informações, consulte Estado do ciclo de vida da associação de repositório de dados.
- Se a configuração de notificação de evento `FSx` no bucket do S3 vinculado for excluída ou alterada. Isso fará com que o estado do ciclo de vida do repositório de dados fique com uma Configuração incorreta. Para obter mais informações, consulte Estado do ciclo de vida da associação de repositório de dados.

Recomendamos que você ative o registro em CloudWatch Registros para registrar informações sobre arquivos ou diretórios que não puderam ser importados automaticamente. Os avisos e erros no log contêm informações sobre o motivo da falha. Para obter mais informações, consulte Registros em log de eventos de repositório de dados.

Pré-requisitos

As seguintes condições são obrigatórias para que o FSx para Lustre importe automaticamente arquivos novos, alterados ou excluídos no bucket do S3 vinculado:

- O sistema de arquivos e o bucket do S3 vinculado estejam localizados na mesma Região da AWS.

- O bucket do S3 não tenha um estado de ciclo de vida configurado incorretamente. Para obter mais informações, consulte Estado do ciclo de vida da associação de repositório de dados.
- Sua conta tenha as permissões necessárias para configurar e receber notificações de evento no bucket do S3 vinculado.

Tipos de alterações de arquivo com suporte

O FSx para Lustre oferece suporte à importação das seguintes alterações em arquivos e diretórios que ocorrem no bucket do S3 vinculado:

- Alterações no conteúdo do arquivo
- Alterações nos metadados de arquivos ou diretórios.
- Alterações no destino ou nos metadados de links simbólicos.
- Exclusões de arquivos e diretórios. Se você excluir um objeto no bucket do S3 vinculado que corresponde a um diretório no sistema de arquivos (ou seja, um objeto com um nome de chave que termina com uma barra), o FSx para Lustre só excluirá o diretório correspondente no sistema de arquivos se ele estiver vazio.

Atualização das configurações de importação

Você pode definir as configurações de importação de um sistema de arquivos para um bucket do S3 vinculado ao criar a associação de repositório de dados. Para obter mais informações, consulte Como criar um link para um bucket do S3.

Você também pode atualizar as configurações de importação a qualquer momento, incluindo a política de importação. Para obter mais informações, consulte Atualização das configurações de associação de repositório de dados.

Monitoramento da importação automática

Se a taxa de alteração em seu bucket do S3 exceder a taxa na qual a importação automática consegue processar essas alterações, as correspondentes alterações de metadados sendo importadas para o sistema de arquivos do FSx para Lustre serão atrasadas. Se isso ocorrer, você poderá usar a métrica `AgeOfOldestQueuedMessage` para monitorar a idade da alteração mais antiga que está aguardando para ser processada pela importação automática. Para obter mais informações sobre essa métrica, consulte Métricas AutoImport e AutoExport.

Se o atraso na importação de alterações de metadados exceder 14 dias (conforme medido usando a métrica `AgeOfOldestQueuedMessage`), as alterações no bucket do S3 que não foram processadas pela importação automática não serão importadas para o sistema de arquivos. Além disso, o ciclo de vida da associação de repositório de dados é marcado como CONFIGURAÇÃO INCORRETA e a importação automática é interrompida. Se você tiver a exportação automática habilitada, ela continuará monitorando seu sistema de arquivos do FSx para Lustre em busca de alterações. No entanto, alterações adicionais não são sincronizadas do sistema de arquivos do FSx para Lustre com o S3.

Para retornar a associação de repositório de dados do estado de ciclo de vida CONFIGURAÇÃO INCORRETA para o estado DISPONÍVEL, você deve atualizar a associação de repositório de dados. Você pode atualizar sua associação de repositório de dados usando o comando update-data-repository-associationCLI (ou a operação de API UpdateDataRepositoryAssociationcorrespondente). O único parâmetro de solicitação necessário é o `AssociationID` da associação de repositório de dados que você deseja atualizar.

Depois que o estado do ciclo de vida da associação de repositório de dados for alterado para DISPONÍVEL, a importação automática (e a exportação automática, se habilitada) será reiniciada. Na reinicialização, a exportação automática retoma a sincronização das alterações do sistema de arquivos com o S3. Para sincronizar os metadados de objetos novos e alterados no S3 com o sistema de arquivos do FSx para Lustre que não foram importados ou são de quando a associação de repositório de dados estava em um estado de configuração incorreta, execute uma tarefa de importação do repositório de dados. As tarefas de importação do repositório de dados não sincronizam as exclusões no bucket do S3 com o sistema de arquivos do FSx para Lustre. Se quiser sincronizar totalmente o S3 com seu sistema de arquivos (inclusive exclusões), você deve recriar seu sistema de arquivos.

Para garantir que os atrasos na importação de alterações de metadados não excedam 14 dias, recomendamos que você defina um alarme na métrica `AgeOfOldestQueuedMessage` e reduza a atividade no bucket do S3 se a métrica `AgeOfOldestQueuedMessage` ultrapassar o limite do alarme. Em um sistema de arquivos do FSx para Lustre conectado a um bucket do S3 com um único fragmento enviando continuamente o número máximo de alterações possíveis do S3, com apenas a importação automática em execução no sistema de arquivos do FSx para Lustre, a importação automática, em 14 dias, consegue processar um backlog de sete horas de alterações do S3.

Além disso, com uma única ação do S3, você pode gerar mais alterações do que a importação automática processará em 14 dias. Exemplos desses tipos de ações incluem, mas não estão limitados a, uploads AWS Snowball para o S3 e exclusões em grande escala. Se você fizer uma

alteração em grande escala no bucket do S3 que deseja sincronizar com o sistema de arquivos do FSx para Lustre, para evitar que as alterações de importação automática excedam 14 dias, exclua o sistema de arquivos e recrie-o quando a alteração do S3 for concluída.

Se a métrica `AgeOfOldestQueuedMessage` estiver crescendo, revise as métricas `GetRequests`, `PutRequests`, `PostRequests` e `DeleteRequests` do bucket do S3 em busca de alterações de atividade que causariam um aumento na taxa e no número de alterações enviadas para importação automática. Para obter informações sobre as métricas disponíveis do S3, consulte Monitoramento do Amazon S3 no Guia do usuário do Amazon S3.

Para obter uma lista de todas as métricas disponíveis do FSx para Lustre, consulte Monitorar com o Amazon CloudWatch.

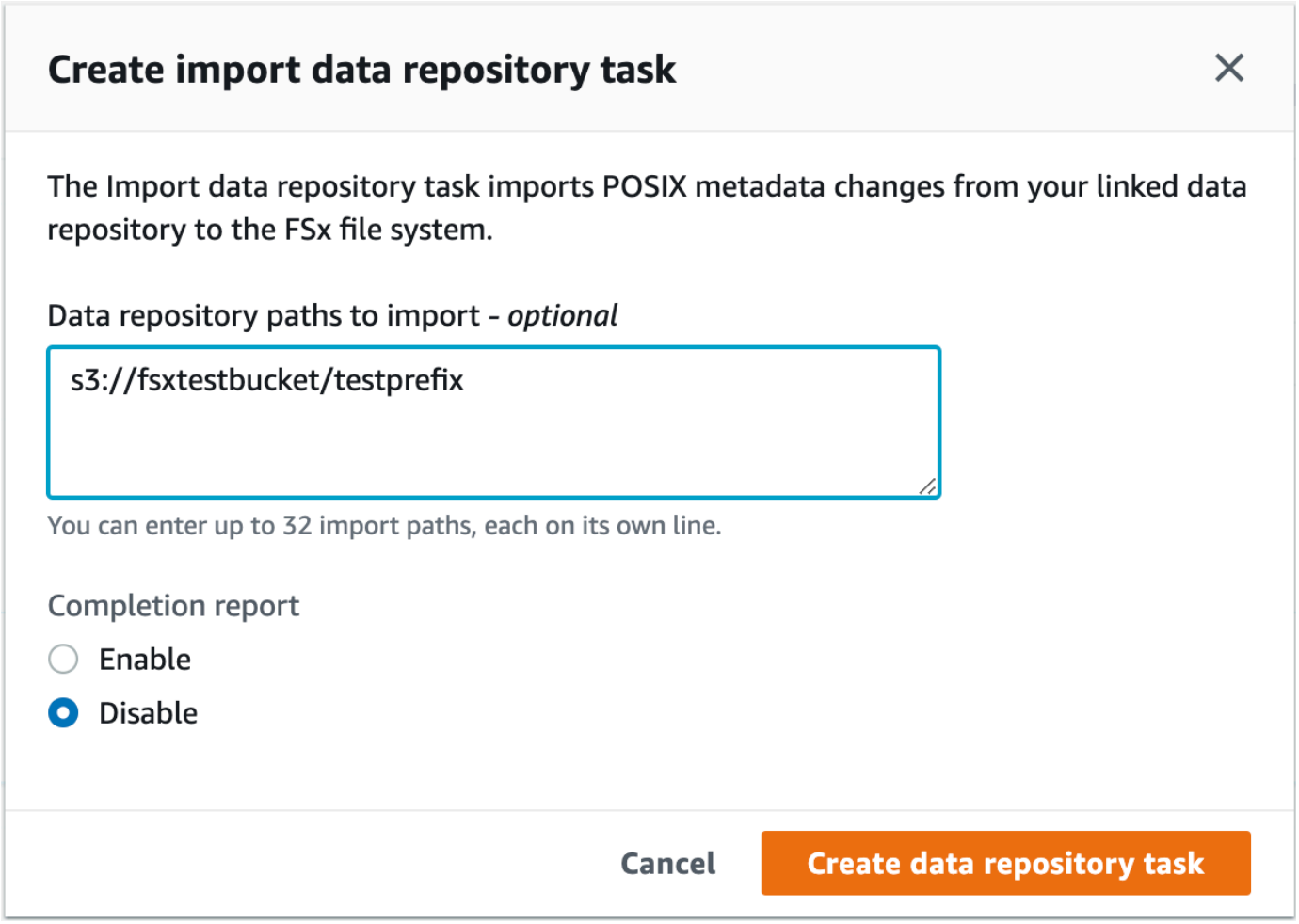
Como usar tarefas do repositório de dados para importar alterações

A tarefa de importação do repositório de dados importa metadados de objetos novos ou alterados no repositório de dados do S3, criando uma nova lista de arquivos ou diretórios para qualquer novo objeto no repositório de dados do S3. Para qualquer objeto que tenha sido alterado no repositório de dados, a listagem de arquivos ou diretórios correspondente é atualizada com os novos metadados. Nenhuma ação é executada para objetos que foram excluídos do repositório de dados.

Use os procedimentos a seguir para importar alterações de metadados usando o console e a CLI do Amazon FSx. Observe que você pode usar uma tarefa de repositório de dados para vários DRAs.

Importar alterações de metadados (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação, escolha Sistemas de arquivos e, em seguida, escolha seu sistema de arquivos Lustre.
3. Escolha a guia Repositório de dados.
4. No painel Associações de repositório de dados, escolha as associações de repositório de dados cuja tarefa de importação você deseja criar.
5. No menu Ações, escolha Tarefa de importação. Essa opção não estará disponível se o sistema de arquivos não estiver vinculado a um repositório de dados. A página Criar tarefa de importação do repositório de dados é exibida.



6. (Opcional) Especifique até 32 diretórios ou arquivos a serem importados dos buckets do S3 vinculados, fornecendo os caminhos para esses diretórios ou arquivos em Caminhos de repositórios de dados a serem importados.

> **Note**
>
> Se um caminho fornecido não for válido, a tarefa falhará.

7. (Opcional) Escolha Habilitar em Relatório de conclusão para gerar um relatório de conclusão da tarefa depois que a tarefa for concluída. Um relatório de conclusão da tarefa fornece detalhes sobre os arquivos processados pela tarefa que atendem ao escopo fornecido em Escopo do relatório. Para especificar o local para o Amazon FSx entregar o relatório, em Caminho do relatório, insira um caminho relativo em um repositório de dados do S3 vinculado.
8. Escolha Criar.

Uma notificação na parte superior da página Sistemas de arquivos mostra a tarefa que você acabou de criar em andamento.

Para ver o status e os detalhes da tarefa, role para baixo até o painel Tarefas do repositório de dados na guia Repositório de dados do sistema de arquivos. A ordem de classificação padrão mostra a tarefa mais recente no topo da lista.

Para ver um resumo da tarefa nessa página, escolha ID da tarefa referente à tarefa que você acabou de criar. A página Resumo da tarefa é exibida.

Importar alterações de metadados (CLI)

- Use o comando `create-data-repository-task` da CLI para importar alterações de metadados em seu sistema de arquivos do FSx para Lustre. A operação de API correspondente é `CreateDataRepositoryTask`.

```
$ aws fsx create-data-repository-task \
    --file-system-id fs-0123456789abcdef0 \
    --type IMPORT_METADATA_FROM_REPOSITORY \
    --paths s3://bucketname1/dir1/path1 \
    --report Enabled=true,Path=s3://bucketname1/dir1/
path1,Format=REPORT_CSV_20191124,Scope=FAILED_FILES_ONLY
```

Depois de criar com êxito a tarefa do repositório de dados, o Amazon FSx retorna a descrição da tarefa como JSON.

Depois de criar a tarefa para importar metadados do repositório de dados vinculado, você pode verificar o status da tarefa de importação do repositório de dados. Para obter mais informações sobre como visualizar tarefas do repositório de dados, consulte Acesso a tarefas do repositório de dados.

Pré-carregamento de arquivos no sistema de arquivos

O Amazon FSx copia dados do repositório de dados do Amazon S3 quando um arquivo é acessado pela primeira vez. Por causa dessa abordagem, a leitura ou gravação inicial em um arquivo incorre em uma pequena quantidade de latência. Se a aplicação for sensível a essa latência e você souber quais arquivos ou diretórios a aplicação precisa acessar, poderá pré-carregar o conteúdo de arquivos ou diretórios individuais. Faça isso usando o comando `hsm_restore` da seguinte maneira.

Você pode usar o comando `hsm_action` (emitido com o utilitário `lfs` do usuário) para verificar se o conteúdo do arquivo terminou de ser carregado no sistema de arquivos. Um valor de retorno `NOOP` indica que o arquivo foi carregado com êxito. Execute os comandos a seguir em uma instância de computação com o sistema de arquivos montado. Substitua *`path/to/file`* pelo caminho do arquivo que você está pré-carregando em seu sistema de arquivos.

```
sudo lfs hsm_restore path/to/file
sudo lfs hsm_action path/to/file
```

Você pode pré-carregar todo o sistema de arquivos ou um diretório inteiro dentro do sistema de arquivos usando os comandos a seguir. (O e comercial final faz com que um comando seja executado como um processo em segundo plano.) Se você solicitar o pré-carregamento de vários arquivos simultaneamente, o Amazon FSx carregará os arquivos do repositório de dados do Amazon S3 em paralelo. Se um arquivo já tiver sido carregado no sistema de arquivos, o comando `hsm_restore` não vai recarregá-lo.

```
nohup find local/directory -type f -print0 | xargs -0 -n 1 sudo lfs hsm_restore &
```

> **Note**
>
> Se o bucket do S3 vinculado for maior que o sistema de arquivos, você poderá importar todos os metadados de arquivos para seu sistema de arquivos. No entanto, você só pode carregar a quantidade real de dados de arquivo que caiba no espaço de armazenamento restante do sistema de arquivos. Você receberá uma mensagem de erro se tentar acessar os dados do arquivo quando não houver mais espaço de armazenamento no sistema de arquivos. Se isso ocorrer, será possível aumentar a capacidade de armazenamento conforme necessário. Para obter mais informações, consulte Como gerenciar a capacidade de armazenamento.

Exportação de alterações para o repositório de dados

Você pode exportar alterações nos dados e nos metadados POSIX do sistema de arquivos do FSx para Lustre para um repositório de dados vinculado. Os metadados POSIX associados incluem propriedade, permissões e timestamps.

Para exportar alterações do sistema de arquivos, use um dos métodos a seguir.

- Configure o sistema de arquivos para exportar automaticamente arquivos novos, alterados ou excluídos para seu repositório de dados vinculado. Para obter mais informações, consulte Exportação automática de atualizações para o bucket do S3.
- Use uma tarefa de exportação do repositório de dados sob demanda. Para obter mais informações, consulte Como usar tarefas do repositório de dados para exportar alterações.

As tarefas de exportação automática e exportação do repositório de dados não podem ser executadas ao mesmo tempo.

> **Important**
>
> A exportação automática não sincronizará as seguintes operações de metadados em seu sistema de arquivos com o S3 se os objetos correspondentes estiverem armazenados na classe S3 Glacier Flexible Retrieval:
>
> - chmod
> - chown
> - rename

Quando você ativa a exportação automática em uma associação de repositório de dados, seu sistema de arquivos exporta automaticamente dados e metadados de arquivos à medida que eles são criados, modificados ou excluídos. Quando você exporta arquivos ou diretórios usando uma tarefa de exportação de repositório de dados, seu sistema de arquivos só exporta arquivos de dados e metadados que foram criados ou modificados desde a última exportação.

As tarefas exportação automática e exportação do repositório de dados exportam metadados POSIX. Para obter mais informações, consulte Suporte a metadados POSIX para repositórios de dados.

> **Important**
>
> - Para garantir que o FSx para Lustre possa exportar seus dados para o bucket do S3, eles devem ser armazenados em um formato compatível com UTF-8.
> - As chaves de objeto do S3 têm um tamanho máximo de 1.024 bytes. O FSx para Lustre não exportará arquivos cuja chave de objeto S3 correspondente tenha mais de 1.024 bytes.

> **Note**
>
> Todos os objetos criados pelas tarefas de exportação automática e exportação do repositório de dados são gravados usando a classe de armazenamento S3 Standard.

Tópicos

Exportação automática de atualizações para o bucket do S3

É possível configurar o sistema de arquivos do FSx para Lustre para atualizar automaticamente o conteúdo de um bucket do S3 vinculado à medida que arquivos são adicionados, alterados ou excluídos no sistema de arquivos. O FSx para Lustre cria, atualiza ou exclui o objeto no S3, correspondendo à alteração no sistema de arquivos.

> **Note**
>
> A exportação automática não está disponível nos sistemas de arquivos do FSx para Lustre 2.10 nem nos sistemas de arquivos `Scratch 1`.

Você pode exportar para um repositório de dados que esteja na mesma Região da AWS que o sistema de arquivos ou em outra Região da AWS.

Você pode configurar a exportação automática ao criar a associação de repositório de dados e atualizar as configurações de exportação automática a qualquer momento usando o console de gerenciamento do FSx, a AWS CLI e a API da AWS..

> **Note**
>
> É possível configurar a exportação e a importação automáticas na mesma associação de repositório de dados. Este tópico descreve apenas o recurso de exportação automática.

Important

- Se um arquivo for modificado no sistema de arquivos com todas as políticas de exportação automática habilitadas e a importação automática desabilitada, o conteúdo desse objeto sempre será exportado para um objeto correspondente no S3. Se um objeto já existir no local de destino, ele será sobrescrito.
- Se um arquivo for modificado no sistema de arquivos e no S3, com todas as políticas de importação e exportação automáticas habilitadas, o arquivo no sistema de arquivos ou o objeto no S3 poderá ser substituído pelo outro. Não é garantido que uma edição posterior em um local substitua uma edição anterior em outro local. Se você modificar o mesmo arquivo no sistema de arquivos e no bucket do S3, certifique-se da coordenação no nível da aplicação para evitar conflitos. O FSx para Lustre não evita gravações conflitantes em vários locais.

A política de exportação especifica como você deseja que o FSx para Lustre atualize seu bucket do S3 vinculado à medida que o conteúdo é alterado no sistema de arquivos. Uma associação de repositório de dados pode ter uma das seguintes políticas de exportação automática:

- Novo: o FSx para Lustre atualiza automaticamente o repositório de dados do S3 somente quando um novo arquivo, diretório ou link simbólico é criado no sistema de arquivos.
- Alterado: o FSx para Lustre atualiza automaticamente o repositório de dados do S3 somente quando um arquivo existente no sistema de arquivos é alterado. Para alterações no conteúdo do arquivo, o arquivo deve ser fechado antes de ser propagado para o repositório do S3. As alterações de metadados (renomeação, propriedade, permissões e timestamps) são propagadas quando a operação é concluída. Para renomear alterações (incluindo movimentações), o objeto do S3 existente (pré-renomeado) é excluído e um novo objeto do S3 é criado com o novo nome.
- Excluído: o FSx para Lustre atualiza automaticamente o repositório de dados do S3 somente quando um arquivo, diretório ou link simbólico é excluído no sistema de arquivos.
- Qualquer combinação de novo, alterado e excluído: o FSx para Lustre atualiza automaticamente o repositório de dados do S3 quando qualquer uma das ações especificadas ocorre no sistema de arquivos. Por exemplo, você pode especificar para que o repositório do S3 seja atualizado quando um arquivo for adicionado (Novo) ou removido (Excluído) no sistema de arquivos, mas não quando um arquivo for alterado.

- Nenhuma política configurada: o FSx para Lustre não atualiza automaticamente o repositório de dados do S3 quando arquivos são adicionados, alterados ou excluídos no sistema de arquivos. Se você não configurar uma política de exportação, a exportação automática será desabilitada. Você ainda pode exportar manualmente as alterações usando uma tarefa de exportação de repositório de dados, conforme descrito em Como usar tarefas do repositório de dados para exportar alterações.

Na maioria dos casos de uso, recomendamos que você configure uma política de exportação de objeto Novo, Alterado e Excluído. Essa política garante que todas as atualizações feitas no sistema de arquivos sejam exportadas automaticamente para o repositório de dados do S3 vinculado.

Recomendamos que você ative o registro no CloudWatch Logs para registrar informações sobre quaisquer arquivos ou diretórios que não puderam ser exportados automaticamente. Os avisos e erros no log contêm informações sobre o motivo da falha. Para obter mais informações, consulte Registros em log de eventos de repositório de dados.

Atualização de configurações de exportação

Você pode definir as configurações de exportação de um sistema de arquivos para um bucket do S3 vinculado ao criar a associação de repositório de dados. Para obter mais informações, consulte Como criar um link para um bucket do S3.

Você também pode atualizar as configurações de exportação a qualquer momento, incluindo a política de exportação. Para obter mais informações, consulte Atualização das configurações de associação de repositório de dados.

Monitoramento da exportação automática

Você pode monitorar associações de repositórios de dados habilitadas para exportação automática usando um conjunto de métricas publicadas na Amazon CloudWatch. A métrica `AgeOfOldestQueuedMessage` representa a idade da atualização mais antiga feita no sistema de arquivos que ainda não foi exportada para o S3. Se a métrica `AgeOfOldestQueuedMessage` ficar acima de zero por um longo período de tempo, recomendamos reduzir temporariamente o número de alterações (especialmente as renomeações de diretórios) que estão sendo feitas ativamente no sistema de arquivos até que a fila de mensagens seja reduzida. Para obter mais informações, consulte Métricas AutoImport e AutoExport.

> **Important**
>
> Ao excluir uma associação de repositório de dados ou sistema de arquivos com a exportação automática habilitada, primeiro verifique se `AgeOfOldestQueuedMessage` é zero, o que significa que não há alterações que ainda não foram exportadas. Se `AgeOfOldestQueuedMessage` for maior que zero quando você excluir sua associação de repositório de dados ou sistema de arquivos, as alterações que ainda não foram exportadas não chegarão ao bucket do S3 vinculado. Para evitar isso, espere `AgeOfOldestQueuedMessage` chegar a zero antes de excluir sua associação de repositório de dados ou sistema de arquivos.

Como usar tarefas do repositório de dados para exportar alterações

A tarefa de exportação do repositório de dados exporta arquivos novos ou alterados em seu sistema de arquivos. Ela cria um novo objeto no S3 para qualquer novo arquivo no sistema de arquivos. Para qualquer arquivo que tenha sido modificado no sistema de arquivos ou cujos metadados tenham sido modificados, o objeto correspondente no S3 é substituído por um novo objeto com os novos dados e metadados. Nenhuma ação é executada para arquivos que foram excluídos do sistema de arquivos.

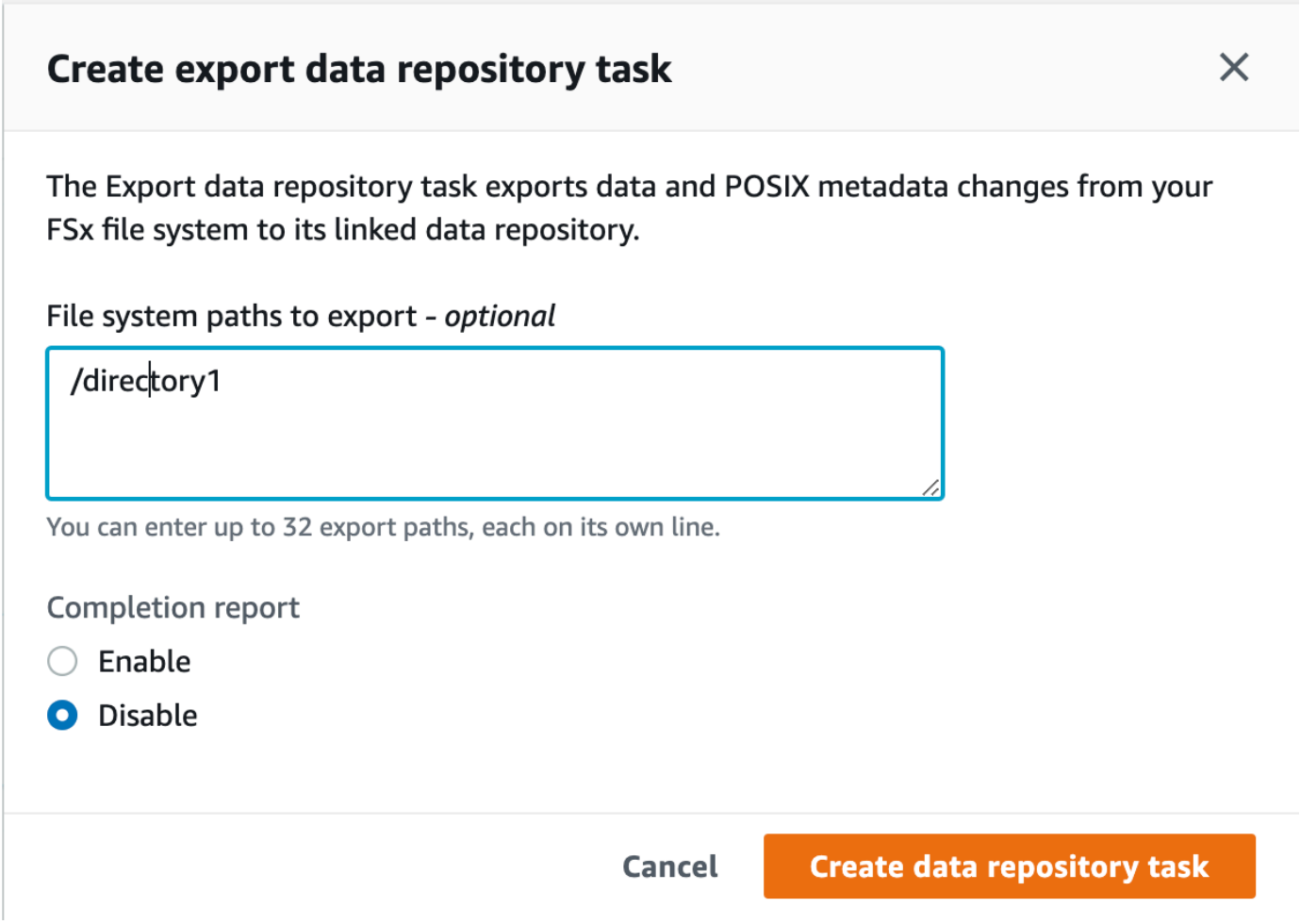
> **Note**
>
> Tenha o seguinte em mente ao usar tarefas de exportação de repositório de dados:
>
> - Não há suporte para o uso de curingas ao incluir ou excluir arquivos para exportação.
> - Ao executar operações `mv`, o arquivo de destino após ser movido será exportado para o S3, mesmo que não haja alteração de UID, GID, permissão ou conteúdo.

Use os procedimentos a seguir para exportar alterações de dados e metadados no sistema de arquivos para buckets do S3 vinculados, usando o console e a CLI do Amazon FSx. Observe que você pode usar uma tarefa de repositório de dados para vários DRAs.

Exportar alterações (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação, escolha Sistemas de arquivos e, em seguida, escolha seu sistema de arquivos Lustre.

3. Escolha a guia Repositório de dados.
4. No painel Associações de repositórios de dados, escolha a associação de repositório de dados para a qual você deseja criar a tarefa de exportação.
5. Em Ações, escolha Tarefa de exportação. Essa opção não estará disponível se o sistema de arquivos não estiver vinculado a um repositório de dados no S3. A caixa de diálogo Criar tarefa de exportação do repositório de dados é exibida.



6. (Opcional) Especifique até 32 diretórios ou arquivos a serem exportados do seu sistema de arquivos do Amazon FSx fornecendo os caminhos para esses diretórios ou arquivos em Caminhos do sistema de arquivos para exportação. Os caminhos fornecidos precisam ser relativos ao ponto de montagem do sistema de arquivos. Se o ponto de montagem for `/mnt/fsx` e `/mnt/fsx/path1` for um diretório ou arquivo no sistema de arquivos que você deseja exportar, o caminho a ser fornecido será `path1`.

> **Note**
>
> Se um caminho fornecido não for válido, a tarefa falhará.

7. (Opcional) Escolha Habilitar em Relatório de conclusão para gerar um relatório de conclusão da tarefa depois que a tarefa for concluída. Um relatório de conclusão da tarefa fornece detalhes sobre os arquivos processados pela tarefa que atendem ao escopo fornecido em Escopo do relatório. Para especificar o local para o Amazon FSx entregar o relatório, em Caminho do relatório, insira um caminho relativo no repositório de dados do S3 vinculado do sistema de arquivos.
8. Escolha Criar.

   Uma notificação na parte superior da página Sistemas de arquivos mostra a tarefa que você acabou de criar em andamento.

Para ver o status e os detalhes da tarefa, role para baixo até o painel Tarefas do repositório de dados na guia Repositório de dados do sistema de arquivos. A ordem de classificação padrão mostra a tarefa mais recente no topo da lista.

Para ver um resumo da tarefa nessa página, escolha ID da tarefa referente à tarefa que você acabou de criar. A página Resumo da tarefa é exibida.

Exportar alterações (CLI)

- Use o comando `create-data-repository-task` da CLI para exportar alterações de dados e metadados em seu sistema de arquivos do FSx para Lustre. A operação de API correspondente é `CreateDataRepositoryTask`.

  ```
  $ aws fsx create-data-repository-task \
      --file-system-id fs-0123456789abcdef0 \
      --type EXPORT_TO_REPOSITORY \
      --paths path1,path2/file1 \
      --report Enabled=true
  ```

  Após a criação com êxito da tarefa do repositório de dados, o Amazon FSx retorna a descrição da tarefa como JSON, conforme mostrado no exemplo a seguir.

  ```
  {
  ```

```
    "Task": {
        "TaskId": "task-123f8cd8e330c1321",
        "Type": "EXPORT_TO_REPOSITORY",
        "Lifecycle": "PENDING",
        "FileSystemId": "fs-0123456789abcdef0",
        "Paths": ["path1", "path2/file1"],
        "Report": {
            "Path":"s3://dataset-01/reports",
            "Format":"REPORT_CSV_20191124",
            "Enabled":true,
            "Scope":"FAILED_FILES_ONLY"
        },
        "CreationTime": "1545070680.120",
        "ClientRequestToken": "10192019-drt-12",
        "ResourceARN": "arn:aws:fsx:us-
east-1:123456789012:task:task-123f8cd8e330c1321"
    }
}
```

Depois de criar a tarefa para exportar dados para o repositório de dados vinculado, você pode verificar o status da tarefa de exportação do repositório de dados. Para obter mais informações sobre como visualizar tarefas do repositório de dados, consulte Acesso a tarefas do repositório de dados.

Exportação de arquivos usando comandos do HSM

> **Note**
>
> Para exportar alterações nos dados e metadados do seu sistema de arquivos do FSx para Lustre para um repositório de dados durável no Amazon S3, use o recurso de exportação automática descrito em Exportação automática de atualizações para o bucket do S3. Você também pode usar as tarefas de exportação do repositório de dados, descritas em Como usar tarefas do repositório de dados para exportar alterações.

Para exportar um arquivo individual para seu repositório de dados e verificar se o arquivo foi exportado com êxito para seu repositório de dados, você pode executar os comandos mostrados a seguir. Um valor de retorno `states: (0x00000009) exists archived` indica que o arquivo foi exportado com êxito.

```
sudo lfs hsm_archive path/to/export/file
```

```
sudo lfs hsm_state path/to/export/file
```

> **Note**
>
> Você deve executar os comandos do HSM (como `hsm_archive`) como usuário raiz ou usando `sudo`.

Para exportar todo o sistema de arquivos ou um diretório inteiro no sistema de arquivos, execute os comandos a seguir. Se você exportar diversos arquivos simultaneamente, o Amazon FSx para Lustre exportará seus arquivos para o repositório de dados do Amazon S3 em paralelo.

```
nohup find local/directory -type f -print0 | xargs -0 -n 1 sudo lfs hsm_archive &
```

Para determinar se a exportação foi concluída, execute o comando a seguir.

```
find path/to/export/file -type f -print0 | xargs -0 -n 1 -P 8 sudo lfs hsm_state | awk
 '!/\<archived\>/ || /\<dirty\>/' | wc -l
```

Se o comando retornar com zero arquivo restante, a exportação estará concluída.

Tarefas de repositório de dados

Ao usar as tarefas de importação e de exportação do repositório de dados, é possível gerenciar a transferência de dados e de metadados entre o sistema de arquivos do FSx para Lustre e qualquer um dos repositórios de dados duráveis no Amazon S3.

As tarefas de repositório de dados otimizam as transferências de dados e de metadados entre o sistema de arquivos do FSx para Lustre e um repositório de dados no S3. Uma maneira pela qual as tarefas fazem isso é ao rastrear as alterações entre o sistema de arquivos do Amazon FSx e o repositório de dados vinculado. Elas também fazem isso ao usar técnicas de transferência paralela para transferir dados em velocidades de até centenas de GB/s. Você cria e visualiza tarefas do repositório de dados usando o console do Amazon FSx, AWS CLI o e a API do Amazon FSx.

As tarefas de repositório de dados mantêm os metadados do Portable Operating System Interface (POSIX) do sistema de arquivos, incluindo as propriedades, as permissões e os carimbos de data/hora. Como as tarefas mantêm esses metadados, é possível implementar e manter controles de acesso entre o sistema de arquivos do FSx para Lustre e os repositórios de dados vinculados.

Você pode usar uma tarefa de repositório de dados de liberação para liberar espaço no sistema de arquivos para novos arquivos ao liberar arquivos exportados para o Amazon S3. O conteúdo dos arquivos liberados é removido, mas os metadados dos arquivos liberados permanecem no sistema de arquivos. Os usuários e as aplicações ainda podem acessar um arquivo liberado ao realizar novamente a leitura do arquivo. Quando o usuário ou a aplicação realiza a leitura do arquivo liberado, o FSx para Lustre recupera de forma transparente o conteúdo do arquivo do Amazon S3.

Tipos de tarefas de repositório de dados

Existem três tipos de tarefas de repositório de dados:

- Tarefas de exportação do repositório de dados que exportam de seu sistema de arquivos do Lustre para um bucket do S3 vinculado.
- Tarefas de importação do repositório de dados que importam de um bucket do S3 vinculado para o seu sistema de arquivos do Lustre.
- Tarefas de repositório de dados de liberação que liberam arquivos exportados para um bucket do S3 vinculado de seu sistema de arquivos do Lustre.

Para ter mais informações, consulte Como criar uma tarefa de repositório de dados.

Tópicos

Noções básicas sobre o status e os detalhes de uma tarefa

Uma tarefa de repositório de dados pode ter um dos seguintes status:

- PENDENTE indica que o Amazon FSx não iniciou a tarefa.
- EM EXECUÇÃO indica que o Amazon FSx está processando a tarefa.
- COM FALHA indica que o Amazon FSx não processou a tarefa com êxito. Por exemplo, pode haver arquivos que a tarefa não conseguiu processar. Os detalhes sobre a tarefa fornecem mais informações sobre a falha. Para obter mais informações sobre tarefas com falha, consulte Solução de problemas para falhas de tarefas de repositório de dados.

- COM ÊXITO indica que o Amazon FSx concluiu a tarefa com êxito.
- CANCELADA indica que a tarefa foi cancelada e não concluída.
- CANCELANDO indica que o Amazon FSx está em processo de cancelamento da tarefa.

Após a criação de uma tarefa, você poderá visualizar as seguintes informações detalhadas para uma tarefa de repositório de dados usando o console do Amazon FSx, a CLI ou a API:

- O tipo de tarefa:
  - `EXPORT_TO_REPOSITORY` indica uma tarefa de exportação.
  - `IMPORT_METADATA_FROM_REPOSITORY` indica uma tarefa de importação.
  - `RELEASE_DATA_FROM_FILESYSTEM` indica uma tarefa de liberação.
- O sistema de arquivos em que a tarefa foi executada.
- O horário de criação da tarefa.
- O status da tarefa.
- O número total de arquivos que a tarefa processou.
- O número total de arquivos que a tarefa processou com êxito.
- O número total de arquivos que a tarefa não conseguiu processar. Este valor é maior que zero quando o status da tarefa for COM FALHA. Informações detalhadas sobre os arquivos que falharam estão disponíveis em um relatório de conclusão da tarefa. Para ter mais informações, consulte Como trabalhar com relatórios de conclusão de tarefas.
- O horário em que a tarefa foi iniciada.
- O horário em que o status da tarefa foi atualizado pela última vez. O status da tarefa é atualizado a cada 30 segundos.

Para obter mais informações sobre como acessar tarefas de repositório de dados existentes, consulte Acesso a tarefas do repositório de dados.

Como usar tarefas de repositório de dados

É possível criar, duplicar, visualizar detalhes e cancelar tarefas de repositório de dados usando o console do Amazon FSx, a CLI ou a API.

Tópicos

- Como criar uma tarefa de repositório de dados

- Duplicação de uma tarefa
- Acesso a tarefas do repositório de dados
- Cancelamento de uma tarefa de repositório de dados

Como criar uma tarefa de repositório de dados

É possível criar uma tarefa de repositório de dados ao usar o console do Amazon FSx, a CLI ou a API. Após criar uma tarefa, você poderá visualizar o progresso e o status da tarefa ao usar o console, a CLI ou a API.

Você pode criar três tipos de tarefas de repositório de dados:

- A tarefa de exportação do repositório de dados exporta de seu sistema de arquivos do Lustre para um bucket do S3 vinculado. Para ter mais informações, consulte Como usar tarefas do repositório de dados para exportar alterações.
- A tarefa de importação do repositório de dados importa de um bucket do S3 vinculado para o seu sistema de arquivos do Lustre. Para ter mais informações, consulte Como usar tarefas do repositório de dados para importar alterações.
- A tarefa de liberação do repositório de dados libera arquivos do sistema de arquivos do Lustre que foram exportados para um bucket do S3 vinculado. Para ter mais informações, consulte Como usar tarefas do repositório de dados para lançar arquivos.

Duplicação de uma tarefa

É possível duplicar uma tarefa de repositório de dados existente no console do Amazon FSx. Ao duplicar uma tarefa, uma cópia exata da tarefa existente será exibida na página Criar tarefa de importação do repositório de dados ou na página Criar tarefa de exportação do repositório de dados. Você pode fazer alterações nos caminhos para exportar ou importar, conforme necessário, antes de criar e executar a nova tarefa.

> **Note**
>
> Uma solicitação para executar uma tarefa duplicada falhará se uma cópia exata dessa tarefa já estiver em execução. Uma cópia exata de uma tarefa que já está em execução contém o mesmo caminho ou os mesmos caminhos do sistema de arquivos no caso de uma tarefa

de exportação ou os mesmos caminhos do repositório de dados no caso de uma tarefa de importação.

É possível duplicar uma tarefa usando a visualização de detalhes da tarefa, no painel Tarefas de repositório de dados na guia Repositório de dados do sistema de arquivos, ou usando a página Tarefas de repositório de dados.

Como duplicar uma tarefa existente

1. Escolha uma tarefa no painel Tarefas de repositório de dados na guia Repositório de dados do sistema de arquivos.
2. Escolha Duplicar tarefa. Dependendo do tipo de tarefa que você escolher, a página Criar tarefa de importação do repositório de dados ou Criar tarefa de exportação do repositório de dados será exibida. Todas as configurações da nova tarefa são idênticas às da tarefa que você está duplicando.
3. Altere ou adicione os caminhos dos quais você deseja importar ou exportar.
4. Escolha Criar.

Acesso a tarefas do repositório de dados

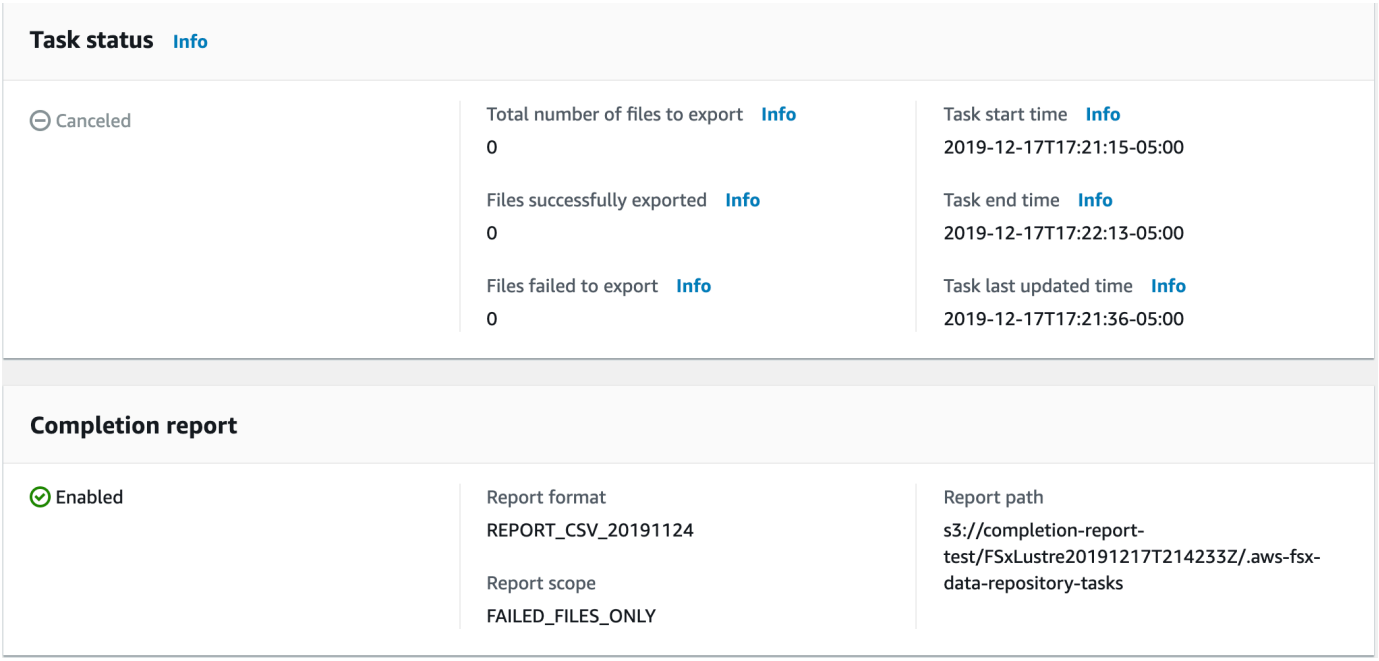
Após criar uma tarefa de repositório de dados, você poderá acessar a tarefa e todas as tarefas existentes em sua conta usando o console do Amazon FSx, a CLI e a API. O Amazon FSx fornece as seguintes informações detalhadas sobre as tarefas:

- Todas as tarefas existentes.
- Todas as tarefas para um sistema de arquivos específico.
- Todas as tarefas para uma associação de repositório de dados específica.
- Todas as tarefas com um status do ciclo de vida específico. Para obter mais informações sobre os valores de status do ciclo de vida da tarefa, consulte Noções básicas sobre o status e os detalhes de uma tarefa.

É possível acessar todas as tarefas de repositório de dados existentes em sua conta usando o console do Amazon FSx, a CLI ou a API, conforme descrito a seguir.

Como visualizar as tarefas de repositório de dados e os detalhes das tarefas (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação, escolha Tarefas de repositório de dados (Lustre). A página Tarefas de repositório de dados será exibida, mostrando as tarefas existentes.
3. Para visualizar os detalhes de uma tarefa, escolha ID da tarefa ou Nome da tarefa na página Tarefas de repositório de dados. A página de detalhes da tarefa será exibida.



Como recuperar as tarefas de repositório de dados e os detalhes das tarefas (CLI)

Ao usar o comando `describe-data-repository-tasks` da CLI do Amazon FSx, é possível visualizar todas as tarefas de repositório de dados e os detalhes em sua conta. `DescribeDataRepositoryTasks` é o comando de API equivalente.

- Use o comando apresentado a seguir para visualizar todos os objetos da tarefa de repositório de dados em sua conta.

```
aws fsx describe-data-repository-tasks
```

Se o comando ocorrer com êxito, o Amazon FSx retornará a resposta no formato JSON.

```
{
    "DataRepositoryTasks": [
```

```
        {
            "Lifecycle": "EXECUTING",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-01/reports",
                "Format":"REPORT_CSV_20191124",
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
            "StartTime": 1591863862.288,
            "EndTime": ,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef3",
            "Status": {
                "SucceededCount": 4255,
                "TotalCount": 4200,
                "FailedCount": 55,
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789a7",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef3"
        },
        {
            "Lifecycle": "FAILED",
            "Paths": [],
            "Report": {
                "Enabled": false,
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef1",
            "Status": {
                "SucceededCount": 1153,
                "TotalCount": 1156,
                "FailedCount": 3,
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1571863850.075,
```

```
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef1"
        },
        {
            "Lifecycle": "SUCCEEDED",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-04/reports",
                "Format":"REPORT_CSV_20191124",
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-04299453935122318",
            "Status": {
                "SucceededCount": 258,
                "TotalCount": 258,
                "FailedCount": 0,
                "LastUpdatedTime": 1771848950.012,
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1771848950.012,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef0"
        }
    ]
}
```

Visualização de tarefas por sistema de arquivos

É possível visualizar todas as tarefas de um sistema de arquivos específico usando o console do Amazon FSx, a CLI ou a API, conforme descrito a seguir.

Como visualizar tarefas por sistema de arquivos (console)

1. Escolha Sistemas de arquivos no painel de navegação. A página Sistema de arquivos será exibida.
2. Escolha o sistema de arquivos para o qual você deseja visualizar as tarefas de repositório de dados. A página de detalhes do sistema de arquivos será exibida.

3. Na página de detalhes do sistema de arquivos, escolha a guia Repositório de dados. Quaisquer tarefas para este sistema de arquivos aparecem no painel Tarefas de repositório de dados.

Como recuperar tarefas por sistema de arquivos (CLI)

- Use o comando apresentado a seguir para visualizar todas as tarefas do repositório de dados para o sistema de arquivos `fs-0123456789abcdef0`.

```
aws fsx describe-data-repository-tasks \
    --filters Name=file-system-id,Values=fs-0123456789abcdef0
```

Se o comando ocorrer com êxito, o Amazon FSx retornará a resposta no formato JSON.

```
{
    "DataRepositoryTasks": [
        {
            "Lifecycle": "FAILED",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-04/reports",
                "Format":"REPORT_CSV_20191124",
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef1",
            "Status": {
                "SucceededCount": 1153,
                "TotalCount": 1156,
                "FailedCount": 3,
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef1"
        },
        {
```

```
            "Lifecycle": "SUCCEEDED",
            "Paths": [],
            "Report": {
                "Enabled": false,
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef0",
            "Status": {
                "SucceededCount": 258,
                "TotalCount": 258,
                "FailedCount": 0,
                "LastUpdatedTime": 1771848950.012,
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1771848950.012,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef0"
        }
    ]
}
```

Cancelamento de uma tarefa de repositório de dados

É possível cancelar uma tarefa de repositório de dados enquanto ela estiver no estado PENDENTE ou EM EXECUÇÃO. Quando você cancela uma tarefa, ocorre o seguinte:

- O Amazon FSx não processa os arquivos que estão na fila para processamento.
- O Amazon FSx continua processando todos os arquivos que estão em processamento no momento.
- O Amazon FSx não reverte os arquivos que a tarefa já processou.

Como cancelar uma tarefa de repositório de dados (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Clique no sistema de arquivos para o qual deseja cancelar uma tarefa de repositório de dados.

3. Abra a guia Repositório de dados e role para baixo para visualizar o painel Tarefas de repositório de dados.
4. Escolha o ID da tarefa ou o Nome da tarefa para a tarefa que você deseja cancelar.
5. Escolha Cancelar tarefa para cancelar a tarefa.
6. Insira o ID da tarefa para confirmar a solicitação de cancelamento.

Como cancelar uma tarefa de repositório de dados (CLI)

Use o comando `cancel-data-repository-task` da CLI do Amazon FSx para cancelar uma tarefa. `CancelDataRepositoryTask` é o comando de API equivalente.

- Use o comando apresentado a seguir para cancelar uma tarefa de repositório de dados.

```
aws fsx cancel-data-repository-task \
    --task-id task-0123456789abcdef0
```

Se o comando ocorrer com êxito, o Amazon FSx retornará a resposta no formato JSON.

```
{
    "Status": "CANCELING",
    "TaskId": "task-0123456789abcdef0"
}
```

Como trabalhar com relatórios de conclusão de tarefas

Um relatório de conclusão da tarefa fornece detalhes sobre os resultados de uma tarefa de exportação, de importação ou de liberação do repositório de dados. O relatório inclui resultados para os arquivos processados pela tarefa que correspondem ao escopo do relatório. É possível especificar se deseja gerar um relatório para uma tarefa ao usar o parâmetro `Enabled`.

O Amazon FSx disponibiliza o relatório para o repositório de dados vinculado do sistema de arquivos no Amazon S3 usando o caminho especificado ao habilitar a geração de um relatório para uma tarefa. O nome do arquivo do relatório é `report.csv` para tarefas de importação e `failures.csv` para tarefas de exportação ou de liberação.

O formato do relatório é um arquivo de valores separados por vírgulas (CSV) que tem três campos: `FilePath`, `FileStatus` e `ErrorCode`.

Os relatórios são codificados usando a codificação no formato RFC-4180, como apresentado abaixo:

- Os caminhos que começam com qualquer um dos seguintes caracteres estão contidos entre aspas simples: `@ + - =`
- Strings que contêm, no mínimo, um dos seguintes caracteres estão contidos entre aspas duplas: `" ,`
- Todas as aspas duplas são delimitadas com aspas duplas adicionais.

A seguir, veja alguns exemplos da codificação de relatórios:

- `@filename.txt` se torna `"""@filename.txt"""`
- `+filename.txt` se torna `"""+filename.txt"""`
- `file,name.txt` se torna `"file,name.txt"`
- `file"name.txt` se torna `"file""name.txt"`

Para obter mais informações sobre a codificação RFC-4180, consulte RFC-4180 - Common Format and MIME Type for Comma-Separated Values (CSV) Files no site do IETF.

Veja a seguir um exemplo das informações fornecidas em um relatório de conclusão da tarefa que inclui somente arquivos com falha.

```
myRestrictedFile,failed,S3AccessDenied
dir1/myLargeFile,failed,FileSizeTooLarge
dir2/anotherLargeFile,failed,FileSizeTooLarge
```

Para obter mais informações sobre as falhas de tarefas e como resolvê-las, consulte Solução de problemas para falhas de tarefas de repositório de dados.

Solução de problemas para falhas de tarefas de repositório de dados

Você pode ativar o registro no CloudWatch Logs para registrar informações sobre quaisquer falhas ocorridas ao importar ou exportar arquivos usando tarefas do repositório de dados. Para obter informações sobre CloudWatch registros de eventos do Logs, consulteRegistros em log de eventos de repositório de dados.

Quando uma tarefa de repositório de dados apresenta falhas, é possível encontrar o número de arquivos que o Amazon FSx não conseguiu processar em Falha ao exportar arquivos na página

Status da tarefa do console. Como alternativa, você pode usar a CLI ou a API e visualizar a propriedade `Status: FailedCount` da tarefa. Para obter informações sobre como acessar essas informações, consulte Acesso a tarefas do repositório de dados.

Para tarefas de repositório de dados, o Amazon FSx também fornece opcionalmente informações sobre arquivos e diretórios específicos que apresentaram falhas em um relatório de conclusão. O relatório de conclusão da tarefa contém o caminho do arquivo ou do diretório no sistema de arquivos do Lustre que apresentou falhas, seu status e o motivo da falha. Para ter mais informações, consulte Como trabalhar com relatórios de conclusão de tarefas.

Uma tarefa de repositório de dados pode falhar por vários motivos, incluindo os listados a seguir.

Código de erro	Explicação
`FileSizeTooLarge`	O tamanho máximo de objetos com suporte pelo Amazon S3 é 5 TiB.
`InternalError`	Ocorreu um erro no sistema de arquivos do Amazon FSx para uma tarefa de importação, de exportação ou de liberação. Geralmente, esse código de erro significa que o sistema de arquivos do Amazon FSx no qual a tarefa com falha foi executada está em um estado do ciclo de vida COM FALHA. Quando isso ocorre, os arquivos afetados podem não ser recuperáveis devido à perda de dados. Caso contrário, você poderá usar os comandos do Hierarchical Storage Management (HSM) para exportar os arquivos e os diretórios para o repositório de dados no S3. Para ter mais informações, consulte Exportação de arquivos usando comandos do HSM.
`OperationNotPermitted`	O Amazon FSx não conseguiu liberar o arquivo porque ele não foi exportado para um bucket do S3 vinculado. Você deve usar a exportação automática ou as tarefas de exportação do repositório de dados para garantir que os

Código de erro	Explicação
	arquivos sejam exportados primeiro para o bucket do Amazon S3 vinculado.
`PathSizeTooLong`	O caminho de exportação é muito longo. O tamanho máximo da chave do objeto com suporte pelo S3 é 1.024 caracteres.
`ResourceBusy`	O Amazon FSx não conseguiu exportar ou liberar o arquivo porque ele estava sendo acessado por outro cliente no sistema de arquivos. Você pode tentar novamente DataRepositoryTask depois que seu fluxo de trabalho terminar de gravar no arquivo.

Código de erro	Explicação
`S3AccessDenied`	O acesso ao Amazon S3 foi negado para uma tarefa de importação ou de exportação do repositório de dados. Para tarefas de exportação, o sistema de arquivos do Amazon FSx deve ter permissão para executar a operação `S3:PutObject` com a finalidade de exportar para um repositório de dados vinculado no S3. Essa permissão é concedida no perfil vinculado ao serviço `AWSServiceRoleForFSxS3Accesss_` *`fs-0123456789abcdef0`* . Para ter mais informações, consulte Como usar perfis vinculados a serviço no Amazon FSx. Para tarefas de exportação, como a tarefa de exportação requer que os dados fluam de forma externa à VPC de um sistema de arquivos, esse erro poderá ocorrer se o repositório de destino tiver uma política de bucket que contenha uma das chaves de condição globais do IAM `aws:SourceVpc` ou `aws:SourceVpce` . Para tarefas de importação, o sistema de arquivos do Amazon FSx deve ter permissão para executar as operações `S3:HeadObject` e `S3:GetObject` com a finalidade de importar de um repositório de dados vinculado no S3. Para tarefas de importação, se seu bucket do S3 usa criptografia do lado do servidor com chaves gerenciadas pelo cliente armazenadas em AWS Key Management Service (SSE-KMS), você deve seguir as configurações de política

Código de erro	Explicação
	em. Como trabalhar com buckets do Amazon S3 criptografados no lado do servidor Se o bucket do S3 contiver objetos carregados de uma conta de bucket Conta da AWS do S3 vinculada ao sistema de arquivos, você pode garantir que as tarefas do repositório de dados possam modificar os metadados do S3 ou sobrescrever objetos do S3, independentemente da conta que os carregou. Recomendamos habilitar o recurso Propriedade de objeto do S3 para seu bucket do S3. Esse recurso permite que você se aproprie de novos objetos que outros Contas da AWS enviam para seu bucket, forçando os uploads a fornecerem a `-/-acl bucket-owner-full-control` ACL padrão. Você habilita a propriedade de objeto do S3 ao escolher a opção Proprietário do bucket preferencial em seu bucket do S3. Para obter mais informações, consulte Controlling ownership of uploaded objects using S3 Object Ownership no Guia do usuário do Amazon S3.
`S3Error`	O Amazon FSx encontrou um erro relacionado ao S3 que era diferente de `S3AccessDenied` .
`S3FileDeleted`	O Amazon FSx não conseguiu exportar um arquivo de link físico porque o arquivo de origem não existe no repositório de dados.

Código de erro	Explicação
`S3ObjectInUnsupportedTier`	O Amazon FSx importou com êxito um objeto que não tem link simbólico de uma classe de armazenamento do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive. O `FileStatus` será `succeeded with warning` no relatório de conclusão da tarefa. O aviso indica que, para recuperar os dados, primeiro é necessário restaurar o objeto da classe do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive e, em seguida, usar um comando `hsm_restore` para importá-lo.
`S3ObjectNotFound`	O Amazon FSx não conseguiu importar ou exportar o arquivo porque ele não existe no repositório de dados.
`S3ObjectPathNotPosixCompliant`	O objeto do Amazon S3 existe, mas não pode ser importado porque não é um objeto compatível com POSIX. Para obter informaçõ es sobre os metadados POSIX com suporte, consulte Suporte a metadados POSIX para repositórios de dados.
`S3ObjectUpdateInProgressFro mFileRename`	O Amazon FSx não conseguiu liberar o arquivo porque a exportação automática está processando uma renomeação do arquivo. O processo de renomeação da exportação automática deve ser concluído antes que o arquivo possa ser liberado.

Código de erro	Explicação
`S3SymlinkInUnsupportedTier`	O Amazon FSx não conseguiu importar um objeto de link simbólico porque ele está em uma classe de armazenamento do Amazon S3 que não tem suporte, como uma classe de armazenamento do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive. O `FileStatus` será `failed` no relatório de conclusão da tarefa.
`SourceObjectDeletedBeforeReleasing`	O Amazon FSx não conseguiu liberar o arquivo do sistema de arquivos porque o arquivo foi excluído do repositório de dados antes que pudesse ser liberado.

Liberação de arquivos

Libere tarefas do repositório de dados libere dados de arquivos do seu sistema de arquivos FSx for Lustre para liberar espaço para novos arquivos. A liberação de um arquivo retém a listagem e os metadados do arquivo, mas remove a cópia local do conteúdo desse arquivo. Se um usuário ou aplicativo acessar um arquivo lançado, os dados serão carregados de volta de forma automática e transparente em seu sistema de arquivos a partir do bucket vinculado do Amazon S3.

> **Note**
>
> As tarefas do repositório de dados da versão não estão disponíveis nos sistemas de arquivos FSx for Lustre 2.10.

Os parâmetros Caminhos do sistema de arquivos para lançamento e Duração mínima desde o último acesso determinam quais arquivos serão liberados.

- Caminhos do sistema de arquivos para liberação: especifica o caminho a partir do qual os arquivos serão liberados.
- Duração mínima desde o último acesso: especifica a duração, em dias, para que qualquer arquivo não acessado nessa duração seja liberado. A duração desde o último acesso de um arquivo é

calculada pela diferença entre a hora de criação da tarefa de liberação e a última vez em que um arquivo foi acessado (valor máximo de `atimemtime`, `ectime`).

Os arquivos só serão liberados ao longo do caminho do arquivo se tiverem sido exportados para o S3 e tiverem uma duração desde o último acesso maior do que a duração mínima desde o valor do último acesso. Fornecer uma duração mínima de `0` dias desde o último acesso liberará arquivos independentemente da duração desde o último acesso.

> **Note**
>
> O uso de curingas para incluir ou excluir arquivos para lançamento não é suportado.

As tarefas do repositório de dados de lançamento só liberarão dados de arquivos que já foram exportados para um repositório de dados vinculado do S3. Você pode exportar dados para o S3 usando o recurso de exportação automática, uma tarefa de repositório de dados de exportação ou comandos do HSM. Para verificar se um arquivo foi exportado para seu repositório de dados, você pode executar o comando a seguir. Um valor de retorno `states: (0x00000009) exists archived` indica que o arquivo foi exportado com êxito.

```
sudo lfs hsm_state path/to/export/file
```

> **Note**
>
> Você deve executar o comando HSM como usuário root ou usando`sudo`.

Para liberar dados de arquivos em um intervalo regular, você pode programar uma tarefa recorrente do repositório de dados de lançamento usando o Amazon EventBridge Scheduler. Para obter mais informações, consulte Introdução ao EventBridge Scheduler no Guia do usuário do Amazon EventBridge Scheduler.

Tópicos

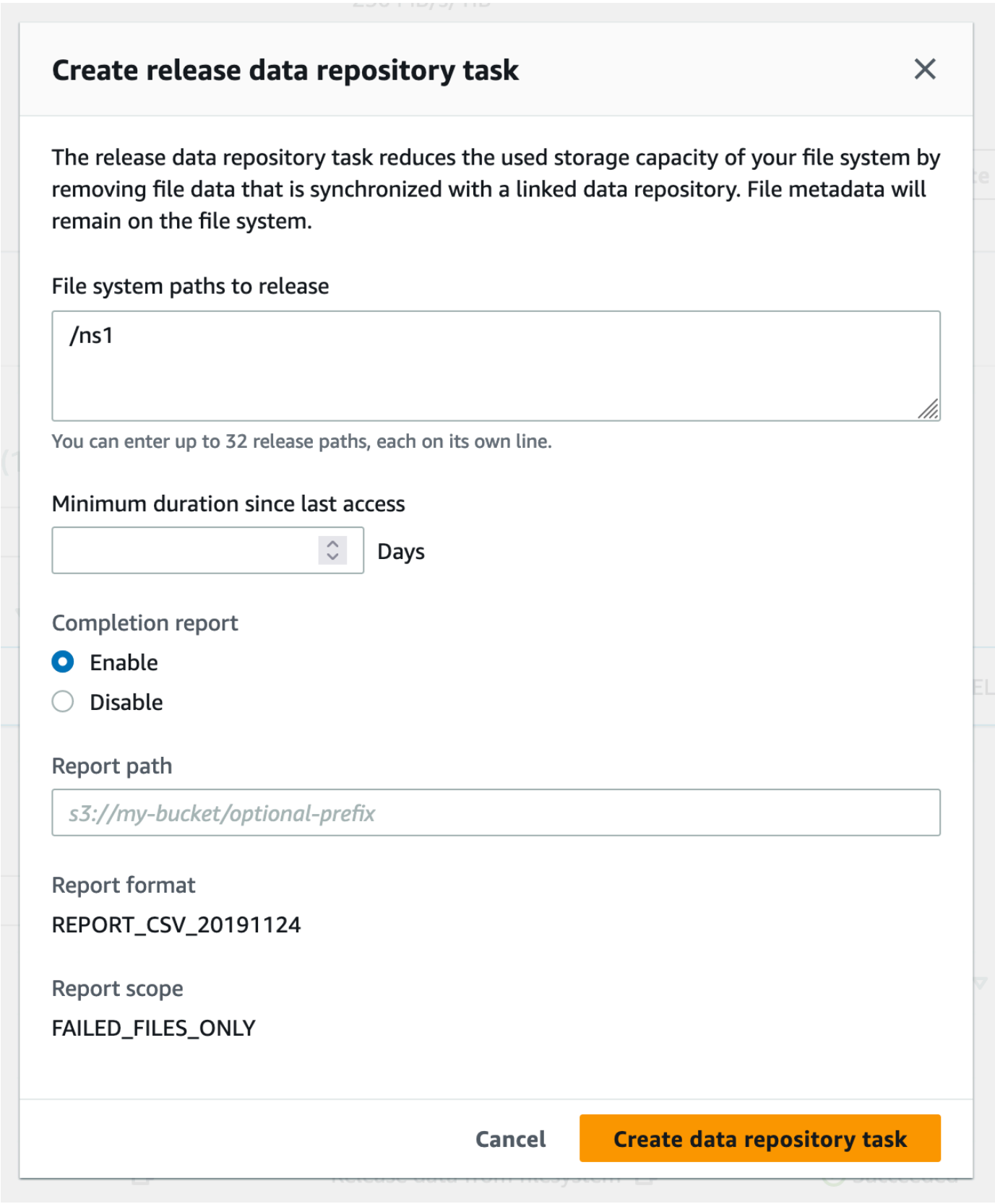
- Como usar tarefas do repositório de dados para lançar arquivos

Como usar tarefas do repositório de dados para lançar arquivos

Use os procedimentos a seguir para criar tarefas que liberam arquivos do sistema de arquivos usando o console e a CLI do Amazon FSx. A liberação de um arquivo retém a listagem e os metadados do arquivo, mas remove a cópia local do conteúdo desse arquivo.

Liberar arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação esquerdo, selecione Sistemas de arquivos e escolha o sistema de arquivos Lustre.
3. Escolha a guia Repositório de dados.
4. No painel Associações de repositórios de dados, escolha a associação de repositório de dados para a qual você deseja criar a tarefa de liberação.
5. Em Ações, escolha Criar tarefa de liberação. Essa opção só estará disponível se o sistema de arquivos estiver vinculado a um repositório de dados no S3. A caixa de diálogo Criar tarefa de liberação do repositório de dados é exibida.


Create release data repository task
The release data repository task reduces the used storage capacity of your file system by removing file data that is synchronized with a linked data repository. File metadata will remain on the file system.
File system paths to release
/ns1
You can enter up to 32 release paths, each on its own line.
Minimum duration since last access
Days
Completion report
Enable
Disable
Report path
s3://my-bucket/optional-prefix
Report format
REPORT_CSV_20191124
Report scope
FAILED_FILES_ONLY
Cancel
Create data repository task

6. Em Caminhos do sistema de arquivos para liberação, especifique até 32 diretórios ou arquivos a serem liberados do seu sistema de arquivos do Amazon FSx fornecendo os caminhos para esses diretórios ou arquivos. Os caminhos fornecidos precisam ser relativos ao ponto de montagem do sistema de arquivos. Por exemplo, se o ponto de montagem for `/mnt/fsx` e `/mnt/fsx/path1` for um arquivo no sistema de arquivos que você deseja liberar, o caminho a ser fornecido será `path1`. Para liberar todos os arquivos no sistema de arquivos, especifique uma barra (/) como caminho.

   > **Note**
   >
   > Se um caminho fornecido não for válido, a tarefa falhará.

7. Em Duração mínima desde o último acesso, especifique a duração, em dias, para que qualquer arquivo não acessado nessa duração seja liberado. O horário do último acesso é calculado usando o valor máximo `atime`, `mtime` e `ctime`. Arquivos com um período de duração do último acesso maior que a duração mínima desde o último acesso (em relação ao horário de criação da tarefa) serão liberados. Arquivos com um período de duração do último acesso menor que esse número de dias não serão liberados, mesmo que estejam no campo Caminhos do sistema de arquivos para liberação. Forneça uma duração de `0` dias para liberar arquivos, independentemente da duração desde o último acesso.
8. (Opcional) Em Relatório de conclusão, escolha Habilitar para gerar um relatório de conclusão de tarefa que forneça detalhes sobre os arquivos que atendem ao escopo fornecido em Escopo do relatório. Para especificar um local para o Amazon FSx entregar o relatório, em Caminho do relatório, insira um caminho relativo no repositório de dados do S3 vinculado do sistema de arquivos.
9. Escolha Criar tarefa de repositório de dados.

   Uma notificação na parte superior da página Sistemas de arquivos mostra a tarefa que você acabou de criar em andamento.

Para ver o status e os detalhes da tarefa, na guia Repositório de dados, role para baixo até Tarefas do repositório de dados. A ordem de classificação padrão mostra a tarefa mais recente no topo da lista.

Para ver um resumo da tarefa nessa página, escolha ID da tarefa referente à tarefa que você acabou de criar.

Liberação de arquivos (CLI)

- Use o comando `create-data-repository-task` da CLI para criar uma tarefa que libere arquivos em seu sistema de arquivos do FSx para Lustre. A operação de API correspondente é `CreateDataRepositoryTask`.

  Defina os seguintes parâmetros:

  - Defina `--file-system-id` como ID do sistema de arquivos do qual você está lançando arquivos.
  - Defina `--paths` como caminhos no sistema de arquivos do qual os dados serão liberados. Se um diretório for especificado, os arquivos dentro do diretório serão liberados. Se um caminho de arquivo for especificado, somente esse arquivo será liberado. Para liberar todos os arquivos no sistema de arquivos que foram exportados para um bucket do S3 vinculado, especifique uma barra (/) no caminho.
  - Defina `--type` como `RELEASE_DATA_FROM_FILESYSTEM`.
  - Defina as opções `--release-configuration DurationSinceLastAccess` desta forma:
    - `Unit`: defina como `DAYS`.
    - `Value`: especifique um número inteiro que represente a duração, em dias, para que qualquer arquivo não acessado nessa duração seja liberado. Arquivos que foram acessados durante um período menor que esse número de dias não serão liberados, mesmo que estejam no parâmetro `--paths`. Forneça uma duração de `0` dias para liberar arquivos, independentemente da duração desde o último acesso.

  Esse exemplo de comando especifica que os arquivos que foram exportados para um bucket do S3 vinculado e atendem aos critérios `--release-configuration` serão liberados dos diretórios nos caminhos especificados.

```
$ aws fsx create-data-repository-task \
    --file-system-id fs-0123456789abcdef0 \
    --type RELEASE_DATA_FROM_FILESYSTEM \
    --paths path1,path2/file1 \
    --release-configuration '{"DurationSinceLastAccess":
{"Unit":"DAYS","Value":10}}' \
    --report Enabled=false
```

Depois de criar com êxito a tarefa do repositório de dados, o Amazon FSx retorna a descrição da tarefa como JSON.

Depois de criar a tarefa para liberar arquivos, você pode verificar o status da tarefa. Para obter mais informações sobre como visualizar tarefas do repositório de dados, consulte Acesso a tarefas do repositório de dados.

Como usar o Amazon FSx com dados on-premises

Você pode usar o FSx para Lustre para processar seus dados on-premises com instâncias de computação na nuvem. O FSx para Lustre fornece suporte ao acesso via AWS Direct Connect e VPN, permitindo que você monte seus sistemas de arquivos em clientes on-premises.

Usar o FSx para Lustre com dados on-premises

1. Crie um sistema de arquivos. Para obter mais informações, consulte Crie seu sistema de arquivos FSx for Lustre no exercício de conceitos básicos.
2. Monte o sistema de arquivos em clientes on-premises. Para obter mais informações, consulte Montagem de sistemas de arquivos do Amazon FSx usando uma Amazon VPC on-premises ou emparelhada.
3. Copie os dados que você deseja processar no sistema de arquivos do FSx para Lustre.
4. Execute sua workload de intensa computação em instâncias do Amazon EC2 na nuvem, montando seu sistema de arquivos.
5. Ao terminar, copie os resultados finais do sistema de arquivos de volta para o local de dados on-premises e exclua o sistema de arquivos do FSx para Lustre.

Registros em log de eventos de repositório de dados

É possível ativar o registro em log para o CloudWatch Logs com a finalidade de registrar em log informações sobre quaisquer falhas ocorridas durante a importação ou a exportação de arquivos usando a importação automática, a exportação automática e as tarefas de repositório de dados. Para obter mais informações, consulte Registro com Amazon CloudWatch Logs.

> **Note**
>
> Quando uma tarefa de repositório de dados apresenta falhas, o Amazon FSx também grava as informações sobre a falha no relatório de conclusão da tarefa. Para obter mais informações sobre as informações sobre falhas nos relatórios de conclusão, consulte Solução de problemas para falhas de tarefas de repositório de dados.

A importação automática, a exportação automática e as tarefas de repositório de dados podem apresentar falhas por diversos motivos, incluindo os listados abaixo. Para obter informações sobre como visualizar esses logs, consulte Visualizar logs do .

Importação de eventos

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ImportListObjectError`	ERROR	Falha ao listar objetos do S3 no bucket do S3 *bucket_name* com o prefixo *prefix*.	O Amazon FSx não conseguiu listar objetos do S3 no bucket do S3. Isto pode acontecer se a política do bucket do S3 não fornecer permissões suficientes para o Amazon FSx.	N/D
`S3ImportUnsupportedTierWarning`	WARN	Falha ao importar objetos do S3 com a chave *key_value*	O Amazon FSx não conseguiu importar um objeto do S3 porque ele está	`S3ObjectInUnsupportedTier`

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
		no bucket do S3 *bucket_name* devido a um objeto do S3 em uma camada sem suporte *S3_tier_name* .	em uma classe de armazenamento do Amazon S3 que não tem suporte, como as classes de armazenamento do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive.	
`S3ImportSymlinkInUnsupportedTierWarning`	WARN	Falha ao importar objetos do S3 com a chave *key_value* no bucket do S3 *bucket_name* devido a um objeto de link simbólico do S3 em uma camada sem suporte *S3_tier_name* .	O Amazon FSx não conseguiu importar um objeto de link simbólico porque ele está em uma classe de armazenamento do Amazon S3 que não tem suporte, como as classes de armazenamento do S3 Glacier Flexible Retrieval ou do S3 Glacier Deep Archive.	`S3SymlinkInUnsupportedTier`

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ImportAccessDenied`	ERROR	Falha ao importar objetos do S3 com a chave *`key_value`* no bucket do S3 *`bucket_name`* porque o acesso ao objeto do S3 foi negado.	O acesso ao Amazon S3 foi negado para uma tarefa de importação ou de exportação do repositório de dados. Para tarefas de importação, o sistema de arquivos do Amazon FSx deve ter permissão para executar as operações `s3:HeadObject` e `s3:GetObject` com a finalidade de importar de um repositório de dados vinculado no S3. Para tarefas de importação, se o bucket do S3 usar criptogra	`S3AccessDenied`

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
			fia do lado do servidor com chaves gerenciadas pelo cliente e armazenadas no AWS Key Managemen t Service (SSE-KMS), você deverá seguir as configurações de política em Como trabalhar com buckets do Amazon S3 criptogra fados no lado do servidor.	

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ImportDeleteAccessDenied`	ERROR	Falha ao excluir o arquivo local para o objeto do S3 com a chave *`key_value`* no bucket do S3 *`bucket_name`* porque o acesso ao objeto do S3 foi negado.	A importação automática teve o acesso negado a um objeto do S3.	N/D

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ImportObjectPathNotPosixCompliant`	ERROR	Falha ao importar objetos do S3 com a chave *`key_value`* no bucket do S3 *`bucket_name`* porque o objeto do S3 não é compatível com POSIX.	O objeto do Amazon S3 existe, mas não pode ser importado porque não é um objeto compatível com POSIX. Para obter informações sobre os metadados POSIX com suporte, consulte Suporte a metadados POSIX para repositórios de dados.	`S3ObjectPathNotPosixCompliant`

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ImportObjectTypeMismatch`	ERROR	Falha ao importar objetos do S3 com a chave *`key_value`* no bucket do S3 *`bucket_name`* porque um objeto do S3 com o mesmo nome já foi importado para o sistema de arquivos.	O objeto do S3 que está sendo importado é de um tipo diferente (arquivo ou diretório) quando comparado com um objeto existente com o mesmo nome no sistema de arquivos.	`S3ObjectTypeMismatch`
`S3ImportDirectoryMetadataUpdateError`	ERROR	Falha ao atualizar os metadados do diretório local devido a um erro interno.	Não foi possível importar os metadados do diretório devido a um erro interno.	N/D

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ImportObjectDeleted`	ERROR	Falha ao importar objetos do S3 com a chave *`key_value`* porque eles não foram encontrados no bucket do S3 *`bucket_name`* .	O Amazon FSx não conseguiu importar metadados do arquivo porque o objeto correspondente não existia no repositório de dados.	`S3FileDeleted`
`S3ImportBucketDoesNotExist`	ERROR	Falha ao importar objetos do S3 com a chave *`key_value`* no bucket do S3 *`bucket_name`* devido ao bucket não existir.	O Amazon FSx não pode importar automaticamente um objeto do S3 para o sistema de arquivos porque o bucket do S3 não existe mais.	N/D

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ImportDeleteBucketDoesNotExist`	ERROR	Falha ao excluir um arquivo local para o objeto do S3 com a chave *`key_value`* no bucket do S3 *`bucket_name`* devido ao bucket não existir.	O Amazon FSx não pode excluir um arquivo vinculado a um objeto do S3 no sistema de arquivos porque o bucket do S3 não existe mais.	N/D
`S3ImportDirectoryCreateError`	ERROR	Falha ao criar o diretório local devido a um erro interno.	O Amazon FSx não conseguiu importar automaticamente a criação de um diretório no sistema de arquivos devido a um erro interno.	N/D

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`NoDiskSpace`	ERROR	Falha ao importar objetos do S3 com a chave *`key_value`* no bucket do S3 *`bucket_name`* porque o sistema de arquivos está cheio.	O sistema de arquivos ficou sem espaço no disco nos servidores de metadados durante a criação do arquivo ou do diretório.	N/D

Exportação de eventos

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ExportInternalError`	ERROR	Falha ao exportar objetos do S3 com a chave *`key_value`* no bucket do S3 *`bucket_name`* devido a um erro interno.	O objeto não foi exportado devido a um erro interno.	`INTERNAL_ERROR`
`S3ExportAccessDenied`	ERROR	Falha ao exportar o arquivo porque o acesso foi	O acesso ao Amazon S3 foi negado para uma tarefa de	`S3AccessDenied`

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
		negado ao objeto do S3 com a chave *key_value* no bucket do S3 *bucket_name* .	exportação do repositório de dados. Para tarefas de exportação, o sistema de arquivos do Amazon FSx deve ter permissão para executar a operação `s3:PutObject` com a finalidade de exportar para um repositório de dados vinculado no S3. Essa permissão é concedida no perfil vinculado ao serviço `AWSServiceRoleForFSxS3Access_` *fs-0123456789abcdef0* . Para obter mais informações, consulte Como usar	

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
			perfis vinculados a serviço no Amazon FSx. Como a tarefa de exportação requer que os dados fluam de forma externa à VPC de um sistema de arquivos, esse erro poderá ocorrer se o repositório de destino tiver uma política de bucket que contenha uma das chaves de condição globais do IAM `aws:SourceVpc` ou `aws:SourceVpce`. Se o bucket do S3 contiver objetos carregados de uma Conta da AWS diferente	

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
			da conta do bucket do S3 vinculada ao sistema de arquivos, você poderá garantir que as tarefas do repositório de dados possam modificar os metadados do S3 ou substitui r os objetos do S3, independe ntemente de qual conta os carregou. Recomenda mos habilitar o recurso Propriedade de objeto do S3 para seu bucket do S3. Esse recurso possibilita que você assuma a proprieda de dos novos objetos que outras Contas da AWS fazem upload em seu	

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
			bucket ao impor aos uploads o fornecime nto da ACL predefinida `--acl bucket-owner-full-control` . Você habilita a propriedade de objeto do S3 ao escolher a opção Proprietá rio do bucket preferencial em seu bucket do S3. Para obter mais informaçõ es, consulte Controlling ownership of uploaded objects using S3 Object Ownership no Guia do usuário do Amazon S3.	

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ExportPathSizeTooLong`	ERROR	Falha ao exportar o arquivo porque o tamanho do caminho do arquivo local excede o tamanho máximo da chave do objeto com suporte pelo S3.	O caminho de exportação é muito longo. O tamanho máximo da chave do objeto com suporte pelo S3 é 1.024 caracteres.	`PathSizeTooLong`
`S3ExportFileSizeTooLarge`	ERROR	Falha ao exportar o arquivo porque o tamanho do arquivo excede o tamanho máximo de objetos com suporte pelo S3.	O tamanho máximo de objetos com suporte pelo Amazon S3 é 5 TiB.	`FileSizeTooLarge`

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ExportKMSKeyNotFound`	ERROR	Falha ao exportar o arquivo para o objeto do S3 com a chave *`key_value`* no bucket do S3 *`bucket_name`* porque a chave do KMS pertencente ao bucket não foi encontrada.	O Amazon FSx não conseguiu exportar o arquivo porque a AWS KMS key não foi encontrada. Certifique-se de usar uma chave que esteja na mesma Região da AWS que o bucket do S3. Para obter mais informações sobre como criar chaves do KMS, consulte Criar chaves no Guia do desenvolvedor do AWS Key Management Service.	`N/A`

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ExportResourceBusy`	ERROR	Falha ao exportar o arquivo porque ele está sendo usado por outro processo.	O Amazon FSx não conseguiu exportar o arquivo porque ele estava sendo modificado por outro cliente no sistema de arquivos. É possível tentar realizar a tarefa novamente depois que o fluxo de trabalho terminar a gravação no arquivo.	`ResourceBusy`
`S3ExportLocalObjectReleaseWithoutS3Source`	WARN	Exportação ignorada: o arquivo local está em estado liberado e um objeto do S3 vinculado com a chave *`key_value`* não foi encontrado no bucket *`bucket_name`* .	O Amazon FSx não conseguiu exportar o arquivo porque ele estava em um estado liberado no sistema de arquivos.	N/D

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3ExportLocalObjectNotMatchDra`	WARN	Exportação ignorada: o arquivo local não pertence a um caminho do sistema de arquivos vinculado ao repositório de dados.	O Amazon FSx não conseguiu realizar a exportação porque o objeto não pertence a um caminho do sistema de arquivos que está vinculado a um repositório de dados.	N/D
`InternalAutoExportError`	ERROR	A exportação automática encontrou um erro interno durante a exportação de um objeto do sistema de arquivos.	A exportação falhou devido a um erro interno (auto-export- ou lustre-level).	N/D
`S3CompletionReportUploadFailure`	ERROR	Falha ao fazer upload do relatório de conclusão da tarefa do repositório de dados para *`bucket_name`* .	O Amazon FSx não conseguiu fazer upload do relatório de conclusão.	N/D

Código de erro	Nível de log	Mensagem de log	Causa raiz	Código de erro no relatório de conclusão
`S3CompletionReportValidateFailure`	ERROR	Falha ao fazer upload do relatório de conclusão da tarefa do repositório de dados no bucket *`bucket_name`* porque o caminho do relatório de conclusão *`report_path`* não pertence a um repositório de dados associado a este sistema de arquivos.	O Amazon FSx não conseguiu fazer upload do relatório de conclusão porque o caminho do S3 fornecido pelo cliente não pertence a um repositório de dados vinculado.	N/D

Como trabalhar com tipos de implantação mais antigos

Esta seção se aplica aos sistemas de arquivos com tipo de implantação Scratch 1 e também aos sistemas de arquivos com tipos de implantação `Scratch 2` ou `Persistent 1` que não usam associações de repositório de dados.

Tópicos

- Vinculação do sistema de arquivos a um bucket do Amazon S3
- Importação automática de atualizações do bucket do S3

Vinculação do sistema de arquivos a um bucket do Amazon S3

Ao criar um sistema de arquivos do Amazon FSx para Lustre, é possível vinculá-lo a um repositório de dados durável no Amazon S3. Antes de criar o sistema de arquivos, certifique-se de já ter criado o bucket do Amazon S3 ao qual ele está sendo vinculando. No assistente Criar sistema de arquivos, você define as propriedades apresentadas a seguir de configuração do repositório de dados no painel opcional Importação e exportação de repositórios de dados.

- Escolha como o Amazon FSx mantém a listagem de arquivos e de diretórios atualizada à medida que você adiciona ou modifica objetos no bucket do S3 após a criação do sistema de arquivos. Para obter mais informações, consulte Importação automática de atualizações do bucket do S3.
- Bucket de importação: insira o nome do bucket do S3 que você está usando para o repositório vinculado.
- Prefixo de importação: insira um prefixo de importação opcional se desejar importar somente algumas listagens de dados de arquivos e de diretórios no bucket do S3 para o sistema de arquivos. O prefixo de importação define de que local os dados no bucket do S3 serão importados.
- Prefixo de exportação: define o local para o qual o Amazon FSx exporta o conteúdo do sistema de arquivos para o bucket do S3 vinculado.

É possível ter um mapeamento de um para um em que o Amazon FSx exporta dados do sistema de arquivos do FSx para Lustre de volta para os mesmos diretórios no bucket do S3 dos quais eles foram importados. Para ter um mapeamento de um para um, especifique um caminho de exportação para o bucket do S3 sem prefixos ao criar o sistema de arquivos.

- Ao criar um sistema de arquivos usando o console, escolha a opção Prefixo de exportação > Um prefixo especificado por você e mantenha o campo de prefixo em branco.
- Ao criar um sistema de arquivos usando a AWS CLI ou a API, especifique o caminho de exportação como o nome do bucket do S3 sem prefixos adicionais, por exemplo, `ExportPath=s3://lustre-export-test-bucket/`.

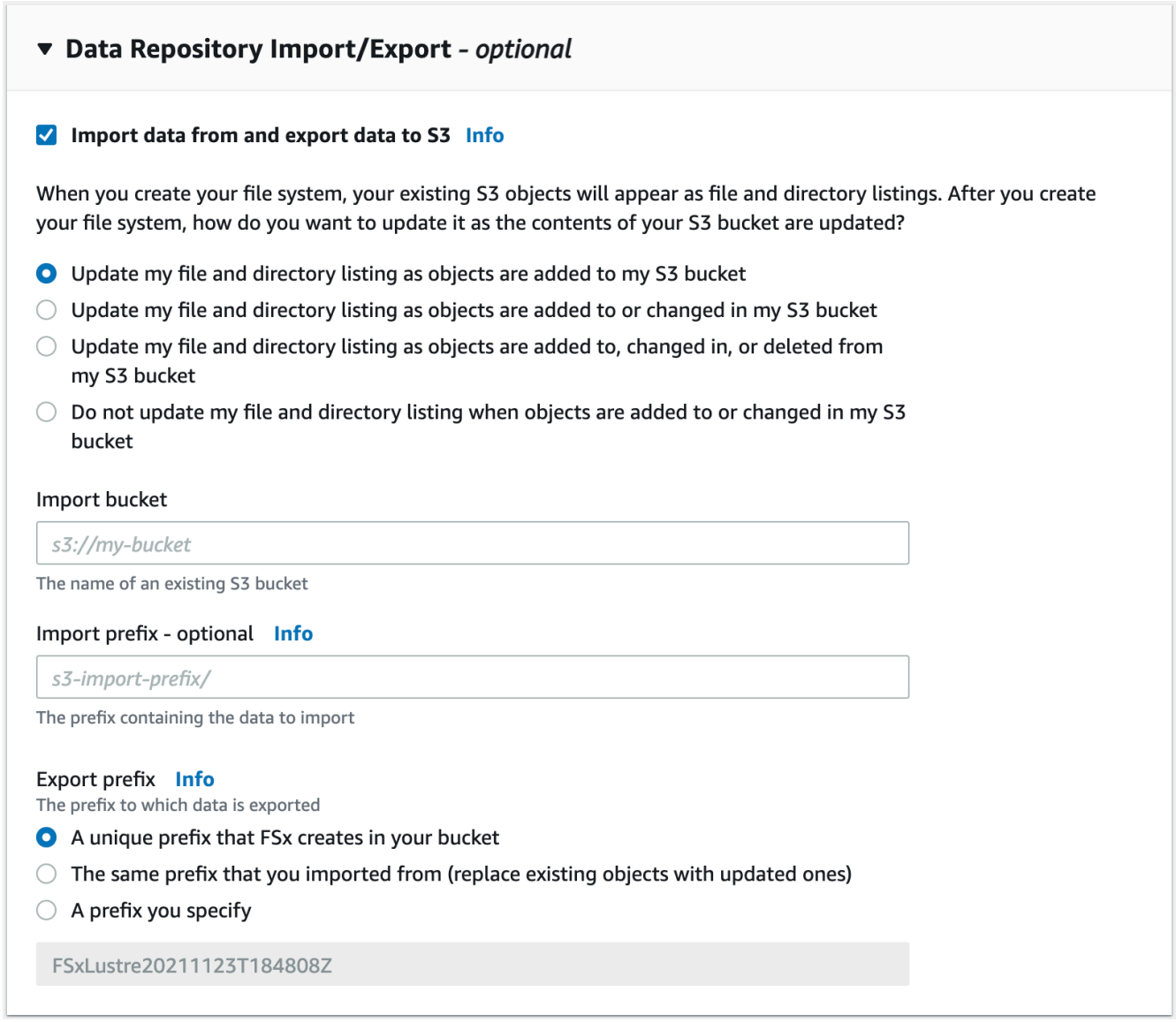
Usando esse método, é possível incluir um prefixo de importação ao especificar o caminho de importação, e isso não afeta um mapeamento individual para as exportações.

Como criar sistemas de arquivos vinculados a um bucket do S3

Os procedimentos apresentados a seguir orientam você no processo de criação de um sistema de arquivos do Amazon FSx vinculado a um bucket do S3 usando o Console de Gerenciamento da AWS e a AWS Command Line Interface (AWS CLI).

Console

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel, escolha Criar sistema de arquivos.
3. Para o tipo de sistema de arquivos, escolha FSx para Lustre e, em seguida, escolha Próximo.
4. Forneça as informações necessárias para as seções Detalhes do sistema de arquivos e Rede e segurança. Para obter mais informações, consulte Crie seu sistema de arquivos FSx for Lustre.
5. Você usa o painel Importação e exportação de repositórios de dados para configurar um repositório de dados vinculado no Amazon S3. Selecione Importar dados do e exportar dados para o S3 para expandir a seção Importação e exportação de repositórios de dados e definir as configurações do repositório de dados.



6. Escolha como o Amazon FSx mantém a listagem de arquivos e de diretórios atualizada à medida que você adiciona ou modifica objetos no bucket do S3. Quando você cria o sistema de arquivos, seus objetos existentes no S3 aparecem como listagens de arquivos e diretórios.

   - Atualizar minha listagem de arquivos e de diretórios à medida que os objetos são adicionados ao meu bucket do S3: (padrão) o Amazon FSx atualiza automaticamente as listagens de arquivos e de diretórios para quaisquer novos objetos adicionados ao bucket do S3 vinculado, os quais não existam no sistema de arquivos do FSx. O Amazon FSx não atualiza listagens para objetos que foram alterados no bucket do S3. O Amazon FSx não exclui listagens de objetos que são excluídos no bucket do S3.

> **Note**
>
> A configuração padrão de preferências de importação para importar dados de um bucket do S3 vinculado usando a CLI e a API é `NONE`. A configuração padrão de preferências de importação ao usar o console é atualizar o Lustre à medida que novos objetos são adicionados ao bucket do S3.

- Atualizar minha listagem de arquivos e de diretórios à medida que os objetos são adicionados ou alterados em meu bucket do S3: o Amazon FSx atualiza automaticamente as listagens de arquivos e de diretórios para quaisquer novos objetos adicionados ao bucket do S3 e para quaisquer objetos existentes que são alterados no bucket do S3 depois que você escolher essa opção. O Amazon FSx não exclui listagens de objetos que são excluídos no bucket do S3.
- Atualizar minha listagem de arquivos e de diretórios à medida que os objetos são adicionados, alterados ou excluídos do meu bucket do S3: o Amazon FSx atualiza automaticamente as listagens de arquivos e de diretórios para quaisquer novos objetos adicionados ao bucket do S3, para quaisquer objetos existentes que são alterados no bucket do S3 e para quaisquer objetos existentes que são excluídos do bucket do S3 depois que você escolher essa opção.
- Não atualizar meu arquivo e listar diretamente quando objetos são adicionados, alterados ou excluídos do meu bucket do S3: o Amazon FSx atualiza somente as listagens de arquivos e de diretórios do bucket do S3 vinculado quando o sistema de arquivos é criado. O FSx não atualiza as listagens de arquivos e de diretórios para objetos novos, alterados ou excluídos após a escolha dessa opção.

7. Insira um Prefixo de importação opcional se desejar importar somente algumas das listagens de dados de arquivos e de diretórios no bucket do S3 para o sistema de arquivos. O prefixo de importação define de que local os dados no bucket do S3 serão importados. Para obter mais informações, consulte Importação automática de atualizações do bucket do S3.
8. Escolha uma das opções de Prefixo de exportação disponíveis:

   - Um prefixo exclusivo que o Amazon FSx cria em seu bucket: escolha esta opção para exportar objetos novos e alterados usando um prefixo gerado pelo FSx para Lustre. O prefixo é semelhante ao seguinte: `/FSxLustre`*`file-system-creation- timestamp`*. O timestamp é no formato UTC, por exemplo `FSxLustre20181105T222312Z`.

- O mesmo prefixo do qual você importou (substituiu objetos existentes por objetos atualizados): escolha esta opção para substituir objetos existentes por objetos atualizados.
- Um prefixo especificado por você: escolha esta opção para preservar os dados importados e exportar objetos novos e alterados usando um prefixo especificado por você. Para obter um mapeamento de um por um ao exportar dados para o bucket do S3, escolha esta opção e deixe o campo de prefixo em branco. O FSx exportará os dados para os mesmos diretórios dos quais eles foram importados.

9. (Opcional) Defina Preferências de manutenção ou use os padrões do sistema.
10. Escolha Próximo e analise as configurações do sistema de arquivos. Realize alterações, se necessário.
11. Escolha Create file system (Criar sistema de arquivos).

AWS CLI

O exemplo apresentado a seguir cria um sistema de arquivos do Amazon FSx vinculado ao `lustre-export-test-bucket`, com uma preferência de importação que importa quaisquer arquivos novos, alterados e excluídos no repositório de dados vinculado após a criação do sistema de arquivos.

> **Note**
>
> A configuração padrão de preferências de importação para importar dados de um bucket do S3 vinculado usando a CLI e a API é `NONE`, que é diferente do comportamento padrão ao usar o console.

Para criar um sistema de arquivos do FSx para Lustre, use o comando `create-file-system` da CLI do Amazon FSx, conforme mostrado abaixo. A operação de API correspondente é `CreateFileSystem`.

```
$ aws fsx create-file-system \
--client-request-token CRT1234 \
--file-system-type LUSTRE \
--file-system-type-version 2.10 \
--lustre-configuration
AutoImportPolicy=NEW_CHANGED_DELETED,DeploymentType=SCRATCH_1,ImportPath=s
3://lustre-export-test-bucket/,ExportPath=s3://lustre-export-test-bucket/export,
```

```
PerUnitStorageThroughput=50 \
--storage-capacity 2400 \
--subnet-ids subnet-123456 \
--tags Key=Name,Value=Lustre-TEST-1 \
--region us-east-2
```

Após criar o sistema de arquivos com êxito, o Amazon FSx retorna a descrição do sistema de arquivos como JSON, conforme mostrado no exemplo a seguir.

```
{
    "FileSystems": [
        {
            "OwnerId": "owner-id-string",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "FileSystemTypeVersion": "2.10",
            "Lifecycle": "CREATING",
            "StorageCapacity": 2400,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "PERSISTENT_1",
                "DataRepositoryConfiguration": {
                    "AutoImportPolicy": "NEW_CHANGED_DELETED",
                    "Lifecycle": "UPDATING",
                    "ImportPath": "s3://lustre-export-test-bucket/",
                    "ExportPath": "s3://lustre-export-test-bucket/export",
                    "ImportedFileChunkSize": 1024
```

```
                },
                "PerUnitStorageThroughput": 50
            }
        }
    ]
}
```

Visualização do caminho de exportação de um sistema de arquivos

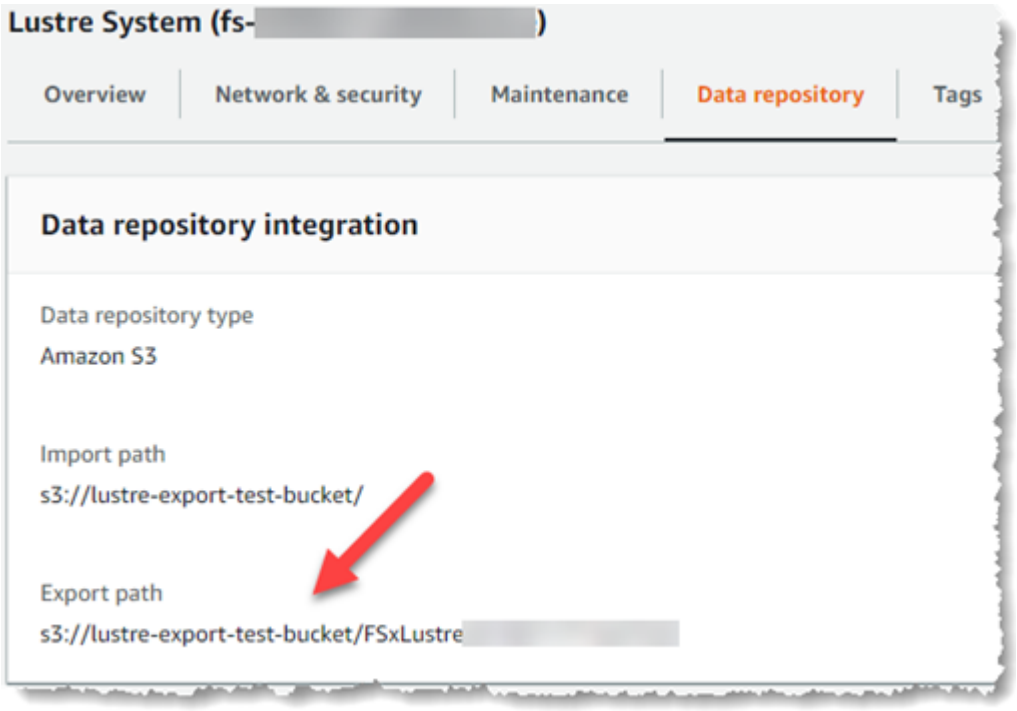
É possível visualizar o caminho de exportação de um sistema de arquivos usando o console do FSx para Lustre, a AWS CLI e a API.

Console

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha Nome do sistema de arquivos ou ID do sistema de arquivos para o sistema de arquivos do FSx para Lustre cujo caminho de exportação você deseja visualizar.

   A página de detalhes do sistema de arquivos é exibida para esse sistema de arquivos.
3. Escolha a guia Repositório de dados.

   O painel Integração do repositório de dados será exibido, mostrando os caminhos de importação e de exportação.



CLI

Para determinar o caminho de exportação para o sistema de arquivos, use o comando `describe-file-systems` da AWS CLI.

```
aws fsx describe-file-systems
```

Procure a propriedade `ExportPath` em `LustreConfiguration` na resposta.

```
{
    "OwnerId": "111122223333",
    "CreationTime": 1563382847.014,
    "FileSystemId": "",
    "FileSystemType": "LUSTRE",
    "Lifecycle": "AVAILABLE",
    "StorageCapacity": 2400,
    "VpcId": "vpc-6296a00a",
    "SubnetIds": [
        "subnet-1111111"
    ],
    "NetworkInterfaceIds": [
        "eni-0c288d5b8cc06c82d",
        "eni-0f38b702442c6918c"
    ],
```

```
    "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
    "ResourceARN": "arn:aws:fsx:us-east-2:267731178466:file-system/
fs-0123456789abcdef0",
    "Tags": [
        {
          "Key": "Name",
          "Value": "Lustre System"
        }
    ],
 "LustreConfiguration": {
    "DeploymentType": "SCRATCH_1",
    "DataRepositoryConfiguration": {
    "AutoImportPolicy": " NEW_CHANGED_DELETED",
    "Lifecycle": "AVAILABLE",
    "ImportPath": "s3://lustre-export-test-bucket/",
    "ExportPath": "s3://lustre-export-test-bucket/FSxLustre20190717T164753Z",
    "ImportedFileChunkSize": 1024
    }
  },
  "PerUnitStorageThroughput": 50,
  "WeeklyMaintenanceStartTime": "6:09:30"
}
```

Estado do ciclo de vida do repositório de dados

O estado do ciclo de vida do repositório de dados fornece informações de status sobre o repositório de dados vinculado do sistema de arquivos. Um repositório de dados pode ter os estados de ciclo de vida apresentados a seguir.

- Criando: o Amazon FSx está criando a configuração do repositório de dados entre o sistema de arquivos e o repositório de dados vinculado. O repositório de dados está indisponível.
- Disponível: o repositório de dados está disponível para uso.
- Atualizando: a configuração do repositório de dados está passando por uma atualização iniciada pelo cliente que pode afetar sua disponibilidade.
- Configuração incorreta: o Amazon FSx não pode importar automaticamente as atualizações do bucket do S3 até que a configuração do repositório de dados seja corrigida. Para obter mais informações, consulte Solução de problemas de um bucket do S3 vinculado configurado incorretamente.

É possível visualizar o estado do ciclo de vida do repositório de dados vinculado de um sistema de arquivos usando o console do Amazon FSx, a AWS Command Line Interface e a API do Amazon FSx. No console do Amazon FSx, você pode acessar o Estado do ciclo de vida do repositório de dados no painel Integração do repositório de dados da guia Repositório de dados do sistema de arquivos. A propriedade `Lifecycle` está localizada no objeto `DataRepositoryConfiguration` na resposta de um comando `describe-file-systems` da CLI (a ação de API equivalente é `DescribeFileSystems`).

Importação automática de atualizações do bucket do S3

Por padrão, quando você cria um novo sistema de arquivos, o Amazon FSx importa os metadados do arquivo (por exemplo, o nome, a propriedade, o carimbo de data/hora e as permissões) de objetos no bucket do S3 vinculado durante a criação do sistema de arquivos. É possível configurar o sistema de arquivos do FSx para Lustre para importar automaticamente metadados de objetos que são adicionados, alterados ou excluídos do bucket do S3 após a criação do sistema de arquivos. O FSx para Lustre atualiza a listagem de arquivos e de diretórios de um objeto alterado após a criação, da mesma maneira que importa os metadados dos arquivos durante a criação do sistema de arquivos. Quando o Amazon FSx atualiza a listagem de arquivos e de diretórios de um objeto alterado, se o objeto alterado no bucket do S3 não contiver mais os metadados, o Amazon FSx manterá os valores atuais de metadados do arquivo, em vez de usar as permissões padrão.

> **Note**
>
> As configurações de importação estão disponíveis em sistemas de arquivos do FSx para Lustre criados após às 17h BRT de 23 de julho de 2020.

Você pode definir preferências de importação ao criar um novo sistema de arquivos, e pode atualizar a configuração em sistemas de arquivos existentes usando o console de gerenciamento do FSx, a AWS CLI e a API da AWS. Quando você cria o sistema de arquivos, seus objetos existentes no S3 aparecem como listagens de arquivos e diretórios. Após criar o sistema de arquivos, como você deseja atualizá-lo à medida que o conteúdo do bucket do S3 é atualizado? Um sistema de arquivos pode ter uma das seguintes preferências de importação:

> **Note**
>
> O sistema de arquivos do FSx para Lustre e o bucket do S3 vinculado devem estar localizados na mesma região da AWS para importar atualizações automaticamente.

- Atualizar minha listagem de arquivos e de diretórios à medida que os objetos são adicionados ao meu bucket do S3: (padrão) o Amazon FSx atualiza automaticamente as listagens de arquivos e de diretórios para quaisquer novos objetos adicionados ao bucket do S3 vinculado, os quais não existam no sistema de arquivos do FSx. O Amazon FSx não atualiza listagens para objetos que foram alterados no bucket do S3. O Amazon FSx não exclui listagens de objetos que são excluídos no bucket do S3.

  > **Note**
  >
  > A configuração padrão de preferências de importação para importar dados de um bucket do S3 vinculado usando a CLI e a API é `NONE`. A configuração padrão de preferências de importação ao usar o console é atualizar o Lustre à medida que novos objetos são adicionados ao bucket do S3.

- Atualizar minha listagem de arquivos e de diretórios à medida que os objetos são adicionados ou alterados em meu bucket do S3: o Amazon FSx atualiza automaticamente as listagens de arquivos e de diretórios para quaisquer novos objetos adicionados ao bucket do S3 e para quaisquer objetos existentes que são alterados no bucket do S3 depois que você escolher essa opção. O Amazon FSx não exclui listagens de objetos que são excluídos no bucket do S3.
- Atualizar minha listagem de arquivos e de diretórios à medida que os objetos são adicionados, alterados ou excluídos do meu bucket do S3: o Amazon FSx atualiza automaticamente as listagens de arquivos e de diretórios para quaisquer novos objetos adicionados ao bucket do S3, para quaisquer objetos existentes que são alterados no bucket do S3 e para quaisquer objetos existentes que são excluídos do bucket do S3 depois que você escolher essa opção.
- Não atualizar meu arquivo e listar diretamente quando objetos são adicionados, alterados ou excluídos do meu bucket do S3: o Amazon FSx atualiza somente as listagens de arquivos e de diretórios do bucket do S3 vinculado quando o sistema de arquivos é criado. O FSx não atualiza as listagens de arquivos e de diretórios para objetos novos, alterados ou excluídos após a escolha dessa opção.

Quando você define as preferências de importação para atualizar as listagens de arquivos e de diretórios do sistema de arquivos com base nas alterações no bucket do S3 vinculado, o Amazon FSx cria uma configuração de notificação de eventos no bucket do S3 vinculado que é chamada `FSx`. Não modifique ou exclua a configuração de notificação de eventos `FSx` no bucket do S3. Isso evita a importação automática de listagens de arquivos e de diretórios novos ou alterados para seu sistema de arquivos.

Quando o Amazon FSx atualiza uma listagem de arquivos que foi alterada no bucket do S3 vinculado, ele substitui o arquivo local pela versão atualizada, mesmo que o arquivo esteja bloqueado para gravação. De forma semelhante, quando o Amazon FSx atualiza uma listagem de arquivos no caso de o objeto correspondente ter sido excluído no bucket do S3 vinculado, ele exclui o arquivo local, mesmo que o arquivo esteja bloqueado para gravação.

O Amazon FSx se esforça ao máximo para atualizar o sistema de arquivos. O Amazon FSx não pode atualizar o sistema de arquivos com alterações nas seguintes situações:

- Quando o Amazon FSx não tem permissão para abrir o objeto do S3 novo ou alterado.
- Quando a configuração de notificação de eventos `FSx` no bucket do S3 vinculado é excluída ou alterada.

Qualquer uma dessas condições faz com que o estado do ciclo de vida do repositório de dados se torne o estado de Configuração incorreta. Para obter mais informações, consulte Estado do ciclo de vida do repositório de dados.

Pré-requisitos

As seguintes condições são obrigatórias para que o Amazon FSx importe automaticamente arquivos novos, alterados ou excluídos do bucket do S3 vinculado:

- O sistema de arquivos e o bucket do S3 vinculado devem estar localizados na mesma região da AWS.
- O bucket do S3 não tem um estado de ciclo de vida de Configuração incorreta. Para obter mais informações, consulte Estado do ciclo de vida do repositório de dados.
- Sua conta deve ter as permissões obrigatórias para configurar e receber notificações de eventos no bucket do S3 vinculado.

Tipos de alterações de arquivo com suporte

O Amazon FSx oferece suporte à importação das seguintes alterações em arquivos e em pastas que ocorrem no bucket do S3 vinculado:

- Alterações no conteúdo do arquivo
- Alterações nos metadados de arquivos ou de pastas
- Alterações no destino do link simbólico ou nos metadados

Atualização das preferências de importação

É possível definir as preferências de importação de um sistema de arquivos ao criar um novo sistema de arquivos. Para obter mais informações, consulte Como vincular o sistema de arquivos a um bucket do S3.

Você também pode atualizar as preferências de importação de um sistema de arquivos após a criação usando o Console de Gerenciamento da AWS, a AWS CLI e a API do Amazon FSx, conforme mostrado no procedimento a seguir.

Console

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel, escolha Sistemas de arquivos.
3. Selecione o sistema de arquivos que deseja gerenciar para exibir os detalhes do sistema de arquivos.
4. Escolha Repositório de dados para visualizar as configurações do repositório de dados. É possível modificar as preferências de importação se o estado do ciclo de vida for DISPONÍVEL ou CONFIGURAÇÃO INCORRETA. Para obter mais informações, consulte Estado do ciclo de vida do repositório de dados.
5. Selecione Ações e, em seguida, escolha Atualizar preferências de importação para exibir a caixa de diálogo Atualizar preferências de importação.
6. Selecione a nova configuração e, em seguida, escolha Atualizar para fazer a alteração.

CLI

Para atualizar as preferências de importação, use o comando `update-file-system` da CLI. A operação de API correspondente é `UpdateFileSystem`.

Após atualizar o sistema de arquivos `AutoImportPolicy` com êxito, o Amazon FSx retorna a descrição do sistema de arquivos atualizado como JSON, conforme mostrado aqui:


```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "Lifecycle": "UPDATING",
            "StorageCapacity": 2400,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "SCRATCH_1",
                "DataRepositoryConfiguration": {
                    "AutoImportPolicy": "NEW_CHANGED_DELETED",
                    "Lifecycle": "UPDATING",
                    "ImportPath": "s3://lustre-export-test-bucket/",
                    "ExportPath": "s3://lustre-export-test-bucket/export",
                    "ImportedFileChunkSize": 1024
                }
                "PerUnitStorageThroughput": 50,
```

```
                "WeeklyMaintenanceStartTime": "2:04:30"
            }
        }
    ]
}
```

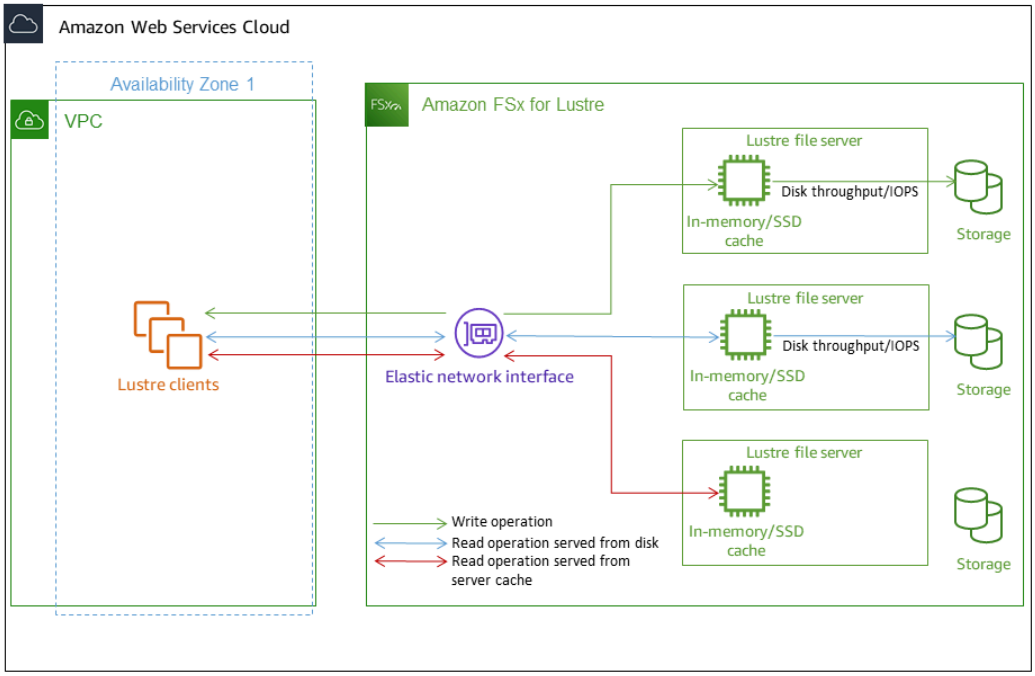
Performance do Amazon FSx para Lustre

O Amazon FSx para Lustre, desenvolvido no Lustre, o popular sistema de arquivos de alta performance, oferece uma performance para aumentar a escala horizontalmente que amplia linearmente com o tamanho do sistema de arquivos. Os sistemas de arquivos do Lustre são escalados horizontalmente em diversos servidores de arquivos e discos. Essa escalabilidade disponibiliza a todos os clientes o acesso direto aos dados armazenados em cada disco para remover muitos dos gargalos presentes nos sistemas de arquivos tradicionais. O Amazon FSx para Lustre se baseia na arquitetura escalável do Lustre para oferecer suporte a altos níveis de performance para um grande número de clientes.

Tópicos

Como funcionam os sistemas de arquivos do FSx para Lustre

Cada sistema de arquivos do FSx para Lustre consiste nos servidores de arquivos com os quais os clientes se comunicam e em um conjunto de discos anexados a cada servidor de arquivos que armazena seus dados. Cada servidor de arquivos emprega um cache na memória rápido para aprimorar a performance dos dados acessados com mais frequência. Além disso, os sistemas de arquivos baseados em HDD podem ser provisionados com um cache de leitura baseado em SSD para aprimorar ainda mais a performance dos dados acessados com mais frequência. Quando um cliente acessa dados que estão armazenados na memória ou no cache baseado em SSD, o servidor de arquivos não precisa lê-los usando o disco, o que reduz a latência e aumenta a quantidade total de throughput que você pode gerar. O diagrama a seguir ilustra os caminhos de uma operação de gravação, uma operação de leitura atendida usando o disco e uma operação de leitura atendida usando a memória ou o cache baseado em SSD.



Quando você realiza a leitura de dados armazenados na memória ou no cache baseado em SSD do servidor de arquivos, a performance do sistema de arquivos é determinada pelo throughput da rede. Quando você grava dados no sistema de arquivos ou quando realiza a leitura de dados que não estão armazenados no cache na memória, a performance do sistema de arquivos é determinada pelo menor throughput da rede e do disco.

Ao provisionar um sistema de arquivos do Lustre baseado em HDD com um cache baseado em SSD, o Amazon FSx cria um cache baseado em SSD que é automaticamente dimensionado para 20% da capacidade de armazenamento em HDD do sistema de arquivos. Fazer isso fornece latências inferiores a um milissegundo e IOPS mais altas para arquivos acessados com frequência.

Performance agregada do sistema de arquivos

O throughput que um sistema de arquivos do FSx para Lustre oferece suporte é proporcional a sua capacidade de armazenamento. Os sistemas de arquivos do Amazon FSx para Lustre são escalados para centenas de Gigabits por segundo (GBps) de throughput e milhões de IOPS. O Amazon FSx para Lustre também oferece suporte ao acesso simultâneo ao mesmo arquivo ou ao diretório de milhares de instâncias de computação. Esse acesso possibilita a rápida verificação de dados da memória até o armazenamento da aplicação, que é uma técnica comum em computação de alta

performance (HPC). Você podel aumentar a quantidade de armazenamento e a capacidade de throughput, conforme necessário, a qualquer momento após a criação do sistema de arquivos. Para ter mais informações, consulte Como gerenciar a capacidade de armazenamento.

Os sistemas de arquivos do FSx para Lustre fornecem um throughput de leitura intermitente usando um mecanismo de crédito de E/S de rede para alocar a largura de banda da rede com base na utilização média da largura de banda. Os sistemas de arquivos acumulam créditos quando o uso da largura de banda da rede está abaixo dos limites da linha de base e esses créditos podem ser usados na execução de transferências de dados pela rede.

As tabelas apresentadas a seguir mostram a performance para a qual as opções de implantação do FSx para Lustre foram projetadas.

Performance do sistema de arquivos para opções de armazenamento em SSD

Tipo de implantação	Throughput da rede (MB/s/TiB de armazenamento provisionado)		IOPS da rede (IOPS/TiB de armazenamento provisionado)	Armazenamento em cache (GiB de RAM/TiB de armazenamento provisionado)	Latências do disco por operação de arquivo (milissegundos, P50)	Throughput do disco (MBps/TiB de armazenamento ou de cache baseado em SSD provisionado)	
	Linha de base	Intermitência				Linha de base	Intermitência
SCRATCH_2	200	1300	Linha de base de dezenas de milhares	6.7	Metadados: inferiores a um milissegundo Dados: inferiores a um milissegundo	200 (leitura) 100 (gravação)	-
PERSISTENT-125	320	1300	Intermitência de centenas de milhares	3.4		125	500
PERSISTENT-250	640	1300		6.8		250	500
PERSISTENT-500	1300	-		13.7		500	-
PERSISTENT-1000	2600	-		27.3		1000	-

Performance do sistema de arquivos para opções de armazenamento em HDD

Tipo de implantação	Throughput da rede (MB/s/TiB de armazenamento ou de cache baseado em SSD provisionado)		IOPS da rede (IOPS/TiB de armazenamento provisionado)	Armazenamento em cache (GiB de RAM/TiB de armazenamento provisionado)	Latências do disco por operação de arquivo (milissegundos, P50)	Throughput do disco (MBps/TiB de armazenamento ou de cache baseado em SSD provisionado)	
	Linha de base	Intermitência				Linha de base	Intermitência
PERSISTENT-12							
Armazenamento em HDD	40	375*	Linha de base de dezenas de milhares Intermitência de centenas de milhares	0.4 memory	Metadados: inferiores a um milissegundo Dados: milissegundo de um dígito	12	80 (leitura) 50 (gravação)
Armazenamento em cache de leitura baseado em SSD	200	1,900		Armazenamento em cache baseado em SSD de 200	Dados: inferiores a um milissegundo	200	-

Performance do sistema de arquivos para opções de armazenamento em SSD da geração anterior

Tipo de implantação	Throughput da rede (MB/s por TiB de armazenamento provisionado)		IOPS da rede (IOPS por TiB de armazenamento provisionado)	Armazenamento em cache (GiB por TiB de armazenamento provisionado)	Latências do disco por operação de arquivo (milissegundos, P50)	Throughput do disco (MBs por TiB de armazenamento ou de cache baseado em SSD provisionado)	
	Linha de base	Intermitência				Linha de base	Intermitência
PERSISTENT-50	250	1,300*	Linha de base de dezenas de milhares	2.2 RAM	Metadados: inferiores a um milissegundo	50	240
PERSISTENT-100	500	1,300*		4.4 RAM		100	240
PERSISTENT-200	750	1,300*	Intermitência de centenas de milhares	8.8 RAM	Dados: inferiores a um milissegundo	200	240

> **Note**
>
> *Os sistemas de arquivos persistentes nas seguintes Regiões da AWS fornecem intermitência de rede de até 530 MB/s por TiB de armazenamento: África (Cidade do Cabo), Ásia-Pacífico (Hong Kong), Asia Pacific (Osaka), Ásia-Pacífico (Singapura), Canadá (Central), Europa (Frankfurt), Europa (Londres), Europa (Milão), Europa (Estocolmo), Oriente Médio (Bahrein), América do Sul (São Paulo), China e Oeste dos EUA (Los Angeles).

> **Note**
>
> A opção de implantação SCRATCH_1 do FSx para Lustre foi projetada para oferecer suporte a 200 MB/s/TiB.

Exemplo: linha de base agregada e throughput de intermitência

O exemplo apresentado a seguir ilustra como a capacidade de armazenamento e o throughput do disco afetam a performance do sistema de arquivos.

Um sistema de arquivos persistente com capacidade de armazenamento de 4,8 TiB e 50 MB/s por TiB de throughput por unidade de armazenamento fornece um throughput do disco de linha de base agregada de 240 MB/s e um throughput do disco de intermitência de 1,152 GB/s.

Independentemente do tamanho do sistema de arquivos, o Amazon FSx para Lustre disponibiliza latências consistentes inferiores a um milissegundo para operações de arquivos.

Layout de armazenamento do sistema de arquivos

Todos os dados de arquivos no Lustre são armazenados em volumes de armazenamento chamados destinos de armazenamento de objetos (OSTs). Todos os metadados de arquivos, incluindo nomes de arquivos, carimbos de data/hora, permissões e muito mais, são armazenados em volumes de armazenamento chamados destinos de metadados (MDTs). Os sistemas de arquivos do Amazon FSx para Lustre são compostos por um único MDT e vários OSTs. Cada OST tem, aproximadamente, 1 a 2 TiB de tamanho, dependendo do tipo de implantação do sistema de arquivos. O Amazon FSx para Lustre distribui os dados de arquivos pelos OSTs que compõem o sistema de arquivos para equilibrar a capacidade de armazenamento com o throughput e a carga de IOPS.

Para visualizar o uso de armazenamento do MDT e dos OSTs que compõem o sistema de arquivos, execute o comando apresentado a seguir em um cliente que tenha o sistema de arquivos montado.

```
lfs df -h mount/path
```

A saída deste comando é semelhante à apresentada a seguir.

Example

```
UUID                       bytes        Used   Available Use% Mounted on
mountname-MDT0000_UUID      68.7G        5.4M       68.7G   0% /fsx[MDT:0]
mountname-OST0000_UUID       1.1T        4.5M        1.1T   0% /fsx[OST:0]
mountname-OST0001_UUID       1.1T        4.5M        1.1T   0% /fsx[OST:1]

filesystem_summary:          2.2T        9.0M        2.2T   0% /fsx
```

Distribuição de dados no sistema de arquivos

É possível otimizar a performance de throughput do seu sistema de arquivos com a distribuição de arquivos. O Amazon FSx para Lustre distribui automaticamente os arquivos entre os OSTs para garantir que os dados sejam fornecidos por todos os servidores de armazenamento. Você pode aplicar um conceito semelhante no nível do arquivo ao configurar como os arquivos são distribuídos em diversos OSTs.

O termo “distribuição” indica que os arquivos podem ser divididos em diversos fragmentos que são armazenados em diferentes OSTs. Quando um arquivo é distribuído em diversos OSTs, as solicitações de leitura ou de gravação para o arquivo são distribuídas por esses OSTs, aumentando o throughput agregado ou a IOPS que as aplicações podem gerar por meio dele.

A seguir, são apresentados os layouts padrão para sistemas de arquivos do Amazon FSx para Lustre.

- Para sistemas de arquivos criados antes de 18 de dezembro de 2020, o layout padrão especifica uma contagem de distribuição de um. Isso significa que, a menos que um layout diferente seja especificado, cada arquivo criado no Amazon FSx para Lustre usando ferramentas padrão do Linux será armazenado em um único disco.
- Para sistemas de arquivos criados após 18 de dezembro de 2020, o layout padrão corresponde a um layout de arquivos progressivo, no qual arquivos com tamanhos inferiores a 1 GiB são

armazenados em uma distribuição e arquivos com tamanhos superiores são atribuídos a uma contagem de distribuição de cinco.

- Para sistemas de arquivos criados após 25 de agosto de 2023, o layout padrão corresponde a um layout de arquivos progressivo de quatro componentes, o qual é explicado em Layouts de arquivos progressivos.
- Para todos os sistemas de arquivos, independentemente da data de criação, os arquivos importados do Amazon S3 não usam o layout padrão. Eles usam o layout presente no parâmetro `ImportedFileChunkSize` do sistema de arquivos. Os arquivos importados do S3 com tamanhos superiores a `ImportedFileChunkSize` serão armazenados em diversos OSTs com uma contagem de distribuição de `(FileSize / ImportedFileChunksize) + 1`. O valor padrão de `ImportedFileChunkSize` é 1 GiB.

É possível visualizar a configuração de layout de um arquivo ou de um diretório usando o comando `lfs getstripe`.

```
lfs getstripe path/to/filename
```

Este comando informa a contagem de distribuição, o tamanho da distribuição e o deslocamento da distribuição de um arquivo. A contagem de distribuição corresponde ao número de OSTs para os quais o arquivo é distribuído. O tamanho da distribuição corresponde à quantidade de dados contínuos que são armazenados em um OST. O deslocamento da distribuição corresponde ao índice do primeiro OST para o qual o arquivo é distribuído.

Modificação da configuração de distribuição

Os parâmetros de layout de um arquivo são definidos quando o arquivo é criado pela primeira vez. Use o comando `lfs setstripe` para criar um arquivo novo e em branco com um layout especificado.

```
lfs setstripe filename --stripe-count number_of_OSTs
```

O comando `lfs setstripe` afeta somente o layout de um novo arquivo. Use-o para especificar o layout de um arquivo antes de criá-lo. Você também pode definir um layout para um diretório. Após ser definido em um diretório, esse layout é aplicado a cada novo arquivo adicionado ao diretório, mas não aos arquivos existentes. Qualquer novo subdiretório criado também herdará o novo layout, que será aplicado a qualquer novo arquivo ou diretório criado nesse subdiretório.

Para modificar o layout de um arquivo existente, use o comando `lfs migrate`. Este comando copia o arquivo, conforme necessário, para distribuir o conteúdo de acordo com o layout especificado no comando. Por exemplo, arquivos anexados ou aumentados em tamanho não alteram a contagem de distribuição, portanto, é necessário migrá-los para alterar o layout do arquivo. Como alternativa, é possível criar um novo arquivo usando o comando `lfs setstripe` para especificar o layout, copiar o conteúdo original para o novo arquivo e, em seguida, renomear o novo arquivo para substituir o arquivo original.

Pode haver casos em que a configuração de layout padrão não seja ideal para a workload. Por exemplo, um sistema de arquivos com dezenas de OSTs e um grande número de arquivos de vários gigabytes pode obter uma performance superior ao realizar a distribuição dos arquivos para mais do que o valor de contagem de distribuição padrão de cinco OSTs. A criação de arquivos grandes com contagens de distribuições baixas pode causar gargalos na performance de E/S e também fazer com que os OSTs fiquem cheios. Nesse caso, você pode criar um diretório com uma contagem de distribuição maior para esses arquivos.

Configurar um layout distribuído para arquivos grandes (especialmente arquivos maiores que um gigabyte) é importante pelos seguintes motivos:

- Aprimora o throughput ao permitir que vários OSTs e seus servidores associados contribuam com IOPS, largura de banda da rede e recursos de CPU ao ler e gravar arquivos grandes.
- Reduz a probabilidade de que um pequeno subconjunto de OSTs se torne um ponto de acesso que limita a performance geral da workload.
- Impede que um único arquivo grande preencha um OST, possivelmente causando erros de disco cheio.

Não existe uma configuração única de layout que seja ideal para todos os casos de uso. Para obter orientação detalhada sobre os layouts de arquivos, consulte Managing File Layout (Striping) and Free Space na documentação do Lustre.org. A seguir, apresentamos as diretrizes gerais:

- O layout distribuído é mais importante para arquivos grandes, especialmente para casos de uso em que os arquivos têm regularmente centenas de megabytes ou mais. Por esse motivo, o layout padrão para um novo sistema de arquivos atribui uma contagem de distribuição de cinco para arquivos com tamanho superior a 1 GiB.
- A contagem de distribuição é o parâmetro de layout que você deve ajustar para sistemas que oferecem suporte a arquivos grandes. A contagem de distribuição especifica o número de volumes de OST que conterão fragmentos de um arquivo distribuído. Por exemplo, com uma contagem de

distribuição de dois e um tamanho da distribuição de 1 MiB, o Lustre grava fragmentos alternativos de 1 MiB de um arquivo em cada um dos dois OSTs.

- A contagem de distribuição efetiva corresponde ao menor número entre o número real de volumes de OST e o valor de contagem de distribuição especificado. É possível usar o valor especial de contagem de distribuição de `-1` para indicar que as distribuições devem ser colocadas em todos os volumes de OST.
- A definição de uma contagem de distribuição grande para arquivos pequenos não é ideal porque, para determinadas operações, o Lustre requer idas e vindas da rede para cada OST no layout, mesmo que o arquivo seja muito pequeno para consumir espaço em todos os volumes de OST.
- Você pode configurar um layout de arquivo progressivo (PFL) que permite que o layout de um arquivo seja alterado com o tamanho. Uma configuração de PFL pode simplificar o gerenciamento de um sistema de arquivos que tem uma combinação de arquivos grandes e pequenos sem que você tenha necessidade de definir explicitamente uma configuração para cada arquivo. Para ter mais informações, consulte Layouts de arquivos progressivos.
- Por padrão, o tamanho da distribuição é 1 MiB. A definição de um deslocamento de distribuição pode ser útil em circunstâncias especiais, mas, em geral, é melhor deixá-lo sem especificação e usar o padrão.

Layouts de arquivos progressivos

É possível especificar uma configuração de layout de arquivo progressivo (PFL) para um diretório com a finalidade de especificar diferentes configurações de distribuição para arquivos pequenos e grandes antes de preenchê-lo. Por exemplo, você pode definir um PFL no diretório de nível superior antes que os dados sejam gravados em um novo sistema de arquivos.

Para especificar uma configuração de PFL, use o comando `lfs setstripe` com opções `-E` para especificar componentes de layout para arquivos de tamanhos diferentes, como o seguinte comando:

```
lfs setstripe -E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32 /mountname/directory
```

Este comando define quatro componentes de layout:

- O primeiro componente (`-E 100M -c 1`) indica um valor de contagem de distribuição de 1 para arquivos de até 100 MiB de tamanho.

- O segundo componente (`-E 10G -c 8`) indica uma contagem de distribuição de 8 para arquivos de até 10 GiB de tamanho.
- O terceiro componente (`-E 100G -c 16`) indica uma contagem de distribuição de 16 para arquivos de até 100 GiB de tamanho.
- O quarto componente (`-E -1 -c 32`) indica uma contagem de distribuição de 32 para arquivos com tamanho superior a 100 GiB.

> **Important**
>
> Anexar dados a um arquivo criado com um layout PFL preencherá todos os componentes do layout. Por exemplo, com o comando de quatro componentes mostrado acima, se você criar um arquivo de 1 MiB e, em seguida, adicionar dados ao final dele, o layout do arquivo será ampliado para ter uma contagem de faixas de -1, ou seja, abrangendo todos os OSTs no sistema. Isso não significa que os dados serão gravados em cada OST, mas uma operação, por exemplo, a leitura do tamanho do arquivo, enviará uma solicitação paralelamente a cada OST, adicionando uma carga de rede significativa ao sistema de arquivos.
> Portanto, tome cuidado em relação a limitar a contagem de distribuição para qualquer arquivo pequeno ou médio que possa, posteriormente, ter dados anexados a ele. Como os arquivos de log geralmente são desenvolvidos com a adição de novos registros, o Amazon FSx para Lustre atribui uma contagem de distribuição padrão de um a qualquer arquivo criado no modo de acréscimo, independentemente da configuração de distribuição padrão especificada pelo diretório primário.

A configuração de PFL padrão nos sistemas de arquivos do Amazon FSx para Lustre criados após 25 de agosto de 2023 é definida com este comando:

```
lfs setstripe -E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32 /mountname
```

Os clientes com workloads que têm acesso com alta simultaneidade a arquivos médios e grandes, provavelmente, serão beneficiados com um layout com mais distribuições em tamanhos menores e distribuição em todos os OSTs para os arquivos maiores, conforme mostrado no exemplo de layout de quatro componentes.

Monitoramento da performance e do uso

A cada minuto, o Amazon FSx for Lustre emite métricas de uso de cada disco (MDT e OST) para a Amazon. CloudWatch

Para visualizar detalhes agregados de uso do sistema de arquivos, é possível consultar a estatística Sum de cada métrica. Por exemplo, a estatística Sum de `DataReadBytes` relata o throughput total de leitura visto por todos os OSTs em um sistema de arquivos. De forma semelhante, a estatística Sum de `FreeDataStorageCapacity` relata a capacidade total de armazenamento disponível para dados de arquivos no sistema de arquivos.

Para obter mais informações sobre como monitorar a performance do sistema de arquivos, consulte Como monitorar o Amazon FSx for Lustre.

Dicas de performance

Ao usar o Amazon FSx para Lustre, lembre-se das dicas de performance apresentadas a seguir. Para saber sobre limites de serviço, consulte Cotas.

- Tamanho médio de E/S: como o Amazon FSx para Lustre é um sistema de arquivos de rede, cada operação de arquivo passa por idas e vindas entre o cliente e o Amazon FSx para Lustre, incorrendo em uma pequena sobrecarga de latência. Por causa dessa latência por operação, o throughput geral normalmente aumenta à medida que o tamanho de E/S cresce, porque a sobrecarga é amortizada em uma quantidade de dados maior.
- Modelo de solicitação: ao habilitar as gravações assíncronas em seu sistema de arquivos, as operações de gravação pendentes serão armazenadas em buffer na instância do Amazon EC2 antes de serem gravadas no Amazon FSx para Lustre de forma assíncrona. Normalmente, gravações assíncronas têm latências mais baixas. Ao executar gravações assíncronas, o kernel usa memória adicional para armazenamento em cache. Um sistema de arquivos que habilitou gravações síncronas emite solicitações síncronas para o Amazon FSx para Lustre. Cada operação passa por idas e vindas entre o cliente e o Amazon FSx para Lustre.

> **Note**
>
> O modelo de solicitação escolhido tem compensações em termos de consistência (se você estiver usando várias instâncias do Amazon EC2) e velocidade.

- Instâncias do Amazon EC2: as aplicações que executam um grande número de operações de leitura e de gravação provavelmente precisam de mais memória ou capacidade de computação do que as aplicações que não o fazem. Ao iniciar as instâncias do Amazon EC2 para a workload com uso intensivo de computação, escolha tipos de instâncias com a quantidade desses recursos que é requerida para sua aplicação. As características de performance dos sistemas de arquivos do Amazon FSx para Lustre não dependem do uso de instâncias otimizadas para o Amazon EBS.
- Ajuste recomendado da instância do cliente para um desempenho ideal

  1. Para todos os tipos e tamanhos de instâncias do cliente, recomendamos aplicar o seguinte ajuste:

     ```
     sudo lctl set_param osc.*.max_dirty_mb=64
     ```

  2. Para tipos de instâncias de clientes com memória superior a 64 GiB, recomendamos aplicar o seguinte ajuste:

     ```
     lctl set_param ldlm.namespaces.*.lru_max_age=600000
     ```

  3. Para tipos de instâncias de clientes com mais de 64 núcleos de vCPU, recomendamos aplicar o seguinte ajuste:

     ```
     echo "options ptlrpc ptlrpcd_per_cpt_max=32" >> /etc/modprobe.d/modprobe.conf
     echo "options ksocklnd credits=2560" >> /etc/modprobe.d/modprobe.conf

     # reload all kernel modules to apply the above two settings
     sudo reboot
     ```

     Após a montagem do cliente, o seguinte ajuste precisa ser aplicado:

     ```
     sudo lctl set_param osc.*OST*.max_rpcs_in_flight=32
     sudo lctl set_param mdc.*.max_rpcs_in_flight=64
     sudo lctl set_param mdc.*.max_mod_rpcs_in_flight=50
     ```

  Observe que `lctl set_param` é conhecido por não persistir durante a reinicialização. Como esses parâmetros não podem ser definidos de forma permanente do lado do cliente, é recomendável implementar tarefas do Cron de inicialização para definir a configuração com os ajustes recomendados.

- Equilíbrio da workload entre OSTs: em alguns casos, a workload não está gerando o throughput agregado que o sistema de arquivos pode fornecer (200 MB/s por TiB de armazenamento). Nesse

caso, você pode usar CloudWatch métricas para solucionar problemas se o desempenho for afetado por um desequilíbrio nos padrões de E/S da sua carga de trabalho. Para identificar se essa é a causa, veja a CloudWatch métrica máxima do Amazon FSx for Lustre.

Em alguns casos, essa estatística mostra uma carga igual ou superior a 240 MBps de throughput (a capacidade de throughput de um único disco do Amazon FSx para Lustre de 1,2 TiB). Nesses casos, a workload não está distribuída uniformemente pelos discos. Se for esse o caso, você poderá usar o comando `lfs setstripe` para modificar a distribuição dos arquivos que a workload acessa com mais frequência. Para obter uma performance ideal, distribua arquivos com requisitos de alto throughput em todos os OSTs que compõem o sistema de arquivos.

Se os arquivos forem importados de um repositório de dados, você poderá adotar outra abordagem para distribuir uniformemente os arquivos de alto throughput em seus OSTs. Para fazer isso, é possível modificar o parâmetro `ImportedFileChunkSize` ao criar seu próximo sistema de arquivos do Amazon FSx para Lustre.

Por exemplo, suponha que a workload use um sistema de arquivos de 7,0 TiB (que é composto por seis OSTs de 1,17 TiB) e precise gerar alto throughput em arquivos de 2,4 GiB. Nesse caso, você pode definir o valor `ImportedFileChunkSize` como `(2.4 GiB / 6 OSTs) = 400 MiB` para que os arquivos sejam distribuídos uniformemente pelos OSTs do sistema de arquivos.

Acesso a sistemas de arquivos

Usando o Amazon FSx, você pode transferir suas cargas de trabalho de computação intensiva do local para a Amazon Web Services Cloud importando dados via VPN. AWS Direct Connect Você pode acessar o sistema de arquivos do Amazon FSx on-premises, copiar dados para seu sistema de arquivos, conforme necessário, e executar workloads com uso intensivo de computação em instâncias na nuvem.

Na seção a seguir, você aprenderá como acessar o sistema de arquivos do Amazon FSx para Lustre em uma instância do Linux. Além disso, poderá descobrir como usar o arquivo `fstab` para remontar o sistema de arquivos automaticamente após a reinicialização de qualquer sistema.

Antes de poder montar um sistema de arquivos, você deve criar, configurar e iniciar os recursos da AWS relacionados. Para obter instruções detalhadas, consulte Conceitos básicos do Amazon FSx para Lustre. Em seguida, você pode instalar e configurar o cliente Lustre em sua instância de computação.

Tópicos

Compatibilidade do sistema de arquivos Lustre e do kernel do cliente

É altamente recomendável usar a versão Lustre para seu sistema de arquivos FSx for Lustre que seja compatível com as versões do kernel Linux de suas instâncias cliente.

Clientes Amazon Linux

Sistema operacional	Versão do SO	Versão mínima para o kernel	Versão máxima para o kernel	Versão do sistema de arquivos		
				2,10	2,12	2,15
Amazon Linux 2023	6.1	6.1.79-99.167	6.1.79-99.167+	não	sim	sim
Amazon Linux 2	5.10	5.10.144-127.601	5.10.144-127.601+	sim	sim	sim
			<5.10.144-127.601	sim	sim	não
	5.4	5.4.214-120.368	5.4.214-120.368+	sim	sim	sim
			<5.4.214-120.368	sim	sim	não
	4.14	4.14.294-220,533	4.14.294-220,533+	sim	sim	sim
			<4.14.294-220.533	sim	sim	não

Clientes Ubuntu

Sistema operacional	Versão do SO	Versão mínima para o kernel	Versão máxima para o kernel	Versão do sistema de arquivos		
				2,10	2,12	2,15
Ubuntu	22	6.2.0.1017.17 ~ 22.04	6.2.0. *	não	sim	sim
		5.15.0-1015-aws	5.15.0-1031-aws	sim	sim	sim
	20	5.15.0-1015-aws	5.15.0+	sim	sim	sim
		5.4.0-1011-aws	5.13.0-1031-aws	sim	sim	não

Clientes RHEL/CentOS/Rocky Linux

Sistema operacional	Versão do SO	Arquitetura	Versão mínima para o kernel	Versão máxima para o kernel	Versão do sistema de arquivos		
					2,10	2,12	2,15
RHEL/CentOS/Rocky Lin	9.3	ARM + x86	5.14.0-362.18.1	5.14.0-362.18.1	não	sim	sim

Sistema operacional	Versão do SO	Arquitetura	Versão mínima para o kernel	Versão máxima para o kernel	Versão do sistema de arquivos		
	9.0	ARM + x86	5.14.0-70.13.1	5.14.0-70.30.1	não	sim	sim
	8.9	ARM + x86	4.18.0-513*	4.18.0-513*	sim	sim	sim
	8.8	ARM + x86	4.18.0-477*	4.18.0-477*	sim	sim	sim
	8.7	ARM + x86	4.18.0-425*	4.18.0-425*	sim	sim	sim
	8.6	ARM + x86	4.18.0-372*	4.18.0-372*	sim	sim	sim
	8.5	ARM + x86	4.18.0-348*	4.18.0-348*	sim	sim	sim
	8.4	ARM + x86	4.18.0-305*	4.18.0-305*	sim	sim	sim
RHEL/CentOS	8.3	ARM + x86	4.18.0-240*	4.18.0-240*	sim	sim	não
	8.2	ARM + x86	4.18.0-193*	4.18.0-193*	sim	sim	não
	7.9	x86	3.10.0-1160*	3.10.0-1160*	sim	sim	sim
	7.8	x86	3.10.0-1127*	3.10.0-1127*	sim	sim	não

Sistema operacional	Versão do SO	Arquitetura	Versão mínima para o kernel	Versão máxima para o kernel	Versão do sistema de arquivos		
	7.7	x86	3.10.0-1062*	3.10.0-1062*	sim	sim	não
CentOS	7.9	Arm	4.18.0-193*	4.18.0-193*	sim	sim	sim
	7.8	Arm	4.18.0-147*	4.18.0-147*	sim	sim	sim

Instalação do cliente Lustre

Para montar o sistema de arquivos do Amazon FSx para Lustre usando uma instância do Linux, comece pela instalação do cliente Lustre de código aberto. Em seguida, dependendo da versão do seu sistema operacional, use um dos procedimentos a seguir. Para obter informações sobre o suporte do kernel, consulte Compatibilidade do sistema de arquivos Lustre e do kernel do cliente.

Se sua instância de computação não estiver executando o kernel do Linux especificado nas instruções de instalação e você não puder alterar o kernel, poderá criar seu próprio cliente Lustre. Para obter mais informações, consulte Compiling Lustre na página Wiki do Lustre.

Amazon Linux

Para instalar o cliente Lustre no Amazon Linux 2023

1. Abra um terminal no seu cliente.
2. Determine qual kernel está em execução, no momento, na sua instância de computação ao executar o comando apresentado a seguir.

```
uname -r
```

3. Analise a resposta do sistema e compare-a com o seguinte requisito mínimo de kernel para instalar o cliente Lustre no Amazon Linux 2023:

- Requisito mínimo do kernel 6.1 - 6.1.79-99.167.amzn2023

Se sua instância do EC2 atender ao requisito mínimo do kernel, vá para a etapa e instale o cliente lustre.

Se o comando retornar um resultado inferior ao requisito mínimo para o kernel, atualize o kernel e reinicialize a instância do Amazon EC2 ao executar o comando apresentado a seguir.

```
sudo dnf -y update kernel && sudo reboot
```

Confirme se o kernel foi atualizado usando o comando uname -r.

4. Faça download e instale o cliente Lustre com o comando apresentado a seguir.

```
sudo dnf install -y lustre-client
```

Como instalar o cliente Lustre no Amazon Linux 2

1. Abra um terminal no seu cliente.
2. Determine qual kernel está em execução, no momento, na sua instância de computação ao executar o comando apresentado a seguir.

```
uname -r
```

3. Analise a resposta do sistema e compare-a com os seguintes requisitos mínimos do kernel para instalar o cliente Lustre no Amazon Linux 2:

- Requisito mínimo para o kernel 5.10: 5.10.144-127.601.amzn2
- Requisito mínimo para o kernel 5.4: 5.4.214-120.368.amzn2
- Requisito mínimo para o kernel 4.14: 4.14.294-220.533.amzn2

Se sua instância do EC2 atender aos requisitos mínimos do kernel, vá para a etapa e instale o cliente lustre.

Se o comando retornar um resultado inferior ao requisito mínimo para o kernel, atualize o kernel e reinicialize a instância do Amazon EC2 ao executar o comando apresentado a seguir.

```
sudo yum -y update kernel && sudo reboot
```

Confirme se o kernel foi atualizado usando o comando uname -r.

4. Faça download e instale o cliente Lustre com o comando apresentado a seguir.

```
sudo amazon-linux-extras install -y lustre
```

Se não for possível atualizar o kernel para o requisito mínimo para o kernel, você poderá instalar o cliente com a versão 2.10 herdada usando o comando apresentado a seguir.

```
sudo amazon-linux-extras install -y lustre2.10
```

Como instalar o cliente Lustre no Amazon Linux

1. Abra um terminal no seu cliente.
2. Determine qual kernel está em execução, no momento, na sua instância de computação ao executar o comando apresentado a seguir. O cliente Lustre requer o kernel `4.14, version 104`, ou versões superiores, do Amazon Linux.

```
uname -r
```

3. Execute um destes procedimentos:

   - Se o comando retornar `4.14.104-78.84.amzn1.x86_64` ou uma versão superior a 4.14, faça download e instale o cliente Lustre usando o comando apresentado a seguir.

     ```
     sudo yum install -y lustre-client
     ```

   - Se o comando retornar um resultado inferior a `4.14.104-78.84.amzn1.x86_64`, atualize o kernel e reinicialize a instância do Amazon EC2 ao executar o comando apresentado a seguir.

     ```
     sudo yum -y update kernel && sudo reboot
     ```

     Confirme se o kernel foi atualizado usando o comando uname -r. Em seguida, faça download e instale o cliente Lustre conforme descrito anteriormente.

CentOS, Rocky Linux e Red Hat

Para instalar o cliente Lustre no CentOS, Red Hat e Rocky Linux 9.0 ou 9.3

É possível instalar e atualizar pacotes de clientes Lustre compatíveis com Red Hat Enterprise Linux (RHEL), Rocky Linux e CentOS usando o repositório de pacotes yum do cliente Lustre do Amazon FSx. Esses pacotes são assinados para ajudar a garantir que não foram violados antes ou durante o download. A instalação do repositório falhará se você não instalar a chave pública correspondente em seu sistema.

Como adicionar o repositório de pacotes yum do cliente Lustre do Amazon FSx

1. Abra um terminal no seu cliente.
2. Instale a chave pública rpm do Amazon FSx ao usar o comando apresentado a seguir.

   ```
   curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
   ```

3. Importe a chave ao usar o comando apresentado a seguir.

   ```
   sudo rpm --import /tmp/fsx-rpm-public-key.asc
   ```

4. Adicione o repositório e atualize o gerenciador de pacotes usando o comando apresentado a seguir.

   ```
   sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/9/fsx-lustre-client.repo -o /etc/yum.repos.d/aws-fsx.repo
   ```

Como configurar o repositório yum do cliente Lustre do Amazon FSx

O repositório de pacotes yum do cliente Amazon FSx Lustre é configurado por padrão para instalar o cliente Lustre que é compatível com a versão do kernel fornecida inicialmente com as versões mais recentes suportadas do CentOS, Rocky Linux e RHEL 9. Para instalar um cliente Lustre compatível com a versão do kernel que você está usando, é possível editar o arquivo de configuração do repositório.

Esta seção descreve como determinar qual kernel você está executando, se é necessário editar a configuração do repositório e como editar o arquivo de configuração.

1. Determine qual kernel está em execução, no momento, na sua instância de computação ao usar o comando apresentado a seguir.

```
uname -r
```

2. Execute um destes procedimentos:

   - Se o comando retornar `5.14.0-362*`, não será necessário modificar a configuração do repositório. Prossiga para o procedimento Como instalar o cliente Lustre.
   - Se o comando retornar`5.14.0-70*`, você deverá editar a configuração do repositório para que ela aponte para o cliente Lustre para as versões CentOS, Rocky Linux e RHEL 9.0.

3. Edite o arquivo de configuração do repositório a fim de direcionar para uma versão específica do RHEL usando o comando apresentado a seguir. *`specific_RHEL_version`*Substitua pela versão RHEL que você precisa usar.

```
sudo sed -i 's#9#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
```

   Por exemplo, para apontar para a versão 9.0, *`specific_RHEL_version`* substitua por `9.0` no comando, como no exemplo a seguir.

```
sudo sed -i 's#9#9.0#' /etc/yum.repos.d/aws-fsx.repo
```

4. Use o comando apresentado a seguir para limpar o cache do yum.

```
sudo yum clean all
```

Como instalar o cliente Lustre

- Instale os pacotes do repositório usando o comando apresentado a seguir.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Informações adicionais (CentOS, Rocky Linux e Red Hat 9.0 e versões mais recentes)

Os comandos anteriores instalam os dois pacotes necessários para montar e interagir com o sistema de arquivos do Amazon FSx. O repositório inclui pacotes adicionais para o Lustre, como um pacote

que contém o código-fonte e pacotes que contém testes, e você pode instalá-los se desejar. Para listar todos os pacotes disponíveis no repositório, use o comando apresentado a seguir.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Para fazer download do rpm de origem, que contém um tarball do código-fonte upstream e o conjunto de patches que aplicamos, use o comando apresentado a seguir.

```
 sudo yumdownloader --source kmod-lustre-client
```

Quando você executa uma atualização do yum, uma versão mais recente do módulo é instalada, se disponível, e a versão existente é substituída. Para evitar que a versão instalada no momento seja removida na atualização, adicione uma linha como a apresentada a seguir ao seu arquivo `/etc/yum.conf`.

```
installonlypkgs=kernel, kernel-PAE, installonlypkg(kernel), installonlypkg(kernel-
module),
              installonlypkg(vm), multiversion(kernel), kmod-lustre-client
```

Esta lista inclui os pacotes padrão somente para a instalação, especificados na página de manual `yum.conf`, e o pacote `kmod-lustre-client`.

Para instalar o cliente Lustre no CentOS e no Red Hat 8.2—8.9 ou no Rocky Linux 8.4—8.9

É possível instalar e atualizar pacotes de clientes Lustre compatíveis com Red Hat Enterprise Linux (RHEL), Rocky Linux e CentOS usando o repositório de pacotes yum do cliente Lustre do Amazon FSx. Esses pacotes são assinados para ajudar a garantir que não foram violados antes ou durante o download. A instalação do repositório falhará se você não instalar a chave pública correspondente em seu sistema.

Como adicionar o repositório de pacotes yum do cliente Lustre do Amazon FSx

1. Abra um terminal no seu cliente.
2. Instale a chave pública rpm do Amazon FSx ao usar o comando apresentado a seguir.

   ```
   curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-
   key.asc -o /tmp/fsx-rpm-public-key.asc
   ```

3. Importe a chave ao usar o comando apresentado a seguir.

```
sudo rpm --import /tmp/fsx-rpm-public-key.asc
```

4. Adicione o repositório e atualize o gerenciador de pacotes usando o comando apresentado a seguir.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/8/fsx-lustre-
client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Como configurar o repositório yum do cliente Lustre do Amazon FSx

O repositório de pacotes yum do cliente Lustre do Amazon FSx é configurado, por padrão, para instalar o cliente Lustre que é compatível com a versão do kernel disponibilizada inicialmente com as versões mais recentes e com suporte para CentOS, Rocky Linux e RHEL 8. Para instalar um cliente Lustre compatível com a versão do kernel que você está usando, é possível editar o arquivo de configuração do repositório.

Esta seção descreve como determinar qual kernel você está executando, se é necessário editar a configuração do repositório e como editar o arquivo de configuração.

1. Determine qual kernel está em execução, no momento, na sua instância de computação ao usar o comando apresentado a seguir.

```
uname -r
```

2. Execute um destes procedimentos:

   - Se o comando retornar `4.18.0-513*`, não será necessário modificar a configuração do repositório. Prossiga para o procedimento Como instalar o cliente Lustre.
   - Se o comando retornar`4.18.0-477*`, você deverá editar a configuração do repositório para que ela aponte para o cliente Lustre para as versões CentOS, Rocky Linux e RHEL 8.8.
   - Se o comando retornar `4.18.0-425*`, você deverá editar a configuração do repositório a fim de que direcione o cliente Lustre para as versões CentOS, Rocky Linux e RHEL 8.7.
   - Se o comando retornar `4.18.0-372*`, você deverá editar a configuração do repositório a fim de que direcione o cliente Lustre para as versões CentOS, Rocky Linux e RHEL 8.6.
   - Se o comando retornar `4.18.0-348*`, você deverá editar a configuração do repositório a fim de que direcione o cliente Lustre para as versões CentOS, Rocky Linux e RHEL 8.5.

- Se o comando retornar `4.18.0-305*`, você deverá editar a configuração do repositório a fim de que direcione o cliente Lustre para as versões CentOS, Rocky Linux e RHEL 8.4.
- Se o comando retornar `4.18.0-240*`, você deverá editar a configuração do repositório a fim de que direcione o cliente Lustre para as versões CentOS e RHEL 8.3.
- Se o comando retornar `4.18.0-193*`, você deverá editar a configuração do repositório a fim de que direcione o cliente Lustre para as versões CentOS e RHEL 8.2.

3. Edite o arquivo de configuração do repositório a fim de direcionar para uma versão específica do RHEL usando o comando apresentado a seguir.

   ```
   sudo sed -i 's#8#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
   ```

   Por exemplo, para apontar para a versão 8.8, *`specific_RHEL_version`* substitua por `8.8` no comando.

   ```
   sudo sed -i 's#8#8.8#' /etc/yum.repos.d/aws-fsx.repo
   ```

4. Use o comando apresentado a seguir para limpar o cache do yum.

   ```
   sudo yum clean all
   ```

Como instalar o cliente Lustre

- Instale os pacotes do repositório usando o comando apresentado a seguir.

  ```
  sudo yum install -y kmod-lustre-client lustre-client
  ```

Informações adicionais (CentOS, Rocky Linux e Red Hat 8.2 e versões mais recentes)

Os comandos anteriores instalam os dois pacotes necessários para montar e interagir com o sistema de arquivos do Amazon FSx. O repositório inclui pacotes adicionais para o Lustre, como um pacote que contém o código-fonte e pacotes que contém testes, e você pode instalá-los se desejar. Para listar todos os pacotes disponíveis no repositório, use o comando apresentado a seguir.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Para fazer download do rpm de origem, que contém um tarball do código-fonte upstream e o conjunto de patches que aplicamos, use o comando apresentado a seguir.

```
sudo yumdownloader --source kmod-lustre-client
```

Quando você executa uma atualização do yum, uma versão mais recente do módulo é instalada, se disponível, e a versão existente é substituída. Para evitar que a versão instalada no momento seja removida na atualização, adicione uma linha como a apresentada a seguir ao seu arquivo `/etc/yum.conf`.

```
installonlypkgs=kernel, kernel-PAE, installonlypkg(kernel), installonlypkg(kernel-
module),
              installonlypkg(vm), multiversion(kernel), kmod-lustre-client
```

Esta lista inclui os pacotes padrão somente para a instalação, especificados na página de manual `yum.conf`, e o pacote `kmod-lustre-client`.

Como instalar o cliente Lustre no CentOS e no Red Hat 7.7, 7.8 ou 7.9 (instâncias x86_64)

É possível instalar e atualizar os pacotes de clientes Lustre compatíveis com Red Hat Enterprise Linux (RHEL) e CentOS usando o repositório de pacotes yum do cliente Lustre do Amazon FSx. Esses pacotes são assinados para ajudar a garantir que não foram violados antes ou durante o download. A instalação do repositório falhará se você não instalar a chave pública correspondente em seu sistema.

Como adicionar o repositório de pacotes yum do cliente Lustre do Amazon FSx

1. Abra um terminal no seu cliente.
2. Instale a chave pública rpm do Amazon FSx usando o comando apresentado a seguir.

   ```
   curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-
   key.asc -o /tmp/fsx-rpm-public-key.asc
   ```

3. Importe a chave usando o comando apresentado a seguir.

   ```
   sudo rpm --import /tmp/fsx-rpm-public-key.asc
   ```

4. Adicione o repositório e atualize o gerenciador de pacotes usando o comando apresentado a seguir.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/7/fsx-lustre-
client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Como configurar o repositório yum do cliente Lustre do Amazon FSx

O repositório de pacotes yum do cliente Lustre do Amazon FSx é configurado, por padrão, para instalar o cliente Lustre que é compatível com a versão do kernel disponibilizada inicialmente com as versões mais recentes e com suporte para CentOS e RHEL 7. Para instalar um cliente Lustre compatível com a versão do kernel que você está usando, é possível editar o arquivo de configuração do repositório.

Esta seção descreve como determinar qual kernel você está executando, se é necessário editar a configuração do repositório e como editar o arquivo de configuração.

1. Determine qual kernel está em execução, no momento, na sua instância de computação ao usar o comando apresentado a seguir.

   ```
   uname -r
   ```

2. Execute um destes procedimentos:

   - Se o comando retornar `3.10.0-1160*`, não será necessário modificar a configuração do repositório. Prossiga para o procedimento Como instalar o cliente Lustre.
   - Se o comando retornar `3.10.0-1127*`, você deverá editar a configuração do repositório a fim de que direcione o cliente Lustre para as versões CentOS e RHEL 7.8.
   - Se o comando retornar `3.10.0-1062*`, você deverá editar a configuração do repositório a fim de que direcione o cliente Lustre para as versões CentOS e RHEL 7.7.

3. Edite o arquivo de configuração do repositório a fim de direcionar para uma versão específica do RHEL usando o comando apresentado a seguir.

   ```
   sudo sed -i 's#7#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
   ```

   Para direcionar para a versão 7.8, substitua *`specific_RHEL_version`* por `7.8` no comando.

   ```
   sudo sed -i 's#7#7.8#' /etc/yum.repos.d/aws-fsx.repo
   ```

   Para direcionar para a versão 7.7, substitua *`specific_RHEL_version`* por `7.7` no comando.

```
sudo sed -i 's#7#7.7#' /etc/yum.repos.d/aws-fsx.repo
```

4. Use o comando apresentado a seguir para limpar o cache do yum.

```
sudo yum clean all
```

Como instalar o cliente Lustre

- Instale os pacotes do cliente Lustre do repositório usando o comando apresentado a seguir.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Informações adicionais (CentOS e Red Hat 7.7 e versões mais recentes)

Os comandos anteriores instalam os dois pacotes necessários para montar e interagir com o sistema de arquivos do Amazon FSx. O repositório inclui pacotes adicionais para o Lustre, como um pacote que contém o código-fonte e pacotes que contém testes, e você pode instalá-los se desejar. Para listar todos os pacotes disponíveis no repositório, use o comando apresentado a seguir.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Para fazer download do rpm de origem que contém um tarball do código-fonte upstream e o conjunto de patches que aplicamos, use o comando apresentado a seguir.

```
 sudo yumdownloader --source kmod-lustre-client
```

Quando você executa uma atualização do yum, uma versão mais recente do módulo é instalada, se disponível, e a versão existente é substituída. Para evitar que a versão instalada no momento seja removida na atualização, adicione uma linha como a apresentada a seguir ao seu arquivo `/etc/yum.conf`.

```
installonlypkgs=kernel, kernel-big-mem, kernel-enterprise, kernel-smp,
              kernel-debug, kernel-unsupported, kernel-source, kernel-devel, kernel-
PAE,
              kernel-PAE-debug, kmod-lustre-client
```

Esta lista inclui os pacotes padrão somente para a instalação, especificados na página de manual `yum.conf`, e o pacote `kmod-lustre-client`.

Para instalar o cliente Lustre no CentOS 7.8 ou 7.9 (instâncias baseadas em Arm baseadas em Graviton) AWS

É possível instalar e atualizar pacotes de clientes Lustre usando o repositório de pacotes yum do cliente Lustre do Amazon FSx que são compatíveis com CentOS 7 para instâncias do EC2 baseadas em ARM e desenvolvidas pelo AWS Graviton. Esses pacotes são assinados para ajudar a garantir que não foram violados antes ou durante o download. A instalação do repositório falhará se você não instalar a chave pública correspondente em seu sistema.

Como adicionar o repositório de pacotes yum do cliente Lustre do Amazon FSx

1. Abra um terminal no seu cliente.
2. Instale a chave pública rpm do Amazon FSx usando o comando apresentado a seguir.

   ```
   curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
   ```

   ```
   curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.cn/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
   ```
3. Importe a chave usando o comando apresentado a seguir.

   ```
   sudo rpm --import /tmp/fsx-rpm-public-key.asc
   ```
4. Adicione o repositório e atualize o gerenciador de pacotes usando o comando apresentado a seguir.

   ```
   sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/centos/7/fsx-lustre-client.repo -o /etc/yum.repos.d/aws-fsx.repo
   ```

Como configurar o repositório yum do cliente Lustre do Amazon FSx

O repositório de pacotes yum do cliente Lustre do Amazon FSx é configurado, por padrão, para instalar o cliente Lustre que é compatível com a versão do kernel disponibilizada inicialmente com as versões mais recentes e com suporte para CentOS 7. Para instalar um cliente Lustre compatível com a versão do kernel que você está usando, é possível editar o arquivo de configuração do repositório.

Esta seção descreve como determinar qual kernel você está executando, se é necessário editar a configuração do repositório e como editar o arquivo de configuração.

1. Determine qual kernel está em execução, no momento, na sua instância de computação ao usar o comando apresentado a seguir.

   ```
   uname -r
   ```

2. Execute um destes procedimentos:

   - Se o comando retornar `4.18.0-193*`, não será necessário modificar a configuração do repositório. Prossiga para o procedimento Como instalar o cliente Lustre.
   - Se o comando retornar `4.18.0-147*`, você deverá editar a configuração do repositório a fim de que direcione o cliente Lustre para a versão CentOS 7.8.

3. Edite o arquivo de configuração do repositório a fim de direcionar para a versão do CentOS 7.8 usando o comando apresentado a seguir.

   ```
   sudo sed -i 's#7#7.8#' /etc/yum.repos.d/aws-fsx.repo
   ```

4. Use o comando apresentado a seguir para limpar o cache do yum.

   ```
   sudo yum clean all
   ```

Como instalar o cliente Lustre

- Instale os pacotes do repositório usando o comando apresentado a seguir.

  ```
  sudo yum install -y kmod-lustre-client lustre-client
  ```

Informações adicionais (CentOS 7.8 ou 7.9 para instâncias EC2 baseadas em AWS Arm baseadas em Graviton)

Os comandos anteriores instalam os dois pacotes necessários para montar e interagir com o sistema de arquivos do Amazon FSx. O repositório inclui pacotes adicionais para o Lustre, como um pacote que contém o código-fonte e pacotes que contém testes, e você pode instalá-los se desejar. Para listar todos os pacotes disponíveis no repositório, use o comando apresentado a seguir.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Para fazer download do rpm de origem, que contém um tarball do código-fonte upstream e o conjunto de patches que aplicamos, use o comando apresentado a seguir.

```
 sudo yumdownloader --source kmod-lustre-client
```

Quando você executa uma atualização do yum, uma versão mais recente do módulo é instalada, se disponível, e a versão existente é substituída. Para evitar que a versão instalada no momento seja removida na atualização, adicione uma linha como a apresentada a seguir ao seu arquivo `/etc/yum.conf`.

```
installonlypkgs=kernel, kernel-big-mem, kernel-enterprise, kernel-smp,
              kernel-debug, kernel-unsupported, kernel-source, kernel-devel, kernel-
PAE,
              kernel-PAE-debug, kmod-lustre-client
```

Esta lista inclui os pacotes padrão somente para a instalação, especificados na página de manual `yum.conf`, e o pacote `kmod-lustre-client`.

Ubuntu

Como instalar o cliente Lustre no Ubuntu 22.04

É possível obter pacotes do Lustre usando o repositório do Amazon FSx para o Ubuntu 22.04. Para validar que o conteúdo do repositório não foi violado antes ou durante o download, uma assinatura GNU Privacy Guard (GPG) é aplicada aos metadados do repositório. A instalação do repositório falhará, a menos que você tenha a chave GPG pública adequada instalada no sistema.

1. Abra um terminal no seu cliente.
2. Siga estas etapas para adicionar o repositório do Amazon FSx para Ubuntu:

    a. Se você ainda não registrou um repositório do Amazon FSx para Ubuntu na instância do cliente, faça download e instale a chave pública obrigatória. Use o comando a seguir.

    ```
    wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-
    ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-
    ubuntu-public-key.gpg >/dev/null
    ```

b. Adicione o repositório de pacotes do Amazon FSx ao gerenciador de pacotes local usando o comando apresentado a seguir.

```
sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-
key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu jammy main" > /
etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
```

3. Determine qual kernel está em execução na instância do cliente no momento e realize atualizações, conforme necessário. O cliente Lustre no Ubuntu 22.04 requer o kernel `5.15.0-1015-aws`, ou versões posteriores, para instâncias do EC2 baseadas em x86 e para instâncias do EC2 baseadas em ARM com tecnologia de processadores do AWS Graviton.

   a. Execute o comando apresentado a seguir para determinar qual kernel está em execução.

   ```
   uname -r
   ```

   b. Execute o comando apresentado a seguir para atualizar para as versões mais recentes do kernel do Ubuntu e do Lustre e, em seguida, reinicialize.

   ```
   sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
   ```

   Se a versão do kernel for superior a `5.15.0-1015-aws` para instâncias do EC2 baseadas em x86 e para instâncias do EC2 baseadas no Graviton, e você não desejar atualizar para a versão mais recente do kernel, poderá instalar o Lustre para o kernel atual com o comando apresentado a seguir.

   ```
   sudo apt install -y lustre-client-modules-$(uname -r)
   ```

   Os dois pacotes do Lustre que são necessários para montar e interagir com o sistema de arquivos do FSx para Lustre estão instalados. Opcionalmente, é possível instalar pacotes relacionados adicionais, como um pacote que contém o código-fonte e pacotes que contém testes, os quais estão inclusos no repositório.

   c. Liste todos os pacotes disponíveis no repositório ao usar o comando apresentado a seguir.

   ```
   sudo apt-cache search ^lustre
   ```

d. (Opcional) Se você deseja que a atualização do sistema também atualize sempre os módulos do cliente Lustre, certifique-se de que o pacote `lustre-client-modules-aws` esteja instalado usando o comando apresentado a seguir.

```
sudo apt install -y lustre-client-modules-aws
```

> **Note**
>
> Se você receber um erro `Module Not Found`, consulte Como solucionar erros de módulos ausentes.

Como instalar o cliente Lustre no Ubuntu 20.04

Os clientes Lustre 2.12 têm suporte no Ubuntu 20.04 com o kernel 5.15.0-1015-aws ou com versões posteriores. Os clientes Lustre 2.10 são suportados no Ubuntu 20.04 com kernel 5.4.0-1011-aws ou posterior em instâncias EC2 baseadas em x86 e kernel 5.4.0-1015-aws ou posterior em instâncias EC2 baseadas em ARM com processadores Graviton. AWS

É possível obter pacotes do Lustre usando o repositório do Amazon FSx para o Ubuntu 20.04. Para validar que o conteúdo do repositório não foi violado antes ou durante o download, uma assinatura GNU Privacy Guard (GPG) é aplicada aos metadados do repositório. A instalação do repositório falhará, a menos que você tenha a chave GPG pública adequada instalada no sistema.

1. Abra um terminal no seu cliente.
2. Siga estas etapas para adicionar o repositório do Amazon FSx para Ubuntu:

   a. Se você ainda não registrou um repositório do Amazon FSx para Ubuntu na instância do cliente, faça download e instale a chave pública obrigatória. Use o comando a seguir.

   ```
   wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-key.gpg >/dev/null
   ```

   b. Adicione o repositório de pacotes do Amazon FSx ao gerenciador de pacotes local usando o comando apresentado a seguir.

```
sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-
key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu focal main" > /
etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
```

3. Determine qual kernel está em execução na instância do cliente no momento e realize atualizações, conforme necessário.

   a. Execute o comando apresentado a seguir para determinar qual kernel está em execução.

   ```
   uname -r
   ```

   b. Execute o comando apresentado a seguir para atualizar para as versões mais recentes do kernel do Ubuntu e do Lustre e, em seguida, reinicialize.

   ```
   sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
   ```

   Se a versão do kernel for superior a `5.4.0-1011-aws` para instâncias do EC2 baseadas em x86 ou superior a `5.4.0-1015-aws` para instâncias do EC2 baseadas no Graviton, e você não desejar atualizar para a versão mais recente do kernel, poderá instalar o Lustre para o kernel atual com o comando apresentado a seguir.

   ```
   sudo apt install -y lustre-client-modules-$(uname -r)
   ```

   Os dois pacotes do Lustre que são necessários para montar e interagir com o sistema de arquivos do FSx para Lustre estão instalados. Opcionalmente, é possível instalar pacotes relacionados adicionais, como um pacote que contém o código-fonte e pacotes que contém testes, os quais estão inclusos no repositório.

   c. Liste todos os pacotes disponíveis no repositório ao usar o comando apresentado a seguir.

   ```
   sudo apt-cache search ^lustre
   ```

   d. (Opcional) Se você deseja que a atualização do sistema também atualize sempre os módulos do cliente Lustre, certifique-se de que o pacote `lustre-client-modules-aws` esteja instalado usando o comando apresentado a seguir.

   ```
   sudo apt install -y lustre-client-modules-aws
   ```

> **Note**
>
> Se você receber um erro `Module Not Found`, consulte Como solucionar erros de módulos ausentes.

Como instalar o cliente Lustre no Ubuntu 18.04

> **Note**
>
> A última versão do kernel com suporte para o Ubuntu 18 é `5.4.0.1103.aws`.

É possível obter pacotes do Lustre usando o repositório do Amazon FSx para o Ubuntu 18.04. Para validar que o conteúdo do repositório não foi violado antes ou durante o download, uma assinatura GNU Privacy Guard (GPG) é aplicada aos metadados do repositório. A instalação do repositório falhará, a menos que você tenha a chave GPG pública adequada instalada no sistema.

1. Abra um terminal no seu cliente.
2. Siga estas etapas para adicionar o repositório do Amazon FSx para Ubuntu:

   a. Se você ainda não registrou um repositório do Amazon FSx para Ubuntu na instância do cliente, faça download e instale a chave pública obrigatória. Use o comando a seguir.

   ```
   wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-key.gpg >/dev/null
   ```

   b. Adicione o repositório de pacotes do Amazon FSx ao gerenciador de pacotes local usando o comando apresentado a seguir.

   ```
   sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu bionic main" > /etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
   ```

3. Determine qual kernel está em execução na instância do cliente no momento e realize atualizações, conforme necessário. O cliente Lustre no Ubuntu 18.04 requer kernel `4.15.0-1054-aws` ou posterior para instâncias EC2 baseadas em x86 e kernel `5.3.0-1023-`

`aws` ou posterior para instâncias EC2 baseadas em ARM alimentadas por processadores Graviton. AWS

a. Execute o comando apresentado a seguir para determinar qual kernel está em execução.

```
uname -r
```

b. Execute o comando apresentado a seguir para atualizar para as versões mais recentes do kernel do Ubuntu e do Lustre e, em seguida, reinicialize.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
```

Se a versão do kernel for superior a `4.15.0-1054-aws` para instâncias do EC2 baseadas em x86 ou superior a `5.3.0-1023-aws` para instâncias do EC2 baseadas no Graviton, e você não desejar atualizar para a versão mais recente do kernel, poderá instalar o Lustre para o kernel atual com o comando apresentado a seguir.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Os dois pacotes do Lustre que são necessários para montar e interagir com o sistema de arquivos do FSx para Lustre estão instalados. Opcionalmente, é possível instalar pacotes relacionados adicionais, como um pacote que contém o código-fonte e pacotes que contém testes, os quais estão inclusos no repositório.

c. Liste todos os pacotes disponíveis no repositório ao usar o comando apresentado a seguir.

```
sudo apt-cache search ^lustre
```

d. (Opcional) Se você deseja que a atualização do sistema também atualize sempre os módulos do cliente Lustre, certifique-se de que o pacote `lustre-client-modules-aws` esteja instalado usando o comando apresentado a seguir.

```
sudo apt install -y lustre-client-modules-aws
```

> **Note**
>
> Se você receber um erro `Module Not Found`, consulte Como solucionar erros de módulos ausentes.

Como solucionar erros de módulos ausentes

Se você receber um erro `Module Not Found` ao realizar a instalação de qualquer versão do Ubuntu, faça o seguinte:

Faça downgrade do kernel para a versão mais recente com suporte. Liste todas as versões disponíveis do lustre-client-modules pacote e instale o kernel correspondente. Para fazer isso, execute o seguinte comando.

```
sudo apt-cache search lustre-client-modules
```

Por exemplo, se a versão mais recente inclusa no repositório for `lustre-client-modules-5.4.0-1011-aws`, faça o seguinte:

1. Instale o kernel para o qual este pacote foi desenvolvido usando os comandos apresentados a seguir.

   ```
   sudo apt-get install -y linux-image-5.4.0-1011-aws
   ```

   ```
   sudo sed -i 's/GRUB_DEFAULT=.\+/GRUB\_DEFAULT="Advanced options for Ubuntu>Ubuntu,
    with Linux 5.4.0-1011-aws"/' /etc/default/grub
   ```

   ```
   sudo update-grub
   ```

2. Reinicialize a instância usando o comando apresentado a seguir.

   ```
   sudo reboot
   ```

3. Instale o cliente Lustre usando o comando apresentado a seguir.

   ```
   sudo apt-get install -y lustre-client-modules-$(uname -r)
   ```

SUSE Linux

Como instalar o cliente Lustre no SUSE Linux 12 SP3, SP4 ou SP5

Como instalar o cliente Lustre no SUSE Linux 12 SP3

1. Abra um terminal no seu cliente.
2. Instale a chave pública rpm do Amazon FSx ao usar o comando apresentado a seguir.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Importe a chave ao usar o comando apresentado a seguir.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Adicione o repositório para o cliente Lustre usando o comando apresentado a seguir.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Faça download e instale o cliente Lustre com os comandos apresentados a seguir.

```
sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
sudo sed -i 's#SLES-12#SP3#' /etc/zypp/repos.d/aws-fsx.repo
sudo zypper refresh
sudo zypper in lustre-client
```

Como instalar o cliente Lustre no SUSE Linux 12 SP4

1. Abra um terminal no seu cliente.
2. Instale a chave pública rpm do Amazon FSx ao usar o comando apresentado a seguir.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Importe a chave ao usar o comando apresentado a seguir.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Adicione o repositório para o cliente Lustre usando o comando apresentado a seguir.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Execute um destes procedimentos:

   - Se você instalou o SP4 diretamente, faça download e instale o cliente Lustre com os comandos apresentados a seguir.

```
sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
sudo sed -i 's#SLES-12#SP4#' /etc/zypp/repos.d/aws-fsx.repo
sudo zypper refresh
sudo zypper in lustre-client
```

   - Se você migrou do SP3 para o SP4 e adicionou previamente o repositório do Amazon FSx para o SP3, faça download e instale o cliente Lustre com os comandos apresentados a seguir.

```
sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
sudo sed -i 's#SP3#SP4#' /etc/zypp/repos.d/aws-fsx.repo
sudo zypper ref
sudo zypper up --force-resolution lustre-client-kmp-default
```

Como instalar o cliente Lustre no SUSE Linux 12 SP5

1. Abra um terminal no seu cliente.
2. Instale a chave pública rpm do Amazon FSx ao usar o comando apresentado a seguir.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Importe a chave ao usar o comando apresentado a seguir.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Adicione o repositório para o cliente Lustre usando o comando apresentado a seguir.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Execute um destes procedimentos:

   - Se você instalou o SP5 diretamente, faça download e instale o cliente Lustre com os comandos apresentados a seguir.

     ```
     sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
     sudo zypper refresh
     sudo zypper in lustre-client
     ```

   - Se você migrou do SP4 para o SP5 e adicionou previamente o repositório do Amazon FSx para o SP4, faça download e instale o cliente Lustre com os comandos apresentados a seguir.

     ```
     sudo sed -i 's#SP4#SLES-12' /etc/zypp/repos.d/aws-fsx.repo
     sudo zypper ref
     sudo zypper up --force-resolution lustre-client-kmp-default
     ```

> **Note**
>
> Pode ser necessário reinicializar a instância de computação para que o cliente conclua a instalação.

Montagem usando uma instância do Amazon Elastic Compute Cloud

É possível montar o seu sistema de arquivos usando uma instância do Amazon EC2.

Montar o sistema de arquivos usando o Amazon EC2

1. Conecte-se à sua instância Amazon EC2.
2. Crie um diretório no sistema de arquivos do FSx para Lustre para o ponto de montagem com o comando apresentado a seguir.

   ```
   $ sudo mkdir -p /fsx
   ```

3. Monte o sistema de arquivos do Amazon FSx para Lustre no diretório que você criou. Use o seguinte comando e substitua os seguintes itens:

- Substitua *file_system_dns_name* pelo nome DNS real do sistema de arquivos.
- Substitua *mountname* pelo nome da montagem do sistema de arquivos. Esse nome da montagem é retornado na resposta da operação de API `CreateFileSystem`. Também é retornado na resposta do describe-file-systems AWS CLI comando e na operação da DescribeFileSystemsAPI.

```
sudo mount -t lustre -o relatime,flock file_system_dns_name@tcp:/mountname /fsx
```

Este comando monta o sistema de arquivos com duas opções, `-o relatime` e `flock`:

- `relatime`: embora a opção `atime` mantenha dados de `atime` (horários de acesso de inodes) para cada vez que um arquivo é acessado, a opção `relatime` também mantém dados de `atime`, mas não para cada vez que um arquivo é acessado. Com a opção `relatime` habilitada, os dados de `atime` serão gravados para o disco somente se o arquivo tiver sido modificado desde a última atualização dos dados de `atime` (`mtime`) ou se o arquivo tiver sido acessado pela última vez há mais tempo do que um determinado período (seis horas por padrão). Usar a opção `relatime` ou `atime` otimizará os processos de liberação de arquivos.

  > **Note**
  >
  > Se a workload requerer uma precisão rigorosa quanto ao horário de acesso, você poderá montar com a opção de montagem `atime`. No entanto, isso pode afetar a performance da workload ao aumentar o tráfego de rede necessário para manter valores rigorosos quanto ao horário de acesso.
  > Se a workload não requerer o horário de acesso aos metadados, usar a opção de montagem `noatime` para desabilitar atualizações relacionadas ao horário de acesso poderá proporcionar um ganho de performance. Esteja ciente de que os processos focados na opção `atime`, como a liberação de arquivos ou a liberação da validade de dados, serão imprecisos em suas liberações.

- `flock`: ativa o bloqueio de arquivos para o sistema de arquivos. Se você não desejar que o bloqueio de arquivos seja habilitado, use o comando `mount` sem `flock`.

4. Verifique se o comando mount ocorreu com êxito ao listar o conteúdo do diretório no qual você montou o sistema de arquivos, /mnt/fsx, usando o comando apresentado a seguir.

```
$ ls /fsx
import-path  lustre
$
```

Você também pode usar o comando `df` apresentado a seguir.

```
$ df
Filesystem                     1K-blocks    Used  Available Use% Mounted on
devtmpfs                         1001808       0    1001808   0% /dev
tmpfs                            1019760       0    1019760   0% /dev/shm
tmpfs                            1019760     392    1019368   1% /run
tmpfs                            1019760       0    1019760   0% /sys/fs/cgroup
/dev/xvda1                       8376300 1263180    7113120  16% /
123.456.789.0@tcp:/mountname 3547698816   13824 3547678848   1% /fsx
tmpfs                             203956       0     203956   0% /run/user/1000
```

Os resultados mostram o sistema de arquivos do Amazon FSx montado em /fsx.

Montagem usando o Amazon Elastic Container Service

Você pode acessar o sistema de arquivos do FSx para Lustre usando um contêiner do Docker do Amazon Elastic Container Service (Amazon ECS) em uma instância do Amazon EC2. É possível fazer isso ao usar uma das seguintes opções:

1. Ao montar o sistema de arquivos do FSx para Lustre usando a instância do Amazon EC2 que hospeda as tarefas do Amazon ECS e exportar esse ponto de montagem para os contêineres.
2. Ao montar o sistema de arquivos diretamente dentro do contêiner de tarefas.

Para obter mais informações sobre o Amazon ECS, consulte O que é o Amazon Elastic Container Service? no Guia do desenvolvedor do Amazon Elastic Container Service.

Recomendamos usar a opção 1 (Montagem usando uma instância do Amazon EC2 que hospeda tarefas do Amazon ECS) porque ela proporciona melhor aproveitamento de recursos, principalmente se você iniciar diversos contêineres (mais de cinco) na mesma instância do EC2 ou se suas tarefas durarem pouco (menos de cinco minutos).

Use a opção 2 (Montagem usando um contêiner do Docker), se não for possível configurar a instância do EC2 ou se a aplicação requerer a flexibilidade do contêiner.

> **Note**
>
> A montagem do FSx for Lustre em AWS um tipo de lançamento Fargate não é suportada.

As seções a seguir descrevem os procedimentos para cada uma das opções de montagem do sistema de arquivos do FSx para Lustre usando um contêiner do Amazon ECS.

Tópicos

- Montagem usando uma instância do Amazon EC2 que hospeda tarefas do Amazon ECS
- Montagem usando um contêiner do Docker

Montagem usando uma instância do Amazon EC2 que hospeda tarefas do Amazon ECS

Este procedimento mostra como você pode configurar uma instância do Amazon ECS no EC2 para montar localmente o sistema de arquivos do FSx para Lustre. O procedimento usa as propriedades de contêiner `volumes` e `mountPoints` para compartilhar o recurso e tornar esse sistema de arquivos acessível para tarefas em execução localmente. Para obter mais informações, consulte Iniciar uma instância de contêiner do Amazon ECS no Guia do desenvolvedor do Amazon Elastic Container Service.

Este procedimento é para uma AMI do Amazon Linux 2 otimizada para o Amazon ECS. Se você estiver usando outra distribuição do Linux, consulte Instalação do cliente Lustre.

Como montar o sistema de arquivos do Amazon ECS em uma instância do EC2

1. Ao iniciar instâncias do Amazon ECS, de forma manual ou ao usar um grupo do Auto Scaling, adicione as linhas do exemplo de código apresentado a seguir ao final do campo Dados do usuário. Substitua os seguintes itens no exemplo:

   - Substitua *`file_system_dns_name`* pelo nome DNS real do sistema de arquivos.
   - Substitua *`mountname`* pelo nome da montagem do sistema de arquivos.
   - Substitua *`mountpoint`* pelo ponto de montagem do sistema de arquivos que você precisa criar.

```
#!/bin/bash

...<existing user data>...

fsx_dnsname=file_system_dns_name
fsx_mountname=mountname
fsx_mountpoint=mountpoint
amazon-linux-extras install -y lustre
mkdir -p "$fsx_mountpoint"
mount -t lustre ${fsx_dnsname}@tcp:/${fsx_mountname} ${fsx_mountpoint} -o
 relatime,flock
```

2. Ao criar as tarefas do Amazon ECS, adicione as propriedades de contêiner `volumes` e `mountPoints` apresentadas a seguir na definição JSON. Substitua *`mountpoint`* pelo ponto de montagem do sistema de arquivos (como `/mnt/fsx`).

```
{
    "volumes": [
           {
                 "host": {
                      "sourcePath": "mountpoint"
                 },
                 "name": "Lustre"
           }
    ],
    "mountPoints": [
           {
                 "containerPath": "mountpoint",
                 "sourceVolume": "Lustre"
           }
    ],
}
```

Montagem usando um contêiner do Docker

O procedimento a seguir mostra como é possível configurar um contêiner de tarefas do Amazon ECS para instalar o pacote `lustre-client` e montar o sistema de arquivos do FSx para Lustre nele. O procedimento usa uma imagem do Docker para o Amazon Linux (`amazonlinux`), mas uma abordagem semelhante pode funcionar para outras distribuições.

Como montar o sistema de arquivos usando um contêiner do Docker

1. Em seu contêiner do Docker, instale o pacote `lustre-client` e monte o sistema de arquivos do FSx para Lustre com a propriedade `command`. Substitua os seguintes itens no exemplo:

   - Substitua *`file_system_dns_name`* pelo nome DNS real do sistema de arquivos.
   - Substitua *`mountname`* pelo nome da montagem do sistema de arquivos.
   - Substitua *`mountpoint`* pelo ponto de montagem do sistema de arquivos.

   ```
   "command": [
     "/bin/sh -c \"amazon-linux-extras install -y lustre; mount -t
    lustre file_system_dns_name@tcp:/mountname mountpoint -o relatime,flock;\""
   ],
   ```

2. Adicione a funcionalidade `SYS_ADMIN` ao contêiner para autorizá-lo a montar o sistema de arquivos do FSx para Lustre, usando a propriedade `linuxParameters`.

   ```
   "linuxParameters": {
     "capabilities": {
         "add": [
           "SYS_ADMIN"
         ]
      }
   }
   ```

Montagem de sistemas de arquivos do Amazon FSx usando uma Amazon VPC on-premises ou emparelhada

É possível acessar o sistema de arquivos do Amazon FSx de duas maneiras. Uma das maneiras é usar instâncias do Amazon EC2 localizadas em uma Amazon VPC emparelhada com a VPC do sistema de arquivos. A outra é de clientes locais que estão conectados à VPC do seu sistema de arquivos AWS Direct Connect usando nossa VPN.

Você conecta a VPC do cliente e a VPC do sistema de arquivos do Amazon FSx usando uma conexão de emparelhamento da VPC ou um gateway de trânsito da VPC. Ao usar uma conexão de emparelhamento da VPC ou um gateway de trânsito para conectar VPCs, as instâncias do Amazon

EC2 que estiverem em uma VPC poderão acessar os sistemas de arquivos do Amazon FSx em outra VPC, mesmo se as VPCs pertencerem a contas diferentes.

Antes de usar o procedimento apresentado a seguir, é necessário configurar uma conexão de emparelhamento da VPC ou um gateway de trânsito da VPC.

Um gateway de trânsito é um hub de trânsito de rede que pode ser usado para interconectar as VPCs e as redes on-premises. Para obter mais informações sobre como usar os gateways de trânsito da VPC, consulte Conceitos básicos de gateways de trânsito no Guia de gateways de trânsito da Amazon VPC.

Uma conexão de emparelhamento de VPC é uma conexão de rede entre duas VPCs. Esse tipo de conexão permite direcionar o tráfego entre elas usando endereços privados IPv4 ou IPv6. Você pode usar o emparelhamento de VPC para conectar VPCs dentro da mesma AWS região ou entre regiões. AWS Para obter mais informações sobre o emparelhamento da VPC, consulte O que é emparelhamento de VPC? no Guia de emparelhamento da Amazon VPC.

É possível montar o sistema de arquivos de forma externa à VPC usando o endereço IP da interface de rede primária dele. A interface de rede primária é a primeira interface de rede retornada quando você executa o `aws fsx describe-file-systems` AWS CLI comando. Você também pode obter esse endereço IP no Console de Gerenciamento da Amazon Web Services.

A tabela a seguir ilustra os requisitos de endereço IP para acessar os sistemas de arquivos do Amazon FSx usando um cliente externo à VPC do sistema de arquivos.

Para clientes localizados em...	Acesso a sistemas de arquivos criados antes de 17 de dezembro de 2020	Acesso a sistemas de arquivos criados em ou após 17 de dezembro de 2020
VPCs emparelhadas usando o emparelhamento da VPC ou o AWS Transit Gateway	Clientes com endereços IP em um intervalo de endereços IP privados do RFC 1918:	✓
Redes emparelhadas usando AWS Direct Connect ou AWS VPN	• 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	✓

Se precisar acessar o sistema de arquivos do Amazon FSx criado antes de 17 de dezembro de 2020 usando um intervalo de endereços IP não privado, você poderá criar um novo sistema de arquivos ao restaurar um backup do sistema de arquivos. Para ter mais informações, consulte Trabalhar com backups.

Como recuperar o endereço IP da interface de rede primária para um sistema de arquivos

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação, escolha Sistemas de arquivos.
3. Escolha seu sistema de arquivos no painel.
4. Na página de detalhes do sistema de arquivos, escolha Rede e segurança.
5. Em Interface de rede, escolha o ID da sua interface de rede elástica primária. Fazer isso direciona você ao console do Amazon EC2.
6. Na guia Detalhes, encontre o endereço de IP IPv4 privado primário. Este é o endereço IP da sua interface de rede primária.

> **Note**
>
> Não é possível usar a resolução de nomes do Sistema de Nomes de Domínio (DNS) ao montar um sistema de arquivos do Amazon FSx externo à VPC à qual ele está associado.

Montagem do sistema de arquivos do Amazon FSx automaticamente

É possível atualizar o arquivo `/etc/fstab` na instância do Amazon EC2 depois de se conectar à instância pela primeira vez. Portanto, ela monte o sistema de arquivos do Amazon FSx sempre que for reinicializada.

Como usar /etc/fstab para montar o FSx para Lustre automaticamente

Para montar automaticamente o diretório do sistema de arquivos do Amazon FSx quando a instância do Amazon EC2 for reinicializada, você pode usar o arquivo `fstab`. O arquivo `fstab` contém informações sobre sistemas de arquivos. O comando `mount -a`, que é executado durante a inicialização da instância, monta os sistemas de arquivos listados no arquivo `fstab`.

> **Note**
>
> Antes de atualizar o arquivo `/etc/fstab` da sua instância do EC2, certifique-se de já ter criado o sistema de arquivos do Amazon FSx. Para obter mais informações, consulte Crie seu sistema de arquivos FSx for Lustre no exercício de Conceitos básicos.

Para atualizar o arquivo /etc/fstab em sua instância do EC2

1. Conecte-se à instância do EC2 e abra o arquivo `/etc/fstab` em um editor.
2. Adicione a linha a seguir ao arquivo `/etc/fstab`.

   Monte o sistema de arquivos do Amazon FSx para Lustre no diretório que você criou. Use o seguinte comando e substitua o seguinte:

   - Substitua *`/fsx`* pelo diretório no qual você deseja montar o sistema de arquivos do Amazon FSx.
   - Substitua *`file_system_dns_name`* pelo nome DNS real do sistema de arquivos.
   - Substitua *`mountname`* pelo nome da montagem do sistema de arquivos. Esse nome da montagem é retornado na resposta da operação de API `CreateFileSystem`. Também é retornado na resposta do describe-file-systems AWS CLI comando e na operação da `DescribeFileSystems` API.

   ```
   file_system_dns_name@tcp:/mountname /fsx lustre defaults,relatime,flock,_netdev,x-systemd.automount,x-systemd.requires=network.service 0 0
   ```

   > **Warning**
   >
   > Use a opção `_netdev`, que serve para identificar sistemas de arquivos de rede, ao montar o sistema de arquivos automaticamente. Se `_netdev` estiver ausente, a instância do EC2 poderá deixar de responder. Isso ocorre porque os sistemas de arquivos de rede precisam ser iniciados depois que a instância de computação inicia suas redes. Para ter mais informações, consulte A montagem automática falha e a instância não responde.

3. Salve a alteração no arquivo.

Agora, a instância do EC2 está configurada para montar o sistema de arquivos do Amazon FSx sempre que for reiniciada.

> **Note**
>
> Em alguns casos, a instância do Amazon EC2 pode precisar ser iniciada independentemente do status do sistema de arquivos do Amazon FSx montado. Nesses casos, adicione a opção `nofail` à entrada do sistema de arquivos no arquivo `/etc/fstab`.

Os campos na linha de código que você adicionou ao arquivo `/etc/fstab` fazem o seguinte:

Campo	Descrição
file_system_dns_name `@tcp:/`	O nome DNS do sistema de arquivos do Amazon FSx, que identifica o sistema de arquivos. Você pode obter esse nome no console ou programaticamente no ou em um AWS CLI AWS SDK.
mountname	O nome da montagem do sistema de arquivos. Você pode obter esse nome no console ou programaticamente AWS CLI usando o describe-file-systems comando ou a AWS API ou o SDK usando a operação. `DescribeFileSystems`
/fsx	O ponto de montagem para o sistema de arquivos do Amazon FSx na instância do EC2.
`lustre`	O tipo de sistema de arquivos, no caso, Amazon FSx.
`mount options`	As opções de montagem para o sistema de arquivos, apresentadas como uma lista separada por vírgulas das seguintes opções: • `defaults`: este valor informa ao sistema operacional para usar as opções de montagem padrão. É possível listar as opções de montagem padrão após a montagem do sistema de arquivos ao visualizar a saída do comando `mount`. • `relatime`: esta opção mantém os dados de `atime` (horários de acesso de inodes), mas não para cada vez que um arquivo é acessado. Com esta opção habilitada, os dados de `atime` serão

Campo	Descrição
	gravados para o disco somente se o arquivo tiver sido modificad o desde a última atualização dos dados de `atime` (`mtime`) ou se o arquivo tiver sido acessado pela última vez há mais tempo do que um determinado período (um dia por padrão). Se você deseja desativar as atualizações relacionadas aos horários de acesso de inodes, use a opção de montagem `noatime`. • `flock`: monta o sistema de arquivos com o bloqueio de arquivos habilitado. Se você não quiser que o bloqueio de arquivos seja ativado, use a opção de `noflock` montagem. • `_netdev`: o valor informa ao sistema operacional que o sistema de arquivos reside em um dispositivo que requer acesso à rede. Essa opção impede que a instância monte o sistema de arquivos até que a rede seja ativada no cliente.
`x-systemd .automount,x- systemd.requir es=networ k.service`	Essas opções garantem que o montador automático não seja executado até que a conectividade de rede esteja on-line. **Note** Para o Ubuntu 22.04, use a opção `x-systemd.requires =systemd-networkd-wait-online.service` em vez da opção `x-systemd.requires=network. service` .
`0`	Um valor que indica se o backup do sistema de arquivos deve ser submetido a um backup por `dump`. Para o Amazon FSx, esse valor deve ser `0`.
`0`	Um valor que indica a ordem na qual `fsck` verifica os sistemas de arquivos na inicialização. Para sistemas de arquivos do Amazon FSx, esse valor deve ser `0` para indicar que `fsck` não deve ser executado na inicialização.

Montagem de conjuntos de arquivos específicos

Ao usar o recurso de conjunto de arquivos do Lustre, é possível montar somente um subconjunto do namespace do sistema de arquivos, que é chamado de conjunto de arquivos. Para montar um conjunto de arquivos do sistema de arquivos, você especifica o caminho do subdiretório após o nome do sistema de arquivos no cliente. Uma montagem de conjunto de arquivos (também chamada de montagem de subdiretório) limita a visibilidade do namespace do sistema de arquivos em um cliente específico.

Exemplo: montagem de um conjunto de arquivos do Lustre

1. Suponha que você tenha um sistema de arquivos do FSx para Lustre com os seguintes diretórios:

   ```
   team1/dataset1/
   team2/dataset2/
   ```

2. Você monta somente o conjunto de arquivos `team1/dataset1`, tornando apenas esta parte do sistema de arquivos visível localmente no cliente. Use o seguinte comando e substitua os seguintes itens:

   - Substitua *`file_system_dns_name`* pelo nome DNS real do sistema de arquivos.
   - Substitua *`mountname`* pelo nome da montagem do sistema de arquivos. Esse nome da montagem é retornado na resposta da operação de API `CreateFileSystem`. Também é retornado na resposta do describe-file-systems AWS CLI comando e na operação da DescribeFileSystemsAPI.

   ```
   mount -t lustre file_system_dns_name@tcp:/mountname/team1/dataset1 /fsx
   ```

Ao usar o recurso de conjunto de arquivos do Lustre, lembre-se do seguinte:

- Não há restrições que impeçam um cliente de remontar o sistema de arquivos usando um conjunto de arquivos diferente ou nenhum conjunto de arquivos.
- Ao usar um conjunto de arquivos, alguns comandos administrativos do Lustre que requerem acesso ao diretório `.lustre/` podem não funcionar, como o comando `lfs fid2path`.

- Se você planeja montar diversos subdiretórios usando o mesmo sistema de arquivos no mesmo host, esteja ciente de que isso consome mais recursos do que um único ponto de montagem e, em vez disso, pode ser mais eficiente montar o diretório raiz do sistema de arquivos somente uma vez.

Para obter mais informações sobre o recurso de conjunto de arquivos do Lustre, consulte o Lustre Operations Manual no site de documentação do Lustre.

Desmontagem de sistemas de arquivos

Antes de excluir um sistema de arquivos, recomendamos desmontá-lo de todas as instâncias do Amazon EC2 às quais ele está conectado. Você pode desmontar um sistema de arquivos em sua instância do Amazon EC2 executando o comando `umount` na instância em si. Você não pode desmontar um sistema de arquivos Amazon FSx por meio do, AWS CLI AWS Management Console do ou por meio de nenhum dos AWS SDKs. Para desmontar um sistema de arquivos do Amazon FSx conectado a uma instância do Amazon EC2 que executa o Linux, use o comando `umount` da seguinte maneira:

```
umount /mnt/fsx
```

Recomendamos não especificar nenhuma outra opção `umount`. Evite configurar quaisquer outras opções `umount` que sejam diferentes dos valores padrão.

Você pode verificar se o sistema de arquivos do Amazon FSx foi desmontado ao executar o comando `df`. Este comando exibe as estatísticas de uso do disco para os sistemas de arquivos que estão montados na instância do Amazon EC2 baseada em Linux. Se o sistema de arquivos do Amazon FSx que você deseja desmontar não estiver listado na saída do comando `df`, isso significa que ele está desmontado.

Example : identificação do status de montagem de um sistema de arquivos do Amazon FSx e desmontagem

```
$ df -T
Filesystem Type 1K-blocks Used Available Use% Mounted on
file-system-id.fsx.aws-region.amazonaws.com@tcp:/mountname /fsx 3547708416 61440
 3547622400 1% /fsx
      /dev/sda1 ext4 8123812 1138920 6884644 15% /
```

```
$ umount /fsx
```

```
$ df -T
```

```
Filesystem Type 1K-blocks Used Available Use% Mounted on
/dev/sda1 ext4 8123812 1138920 6884644 15% /
```

Como trabalhar com instâncias spot do Amazon EC2

O FSx para Lustre pode ser usado com instâncias spot do EC2 para reduzir significativamente os custos do Amazon EC2. Uma instância spot é uma instância do EC2 não usada que está disponível por um valor mais baixo que o preço sob demanda. O Amazon EC2 pode interromper a instância spot quando o preço spot exceder o preço máximo, quando a demanda por instâncias spot aumentar ou quando a disponibilização de instâncias spot diminuir.

Quando o Amazon EC2 interrompe uma instância spot, ele fornece um aviso de interrupção de instância spot, enviando à instância um aviso de dois minutos antes que o Amazon EC2 a interrompa. Para obter mais informações, consulte Instâncias spot no Guia do usuário do Amazon EC2 para instâncias do Linux.

Para garantir que os sistemas de arquivos do Amazon FSx não sejam afetados pelas interrupções de instâncias spot do EC2, recomendamos desmontar os sistemas de arquivos do Amazon FSx antes de encerrar ou hibernar as instâncias spot do EC2. Para ter mais informações, consulte Desmontagem de sistemas de arquivos.

Como lidar com interrupções de instâncias spot do Amazon EC2

O FSx para Lustre é um sistema de arquivos distribuído no qual as instâncias do servidor e do cliente cooperam para disponibilizar um sistema de arquivos confiável e com alta performance. É mantido um estado distribuído e coerente nas instâncias do cliente e do servidor. Os servidores FSx para Lustre delegam permissões de acesso temporário aos clientes enquanto eles estão ativamente realizando E/S e armazenando em cache os dados do sistema de arquivos. Espera-se que os clientes respondam em um curto período quando os servidores solicitarem a revogação das permissões de acesso temporário. Para proteger o sistema de arquivos contra clientes com comportamentos inadequados, os servidores podem realizar a remoção dos clientes Lustre que não responderem após alguns minutos. Para evitar aguardar vários minutos até que um cliente que não responde envie uma resposta à solicitação do servidor, é importante desmontar corretamente os clientes Lustre, especialmente antes de encerrar as instâncias spot do EC2.

O spot do EC2 envia avisos de encerramento com dois minutos de antecedência antes de encerrar uma instância. Recomendamos automatizar o processo de desmontagem correta para clientes Lustre antes de encerrar as instâncias spot do EC2.

Example : script para desmontar corretamente as instâncias spot do EC2 que estão sendo encerradas

Este script de exemplo desmonta corretamente as instâncias spot do EC2 que estão sendo encerradas ao realizar o seguinte:

- Prestar atenção aos avisos de encerramento do spot.
- Quando receber um aviso de encerramento:
  - Interromper as aplicações que acessam o sistema de arquivos.
  - Desmontar o sistema de arquivos antes que a instância seja encerrada.

É possível adaptar o script conforme necessário, especialmente para encerrar a aplicação normalmente. Para obter mais informações sobre as práticas recomendadas para lidar com interrupções de instâncias spot, consulte Best practices for handling EC2 Spot Instance interruptions.

```
#!/bin/bash

# TODO: Specify below the FSx mount point you are using
*FSXPATH=/fsx*

cd /

TOKEN=$(curl -s -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600")
if [ "$?" -ne 0 ]; then
    echo "Error running 'curl' command" >&2
    exit 1
fi

# Periodically check for termination
while sleep 5
do

    HTTP_CODE=$(curl -H "X-aws-ec2-metadata-token: $TOKEN" -s -w %{http_code} -o /dev/
null http://169.254.169.254/latest/meta-data/instance-action)

    if [[ "$HTTP_CODE" -eq 401 ]] ; then
```

```
        # Refreshing Authentication Token
        TOKEN=$(curl -s -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 30")
        continue
    elif [[ "$HTTP_CODE" -ne 200 ]] ; then
        # If the return code is not 200, the instance is not going to be interrupted
        continue
    fi

    echo "Instance is getting terminated. Clean and unmount '$FSXPATH' ..."
    curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-
data/instance-action
    echo

    # Gracefully stop applications accessing the filesystem
    #
    # TODO*: Replace with the proper command to stop your application if possible*

    # Kill every process still accessing Lustre filesystem
    echo "Kill every process still accessing Lustre filesystem..."
    fuser -kMm -TERM "${FSXPATH}"; sleep 2
    fuser -kMm -KILL "${FSXPATH}"; sleep 2

    # Unmount FSx For Lustre filesystem
    if ! umount -c "${FSXPATH}"; then
        echo "Error unmouting '$FSXPATH'. Processes accessing it:" >&2
        lsof "${FSXPATH}"

        echo "Retrying..."
        continue
    fi

    # Start a graceful shutdown of the host
    shutdown now

done
```

Como administrar sistemas de arquivos

O FSx para Lustre disponibiliza um conjunto de recursos que simplificam a performance de suas tarefas administrativas. Isso inclui a capacidade de fazer point-in-time backups, gerenciar cotas de armazenamento do sistema de arquivos, gerenciar sua capacidade de armazenamento e taxa de transferência, gerenciar a compactação de dados e definir janelas de manutenção para a execução de patches de software de rotina no sistema.

Você pode administrar seus sistemas de arquivos FSx for Lustre usando o Amazon FSx Management Console, (AWS Command Line Interface)AWS CLI, a API Amazon FSx ou SDKs. AWS

Tópicos

Trabalhar com backups

Com o Amazon FSx para Lustre, você pode fazer backups diários automáticos e backups iniciados pelo usuário de sistemas de arquivos persistentes que não estão vinculados a um repositório de dados durável do Amazon S3. Os backups do Amazon FSx são file-system-consistent altamente duráveis e incrementais. Para garantir alta durabilidade, o Amazon FSx para Lustre armazena backups no Amazon Simple Storage Service (Amazon S3) com durabilidade de 99.999999999% (11 9's) .

Os backups do sistema de arquivos do FSx para Lustre são incrementais e baseados em blocos, quer sejam gerados usando o backup diário automático ou o recurso de backup iniciado pelo

usuário. Isso significa que, quando você faz um backup, o Amazon FSx compara os dados do seu sistema de arquivos com o backup anterior no nível do bloco. Em seguida, o Amazon FSx armazena no novo backup uma cópia de todas as alterações no nível do bloco. Os dados no nível do bloco que permanecem inalterados desde o backup anterior não são armazenados no novo backup. A duração do processo de backup depende da quantidade de dados que foram alterados desde a realização do último backup e é independente da capacidade de armazenamento do sistema de arquivos. A lista a seguir ilustra os tempos de backup em diferentes circunstâncias:

- O backup inicial de um sistema de arquivos totalmente novo com poucos dados leva minutos para ser concluído.
- O backup inicial de um sistema de arquivos totalmente novo feito após o carregamento de TBs de dados leva horas para ser concluído.
- Um segundo backup feito do sistema de arquivos com TBs de dados e alterações mínimas dos dados no nível de bloco (relativamente poucas criações/modificações) leva segundos para ser concluído.
- Um terceiro backup do mesmo sistema de arquivos após a adição e modificação de uma grande quantidade de dados leva horas para ser concluído.

Ao excluir um backup, somente os dados exclusivos desse backup serão removidos. Cada backup do FSx for Lustre contém todas as informações necessárias para criar um novo sistema de arquivos a partir do backup, point-in-time restaurando efetivamente um instantâneo do sistema de arquivos.

Criar backups regulares do sistema de arquivos é uma melhor prática que complementa a replicação que o Amazon FSx para Lustre faz do sistema de arquivos. Os backups do Amazon FSx ajudam a atender às suas necessidades de retenção e conformidade de backup. Trabalhar com backups do Amazon FSx para Lustre é fácil, seja para criar backups, copiar um backup, restaurar um sistema de arquivos usando um backup ou excluir um backup.

Não há suporte para backups em sistemas de arquivos transitórios porque esses sistemas são projetados para armazenamento temporário e para processamento de dados de prazo mais curto. Não há suporte para backups nos sistemas de arquivos vinculados a um bucket do Amazon S3 porque o bucket do S3 serve como repositório de dados primário, e o sistema de arquivos do Lustre não necessariamente contém o conjunto de dados completo em qualquer momento determinado.

Tópicos

- Como trabalhar com backups iniciados pelo usuário
- Como usar o AWS Backup com o Amazon FSx
- Copiar backups
- Copiando backups dentro do mesmo Conta da AWS
- Como restaurar backups
- Excluir backups

Suporte de backup no FSx para Lustre

Só há suporte para backups em sistemas de arquivos persistentes do FSx para Lustre que não estão vinculados a um repositório de dados do Amazon S3.

O Amazon FSx não oferece suporte para backups em sistemas de arquivos transitórios porque esses sistemas são projetados para armazenamento temporário e para processamento de dados de prazo mais curto. O Amazon FSx não oferece suporte para backups nos sistemas de arquivos vinculados a um bucket do Amazon S3 porque o bucket do S3 serve como repositório de dados primário, e o sistema de arquivos não necessariamente contém o conjunto de dados completo em qualquer momento determinado. Para obter mais informações, consulte Como usar repositórios de dados e Opções de implantação para sistemas de arquivos.

Como trabalhar com backups diários automáticos

O Amazon FSx para Lustre pode fazer um backup diário automático do sistema de arquivos. Esses backups diários automáticos ocorrem durante a janela de backup diário estabelecida quando você criou o sistema de arquivos. Em algum momento durante a janela de backup diário, as E/S de armazenamento podem ser suspensas brevemente enquanto o processo de backup é inicializado (geralmente, durante alguns segundos). Ao escolher sua janela de backup diário, recomendamos que seja uma hora do dia conveniente. O ideal é que esse horário esteja fora do horário normal de funcionamento das aplicações que usam o sistema de arquivos.

Os backups diários automáticos são mantidos por um determinado período, conhecido como período de retenção. Você pode definir o período de retenção entre zero e noventa dias. Definir o período de retenção como zero dia desativa os backups diários automáticos. O período de retenção padrão para backups diários automáticos é de 0 dia. Os backups diários automáticos são excluídos quando o sistema de arquivos é excluído.

> **Note**
>
> Definir o período de retenção como zero dia significa que o backup do sistema de arquivos nunca é realizado automaticamente. É altamente recomendável que você use backups diários automáticos para sistemas de arquivos que tenham qualquer nível de funcionalidade crítica associada a eles.

Você pode usar a AWS CLI ou um dos SDKs da AWS para alterar a janela de backup e o período de retenção de backup para seus sistemas de arquivos. Use a operação`UpdateFileSystem` da API ou o comando `update-file-system` da CLI.

Como trabalhar com backups iniciados pelo usuário

O Amazon FSx para Lustre permite que você faça backups manualmente dos seus sistemas de arquivos a qualquer momento. Você pode fazer isso usando o console do Amazon FSx para Lustre, a API ou a AWS Command Line Interface (CLI). Os backups iniciados pelo usuário dos sistemas de arquivos do Amazon FSx nunca expiram e ficam disponíveis pelo tempo que você quiser mantê-los. Os backups iniciados pelo usuário são mantidos mesmo depois de você excluir o sistema de arquivos do qual foi feito o backup. Você só pode excluir backups iniciados pelo usuário usando o console, a API ou a CLI do Amazon FSx para Lustre, e eles nunca serão excluídos automaticamente pelo Amazon FSx. Para ter mais informações, consulte Excluir backups.

Como criar backups iniciados pelo usuário

O procedimento a seguir orienta você sobre como criar um backup iniciado pelo usuário no console do Amazon FSx para um sistema de arquivos existente.

Criar um backup do sistema de arquivos iniciado pelo usuário

1. Abra o console do Amazon FSx para Lustre em https://console.aws.amazon.com/fsx/.
2. No painel do console, escolha o nome do sistema de arquivos do qual deseja fazer backup.
3. Em Ações, escolha Criar backup.
4. Na caixa de diálogo Criar backup que é aberta, forneça um nome para o backup. Os nomes de backup podem ter no máximo 256 caracteres Unicode, incluindo letras, espaço em branco, números e os caracteres especiais . + - = _ : /
5. Escolha Create backup.

Agora você criou o backup do sistema de arquivos. Você pode encontrar uma tabela de todos os backups no console do Amazon FSx para Lustre ao escolher Backups na navegação do lado esquerdo. Você pode pesquisar pelo nome que deu ao backup e pelos filtros da tabela para mostrar apenas os resultados correspondentes.

Quando você cria um backup iniciado pelo usuário conforme descrito neste procedimento, ele tem o tipo `USER_INITIATED` e o status Criando enquanto o Amazon FSx cria o backup. O status muda para Transferindo enquanto o backup é transferido para o Amazon S3, até que esteja totalmente disponível.

Como usar o AWS Backup com o Amazon FSx

O AWS Backup é uma maneira simples e econômica de proteger seus dados fazendo backup dos sistemas de arquivos do Amazon FSx. O AWS Backup é um serviço de backup unificado projetado para simplificar a criação, a cópia, a restauração e a exclusão de backups, além de fornecer relatórios e auditorias aprimorados. O AWS Backup facilita o desenvolvimento de uma estratégia de backup centralizada para fins de conformidade legal, regulatória e profissional. O AWS Backup também simplifica a proteção dos seus volumes de armazenamento, bancos de dados e sistemas de arquivos da AWS, fornecendo um local central no qual é possível fazer o seguinte:

- Configure e audite os recursos da AWS dos quais deseja fazer backup.
- Automatizar a programação de backups.
- Definir políticas de retenção.
- Fazer cópias de backups entre regiões da AWS e entre contas da AWS.
- Monitorar todas as atividades recentes de backup e restauração.

O AWS Backup usa a funcionalidade de backup integrada do Amazon FSx. Os backups feitos no console do AWS Backup têm o mesmo nível de consistência e performance do sistema de arquivos e as mesmas opções de restauração que os backups feitos por meio do console do Amazon FSx. Caso use o AWS Backup para gerenciar esses backups, você terá funcionalidades adicionais, como opções de retenção ilimitadas e a capacidade de criar backups programados com a frequência de até uma hora. Além disso, o AWS Backup mantém seus backups imutáveis mesmo após a exclusão do sistema de arquivos de origem. Isso ajuda na proteção contra exclusões acidentais ou mal-intencionadas.

Os backups feitos pelo AWS Backup são considerados backups iniciados pelo usuário e fazem parte da cota de backups iniciados pelo usuário do Amazon FSx. Você pode visualizar e restaurar backups

feitos pelo AWS Backup no console do Amazon FSx, na CLI e na API. Os backups criados pelo AWS Backup têm o tipo de backup `AWS_BACKUP`. No entanto, você não pode excluir os backups feitos pelo AWS Backup no console do Amazon FSx, na CLI ou na API. Para obter mais informações sobre como usar o AWS Backup para fazer backup dos sistemas de arquivos do Amazon FSx, consulte Como trabalhar com sistemas de arquivos do Amazon FSx no Guia do desenvolvedor do AWS Backup.

Copiar backups

Você pode usar o Amazon FSx para copiar manualmente os backups dentro da mesma conta da AWS para outra região da AWS (cópias entre regiões) ou dentro da mesma região da AWS (cópias dentro da região). Você só pode fazer cópias entre regiões dentro da mesma partição da AWS. É possível criar cópias de backup iniciadas pelo usuário usando o console do Amazon FSx, a AWS CLI ou a API. Quando você cria uma cópia de backup iniciada pelo usuário, ela é do tipo `USER_INITIATED`.

Você também pode usar o AWS Backup para copiar backups entre regiões da AWS e entre contas da AWS. O AWS Backup é um serviço de gerenciamento de backup totalmente gerenciado que oferece uma interface central para planos de backup baseados em políticas. Com o gerenciamento entre contas, você pode usar automaticamente as políticas de backup para aplicar planos de backup em todas as contas da sua organização.

As cópias de backup entre regiões são particularmente valiosas para a recuperação de desastres entre regiões. Você faz backups e os copia para outra região da AWS para que, no caso de um desastre na região principal da AWS, você possa restaurar pelo backup e recuperar a disponibilidade rapidamente na outra região da AWS. Você também pode usar cópias de backup para clonar seu conjunto de dados de arquivos para outra região da AWS ou dentro da mesma região da AWS. Você faz cópias de backup dentro da mesma conta da AWS (entre regiões ou dentro da região) usando o console do Amazon FSx, a AWS CLI, ou a API do Amazon FSx para Lustre. Você também pode usar o AWS Backup para fazer cópias de backup, sob demanda ou com base em políticas.

As cópias de backup entre contas são valiosas para atender aos requisitos de conformidade regulatória para a cópia de backups em uma conta isolada. Elas também fornecem uma camada adicional de proteção de dados para ajudar a evitar exclusões acidentais ou mal-intencionadas de backups, perda de credenciais ou comprometimento de chaves AWS KMS. Os backups entre contas oferecem suporte a fan-in (cópia de backups de várias contas primárias para uma conta de cópia de backup isolada) e fan-out (cópia de backups de uma conta primária para várias contas de cópia de backup isoladas).

Você pode fazer cópias de backup entre contas usando o AWS Backup com suporte do AWS Organizations. Os limites da conta para cópias entre contas são definidos por políticas do AWS Organizations. Para obter mais informações sobre o uso do AWS Backup para fazer cópias de backup entre contas, consulte Criação de cópias de backup entre Contas da AWS no Guia do desenvolvedor do AWS Backup.

Limitações de cópias de backup

Veja abaixo algumas limitações quando você copia backups:

- Cópias de backup entre regiões são suportadas somente entre quaisquer duas regiões comerciaisRegiões da AWS, entre as regiões da China (Pequim) e China (Ningxia) e entre as regiões AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA), mas não entre esses conjuntos de regiões.
- Não há suporte para cópias de backup entre regiões nas regiões de aceitação.
- Você pode fazer cópias de backup dentro da região em qualquer região da AWS.
- O backup de origem deve ter o status `AVAILABLE` para que você possa copiá-lo.
- Não será possível excluir um backup de origem se ele estiver sendo copiado. Pode haver um pequeno atraso entre o momento em que o backup de destino fica disponível e o momento em que você tem permissão para excluir o backup de origem. Leve em consideração esse atraso se tentar excluir novamente um backup de origem.
- É possível ter até cinco solicitações de cópia de backup em andamento para uma única região da AWS de destino por conta.

Permissões para cópias de backup entre regiões

Você usa uma declaração de política do IAM para conceder permissões para executar uma operação de cópia de backup. Para se comunicar com a região da AWS de origem e solicitar uma cópia de backup entre regiões, o solicitante (perfil do IAM ou usuário do IAM) deve ter acesso ao backup de origem e à região da AWS de origem.

Você usa a política para conceder permissões à ação `CopyBackup` para a operação de cópia de backup. Você especifica a ação no campo `Action` da política e especifica o valor do recurso no campo `Resource` da política, como no exemplo a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111122223333:backup/*"
        }
    ]
}
```

Para obter mais informações sobre as políticas do IAM, consulte Políticas e permissões no IAM no Guia do usuário do IAM.

Cópias completas e incrementais

Quando você copia um backup em um backup Região da AWS diferente do de origem, a primeira cópia é uma cópia de backup completa. Após a primeira cópia de backup, todas as cópias subsequentes para a mesma região de destino dentro da mesma conta da AWS serão incrementais, desde que você não tenha excluído todos os backups copiados anteriormente nessa região e esteja usando a mesma chave do AWS KMS. Se ambas as condições não forem atendidas, a operação de cópia resultará em uma cópia de backup completa (não incremental).

Copiando backups dentro do mesmo Conta da AWS

Você pode copiar backups dos sistemas de arquivos FSx for Lustre usando AWS Management Console a CLI e a API, conforme descrito nos procedimentos a seguir.

Copiar um backup dentro da mesma conta (entre regiões ou dentro da região) usando o console

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação, selecione Backups.
3. Na tabela Backups, escolha o backup que você deseja copiar e, em seguida, selecione Copiar backup.
4. Na seção Configurações, faça o seguinte:

    - Na lista Região de destino, escolha uma região da AWS de destino para a qual copiar o backup. O destino pode estar em outra região da AWS (cópia entre regiões) ou na mesma região da AWS (cópia dentro da região).
    - (Opcional) Selecione Copiar tags para copiar tags do backup de origem para o backup de destino. Se você selecionar Copiar tags e também adicionar tags na etapa 6, todas as tags serão mescladas.

5. Em Criptografia, escolha a chave de criptografia do AWS KMS para criptografar o backup copiado.
6. Em Tags: opcional, insira uma chave e um valor para adicionar tags ao backup copiado. Se você adicionar tags aqui e também tiver selecionado Copiar tags na etapa 4, todas as tags serão mescladas.
7. Selecione Copy backup (Copiar backup).

   Seu backup é copiado dentro do mesmo Conta da AWS para o selecionadoRegião da AWS.

Copiar um backup dentro da mesma conta (entre regiões ou dentro da região) usando a CLI

- Use o comando `copy-backup` CLI ou a operação da CopyBackupAPI para copiar um backup na mesma AWS conta, em uma AWS região ou em uma AWS região.

  O comando a seguir copia um backup com um ID de `backup-0abc123456789cba7` da região `us-east-1`.

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  A resposta mostra a descrição do backup copiado.

  Você pode visualizar seus backups no console Amazon FSx ou programaticamente usando o comando `describe-backups` CLI ou a operação da API. DescribeBackups

Como restaurar backups

Você pode usar um backup disponível para criar um novo sistema de arquivos, restaurando efetivamente um point-in-time instantâneo de outro sistema de arquivos. Você pode restaurar um backup usando o console, a AWS CLI ou um dos SDKs da AWS. A restauração de um backup em um novo sistema de arquivos leva o mesmo tempo que a criação de um novo sistema de arquivos. Os dados restaurados do backup são carregados lentamente no sistema de arquivos, e durante esse tempo você perceberá uma latência um pouco maior.

O procedimento a seguir apresenta instruções sobre como restaurar um backup usando o console para criar um novo sistema de arquivos.

> **Note**
>
> Você só pode restaurar seu backup em um sistema de arquivos do mesmo tipo de versão do Lustre, tipo de implantação, throughput por unidade de armazenamento, capacidade de armazenamento, tipo de compactação de dados e a região da AWS do original. Você poderá aumentar a capacidade de armazenamento do sistema de arquivos restaurado depois que ele estiver disponível. Para ter mais informações, consulte Como gerenciar a capacidade de armazenamento.

Restaurar um sistema de arquivos de um backup

1. Abra o console do Amazon FSx para Lustre em https://console.aws.amazon.com/fsx/.
2. No painel do console, escolha Backups na navegação do lado esquerdo.
3. Escolha o backup que você deseja restaurar na tabela Backups e, em seguida, selecione Restaurar backup.

   Isso abre o assistente de criação do sistema de arquivos. Esse assistente é idêntico ao assistente de criação de sistema de arquivos padrão, exceto a configuração do sistema de arquivos (por exemplo, tipo de implantação, throughput por unidade de armazenamento). No entanto, você pode alterar a VPC e as configurações de backup associadas.
4. Conclua o assistente da forma como você faz quando cria um novo sistema de arquivos.
5. Selecione Review and create.
6. Analise as configurações escolhidas para o sistema de arquivos do Amazon FSx para Lustre e, em seguida, escolha Criar sistema de arquivos.

Você restaurou por meio de um backup e um novo sistema de arquivos agora está sendo criado. Quando seu status mudar para `AVAILABLE`, você poderá usar o sistema de arquivos normalmente.

Excluir backups

A exclusão de um backup é uma ação permanente e irrecuperável. Todos os dados em um backup excluído também são excluídos. Não exclua um backup, a menos que tenha certeza de que não precisará dele novamente no futuro. Você não pode excluir backups feitos pelo AWS Backup no console do Amazon FSx, na CLI ou na API.

Para excluir um backup

1. Abra o console do Amazon FSx para Lustre em https://console.aws.amazon.com/fsx/.
2. No painel do console, escolha Backups na navegação do lado esquerdo.
3. Escolha o backup que você deseja excluir da tabela Backups e, em seguida, escolha Excluir backup.
4. Na caixa de diálogo Excluir backups que é aberta, confirme se o ID do backup identifica o backup que você deseja excluir.
5. Confirme se a caixa de seleção do backup que deseja excluir está marcada.
6. Escolha Excluir backups.

Seu backup e todos os dados incluídos agora são excluídos de forma permanente e irrecuperável.

Cotas de armazenamento

É possível criar cotas de armazenamento para usuários, grupos e projetos em sistemas de arquivos do FSx para Lustre. Com as cotas de armazenamento, você pode limitar a quantidade de espaço em disco e o número de arquivos que um usuário, grupo ou projeto pode consumir. As cotas de armazenamento rastreiam automaticamente o uso em nível de usuário, de grupo e de projeto para que você possa monitorar o consumo, independentemente de definir ou não limites de armazenamento.

O Amazon FSx aplica cotas e evita que os usuários que as excederam realizem gravações no espaço de armazenamento. Quando os usuários excedem as cotas, eles devem excluir arquivos suficientes para retornar abaixo dos limites de cota com a finalidade de que possam realizar gravações no sistema de arquivos novamente.

Tópicos

Aplicação de cotas

A aplicação de cotas para usuários, grupos e projetos é habilitada automaticamente em todos os sistemas de arquivos do FSx para Lustre. Não é possível desabilitar a aplicação de cotas.

Tipos de cotas

Os administradores do sistema com credenciais de usuário raiz da AWS conta podem criar os seguintes tipos de cotas:

- Uma cota de usuário se aplica a um usuário individual. Uma cota de usuário para um determinado usuário pode ser diferente das cotas de outros usuários.
- Uma cota de grupo se aplica a todos os usuários que são membros de um grupo específico.
- Uma cota de projeto se aplica a todos os arquivos ou os diretórios associados a um projeto. Um projeto pode incluir diversos diretórios ou arquivos individuais localizados em diretórios diferentes dentro de um sistema de arquivos.

  > **Note**
  >
  > As cotas de projeto são suportadas somente na versão 2.15 do Lustre nos sistemas de arquivos FSx for Lustre.

- Uma cota de bloqueio limita a quantidade de espaço em disco que um usuário, um grupo ou um projeto pode consumir. O tamanho do armazenamento é configurado em kilobytes.
- Uma cota de inode limita o número de arquivos ou de diretórios que um usuário, um grupo ou um projeto pode criar. O número máximo de inodes é configurado como um número inteiro.

> **Note**
>
> Não há suporte para as cotas padrão.

Se você definir cotas para um usuário e um grupo específicos, e o usuário for membro desse grupo, o uso de dados por parte do usuário se aplicará a ambas as cotas. O uso também é limitado por ambas as cotas. Se um dos limites de cota for atingido, o usuário será impedido de realizar gravações no sistema de arquivos.

> **Note**
>
> As cotas definidas para o usuário raiz não são aplicadas. De forma semelhante, a gravação de dados como usuário raiz usando o comando `sudo` ignora a aplicação da cota.

Limites de cotas e períodos de carência

O Amazon FSx aplica cotas de usuários, de grupos e de projetos como um limite rígido ou flexível com um período de carência configurável.

O limite rígido corresponde ao limite absoluto. Se os usuários excederem o limite rígido, um bloqueio ou uma alocação de inodes falha e eles recebem uma mensagem Disk quota exceeded. Os usuários que atingiram o limite rígido de cota devem excluir arquivos ou diretórios suficientes para retornar abaixo do limite de cota antes que eles possam realizar gravações no sistema de arquivos novamente. Quando um período de carência é definido, os usuários podem exceder o limite flexível dentro do período de carência se este limite estiver abaixo do limite rígido.

Para limites flexíveis, você configura um período de carência em segundos. O limite flexível deve ser inferior ao limite rígido.

É possível definir diferentes períodos de carência para cotas de inodes e de bloqueios. Além disso, você pode definir diferentes períodos de carência para uma cota de usuário, uma cota de grupo e uma cota de projeto. Quando as cotas de usuário, de grupo e de projeto têm períodos de carência diferentes, o limite flexível se transforma em um limite rígido após a expiração do período de carência de qualquer uma dessas cotas.

Quando os usuários excedem um limite flexível, o Amazon FSx permite que eles continuem excedendo a cota até que o período de carência expire ou até que o limite rígido seja atingido. Após a expiração do período de carência, o limite flexível é convertido em um limite rígido e os usuários são bloqueados de qualquer operação de gravação adicional até que o uso de armazenamento retorne abaixo dos limites definidos para a cota de bloqueio ou para a cota de inode. Os usuários não recebem uma notificação ou um aviso quando o período de carência começa.

Definição e visualização de cotas

Você define cotas de armazenamento usando comandos `lfs` do sistema de arquivos do Lustre em seu terminal do Linux. O comando `lfs setquota` define os limites de cotas e o comando `lfs quota` exibe as informações relacionadas às cotas.

Para obter mais informações sobre os comandos de cotas do Lustre, consulte Manual de operações do Lustre no site de documentação do Lustre.

Definição de cotas de usuário, de grupo e de projeto

A sintaxe do comando `setquota` para definir cotas de usuário, de grupo ou de projeto é semelhante à apresentada a seguir.

```
lfs setquota {-u|--user|-g|--group|-p|--project} username|groupname|projectid
             [-b block_softlimit] [-B block_hardlimit]
             [-i inode_softlimit] [-I inode_hardlimit]
             /mount_point
```

Em que:

- `-u` ou `--user` especifica um usuário para o qual uma cota será definida.
- `-g` ou `--group` especifica um grupo para o qual uma cota será definida.
- `-p` ou `--project` especifica um projeto para o qual uma cota será definida.
- `-b` define uma cota de bloqueio com um limite flexível. `-B` define uma cota de bloqueio com um limite rígido. Tanto o *`block_softlimit`* quando o *`block_hardlimit`* são expressos em kilobytes, e o valor mínimo é 1.024 KB.
- `-i` define uma cota de inode com um limite flexível. `-I` define uma cota de inode com um limite rígido. Tanto o *`inode_softlimit`* quanto o *`inode_hardlimit`* são expressos em número de inodes, e o mínimo o valor é 1.024 inodes.
- *`mount_point`* corresponde ao diretório no qual o sistema de arquivos foi montado.

Exemplo de cota de usuário: o comando apresentado a seguir define um limite de bloqueio flexível de 5.000 KB, um limite de bloqueio rígido de 8.000 KB, um limite de inode flexível de dois mil e uma cota de limite de inode rígido de três mil para `user1` no sistema de arquivos montado em `/mnt/fsx`.

```
sudo lfs setquota -u user1 -b 5000 -B 8000 -i 2000 -I 3000 /mnt/fsx
```

Exemplo de cota de grupo: o comando apresentado a seguir define um limite de bloqueio rígido de 100.000 KB para o grupo chamado `group1` no sistema de arquivos montado em `/mnt/fsx`.

```
sudo lfs setquota -g group1 -B 100000 /mnt/fsx
```

Exemplo de cota de projeto: primeiro, é necessário se certificar de que você usou o comando `project` para associar os arquivos e os diretórios desejados ao projeto. Por exemplo, o comando apresentado a seguir associa todos os arquivos e os subdiretórios do diretório `/mnt/fsxfs/dir1` ao projeto cujo ID do projeto é `100`.

```
sudo lfs project -p 100 -r -s /mnt/fsxfs/dir1
```

Em seguida, use o comando `setquota` para definir a cota de projeto. O comando apresentado a seguir define um limite de bloqueio flexível de 307.200 KB, um limite de bloqueio rígido de 309.200 KB, um limite de inode flexível de dez mil e uma cota de limite de inode rígido de onze mil para o projeto `250` no sistema de arquivos montado em `/mnt/fsx`.

```
sudo lfs setquota -p 250 -b 307200 -B 309200 -i 10000 -I 11000 /mnt/fsx
```

Definição de períodos de carência

O período de carência padrão é de uma semana. É possível ajustar o período de carência padrão para usuários, grupos ou projetos usando a sintaxe apresentada a seguir.

```
lfs setquota -t {-u|-g|-p}
             [-b block_grace]
             [-i inode_grace]
             /mount_point
```

Em que:

- `-t` indica que um período de carência será definido.
- `-u` define um período de carência para todos os usuários.
- `-g` define um período de carência para todos os grupos.
- `-p` define um período de carência para todos os projetos.
- `-b` define um período de carência para as cotas de bloqueio. `-i` define um período de carência para as cotas de inode. Tanto *`block_grace`* quanto *`inode_grace`* são expressos em segundos inteiros ou no formato `XXwXXdXXhXXmXXs`.
- *`mount_point`* corresponde ao diretório no qual o sistema de arquivos foi montado.

O comando apresentado a seguir define períodos de carência de mil segundos para as cotas de bloqueio do usuário e de uma semana e quatro dias para as cotas de inode do usuário.

```
sudo lfs setquota -t -u -b 1000 -i 1w4d /mnt/fsx
```

Visualização de cotas

O comando `quota` exibe informações sobre cotas de usuário, cotas de grupo, cotas de projeto e períodos de carência.

Visualização do comando de cotas	Informações exibidas sobre as cotas
`lfs quota /mount_point`	Informações gerais sobre a cota (por exemplo, uso do disco e limites) para o usuário que executa o comando e o grupo principal do usuário.
`lfs quota -u username /mount_point`	Informações gerais sobre a cota para um usuário específico. Usuários com credenciais de usuário raiz da AWS conta podem executar esse comando para qualquer usuário, mas usuários não root não podem executar esse comando para obter informações de cotas sobre outros usuários.
`lfs quota -u username -v /mount_point`	Informações gerais sobre a cota para um usuário específico e estatísticas detalhadas sobre a cota para cada destino de armazenamento de objetos (OST) e destino de metadados (MDT). Usuários com credenciais de usuário raiz da AWS conta podem

Visualização do comando de cotas	Informações exibidas sobre as cotas
	executar esse comando para qualquer usuário, mas usuários não root não podem executar esse comando para obter informações de cotas sobre outros usuários.
`lfs quota -g groupname /mount_point`	Informações gerais sobre a cota para um grupo específico.
`lfs quota -p projectid /mount_point`	Informações gerais sobre a cota para um projeto específico.
`lfs quota -t -u /mount_point`	Períodos de carência de bloqueio e de inode para cotas de usuário.
`lfs quota -t -g /mount_point`	Períodos de carência de bloqueio e de inode para cotas de grupo.
`lfs quota -t -p /mount_point`	Períodos de carência de bloqueio e de inode para cotas de projeto.

Cotas e buckets vinculados do Amazon S3

É possível vincular seu sistema de arquivos do FSx para Lustre a um repositório de dados do Amazon S3. Para ter mais informações, consulte Como vincular o sistema de arquivos a um bucket do S3.

Opcionalmente, você pode escolher uma pasta ou um prefixo específico em um bucket do S3 vinculado como um caminho de importação para o sistema de arquivos. Quando uma pasta no

Amazon S3 é especificada e importada para o sistema de arquivos usando o S3, somente os dados dessa pasta são aplicados à cota. Os dados de todo o bucket não são contabilizados nos limites de cotas.

Os metadados de arquivo em um bucket do S3 vinculado são importados para uma pasta com uma estrutura correspondente à pasta importada do Amazon S3. Esses arquivos são contabilizados para as cotas de inodes de usuários e grupos que têm os arquivos.

Quando um usuário executa um `hsm_restore` ou carrega lentamente um arquivo, o tamanho total do arquivo é contabilizado para a cota de bloqueio associada ao proprietário do arquivo. Por exemplo, se o usuário A carregar lentamente um arquivo de propriedade do usuário B, a quantidade de armazenamento e o uso de inodes serão contabilizados na cota do usuário B. De forma semelhante, quando um usuário usa a API do Amazon FSx para liberar um arquivo, os dados são liberados das cotas de bloqueio do usuário ou de grupo proprietário do arquivo.

Como as restaurações e o carregamento lento do HSM são executados com acesso raiz, eles ignoram a aplicação de cotas. Depois que os dados forem importados, eles serão contabilizados para o usuário ou para o grupo com base na propriedade definida no S3, o que pode fazer com que os usuários ou os grupos excedam os limites de bloqueio. Se isso ocorrer, eles precisarão liberar arquivos para realizar gravações no sistema de arquivos novamente.

De forma semelhante, os sistemas de arquivos com importação automática habilitada criarão automaticamente novos inodes para objetos adicionados ao S3. Esses novos inodes são criados com acesso raiz e ignoram a aplicação de cotas enquanto estão sendo criados. Esses novos inodes serão contabilizados para os usuários e para os grupos, com base em quem é o proprietário do objeto no S3. Se esses usuários e grupos excederem as cotas de inode com base na atividade de importação automática, eles terão que excluir arquivos para liberar capacidade adicional e retornar abaixo dos limites de cotas.

Cotas e restauração de backups

Ao restaurar um backup, as configurações de cotas do sistema de arquivos original são implementadas no sistema de arquivos restaurado. Por exemplo, se as cotas forem definidas no sistema de arquivos A e o sistema de arquivos B for criado de um backup do sistema de arquivos A, as cotas do sistema de arquivos A serão aplicadas no sistema de arquivos B.

Como gerenciar a capacidade de armazenamento

É possível aumentar a capacidade de armazenamento configurada no sistema de arquivos do FSx para Lustre à medida que precisar de armazenamento e de throughput adicionais. Como o throughput de um sistema de arquivos do FSx para Lustre é escalado linearmente com a capacidade de armazenamento, você também obtém um aumento comparável na capacidade de throughput. Para aumentar a capacidade de armazenamento, é possível usar o console do Amazon FSx, a AWS Command Line Interface (AWS CLI) ou a API do Amazon FSx.

Quando você solicita uma atualização para a capacidade de armazenamento do sistema de arquivos, o Amazon FSx adiciona automaticamente novos servidores de arquivos de rede e escala o servidor de metadados. Ao escalar a capacidade de armazenamento, o sistema de arquivos pode ficar indisponível por alguns minutos. As operações de arquivo emitidas pelos clientes enquanto o sistema de arquivos estiver indisponível serão repetidas de forma transparente e, eventualmente, terão êxito após a conclusão da escalabilidade do armazenamento. Durante o tempo em que o sistema de arquivos estiver indisponível, o status do sistema de arquivos estará definido como `UPDATING`. Depois que a escalabilidade do armazenamento for concluída, o status do sistema de arquivos será definido para `AVAILABLE`.

Em seguida, o Amazon FSx executa um processo de otimização de armazenamento que realiza o rebalanceamento dos dados de forma transparente entre os servidores de arquivos existentes e os recentemente adicionados. O rebalanceamento é executado em segundo plano, sem impacto para a disponibilidade do sistema de arquivos. Durante o rebalanceamento, você poderá observar uma diminuição na performance do sistema de arquivos à medida que os recursos são consumidos para a movimentação de dados. Para a maioria dos sistemas de arquivos, a otimização do armazenamento demora de algumas horas a alguns dias. É possível acessar e usar o sistema de arquivos durante a fase de otimização.

Você pode acompanhar o progresso da otimização do armazenamento a qualquer momento usando o console do Amazon FSx, a CLI e a API. Para ter mais informações, consulte Como monitorar os aumentos da capacidade de armazenamento.

Tópicos

- Como monitorar os aumentos da capacidade de armazenamento

Considerações ao aumentar a capacidade de armazenamento

Aqui estão alguns itens importantes a serem considerados ao aumentar a capacidade de armazenamento:

- Somente aumento: é possível somente aumentar a quantidade de capacidade de armazenamento de um sistema de arquivos. Não é possível diminuir a capacidade de armazenamento.
- Incrementos de aumento: ao aumentar a capacidade de armazenamento, use os incrementos listados na caixa de diálogo Aumentar capacidade de armazenamento.
- Tempo entre os aumentos: não é possível fazer mais aumentos de capacidade de armazenamento em um sistema de arquivos até seis horas após a solicitação do último aumento ou até que o processo de otimização de armazenamento seja concluído, o que for mais longo.
- Capacidade de throughput: você aumenta automaticamente a capacidade de throughput ao aumentar a capacidade de armazenamento. Para sistemas de arquivos persistentes baseados em HDD com cache SSD, a capacidade de armazenamento do cache de leitura também é aumentada de forma semelhante para manter um cache SSD dimensionado para 20% da capacidade de armazenamento em HDD. O Amazon FSx calcula os novos valores para as unidades de capacidade de throughput e de armazenamento e os lista na caixa de diálogo Aumentar capacidade de armazenamento.

  > **Note**
  >
  > É possível modificar, de forma independente, a capacidade de throughput de um sistema de arquivos persistente baseado em SSD sem precisar atualizar a capacidade de armazenamento do sistema de arquivos. Para ter mais informações, consulte Como gerenciar a capacidade de throughput.

- Tipo de implantação: é possível aumentar a capacidade de armazenamento de todos os tipos de implantação, exceto sistemas de arquivos Scratch 1. Se você tiver um sistema de arquivos Scratch 1, poderá criar um novo sistema de arquivos com maior capacidade de armazenamento.

Quando aumentar a capacidade de armazenamento

Aumente a capacidade de armazenamento do sistema de arquivos quando ele estiver com pouca capacidade de armazenamento livre. Use a `FreeStorageCapacity` CloudWatch métrica para monitorar a quantidade de armazenamento gratuito disponível no sistema de arquivos. Você pode criar um CloudWatch alarme da Amazon sobre essa métrica e ser notificado quando ela cair abaixo de um limite específico. Para ter mais informações, consulte Monitorar com o Amazon CloudWatch.

Você pode usar CloudWatch métricas para monitorar os níveis contínuos de uso da taxa de transferência do seu sistema de arquivos. Se você determinar que o sistema de arquivos precisa de uma capacidade de throughput mais alta, poderá usar as informações referentes às métricas para auxiliar na decisão do momento mais adequado para aumentar a capacidade de armazenamento. Para obter informações sobre como determinar o throughput atual do sistema de arquivos, consulte Como usar as métricas do Amazon FSx para Lustre. Para obter informações sobre como a capacidade de armazenamento afeta a capacidade de throughput, consulte Performance do Amazon FSx para Lustre.

Você também pode visualizar a capacidade de armazenamento e o throughput total do sistema de arquivos no painel Resumo da página de detalhes do sistema de arquivos.

Como as solicitações simultâneas de escalabilidade de armazenamento e de backup são tratadas

É possível solicitar um backup logo antes do início de um fluxo de trabalho de escalabilidade de armazenamento ou enquanto ele estiver em andamento. A sequência de como o Amazon FSx trata as duas solicitações é a seguinte:

- Se um fluxo de trabalho de escalabilidade de armazenamento estiver em andamento (o status de escalabilidade de armazenamento for `IN_PROGRESS` e o status do sistema de arquivos for `UPDATING`) e você solicitar um backup, a solicitação de backup será colocada na fila. A tarefa de backup será iniciada quando a escalabilidade de armazenamento estiver na fase de otimização de armazenamento (o status da escalabilidade de armazenamento for `UPDATED_OPTIMIZING` e o status do sistema de arquivos for `AVAILABLE`).
- Se o backup estiver em andamento (o status do backup for `CREATING`) e você solicitar a escalabilidade de armazenamento, a solicitação de escalabilidade de armazenamento será colocada na fila. O fluxo de trabalho de escalabilidade de armazenamento será iniciado quando o Amazon FSx estiver transferindo o backup para o Amazon S3 (o status do backup for `TRANSFERRING`).

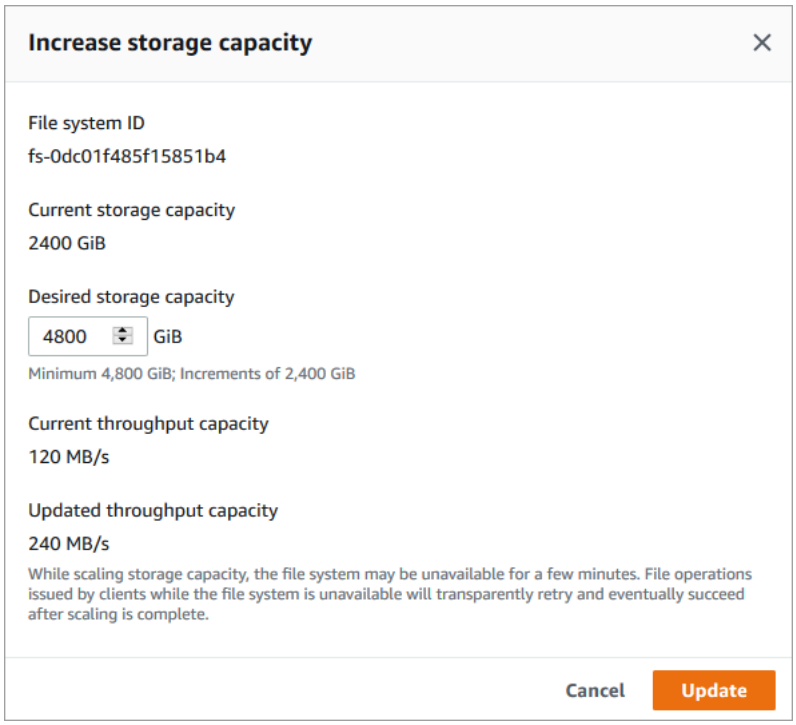
Se uma solicitação de escalabilidade de armazenamento estiver pendente e uma solicitação de backup do sistema de arquivos também estiver pendente, a tarefa de backup terá precedência. A tarefa de escalabilidade de armazenamento não será iniciada até que a tarefa de backup seja concluída.

Como aumentar a capacidade de armazenamento

Você pode aumentar a capacidade de armazenamento de um sistema de arquivos usando o console do Amazon FSx, a AWS CLI ou a API do Amazon FSx.

Aumentar a capacidade de armazenamento de um sistema de arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do Lustre para o qual deseja aumentar a capacidade de armazenamento.
3. Em Ações, escolha Atualizar capacidade de armazenamento. Como alternativa, no painel Resumo, escolha Atualizar ao lado da Capacidade de armazenamento do sistema de arquivos para exibir a caixa de diálogo Aumentar capacidade de armazenamento.



4. Em Capacidade de armazenamento desejada, forneça uma nova capacidade de armazenamento em GiB que seja maior do que a capacidade de armazenamento atual do sistema de arquivos:

- Para um sistema de arquivos persistente baseado em SSD ou Scratch 2, esse valor deve ser múltiplo de 2.400 GiB.
- Para um sistema de arquivos persistente baseado em HDD, esse valor deve ser múltiplo de 6.000 GiB para sistemas de arquivos de 12 MB/s/TiB e deve ser múltiplo de 1.800 GiB para sistemas de arquivos de 40 MB/s/TiB.

> **Note**
>
> Não é possível aumentar a capacidade de armazenamento dos sistemas de arquivos Scratch 1.

5. Escolha Atualizar para iniciar a atualização da capacidade de armazenamento.
6. Você pode monitorar o progresso da atualização na página de detalhes dos sistemas de arquivos na guia Atualizações.

Aumentar a capacidade de armazenamento de um sistema de arquivos (CLI)

1. Para aumentar a capacidade de armazenamento de um sistema de arquivos FSx for Lustre, AWS CLI use o comando. update-file-system Defina os seguintes parâmetros:

   Defina `--file-system-id` como o ID do sistema de arquivos que você está atualizando.

   Defina `--storage-capacity` como um valor inteiro que corresponda à quantidade, em GiB, do aumento da capacidade de armazenamento. Para um sistema de arquivos persistente baseado em SSD ou Scratch 2, esse valor deve ser múltiplo de 2.400. Para um sistema de arquivos persistente baseado em HDD, esse valor deve ser múltiplo de 6.000 para sistemas de arquivos de 12 MB/s/TiB e deve ser múltiplo de 1.800 para sistemas de arquivos de 40 MB/s/TiB. O novo valor de destino deve ser superior à capacidade de armazenamento atual do sistema de arquivos.

   Este comando especifica um valor de destino para a capacidade de armazenamento de 9.600 GiB para um sistema de arquivos persistente baseado em SSD ou Scratch 2.

```
$ aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --storage-capacity 9600
```

2. Você pode monitorar o progresso da atualização usando o AWS CLI comando describe-file-systems. Procure `administrative-actions` na saída.

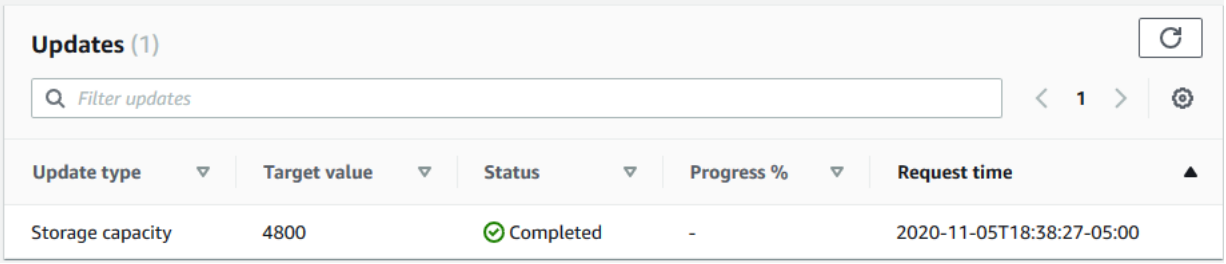
   Para obter mais informações, consulte AdministrativeAction.

Como monitorar os aumentos da capacidade de armazenamento

Você pode monitorar o progresso de um aumento na capacidade de armazenamento usando o console do Amazon FSx, a API ou a AWS CLI.

Como monitorar os aumentos no console

Na guia Atualizações, na página de detalhes do sistema de arquivos, é possível visualizar as dez atualizações mais recentes para cada tipo de atualização.



Você pode visualizar as seguintes informações:

Tipo de atualização

Os tipos com suporte são Capacidade de armazenamento e Otimização do armazenamento.

Target value (Valor de destino)

O valor desejado para a atualização da capacidade de armazenamento do sistema de arquivos.

Status

O status atual das atualizações da capacidade de armazenamento. Os valores possíveis são:

- Pendente: o Amazon FSx recebeu a solicitação de atualização, mas não começou a processá-la.
- Em andamento: o Amazon FSx está processando a solicitação de atualização.
- Atualizado; Otimizando: o Amazon FSx aumentou a capacidade de armazenamento do sistema de arquivos. Agora, o processo de otimização do armazenamento está realizando o rebalanceamento dos dados entre os servidores de arquivos.
- Concluído: o aumento da capacidade de armazenamento foi concluído com êxito.

- Com falha: o aumento da capacidade de armazenamento falhou. Escolha o ponto de interrogação (?) para ver os detalhes sobre o motivo da falha na atualização do armazenamento.

% de progresso

Exibe o progresso do processo de otimização do armazenamento como a porcentagem concluída.

Horário da solicitação

O horário em que o Amazon FSx recebeu a solicitação de ação de atualização.

Como monitorar os aumentos com a AWS CLI e a API

Você pode visualizar e monitorar as solicitações de aumento da capacidade de armazenamento do sistema de arquivos usando o describe-file-systemsAWS CLIcomando e a ação da DescribeFileSystemsAPI. A matriz `AdministrativeActions` lista as dez ações de atualização mais recentes para cada tipo de ação administrativa. Ao aumentar a capacidade de armazenamento de um sistema de arquivos, duas `AdministrativeActions` são geradas: uma ação `FILE_SYSTEM_UPDATE` e uma `STORAGE_OPTIMIZATION`.

O exemplo apresentado a seguir mostra um trecho da resposta de um comando describe-file-systems da CLI. O sistema de arquivos tem uma capacidade de armazenamento de 4.800 GB, e há uma ação administrativa pendente para aumentar a capacidade de armazenamento para 9.600 GB.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 4800,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 9600
                     }
                },
```

```
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "PENDING",
                }
            ]
```

Primeiro, o Amazon FSx processa a ação `FILE_SYSTEM_UPDATE`, adicionando novos servidores de arquivos ao sistema de arquivos. Quando o novo armazenamento estiver disponível para o sistema de arquivos, o status `FILE_SYSTEM_UPDATE` será alterado para `UPDATED_OPTIMIZING`. A capacidade de armazenamento mostra o novo valor superior, e o Amazon FSx começa a processar a ação administrativa `STORAGE_OPTIMIZATION`. Isso é mostrado no trecho a seguir da resposta de um comando describe-file-systems da CLI.

A propriedade `ProgressPercent` exibe o andamento do processo de otimização do armazenamento. Após a conclusão com êxito do processo de otimização do armazenamento, o status da ação `FILE_SYSTEM_UPDATE` é alterado para `COMPLETED` e a ação `STORAGE_OPTIMIZATION` não aparece mais.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 9600,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 9600
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
```

```
            ]
```

Se o aumento da capacidade de armazenamento falhar, o status da ação `FILE_SYSTEM_UPDATE` será alterado para `FAILED`. A propriedade `FailureDetails` fornece informações sobre a falha, mostradas no exemplo a seguir.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 4800,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 9600
                }
            ]
```

Como gerenciar a capacidade de throughput

Cada sistema de arquivos do FSx para Lustre tem uma capacidade de throughput que é configurada quando o sistema de arquivos é criado. O throughput de um sistema de arquivos do FSx para Lustre é medida em megabytes por segundo por tebibyte (MB/s/TiB). A capacidade de throughput é um fator que determina a velocidade com que o servidor de arquivos que hospeda o sistema de arquivos pode disponibilizar os dados de arquivos. Níveis mais elevados de capacidade de throughput também apresentam níveis mais elevados de operações de E/S por segundo (IOPS) e mais memória para armazenamento em cache de dados no servidor de arquivos. Para ter mais informações, consulte Performance do Amazon FSx para Lustre.

É possível modificar o nível de throughput de um sistema de arquivos persistente baseado em SSD ao aumentar ou ao diminuir o valor de throughput do sistema de arquivos por unidade de

armazenamento. Os valores válidos dependem do tipo de implantação do sistema de arquivos, conforme apresentado a seguir:

- Para os tipos de implantação Persistent_1 baseados em SSD, os valores válidos são 50, 100 e 200 MB/s/TiB.
- Para os tipos de implantação Persistent_2 baseados em SSD, os valores válidos são 125, 250, 500 e 1.000 MB/s/TiB.

É possível visualizar o valor atual do throughput do sistema de arquivos por unidade de armazenamento, da seguinte forma:

- Ao usar o console: no painel Resumo da página de detalhes do sistema de arquivos, o campo Throughput por unidade de armazenamento mostrará o valor atual.
- Usando a CLI ou a API — Use o comando describe-file-systemsCLI ou a operação da DescribeFileSystemsAPI e procure a propriedade. `PerUnitStorageThroughput`

Quando você modifica a capacidade de throughput do sistema de arquivos, em segundo plano, o Amazon FSx altera os servidores de arquivos do sistema de arquivos. O sistema de arquivos ficará indisponível por alguns minutos durante a escalabilidade da capacidade de throughput. Você será cobrado pela nova capacidade de throughput quando ela estiver disponível para o sistema de arquivos.

Tópicos

Considerações ao atualizar a capacidade de throughput

A seguir, são apresentados alguns itens importantes a serem considerados ao atualizar a capacidade de throughput:

- Aumento ou diminuição: é possível aumentar ou diminuir a quantidade de capacidade de throughput para um sistema de arquivos.

- Atualizar incrementos — Ao modificar a capacidade de taxa de transferência, use os incrementos listados na caixa de diálogo Atualizar camada de taxa de transferência.
- Tempo entre os aumentos: não é possível fazer mais alterações de capacidade de throughput em um sistema de arquivos até seis horas após a última solicitação ou até que o processo de otimização de throughput seja concluído, o que for mais longo.
- Tipo de implantação: é possível atualizar a capacidade de throughput somente para tipos de implantação persistentes baseados em SSD.

Quando modificar a capacidade de throughput

O Amazon FSx se integra à Amazon CloudWatch, permitindo que você monitore os níveis contínuos de uso da taxa de transferência do seu sistema de arquivos. A performance (throughput e IOPS) que você pode gerar usando o sistema de arquivos depende das características específicas da workload, além da capacidade de throughput, da capacidade de armazenamento e do tipo de armazenamento do sistema de arquivos. Para obter informações sobre como determinar o throughput atual do sistema de arquivos, consulte Como usar as métricas do Amazon FSx para Lustre. Para obter informações sobre CloudWatch métricas, consulteMonitorar com o Amazon CloudWatch.

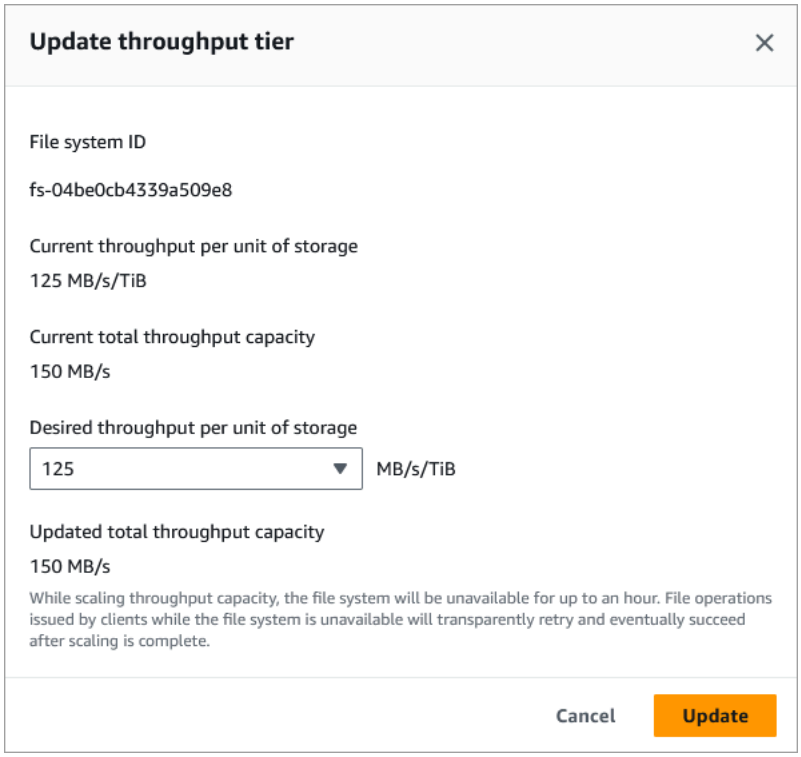
Como modificar a capacidade de throughput

Você pode modificar a capacidade de throughput de um sistema de arquivos usando o console do Amazon FSx, a AWS Command Line Interface (AWS CLI) ou a API do Amazon FSx.

Modificar a capacidade de throughput de um sistema de arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do FSx para Lustre para o qual você deseja modificar a capacidade de throughput.
3. Em Ações, escolha Atualizar nível de taxa de transferência. Como alternativa, no painel Resumo, escolha Atualizar ao lado de Throughput por unidade de armazenamento do sistema de arquivos.

   A janela Atualizar nível de taxa de transferência é exibida.
4. Escolha o novo valor para Throughput por unidade de armazenamento desejado na lista.



5. Escolha Atualizar para iniciar a atualização da capacidade de throughput.

> **Note**
>
> O sistema de arquivos pode passar por um breve período de indisponibilidade durante a atualização.

Modificar a capacidade de throughput de um sistema de arquivos (CLI)

- Para modificar a capacidade de taxa de transferência de um sistema de arquivos, use o comando update-file-systemCLI (ou a operação de API UpdateFileSystemequivalente). Defina os seguintes parâmetros:
  - Defina `--file-system-id` como o ID do sistema de arquivos que está sendo atualizado.
  - Defina `--lustre-configuration PerUnitStorageThroughput` como um valor de `50`, `100` ou `200` MB/s/TiB para sistemas de arquivos Persistent_1 baseados em SSD ou como um valor de `125`, `250`, `500` ou `1000` MB/s/TiB para sistemas de arquivos Persistent_2 baseados em SSD.

Este comando especifica que a capacidade de throughput seja configurada como 1.000 MB/s/TiB para o sistema de arquivos.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration PerUnitStorageThroughput=1000
```

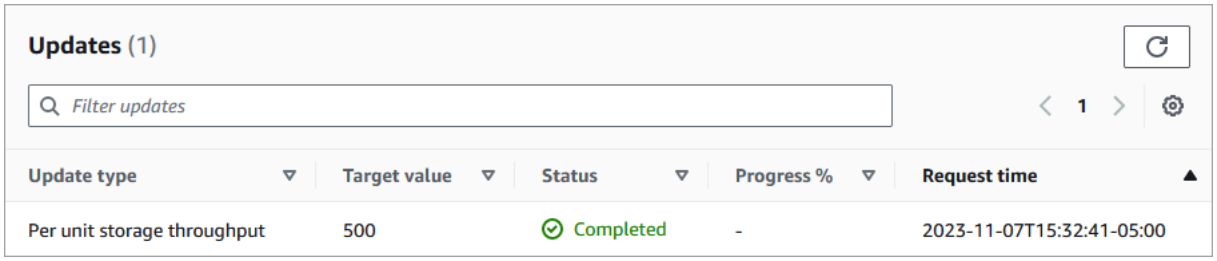
Como monitorar as alterações na capacidade de throughput

Você pode monitorar o progresso de uma modificação da capacidade de throughput usando o console do Amazon FSx, a API e a AWS CLI.

Monitorando mudanças na capacidade de processamento (console)

Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.

- Na guia Atualizações, na página de detalhes do sistema de arquivos, é possível visualizar as dez ações de atualização mais recentes para cada tipo de ação de atualização.



Nas ações de atualização da capacidade de throughput, é possível visualizar as informações apresentadas a seguir.

Tipo de atualização

O tipo com suporte é Throughput por unidade de armazenamento.

Target value (Valor de destino)

O valor desejado para o qual alterar o throughput do sistema de arquivos por unidade de armazenamento.

Status

O status atual da atualização. Para atualizações de capacidade de throughput, os valores possíveis são:

- Pendente: o Amazon FSx recebeu a solicitação de atualização, mas não começou a processá-la.
- Em andamento: o Amazon FSx está processando a solicitação de atualização.
- Atualizado; Otimizando: o Amazon FSx atualizou os recursos de E/S da rede, de CPU e de memória do sistema de arquivos. O novo nível de performance de E/S de disco está disponível para operações de gravação. As operações de leitura terão uma performance de E/S de disco entre o nível anterior e o novo nível até que o sistema de arquivos não esteja mais neste estado.
- Concluído: a atualização da capacidade de throughput foi concluída com êxito.
- Com falha: a atualização da capacidade de throughput falhou. Escolha o ponto de interrogação (?) para ver os detalhes sobre o motivo da falha na atualização do throughput.

Horário da solicitação

O horário em que o Amazon FSx recebeu a solicitação de atualização.

Monitorando atualizações do sistema de arquivos (CLI)

- Você pode visualizar e monitorar as solicitações de modificação da capacidade da taxa de transferência do sistema de arquivos usando o comando describe-file-systemsCLI e DescribeFileSystemsa ação da API. A matriz `AdministrativeActions` lista as dez ações de atualização mais recentes para cada tipo de ação administrativa. Ao modificar a capacidade de throughput de um sistema de arquivos, é gerada uma ação administrativa `FILE_SYSTEM_UPDATE`.

  O exemplo apresentado a seguir mostra um trecho da resposta de um comando `describe-file-systems` da CLI. O sistema de arquivos tem um throughput de destino por unidade de armazenamento de 500 MB/s/TiB.

```
.
.
.
"AdministrativeActions": [
    {
```

```
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "LustreConfiguration": {
            "PerUnitStorageThroughput": 500
          }
        }
    }
]
```

Quando o Amazon FSx processa a ação com êxito, o status é alterado para `COMPLETED`. A nova capacidade de throughput fica então disponível para o sistema de arquivos e é mostrada na propriedade `PerUnitStorageThroughput`.

Se a modificação da capacidade de throughput apresentar falhas, o status será alterado para `FAILED` e a propriedade `FailureDetails` fornecerá informações sobre a falha.

Compactação de dados do Lustre

É possível usar o recurso de compactação de dados do Lustre para obter economia de custos em sistemas de arquivos do Amazon FSx para Lustre de alta performance e em armazenamentos de backup. Quando a compactação de dados está habilitada, o Amazon FSx para Lustre compacta os arquivos gravados recentemente de forma automática antes que eles sejam gravados no disco e os descompacta automaticamente quando são lidos.

A compactação de dados usa o algoritmo LZ4, que é otimizado para fornecer altos níveis de compactação sem afetar negativamente a performance do sistema de arquivos. O LZ4 é um algoritmo do Lustre de confiança por parte da comunidade e orientado para a performance que fornece um equilíbrio entre a velocidade de compactação e o tamanho do arquivo compactado. A habilitação da compactação de dados, normalmente, não tem um impacto mensurável na latência.

A compactação de dados reduz a quantidade de dados que é transferida entre os servidores de arquivos e o armazenamento do Amazon FSx para Lustre. Se você ainda não estiver usando formatos de arquivos compactados, visualizará um aumento na capacidade de throughput geral do sistema de arquivos ao usar a compactação de dados. Os aumentos na capacidade de throughput que estão relacionados à compactação de dados serão limitados depois que você tiver saturado as placas de interface da rede de front-end.

Por exemplo, se o seu sistema de arquivos for do tipo de implantação PERSISTENT-50 baseado em SSD, o throughput da rede terá uma linha de base de 250 MB/s por TiB de armazenamento. O throughput do disco tem uma linha de base de 50 MB/s por TiB. Com a compactação de dados, o throughput do disco pode aumentar de 50 MB/s por TiB para um máximo de 250 MB/s por TiB, que é o limite de linha de base de throughput da rede. Para obter mais informações sobre os limites de throughput da rede e do disco, consulte as tabelas de performance do sistema de arquivos em Performance agregada do sistema de arquivos. Para obter mais informações sobre a performance da compactação de dados, consulte a publicação Spend less while increasing performance with Amazon FSx for Lustre data compression no blog do AWS Storage.

Tópicos

Como gerenciar a compactação de dados

É possível ativar ou desativar a compactação de dados ao criar um novo sistema de arquivos do Amazon FSx para Lustre. A compactação de dados está desativada por padrão quando você cria um sistema de arquivos do Amazon FSx para Lustre usando o console, a AWS CLI ou a API.

Como ativar a compactação de dados ao criar um sistema de arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para a criação de um novo sistema de arquivos descrito na Crie seu sistema de arquivos FSx for Lustre na seção Conceitos básicos.
3. Na seção Detalhes do sistema de arquivos, em Tipo de compactação de dados, escolha LZ4.
4. Conclua o assistente da forma como você faz quando cria um novo sistema de arquivos.
5. Selecione Review and create.
6. Analise as configurações escolhidas para o sistema de arquivos do Amazon FSx para Lustre e, em seguida, escolha Criar sistema de arquivos.

Quando o sistema de arquivos estiver Disponível, a compactação de dados estará ativada.

Como ativar a compactação de dados ao criar um sistema de arquivos (CLI)

- Para criar um sistema de arquivos do FSx para Lustre com a compactação de dados ativada, use o comando `create-file-system` da CLI do Amazon FSx com o parâmetro `DataCompressionType`, conforme mostrado a seguir. A operação de API correspondente é CreateFileSystem.

```
$ aws fsx create-file-system \
      --client-request-token CRT1234 \
      --file-system-type LUSTRE \
      --file-system-type-version 2.12 \
      --lustre-configuration
 DeploymentType=PERSISTENT_1,PerUnitStorageThroughput=50,DataCompressionType=LZ4 \
      --storage-capacity 3600 \
      --subnet-ids subnet-123456 \
      --tags Key=Name,Value=Lustre-TEST-1 \
      --region us-east-2
```

Após criar o sistema de arquivos com êxito, o Amazon FSx retorna a descrição do sistema de arquivos como JSON, conforme mostrado no exemplo a seguir.

```
{

    "FileSystems": [
        {
            "OwnerId": "111122223333",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "FileSystemTypeVersion": "2.12",
            "Lifecycle": "CREATING",
            "StorageCapacity": 3600,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
```

```
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "PERSISTENT_1",
                "DataCompressionType": "LZ4",
                "PerUnitStorageThroughput": 50
            }
        }
    ]
}
```

Você também pode alterar a configuração de compactação de dados dos sistemas de arquivos existentes. Ao ativar a compactação de dados para um sistema de arquivos existente, somente os arquivos gravados recentemente são compactados e os arquivos existentes não são compactados. Para obter mais informações, consulte Compactação de arquivos gravados anteriormente.

Como atualizar a compactação de dados em um sistema de arquivos existente (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do Lustre para o qual você deseja gerenciar a compactação de dados.
3. Em Ações, escolha Atualizar tipo de compactação de dados.
4. Na caixa de diálogo Atualizar tipo de compactação de dados, escolha LZ4 para ativar a compactação de dados ou escolha NONE para desativá-la.
5. Escolha Atualizar.
6. Você pode monitorar o progresso da atualização na página de detalhes dos sistemas de arquivos na guia Atualizações.

Como atualizar a compactação de dados em um sistema de arquivos existente (CLI)

Para atualizar a configuração de compactação de dados de um sistema de arquivos do FSx para Lustre existente, use o comando update-file-system da AWS CLI. Defina os seguintes parâmetros:

- Defina `--file-system-id` como o ID do sistema de arquivos que está sendo atualizado.
- Defina `--lustre-configuration DataCompressionType` como `NONE` para desativar a compactação de dados ou `LZ4` para ativar a compactação de dados com o algoritmo LZ4.

Este comando especifica que a compactação de dados está ativada com o algoritmo LZ4.

```
$ aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration DataCompressionType=LZ4
```

Configuração de compactação de dados ao criar um sistema de arquivos usando um backup

É possível usar um backup disponível para criar um novo sistema de arquivos do Amazon FSx para Lustre. Ao criar um novo sistema de arquivos usando o backup, não há necessidade de especificar o `DataCompressionType`, pois a configuração será aplicada usando a configuração `DataCompressionType` do backup. Se você optar por especificar o `DataCompressionType` ao criar usando o backup, o valor deverá corresponder à configuração `DataCompressionType` do backup.

Para visualizar as configurações de um backup, escolha-o na guia Backups do console do Amazon FSx. Os detalhes do backup serão listados na página Resumo para o backup. Você também pode executar o comando `describe-backups` da AWS CLI (a ação de API equivalente é `DescribeBackups`).

Compactação de arquivos gravados anteriormente

Os arquivos serão descompactados se tiverem sido criados quando a compactação de dados estava desativada no sistema de arquivos do Amazon FSx para Lustre. Ativar a compactação de dados não compactará automaticamente os dados descompactados existentes.

É possível usar o comando `lfs_migrate` que foi instalado como uma parte da instalação do cliente Lustre para compactar arquivos existentes. Para obter um exemplo, consulte FSxL-Compression que está disponível no GitHub.

Visualização de tamanhos de arquivos

É possível usar os comandos apresentados a seguir para visualizar os tamanhos descompactados e compactados de seus arquivos e diretórios.

- du exibe tamanhos compactados.
- `du --apparent-size` exibe tamanhos descompactados.
- `ls -l` exibe tamanhos descompactados.

Os exemplos apresentados a seguir mostram a saída de cada comando com base no mesmo arquivo.

```
$ du -sh samplefile
272M samplefile
$ du -sh --apparent-size samplefile
1.0G samplefile
$ ls -lh samplefile
-rw-r--r-- 1 root root 1.0G May 10 21:16 samplefile
```

A opção `-h` é útil para esses comandos porque imprime tamanhos em um formato legível por humanos.

Usar métricas do Amazon CloudWatch

É possível usar as métricas do Amazon CloudWatch Logs para visualizar o seu uso do sistema de arquivos. A métrica `LogicalDiskUsage` mostra o uso total do disco lógico (sem compactação) e a métrica `PhysicalDiskUsage` mostra o uso total do disco físico (com compactação). Essas duas métricas estarão disponíveis somente se o seu sistema de arquivos tiver a compactação de dados habilitada ou já a tiver habilitado.

Você pode determinar a taxa de compactação do sistema de arquivos ao dividir a `Sum` da estatística `LogicalDiskUsage` pela `Sum` da estatística `PhysicalDiskUsage`. Para obter informações sobre como usar a matemática em métricas para calcular essa taxa, consulte Matemática em métricas: taxa de compactação de dados.

Para obter mais informações sobre como monitorar a performance do sistema de arquivos, consulte Como monitorar o Amazon FSx for Lustre.

Lustre root squash

Root squash é um recurso administrativo que adiciona outra camada do controle de acesso a arquivos sobre o atual controle de acesso baseado em rede e as permissões de arquivo POSIX.

Usando o recurso root squash, você pode restringir o acesso no nível raiz dos clientes que tentam acessar o sistema de arquivos do FSx para Lustre como raiz.

As permissões do usuário raiz são obrigatórias para realizar ações administrativas, como gerenciar permissões nos sistemas de arquivos do FSx para Lustre. No entanto, o acesso raiz fornece acesso irrestrito aos usuários, permitindo que eles ignorem as verificações de permissão para acessar, modificar ou excluir objetos do sistema de arquivos. Usando o recurso root squash, você pode impedir o acesso não autorizado ou a exclusão de dados especificando um ID de usuário não raiz (UID) e um ID de grupo (GID) para o sistema de arquivos. Os usuários raiz que acessam o sistema de arquivos serão automaticamente convertidos no usuário/grupo menos privilegiado especificado, com permissões limitadas definidas pelo administrador de armazenamento.

O recurso root squash também permite, opcionalmente, fornecer uma lista de clientes que não são afetados pela configuração do root squash. Esses clientes podem acessar o sistema de arquivos como raiz, com privilégios irrestritos.

Tópicos

Como o root squash funciona

O recurso root squash funciona remapeando o ID de usuário (UID) e o ID de grupo (GID) do usuário raiz para um UID e GID especificados pelo administrador do sistema Lustre. O recurso root squash também permite especificar opcionalmente um conjunto de clientes aos quais o remapeamento de UID/GID não se aplica.

Quando um sistema de arquivos do FSx para Lustre é criado, o root squash está desabilitado por padrão. Você o habilita definindo uma configuração de root squash UID e GID para seu sistema de arquivos do FSx para Lustre. Os valores UID e GID são números inteiros que podem variar de `0` a `4294967294`.

- Um valor diferente de zero para UID e GID habilita o root squash. Os valores UID e GID podem ser diferentes, mas cada um deve ser um valor diferente de zero.
- Um valor `0` (zero) para UID e GID indica raiz e, portanto, desabilita o root squash.

Durante a criação do sistema de arquivos, você pode usar o console do Amazon FSx para fornecer os valores UID e GID do root squash na propriedade Root Squash, conforme mostrado em. Para habilitar o root squash ao criar um sistema de arquivos (console) Você também pode usar o `RootSquash` parâmetro com a API AWS CLI ou para fornecer os valores de UID e GID, conforme mostrado em. Habilitar o root squash ao criar um sistema de arquivos (CLI)

Você também pode especificar uma lista de NIDs de clientes aos quais o root squash não se aplica. Um NID de cliente é um identificador de rede do Lustre usado para identificar um cliente de forma exclusiva. Você pode especificar o NID como endereço único ou um intervalo de endereços:

- Um endereço único é descrito no formato NID padrão do Lustre, especificando o endereço IP do cliente seguido pelo ID de rede do Lustre (por exemplo, `10.0.1.6@tcp`)
- Um intervalo de endereços é descrito usando um traço para separar o intervalo (por exemplo, `10.0.[2-10].[1-255]@tcp`).
- Se você não especificar nenhum NID de cliente, não haverá exceções ao root squash.

Ao criar ou atualizar seu sistema de arquivos, você pode usar a propriedade Exceptions to Root Squash no console do Amazon FSx para fornecer a lista de NIDs de clientes. Na API AWS CLI or, use o `NoSquashNids` parâmetro. Para obter mais informações, consulte os procedimentos emComo gerenciar root squash.

> **Note**
>
> Não há suporte para root squash em backups e restaurações. Para usar backups e restaurações, você deve desativar o root squash definindo o `RootSquash` parâmetro como `0:0` e o parâmetro `[]` com a `NoSquashNids` API AWS CLI ou, ou escolhendo Disable na caixa de diálogo Update Root Squash Settings no console do Amazon FSx.

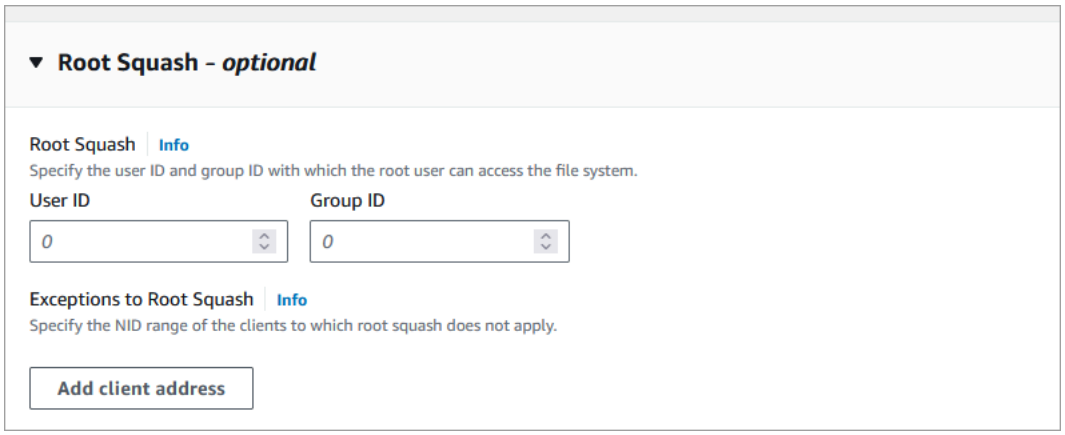
Como gerenciar root squash

Durante a criação do sistema de arquivos, o root squash é desativado por padrão. Você pode ativar o root squash ao criar um novo sistema de arquivos Amazon FSx for Lustre a partir do console ou API do Amazon FSx. AWS CLI

Para habilitar o root squash ao criar um sistema de arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.

2. Siga o procedimento para a criação de um novo sistema de arquivos descrito na Crie seu sistema de arquivos FSx for Lustre na seção Conceitos básicos.
3. Abra a seção Root Squash - opcional.



4. Para o Root Squash, forneça os IDs de usuário e grupo com os quais o usuário root pode acessar o sistema de arquivos. Você pode especificar qualquer número inteiro no intervalo de 1 —4294967294:
   1. Em ID do usuário, especifique o ID do usuário para o usuário root usar.
   2. Em ID do grupo, especifique a ID do grupo a ser usada pelo usuário raiz.
5. (Opcional) Para exceções ao Root Squash, faça o seguinte:
   1. Escolha Adicionar endereço do cliente.
   2. No campo Endereços do cliente, especifique o endereço IP de um cliente ao qual o root squash não se aplica. Para obter informações sobre o formato do endereço IP, consulteComo o root squash funciona.
   3. Repita conforme necessário para adicionar mais endereços IP do cliente.
6. Conclua o assistente da forma como você faz quando cria um novo sistema de arquivos.
7. Selecione Review and create.
8. Analise as configurações escolhidas para o sistema de arquivos do Amazon FSx para Lustre e, em seguida, escolha Criar sistema de arquivos.

Quando o sistema de arquivos está disponível, o root squash é ativado.

Habilitar o root squash ao criar um sistema de arquivos (CLI)

- Para criar um sistema de arquivos do FSx para Lustre com o root squash habilitado, use o comando da CLI `create-file-system` do Amazon FSx com o parâmetro `RootSquashConfiguration`. A operação de API correspondente é CreateFileSystem.

  Para o parâmetro `RootSquashConfiguration`, defina as seguintes opções:

  - `RootSquash`: os valores UID:GID separados por dois pontos que especificam o ID do usuário e o ID do grupo para o usuário raiz. Você pode especificar qualquer número inteiro no intervalo de `0` a `4294967294` (0 é raiz) para cada ID (por exemplo, `65534:65534`).
  - `NoSquashNids`: especifique os identificadores de rede (NIDs) do Lustre dos clientes aos quais o root squash não se aplica. Para obter informações sobre o formato do NID do cliente, consulte Como o root squash funciona.

  O exemplo a seguir cria um sistema de arquivos do FSx para Lustre com o root squash habilitado:

```
$ aws fsx create-file-system \
      --client-request-token CRT1234 \
      --file-system-type LUSTRE \
      --file-system-type-version 2.15 \
      --lustre-configuration
 "DeploymentType=PERSISTENT_2,PerUnitStorageThroughput=250,DataCompressionType=LZ4,
\
          RootSquashConfiguration={RootSquash="65534:65534",\
          NoSquashNids=["10.216.123.47@tcp", "10.216.12.176@tcp"]}" \
      --storage-capacity 2400 \
      --subnet-ids subnet-123456 \
      --tags Key=Name,Value=Lustre-TEST-1 \
      --region us-east-2
```

Após criar o sistema de arquivos com êxito, o Amazon FSx retorna a descrição do sistema de arquivos como JSON, conforme mostrado no exemplo a seguir.

```
{

    "FileSystems": [
        {
```

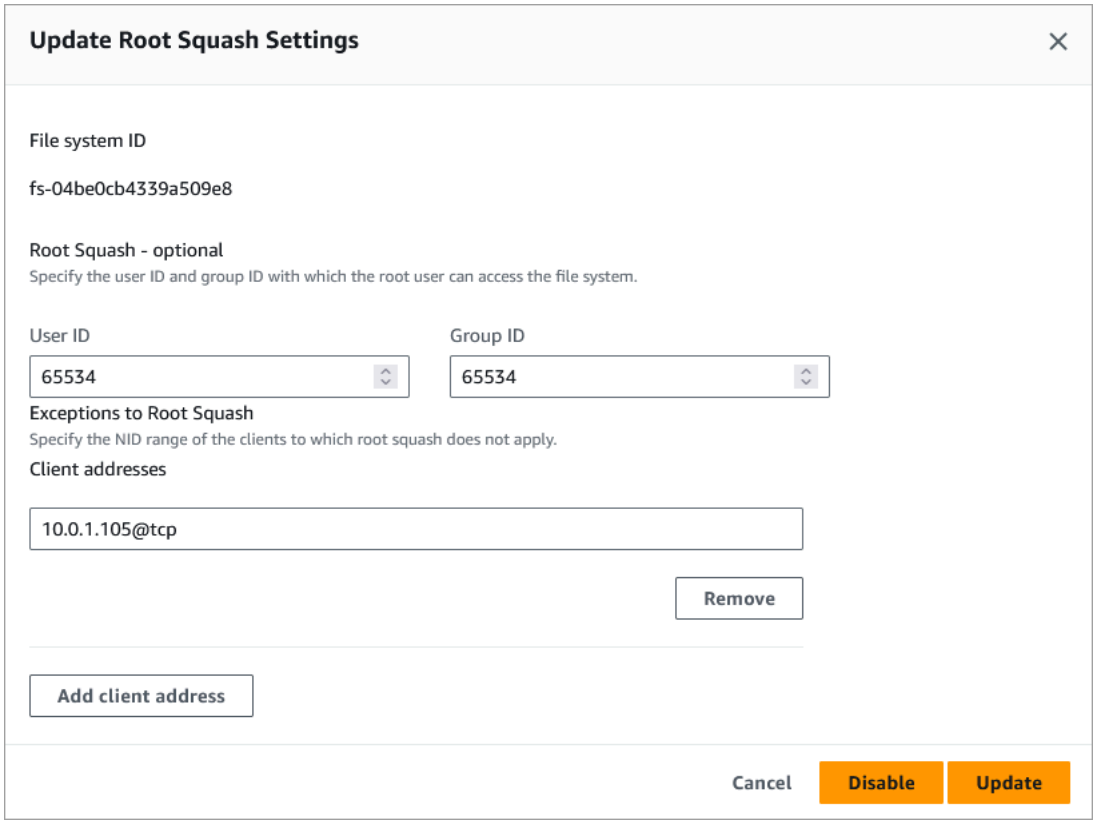
```
            "OwnerId": "111122223333",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "FileSystemTypeVersion": "2.15",
            "Lifecycle": "CREATING",
            "StorageCapacity": 2400,
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "PERSISTENT_2",
                "DataCompressionType": "LZ4",
                "PerUnitStorageThroughput": 250,
                "RootSquashConfiguration": {
                    "RootSquash": "65534:65534",
                    "NoSquashNids": "10.216.123.47@tcp 10.216.29.176@tcp"
            }
        }
    ]
}
```

Você também pode atualizar as configurações do root squash do seu sistema de arquivos existente usando o console AWS CLI ou a API do Amazon FSx. Por exemplo, você pode alterar os valores UID e GID do root squash, adicionar ou remover NIDs do cliente ou desabilitar o root squash.

Para atualizar as configurações do root squash em um sistema de arquivos existente (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.

2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos Lustre para o qual você deseja gerenciar o root squash.
3. Em Ações, escolha Atualizar root squash. Ou, no painel Resumo, escolha Atualizar ao lado do campo Root Squash do sistema de arquivos para exibir a caixa de diálogo Atualizar configurações do Root Squash.



4. Para o Root Squash, atualize os IDs de usuário e grupo com os quais o usuário root pode acessar o sistema de arquivos. Você pode especificar qualquer número inteiro no intervalo de `0` -`4294967294`. Para desativar o root squash, especifique `0` (zero) para ambas as IDs.
    1. Em ID do usuário, especifique o ID do usuário para o usuário root usar.
    2. Em ID do grupo, especifique a ID do grupo a ser usada pelo usuário raiz.
5. Para exceções ao Root Squash, faça o seguinte:
    1. Escolha Adicionar endereço do cliente.
    2. No campo Endereços do cliente, especifique o endereço IP de um cliente ao qual o root squash não se aplica,
    3. Repita conforme necessário para adicionar mais endereços IP do cliente.
6. Escolha Atualizar.

> **Note**
>
> Se o root squash estiver ativado e você quiser desativá-lo, escolha Desativar em vez de executar as etapas 4 a 6.

Você pode monitorar o progresso da atualização na página de detalhes dos sistemas de arquivos na guia Atualizações.

Atualizar as configurações do root squash em um sistema de arquivos (CLI) existente

Para atualizar as configurações do root squash para um sistema de arquivos FSx for Lustre existente, use o comando. AWS CLI update-file-system A operação de API correspondente é UpdateFileSystem.

Defina os seguintes parâmetros:

- Defina `--file-system-id` como o ID do sistema de arquivos que está sendo atualizado.
- Defina as opções `--lustre-configuration RootSquashConfiguration` desta forma:
  - `RootSquash`: defina os valores UID:GID separados por dois pontos que especificam o ID do usuário e o ID do grupo para o usuário raiz. Você pode especificar qualquer número inteiro no intervalo de `0` a `4294967294` (0 é raiz) para cada ID. Para desabilitar o root squash, especifique `0:0` para os valores UID:GID.
  - `NoSquashNids`: especifique os identificadores de rede (NIDs) do Lustre dos clientes aos quais o root squash não se aplica. Use `[]` para remover todos os NIDs de cliente, o que significa que não haverá exceções ao root squash.

Esse comando especifica que o root squash é habilitado usando `65534` como valor para o ID do usuário e o ID do grupo do usuário raiz.

```
$ aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration RootSquashConfiguration={RootSquash="65534:65534", \
          NoSquashNids=["10.216.123.47@tcp", "10.216.12.176@tcp"]}
```

Se o comando ocorrer com êxito, o Amazon FSx para Lustre retornará a resposta no formato JSON.

Você pode visualizar as configurações do root squash do seu sistema de arquivos no painel Resumo da página de detalhes do sistema de arquivos no console do Amazon FSx ou na resposta de um comando da `describe-file-systems`CLI (a ação de API equivalente é). `DescribeFileSystems`

Status do sistema de arquivos FSx for Lustre

Você pode visualizar o status de um sistema de arquivos Amazon FSx usando o console do Amazon FSx, o AWS CLI comando ou a operação da describe-file-systemsAPI. DescribeFileSystems

Status do sistema de arquivos	Descrição
DISPONÍVEL	O sistema de arquivos está em um estado íntegro e está acessível e disponível para uso.
CRIANDO	O Amazon FSx está criando um novo sistema de arquivos.
EXCLUINDO	O Amazon FSx está excluindo um sistema de arquivos existente.
ATUALIZANDO	O sistema de arquivos está passando por uma atualização iniciada pelo cliente.
CONFIGURAÇÃO INCORRETA	O sistema de arquivos está em um estado de falha, mas é recuperável.
COM FALHA	Esse status pode significar um dos seguintes: • O sistema de arquivos falhou e o Amazon FSx não consegue recuperá-lo. • Ao criar um novo sistema de arquivos, o Amazon FSx não conseguiu criar o sistema de arquivos.

Marcar os recursos do Amazon FSx

Para ajudar você a gerenciar os sistemas de arquivos e outros recursos do Amazon FSx para Lustre, é possível atribuir seus próprios metadados a cada recurso na forma de tags. As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Isso é útil quando você tem muitos recursos do mesmo tipo — é possível identificar rapidamente um recurso específico baseado nas tags que você atribuiu a ele. Este tópico descreve tags e mostra a você como criá-los.

Tópicos

Conceitos básicos de tags

Uma tag é um rótulo atribuído a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional, ambos definidos por você.

As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Por exemplo, é possível definir um conjunto de tags para os sistemas de arquivos do Amazon FSx para Lustre da sua conta que ajudam a rastrear o proprietário e o nível de pilha de cada instância.

Recomendamos que você desenvolva um conjunto de chave de tags que atenda suas necessidades para cada tipo de recurso. Usar um conjunto consistente de chaves de tags facilita para você gerenciar seus recursos. É possível pesquisar e filtrar os recursos de acordo com as tags que adicionar.

As tags não têm nenhum significado semântico para o Amazon FSx e são interpretadas estritamente como uma sequência de caracteres. Além disso, as tags não são automaticamente atribuídas aos seus recursos. É possível editar chaves de tags e valores, e é possível remover as tags de um recurso a qualquer momento. É possível definir o valor de uma tag a uma string vazia, mas não pode configurar o valor de um tag como nula. Se você adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo. Se você excluir um recurso, todas as tags do recurso também serão excluídas.

Se estiver usando a API do Amazon FSx para Lustre, a AWS CLI ou um AWS SDK, poderá usar a ação de API `TagResource` para aplicar tags aos recursos existentes. Além disso, algumas ações de criação de recursos permitem que você especifique tags para um recurso quando ele é criado. Se as tags não puderem ser aplicadas durante a criação dos recursos, nós reverteremos o processo de criação de recursos. Isso garante que os recursos sejam criados com tags ou, então, não criados, e que nenhum recurso seja deixado sem tags. Ao marcar com tags os recursos no momento da criação, você elimina a necessidade de executar scripts personalizados de uso de tags após a criação do recurso. Para obter mais informações sobre como permitir que os usuários marquem os recursos durante a criação, consulte Conceder permissão para marcar recursos durante a criação.

Marcar recursos da

É possível marcar os recursos do Amazon FSx para Lustre que existem em sua conta. Caso esteja usando o console do Amazon FSx, você poderá aplicar tags aos recursos ao usar a guia Tags na tela do recurso relevante. Ao criar recursos, você pode aplicar a chave Nome com um valor e aplicar tags de sua escolha ao criar um sistema de arquivos. O console pode organizar os recursos de acordo com a tag Nome, mas essa tag não tem nenhum significado semântico para o serviço do Amazon FSx para Lustre.

Você pode aplicar permissões no nível de recurso que são baseadas em tags em suas políticas do IAM às ações de API do Amazon FSx para Lustre que oferecem suporte à marcação durante a criação para a implementação de controle granular sobre os usuários e os grupos que podem marcar recursos na criação. Seus recursos estão devidamente protegidos contra criação — as tags aplicadas imediatamente aos recursos; portanto, todas as permissões em nível de recurso baseadas em tags que controlam o uso de recursos entram imediatamente em vigor. Seus recursos podem ser rastreados e relatados com mais precisão. É possível obrigar o uso de marcação com tags nos novos recursos e controlar quais chaves e valores de tag são definidos nos seus recursos.

Também é possível aplicar permissões em nível de recurso às ações de API `TagResource` e `UntagResource` do Amazon FSx para Lustre em suas políticas do IAM para controlar quais chaves e valores de tags são definidos nos recursos existentes.

Para obter mais informações sobre a aplicação de tags nos seus recursos para faturamento, consulte Uso de tags de alocação de custos no Guia do usuário do AWS Billing.

Restrições de tags

As restrições básicas a seguir se aplicam às tags:

- Número máximo de tags por recurso: 50
- Em todos os recursos, cada chave de tag deve ser exclusiva e pode ter apenas um valor.
- Comprimento máximo da chave: 128 caracteres Unicode em UTF-8
- Comprimento máximo do valor: 256 caracteres Unicode em UTF-8
- Os caracteres permitidos para tags do Amazon FSx para Lustre são: letras, números e espaços representáveis em UTF-8, além dos seguintes caracteres: + - = . _ : / @.
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.
- O prefixo `aws:` é reservado para uso da AWS. Não é possível editar nem excluir a chave ou o valor de uma tag quando ela tem uma chave de tag com esse prefixo. As tags com o prefixo `aws:` não contam para as tags por limite de recurso.

Você não pode excluir um recurso unicamente com base em suas tags, portanto, você deve especificar o identificador de recursos. Por exemplo, para excluir um sistema de arquivos marcado com uma chave de tag denominada `DeleteMe`, você deve usar a ação `DeleteFileSystem` com o identificador de recursos do sistema de arquivos, como fs-1234567890abcdef0.

Ao marcar recursos públicos ou compartilhados, as tags atribuídas tornam-se disponíveis somente para sua Conta da AWS. Nenhuma outra Conta da AWS terá acesso a essas tags. Para obter um controle de acesso baseado em tags para os recursos compartilhados, cada Conta da AWS deve atribuir seu próprio conjunto de tags para controlar o acesso ao recurso.

Permissões e tag

Para obter mais informações sobre as permissões necessárias para marcar os recursos do Amazon FSx no momento da criação, consulte Conceder permissão para marcar recursos durante a criação. Para obter mais informações sobre usar tags para restringir o acesso aos recursos do Amazon FSx nas políticas do IAM, consulte Como usar tags para controlar o acesso aos seus recursos do Amazon FSx.

Janelas de manutenção do Amazon FSx para Lustre

O Amazon FSx para Lustre executa aplicações de patches de software rotineiras para o software do Lustre que ele gerencia. A janela de manutenção é a sua oportunidade de controlar em que dia e em qual horário da semana ocorrerá a aplicação de patch de software.

A aplicação de patches deve precisar de apenas uma fração da janela de manutenção de 30 minutos. Durante esses poucos minutos, o sistema de arquivos ficará temporariamente indisponível.

Você escolhe a janela de manutenção durante a criação do sistema de arquivos. Se você não tiver uma preferência de horário, será atribuída uma janela padrão de 30 minutos.

O FSx para Lustre permite ajustar sua janela de manutenção conforme necessário para acomodar a workload e os requisitos operacionais. É possível mover a janela de manutenção com a frequência necessária, desde que uma janela de manutenção seja programada, no mínimo, uma vez a cada 14 dias. Se um patch for liberado e você não tiver programado uma janela de manutenção em até 14 dias, o FSx para Lustre prosseguirá com a manutenção do sistema de arquivos para garantir a segurança e a confiabilidade.

Você pode usar o console de gerenciamento do Amazon FSx, a AWS CLI, a API da AWS ou um dos AWS SDKs para alterar a janela de manutenção dos seus sistemas de arquivos.

Como alterar a janela de manutenção usando o console

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha Sistemas de arquivos no painel de navegação.
3. Escolha o sistema de arquivos para o qual deseja alterar a janela de manutenção. A página de detalhes do sistema de arquivos será exibida.
4. Escolha a guia Manutenção. O painel Configurações da janela de manutenção será exibido.
5. Escolha Editar e insira o novo dia e horário em que deseja que a janela de manutenção comece.
6. Escolha Save (Salvar) para salvar as alterações. O novo horário de início da manutenção será exibido no painel Configurações.

É possível alterar a janela de manutenção do sistema de arquivos usando o comando update-file-system da CLI. Execute o comando a seguir, substituindo o ID do sistema de arquivos pelo ID do seu sistema de arquivos e a data e o horário em que você deseja iniciar a janela.

```
aws fsx update-file-system --file-system-id fs-01234567890123456 --lustre-configuration
 WeeklyMaintenanceStartTime=1:01:30
```

Excluir um sistema de arquivos

Você pode excluir um sistema de arquivos Amazon FSx for Lustre usando o console do Amazon FSx, AWS CLI o e a API do Amazon FSx. Antes de excluir um sistema de arquivos do FSx para Lustre, é necessário desmontá-lo de cada instância conectada do Amazon EC2. Nos sistemas de arquivos vinculados ao S3, para garantir que todos os seus dados sejam

gravados de volta no S3 antes de excluir o sistema de arquivos, você pode monitorar se a AgeOfOldestQueuedMessagemétrica é zero (se estiver usando a exportação automática) ou executar uma tarefa de repositório de dados de exportação. Se você tiver a exportação automática habilitada e desejar usar uma tarefa de exportação do repositório de dados, será necessário desabilitar a exportação automática antes de executar a tarefa de exportação do repositório de dados.

Como excluir um sistema de arquivos após a desmontagem de cada instância do Amazon EC2:

- Como usar o console: siga o procedimento descrito em Limpeza de recursos.
- Usando a API ou a CLI — Use a operação da DeleteFileSystemAPI ou o comando da CLI delete-file-system.

Como migrar para o Amazon FSx para Lustre usando o AWS DataSync

É possível usar o AWS DataSync para transferir dados entre sistemas de arquivos do FSx para Lustre. O DataSync corresponde a um serviço de transferência de dados que simplifica, automatiza e acelera a movimentação e a replicação de dados entre sistemas de armazenamento autogerenciados e serviços de armazenamento da AWS pela Internet ou pelo AWS Direct Connect. O DataSync pode transferir dados e metadados do sistema de arquivos, como propriedade, carimbos de data e hora e permissões de acesso.

Como migrar arquivos existentes para o FSx para Lustre usando o AWS DataSync

É possível usar o DataSync com sistemas de arquivos do FSx para Lustre com a finalidade de executar migrações de dados únicas, ingerir dados periodicamente para workloads distribuídas e programar replicações para proteção e recuperação de dados. Para obter informações sobre cenários de transferência específicos, consulte Where can I transfer my data? no Guia do usuário do AWS DataSync.

Pré-requisitos

Para migrar dados para a configuração do FSx para Lustre, é necessário um servidor e uma rede que atendam aos requisitos do DataSync. Para obter mais informações, consulte Requirements for DataSync no Guia do usuário do AWS DataSync.

- Você criou um destino para o sistema de arquivos do FSx para Lustre. Para obter mais informações, consulte Crie seu sistema de arquivos FSx for Lustre.
- Os sistemas de arquivos de origem e de destino estão conectados na mesma nuvem privada virtual (VPC). O sistema de arquivos de origem pode estar localizado on-premises ou em outra Amazon VPC, Conta da AWS ou Região da AWS, mas deve estar em uma rede emparelhada com a do sistema de arquivos de destino usando o emparelhamento da Amazon VPC, o Transit Gateway, o AWS Direct Connect ou o AWS VPN. Para obter mais informações, consulte O que é emparelhamento de VPC? no Guia de emparelhamento da Amazon VPC.

> **Note**
>
> O DataSync poderá realizar transferências entre Contas da AWS de ou para o FSx para Lustre somente se o outro local de transferência for o Amazon S3.

Primeiros passos para migrar arquivos usando o DataSync

A transferência de arquivos de uma origem para um destino usando o DataSync envolve os seguintes passos básicos:

- Faça download e implante um agente em seu ambiente, e ative-o (não é necessário se a transferência ocorrer entre Serviços da AWS).
- Crie um local de origem e de destino.
- Crie uma tarefa.
- Execute a tarefa para transferir arquivos da origem para o destino.

Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS DataSync:

- Transferring between on-premises storage and AWS
- Configuring AWS DataSync transfers with Amazon FSx for Lustre no Guia do usuário do AWS DataSync.
- Deploy your agent on Amazon EC2

Como monitorar o Amazon FSx for Lustre

É possível usar as seguintes ferramentas de monitoramento automatizado para supervisionar o Amazon FSx para Lustre e gerar relatórios quando algo estiver errado:

- Monitoramento usando o Amazon CloudWatch: o CloudWatch coleta e processa dados brutos do Amazon FSx para Lustre em métricas legíveis e quase em tempo real. Você pode criar um alarme do CloudWatch que envia uma mensagem do Amazon SNS quando o alarme muda de estado.
- Monitoramento usando o registro em log do Lustre: é possível monitorar os eventos de logs habilitados para o seu sistema de arquivos. O registro em log do Lustre grava esses eventos no Amazon CloudWatch Logs.
- Monitoramento de log do AWS CloudTrail: compartilhe arquivos de log entre contas, monitore arquivos de log do CloudTrail em tempo real ao enviá-los para o CloudWatch Logs, grave aplicações de processamento de log em Java e valide se os arquivos de log não foram alterados após a entrega pelo CloudTrail.

Tópicos

Monitorar com o Amazon CloudWatch

É possível monitorar sistemas de arquivos usando o Amazon CloudWatch, que coleta e processa dados brutos do Amazon FSx para Lustre em métricas legíveis e quase em tempo real. Essas estatísticas são retidas por um período de 15 meses, com a finalidade de que você possa acessar informações históricas e obter uma melhor perspectiva sobre a performance da aplicação ou do serviço Web. Por padrão, os dados de métricas do Amazon FSx para Lustre são enviados automaticamente para o CloudWatch em períodos de um minuto. Para obter mais informações sobre o CloudWatch, consulte O que é o Amazon CloudWatch? no Guia do usuário do Amazon CloudWatch.

As métricas do CloudWatch são relatadas como bytes brutos. Os bytes não são arredondados para um múltiplo decimal ou binário da unidade.

Métricas do sistema de arquivos

O FSx para Lustre publica as métricas apresentadas a seguir no namespace `FSx` no CloudWatch. Para cada métrica, o FSx para Lustre emite um ponto de dados por disco por minuto. Para visualizar os detalhes agregados do sistema de arquivos, é possível usar a estatística `Sum`. Observe que os servidores de arquivos por trás dos sistemas de arquivos do FSx para Lustre estão espalhados por vários discos.

Métrica	Descrição
`DataReadBytes`	O número de bytes para operações de leitura do sistema de arquivos. A estatística `Sum` corresponde ao número total de bytes associado s às operações de leitura durante o período. A estatística `Minimum` corresponde ao número mínimo de bytes associados às operações de leitura em um único disco. A estatística `Maximum` corresponde ao número máximo de bytes associados às operações de leitura no disco. A estatística `Average` corresponde ao número médio de bytes associados às operações de leitura por disco. A estatística `SampleCou nt` corresponde ao número de discos. Para calcular a média de throughput (bytes por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período. Unidades: • Bytes para `Sum`, `Minimum`, `Maximum` e `Average`. • Contagem de `SampleCount` . Estatísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCou nt`
`DataWriteBytes`	O número de bytes para operações de gravação do sistema de arquivos. A estatística `Sum` é o número total de bytes associados às operações de gravação. A estatística `Minimum` corresponde ao número mínimo de bytes associados às operações de gravação em um único disco.

Métrica	Descrição
	A estatística `Maximum` corresponde ao número máximo de bytes associados às operações de gravação no disco. A estatística `Average` corresponde ao número médio de bytes associados às operações de gravação por disco. A estatística `SampleCount` corresponde ao número de discos. Para calcular a média de throughput (bytes por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período. Unidades: • Bytes para `Sum`, `Minimum`, `Maximum` e `Average`. • Contagem de `SampleCount` . Estatísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrica	Descrição
`DataReadOperations`	O número de operações de leitura. A estatística `Sum` corresponde ao número total de operações de leitura. A estatística `Minimum` corresponde ao número mínimo de operações de leitura em um único disco. A estatística `Maximum` corresponde ao número máximo de operações de leitura no disco. A estatística `Average` corresponde ao número médio de operações de leitura por disco. A estatística `SampleCount` corresponde ao número de discos. Para calcular o número médio de operações de leitura (operações por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período. Unidades: • Bytes para `Sum`, `Minimum`, `Maximum` e `Average`. • Contagem de `SampleCount` . Estatísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrica	Descrição
`DataWriteOperations`	O número de operações de gravação. A estatística `Sum` corresponde ao número total de operações de gravação. A estatística `Minimum` corresponde ao número mínimo de operações de gravação em um único disco. A estatística `Maximum` corresponde ao número máximo de operações de gravação no disco. A estatística `Average` corresponde ao número médio de operações de gravação por disco. A estatística `SampleCount` corresponde ao número de discos. Para calcular o número médio de operações de gravação (operações por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período. Unidades: • Bytes para `Sum`, `Minimum`, `Maximum` e `Average`. • Contagem de `SampleCount` . Estatísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrica	Descrição
`Metadata0perations`	O número de operações de metadados. A estatística `Sum` corresponde à contagem de operações de metadados . A estatística `Minimum` corresponde ao número mínimo de operações de metadados por disco. A estatística `Maximum` corresponde ao número máximo de operações de metadados por disco. A estatística `Average` corresponde ao número médio de operações de metadados por disco. A estatística `SampleCount` corresponde ao número de discos. Para calcular o número médio de operações de metadados (operações por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período. Unidades: • Contagem para `Sum`, `Minimum`, `Maximum`, `Average` e `SampleCount` . Estatísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrica	Descrição
`FreeDataStorageCapacity`	A quantidade de capacidade de armazenamento disponível. A estatística `Sum` corresponde ao número total de bytes disponíveis no sistema de arquivos. A estatística `Minimum` corresponde ao número total de bytes disponíveis no disco que está mais cheio. A estatística `Maximum` corresponde ao número total de bytes disponíveis no disco com o maior armazenamento disponível restante. A estatística `Average` corresponde ao número médio de bytes disponíveis por disco. A estatística `SampleCount` corresponde ao número de discos. Unidades: • Bytes para `Sum`, `Minimum` e `Maximum`. • Contagem de `SampleCount` . Estatísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrica	Descrição
`LogicalDiskUsage`	A quantidade de dados lógicos armazenados (descompactados). A estatística `Sum` corresponde ao número total de bytes lógicos armazenados no sistema de arquivos. A estatística `Minimum` corresponde ao menor número de bytes lógicos armazenados em um disco no sistema de arquivos. A estatística `Maximum` corresponde ao maior número de bytes lógicos armazenados em um disco no sistema de arquivos. A estatística `Average` corresponde ao número médio de bytes lógicos armazenados por disco. A estatística `SampleCount` corresponde ao número de discos. Unidades: • Bytes para `Sum`, `Minimum` e `Maximum`. • Contagem de `SampleCount`. Estatísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métrica	Descrição
`PhysicalDiskUsage`	A quantidade de armazenamento ocupada fisicamente pelos dados do sistema de arquivos (compactados). A estatística `Sum` corresponde ao número total de bytes ocupados em discos no sistema de arquivos. A estatística `Minimum` corresponde ao número total de bytes ocupados no disco que está mais vazio. A estatística `Maximum` corresponde ao número total de bytes ocupados no disco que está mais cheio. A estatística `Average` corresponde ao número médio de bytes ocupados por disco. A estatística `SampleCount` corresponde ao número de discos. Unidades: • Bytes para `Sum`, `Minimum` e `Maximum`. • Contagem de `SampleCount` . Estatísticas válidas: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Métricas AutoImport e AutoExport

O FSx para Lustre publica as métricas `AutoImport` (importação automática) e `AutoExport` (exportação automática) apresentadas a seguir no namespace `FSx` no CloudWatch. Essas métricas usam dimensões para possibilitar medições mais granulares dos seus dados. Todas as métricas `AutoImport` e `AutoExport` têm as dimensões `FileSystemId` e `Publisher`.

Métrica	Descrição
`AgeOfOldestQueuedMessage` Dimensão: `AutoExport`	A idade, em segundos, da mensagem mais antiga que aguarda para ser exportada. A estatística `Average` corresponde à idade média da mensagem mais antiga que aguarda para ser exportada. A estatística `Maximum` corresponde ao número máximo de segundos que uma mensagem permaneceu na fila de exportação. A estatística `Minimum` corresponde

Métrica	Descrição
	ao número mínimo de segundos que uma mensagem permaneceu na fila de exportação. Um valor zero indica que nenhuma mensagem está aguardando para ser exportada. Unidade: segundos Estatísticas válidas: `Average`, `Minimum`, `Maximum`
`RepositoryRenameOperations` Dimensão: `AutoExport`	O número de renomeações processadas pelo sistema de arquivos em resposta a uma renomeação de diretório maior. A estatística `Sum` corresponde ao número total de operações de renomeação resultantes de uma renomeação de diretório. A estatística `Average` corresponde ao número médio de operações de renomeação para o sistema de arquivos. A estatística `Maximum` corresponde ao número máximo de operações de renomeação associadas com uma renomeação de diretório no sistema de arquivos. A estatística `Minimum` corresponde ao número mínimo de renomeações associadas com uma renomeação de diretório no sistema de arquivos. Unidade: contagem Estatísticas válidas: `Sum`, `Minimum`, `Maximum` e `Average`
`AgeOfOldestQueuedMessage` Dimensão: `AutoImport`	A idade, em segundos, da mensagem mais antiga que aguarda para ser importada. A estatística `Average` corresponde à idade média da mensagem mais antiga que aguarda para ser importada. A estatística `Maximum` corresponde ao número máximo de segundos que uma mensagem permaneceu na fila de importação. A estatística `Minimum` corresponde ao número mínimo de segundos que uma mensagem permaneceu na fila de importação. Um valor zero indica que nenhuma mensagem está aguardando para ser importada. Unidade: segundos Estatísticas válidas: `Average`, `Minimum`, `Maximum`

Dimensões do Amazon FSx para Lustre

As métricas do Amazon FSx para Lustre usam o namespace `FSx` e fornecem métricas para a dimensão `FileSystemId`. O ID de um sistema de arquivos pode ser encontrado usando o comando `describe-file-systems` da AWS CLI e assume o formato *`fs-01234567890123456`*.

Uma dimensão adicional, denominada `Publisher`, está disponível no CloudWatch e na AWS CLI para as métricas `AutoImport` e `AutoImport` com a finalidade de indicar qual serviço publicou as métricas.

Como usar as métricas do Amazon FSx para Lustre

As métricas relatadas pelo Amazon FSx para Lustre fornecem informações que podem ser analisadas de diferentes maneiras. A lista apresentada a seguir mostra alguns usos comuns para as métricas. Essas são sugestões para você começar, e não uma lista abrangente.

Como faço para determinar...	Métricas relevantes (dimensão | métrica)
O throughput do meu sistema de arquivos?	SUM(DataReadBytes + DataWriteBytes)/período (em segundos)
As IOPS do meu sistema de arquivos?	Total de IOPS = SUM(DataReadOperations + DataWriteOperations + MetadataOperations)/período (em segundos)
A taxa de compactação de dados do meu sistema de arquivos?	SUM(LogicalDiskUsage)/SUM(PhysicalDiskUsage)
Se as atualizações do meu sistema de arquivos foram sincronizadas com meu bucket do S3?	AutoExport | AgeOfOldestQueuedMessage
Se as atualizações do meu bucket do S3 foram sincronizadas	AutoImport | AgeOfOldestQueuedMessage

Como faço para determinar...	Métricas relevantes (dimensão | métrica)
com meu sistema de arquivos?	

Matemática em métricas: taxa de compactação de dados

Com matemática métrica, você pode consultar várias métricas do CloudWatch e usar expressões matemáticas para criar novas séries temporais de acordo com essas métricas. Você pode visualizar as séries temporais resultantes no console do CloudWatch e adicioná-las aos painéis. Para obter mais informações sobre a matemática em métricas, consulte Usar matemática em métricas no Guia do usuário do Amazon CloudWatch.

Essa expressão matemática em métricas calcula a taxa de compactação de dados do seu sistema de arquivos do Amazon FSx para Lustre. Para calcular essa taxa, primeiro é necessário obter a estatística da soma do uso total do disco lógico (sem compactação), que é fornecida pela métrica `LogicalDiskUsage`. Em seguida, divida isso pela estatística da soma do uso total do disco físico (com compactação), fornecida pela métrica `PhysicalDiskUsage`.

Portanto, se sua lógica corresponde a soma de `LogicalDiskUsage` dividida (÷) pela soma de `PhysicalDiskUsage`,

Então, as informações da sua métrica do são as seguintes:

ID	Métrica utilizável	Estatística	Período
m1	`LogicalDiskUsage`	Sum	1 minuto
m2	`PhysicalDiskUsage`	Sum	1 minuto

O ID e a expressão matemáticos da métrica são os seguintes:

ID	Expressão
e1	m1/m2

e1 corresponde à taxa de compactação de dados.

Acessar métricas do CloudWatch

É possível visualizar as métricas do Amazon FSx para Lustre para o CloudWatch de diversas maneiras. Você pode visualizá-las usando o console do CloudWatch, ou acessá-las usando a CLI do CloudWatch ou a API do CloudWatch. Os procedimentos a seguir mostram como acessar as métricas usando essas diversas ferramentas.

Como visualizar métricas usando o console do CloudWatch

1. Abra o console do CloudWatch.
2. No painel de navegação, escolha Metrics (Métricas).
3. Selecione o namespace FSx.
4. (Opcional) Para visualizar um tipo de métrica, digite seu nome no campo de pesquisa.
5. (Opcional) Para filtrar por dimensão, selecione FileSystemId.

Para acessar as métricas a partir da AWS CLI

- Use o comando `list-metrics` com o namespace `--namespace "AWS/FSx"`. Para obter mais informações, consulte Referência de comandos da AWS CLI.

Acessar as métricas com a API do CloudWatch

- Chame `GetMetricStatistics`. Para obter mais informações, consulte a referência de APIs do Amazon CloudWatch.

Como criar alarmes do CloudWatch para monitorar o Amazon FSx para Lustre

Você pode criar um alarme do CloudWatch que envia uma mensagem do Amazon SNS quando o alarme muda de estado. Um alarme observa uma única métrica ao longo de um período especificado por você e realiza uma ou mais ações com base no valor da métrica relativo a um determinado limite ao longo de vários períodos. A ação é uma notificação enviada para um tópico do Amazon SNS ou uma política de Auto Scaling.

Os alertas invocam ações apenas para alterações de estado mantidas. Os alarmes do CloudWatch não invocam ações simplesmente por estarem em um estado específico. O estado deve ter sofrido alteração e deve ter sido mantido por um determinado número de períodos.

Os procedimentos apresentados a seguir descrevem como criar alarmes para o Amazon FSx para Lustre.

Para definir alertas usando o console do CloudWatch

1. Faça login no AWS Management Console e abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. Escolha Create Alarm. Isso executa o Assistente para criação de alarmes.
3. Escolha Métricas do FSx e navegue pelas métricas do Amazon FSx para Lustre para localizar a métrica na qual você deseja estabelecer um alarme. Para exibir apenas as métricas do Amazon FSx para Lustre nesta caixa de diálogo, pesquise o ID do sistema de arquivos do seu sistema de arquivos. Escolha a métrica para a qual um alarme será criado e clique em Próximo.
4. Na seção Condições, escolha as condições desejadas para o alarme e clique em Próximo.

   > **Note**
   >
   > As métricas não podem ser publicadas durante a manutenção do sistema de arquivos. Para evitar alterações desnecessárias e equivocadas nas condições de alarmes e configurar os alarmes para que sejam resilientes a pontos de dados ausentes, consulte Configurar como os alarmes do CloudWatch tratam dados ausentes no Guia do usuário do Amazon CloudWatch.

5. Se você quiser que o CloudWatch envie um e-mail quando o estado do alarme for atingido, em Sempre que este alarme, escolha Estado ALARM. Em Enviar notificação para, escolha um

tópico do SNS existente. Se escolher Create topic (Criar tópico), você poderá definir o nome e o endereço de e-mail para uma nova lista de assinaturas de e-mail. Esta lista será salva e será exibida nesta caixa para alarmes futuros.

> **Note**
>
> Se você usar Criar tópico para criar um novo tópico do Amazon SNS, verifique os endereços de e-mail antes de enviar notificações. Os e-mails são enviados apenas quando o alarme entra em um status de alarme. Se essa alteração no status de alarme ocorrer antes que os endereços de e-mail sejam verificados, eles não receberão notificação.

6. Visualize o alarme que você está prestes a criar na área Visualização do alarme. Se aparecer conforme o esperado, escolha Criar alarme.

Para definir um alarme usando a AWS CLI

- Chame `put-metric-alarm`. Para obter mais informações, consulte Referência de comandos da AWS CLI.

Para definir um alarme usando a API do CloudWatch

- Chame `PutMetricAlarm`. Para obter mais informações, consulte a referência de APIs do Amazon CloudWatch.

Registro com Amazon CloudWatch Logs

O FSx for Lustre suporta o registro de eventos de erro e aviso para repositórios de dados associados ao seu sistema de arquivos no Amazon Logs. CloudWatch

> **Note**
>
> O registro com o Amazon CloudWatch Logs só está disponível nos sistemas de arquivos Amazon FSx for Lustre criados após as 15h PST de 30 de novembro de 2021.

Tópicos

Visão geral do registro em log

Se você tiver repositórios de dados vinculados ao seu sistema de arquivos FSx for Lustre, você pode habilitar o registro de eventos do repositório de dados no Amazon Logs. CloudWatch Eventos de erros e de avisos podem ser registrados em log usando as seguintes operações do repositório de dados:

- Exportação automática
- Tarefas de repositório de dados

Para obter mais informações sobre essas operações e sobre a vinculação a repositórios de dados, consulte Como usar repositórios de dados com o Amazon FSx para Lustre.

É possível configurar os níveis de log que o Amazon FSx registra. Em outras palavras, se o Amazon FSx registrará em log somente eventos de erros, somente eventos de avisos ou eventos de erros e de avisos. Você também pode desativar o registro em log de eventos a qualquer momento.

> **Note**
>
> É altamente recomendável habilitar logs para sistemas de arquivos que tenham qualquer nível de funcionalidade crítica associada a eles.

Destinos de logs

Quando o registro está ativado, o FSx for Lustre deve ser configurado com um destino CloudWatch Amazon Logs. O destino do log de eventos é um grupo de CloudWatch logs do Amazon Logs, e o Amazon FSx cria um stream de log para seu sistema de arquivos dentro desse grupo de logs. CloudWatch O Logs permite que você armazene, visualize e pesquise registros de eventos de auditoria no CloudWatch console da Amazon, execute consultas nos CloudWatch registros usando o Logs Insights e acione CloudWatch alarmes ou funções Lambda.

Você escolhe o destino do log ao criar o sistema de arquivos do FSx para Lustre ou posteriormente ao atualizá-lo. Para ter mais informações, consulte Como gerenciar registros em log.

Por padrão, o Amazon FSx criará e usará um grupo padrão de CloudWatch registros de registros em sua conta como destino do registro de eventos. Se você quiser usar um grupo de registros de CloudWatch registros personalizado como destino do registro de eventos, aqui estão os requisitos para o nome e a localização do destino do registro de eventos:

- O nome do grupo de CloudWatch registros de registros deve começar com o `/aws/fsx/` prefixo.
- Se você não tiver um grupo de registros de CloudWatch registros existente ao criar ou atualizar um sistema de arquivos no console, o Amazon FSx for Lustre poderá criar e usar um fluxo de registros padrão CloudWatch `/aws/fsx/lustre` no grupo de registros de registros. O fluxo de logs será criado com o formato `datarepo_`*`file_system_id`* (por exemplo, `datarepo_fs-0123456789abcdef0`).
- Se você não quiser usar o grupo de registros padrão, a interface de configuração permite criar um grupo de CloudWatch registros de registros ao criar ou atualizar seu sistema de arquivos no console.
- O grupo de CloudWatch logs de Logs de destino deve estar na mesma AWS partição e em seu Conta da AWS sistema de arquivos Amazon FSx for Lustre. Região da AWS

É possível alterar o destino do log de eventos a qualquer momento. Ao fazer isso, novos logs de eventos serão enviados somente para o novo destino.

Como gerenciar registros em log

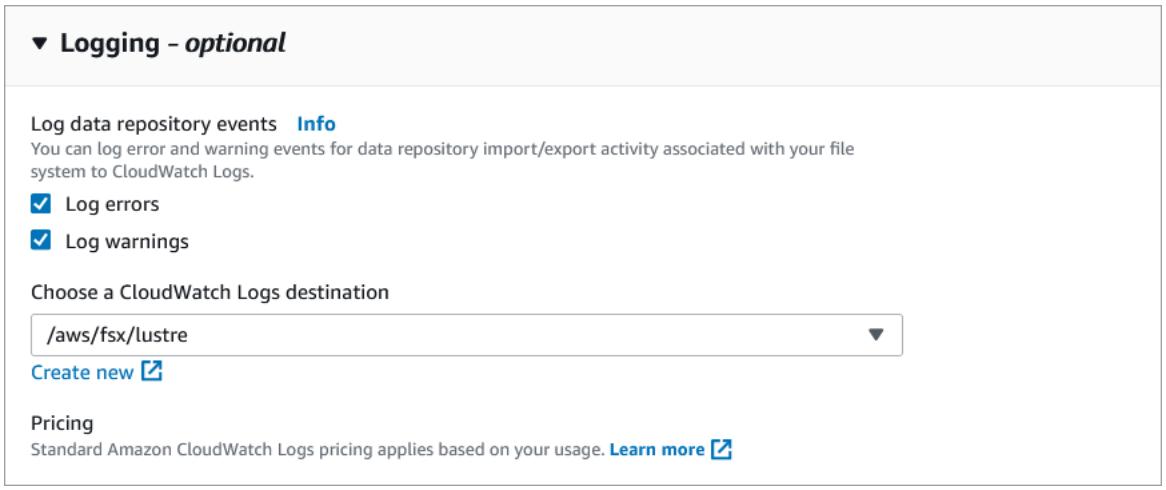
É possível habilitar o registro em log ao criar um novo sistema de arquivos do FSx para Lustre ou posteriormente ao atualizá-lo. O registro em log está ativado por padrão quando você cria um sistema de arquivos usando o console do Amazon FSx. No entanto, o registro é desativado por padrão quando você cria um sistema de arquivos com a API Amazon FSx AWS CLI ou Amazon FSx.

Em sistemas de arquivos existentes que têm o registro em log habilitado, é possível alterar as configurações de registro em log de eventos, incluindo o nível de log em que os eventos serão registrados em log e o destino do log. Você pode realizar essas tarefas usando o console Amazon FSx ou a API AWS CLI Amazon FSx.

Como habilitar o registro em log ao criar um sistema de arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.

2. Siga o procedimento para a criação de um novo sistema de arquivos descrito na Crie seu sistema de arquivos FSx for Lustre na seção de Conceitos básicos.
3. Abra a seção Registro em log (opcional). Por padrão, o registro em log está habilitado.



4. Prossiga para a próxima seção do assistente de criação do sistema de arquivos.

Quando o sistema de arquivos se tornar Disponível, o registro em log será habilitado.

Como habilitar o registro em log ao criar um sistema de arquivos (CLI)

1. Ao criar um novo sistema de arquivos, use a `LogConfiguration` propriedade com a CreateFileSystemoperação para habilitar o registro para o novo sistema de arquivos.

```
create-file-system --file-system-type LUSTRE \
    --storage-capacity 1200 --subnet-id subnet-08b31917a72b548a9  \
    --lustre-configuration "LogConfiguration={Level=WARN_ERROR, \
        Destination="arn:aws:logs:us-east-1:234567890123:log-group:/aws/fsx/
testEventLogging"}"
```

2. Quando o sistema de arquivos se tornar Disponível, o recurso de registro em log será habilitado.

Como alterar a configuração de registro em log (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do Lustre para o qual você deseja gerenciar o registro em log.
3. Escolha a guia Monitoring (Monitoramento).
4. No painel Registro em log, escolha Atualizar.

5. Na caixa de diálogo Atualizar a configuração de registro em log, altere as configurações desejadas.

   a. Escolha Registro em log de erros para registrar somente eventos de erros, Registro em log de avisos para registrar somente eventos de aviso, ou ambos. O registro em log será desabilitado se você não realizar uma seleção.

   b. Escolha um destino de registro de CloudWatch registros existente ou crie um novo.

6. Escolha Salvar.

Como alterar a configuração de registro em log (CLI)

- Use o comando `update-file-system` da CLI ou a operação de API `UpdateFileSystem` equivalente.

```
update-file-system --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration "LogConfiguration={Level=WARN_ERROR, \
        Destination="arn:aws:logs:us-east-1:234567890123:log-group:/aws/fsx/
testEventLogging"}"
```

Visualizar logs do

É possível visualizar os logs depois que o Amazon FSx começar a emiti-los. Você pode visualizar os logs da seguinte forma:

- Você pode visualizar os registros acessando o CloudWatch console da Amazon e escolhendo o grupo de registros e o stream de registros para os quais seus registros de eventos são enviados. Para obter mais informações, consulte Exibir dados de log enviados para CloudWatch Logs no Guia do usuário do Amazon CloudWatch Logs.
- Você pode usar o CloudWatch Logs Insights para pesquisar e analisar interativamente seus dados de registro. Para obter mais informações, consulte Análise de dados de log com o CloudWatch Logs Insights, no Guia do usuário do Amazon CloudWatch Logs.
- Você também pode exportar logs para o Amazon S3. Para obter mais informações, consulte Exportação de dados de log para o Amazon S3, no Guia do usuário do CloudWatch Amazon Logs.

Para saber mais sobre os motivos das falhas, consulte Registros em log de eventos de repositório de dados.

Registro em log de chamadas de API do FSx para Lustre com o AWS CloudTrail

O Amazon FSx para Lustre é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações executadas por um usuário, um perfil ou um serviço da AWS no Amazon FSx para Lustre. O CloudTrail captura todas as chamadas de API para o Amazon FSx para Lustre como eventos. As chamadas capturadas incluem as chamadas do console do Amazon FSx para Lustre e as chamadas de códigos para as operações de API do Amazon FSx para Lustre.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo os eventos para o Amazon FSx para Lustre. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Com as informações coletadas pelo CloudTrail, é possível determinar a solicitação que foi realizada ao Amazon FSx para Lustre. Você também pode determinar o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, e detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações do Amazon FSx para Lustre no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre uma atividade da API no Amazon FSx para Lustre, essa atividade é registrada em um evento do CloudTrail em conjunto com outros eventos de serviços da AWS em Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo dos eventos em sua conta da AWS, incluindo os eventos do Amazon FSx para Lustre, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões da AWS na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS CloudTrail:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas

Todas as chamadas de API do Amazon FSx para Lustre são registradas em log pelo CloudTrail. Por exemplo, as chamadas para as operações `CreateFileSystem` e `TagResource` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o Elemento userIdentity do CloudTrail no Manual do usuário do AWS CloudTrail.

Noções básicas sobre as entradas de arquivos de log do Amazon FSx para Lustre

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a operação `TagResource` quando uma tag para um sistema de arquivos é criada no console.

```
{
```

```
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `UntagResource` quando uma tag para um sistema de arquivos é excluída do console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

Segurança no FSx para Lustre

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS serviços na Amazon Web Services Cloud. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Amazon FSx para Lustre, consulte Serviços da AWS no escopo pelo programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon FSx para Lustre. Os tópicos a seguir mostram como configurar o Amazon FSx para atender aos seus objetivos de segurança e compatibilidade. Você também aprende a usar outros serviços da Amazon que ajudam a monitorar e proteger os recursos do Amazon FSx para Lustre.

A seguir, você poderá encontrar uma descrição das considerações de segurança para trabalhar com o Amazon FSx.

Tópicos

Proteção de dados no Amazon FSx para Lustre

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no Amazon FSx for Lustre. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Amazon FSx ou outros Serviços da AWS usando o console, a API ou AWS os AWS CLI SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de

diagnóstico. Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Tópicos

Criptografia de dados no Amazon FSx para Lustre

O Amazon FSx para Lustre oferece suporte a duas formas de criptografia para sistemas de arquivos: a criptografia de dados em repouso e a criptografia em trânsito. A criptografia de dados em repouso é habilitada automaticamente ao criar um sistema de arquivos do Amazon FSx. A criptografia de dados em trânsito é automaticamente habilitada quando você acessa um sistema de arquivos do Amazon FSx usando instâncias do Amazon EC2 que oferecem suporte a esse recurso.

Quando usar a criptografia

Se a sua organização estiver sujeita a políticas corporativas ou regulatórias que requerem criptografia de dados e de metadados em repouso, recomendamos criar um sistema de arquivos criptografado e montar o sistema de arquivos usando a criptografia de dados em trânsito.

Para obter mais informações sobre como criar um sistema de arquivos criptografado em repouso usando o console, consulte Como criar o sistema de arquivos do Amazon FSx para Lustre.

Tópicos

Criptografia de dados em repouso

A criptografia de dados em repouso é ativada automaticamente quando você cria um sistema de arquivos Amazon FSx for Lustre por AWS Management Console meio do AWS CLI, do ou programaticamente por meio da API Amazon FSx ou de um dos SDKs. AWS Sua organização pode exigir a criptografia de todos os dados que atendem a uma classificação específica ou estejam associados a um determinado aplicativo, workload ou ambiente. Se você criar um sistema de arquivos persistente, poderá especificar a AWS KMS chave com a qual criptografar os dados. Se você criar um sistema de arquivos transitório, os dados serão criptografados usando chaves

gerenciadas pelo Amazon FSx. Para obter mais informações sobre como criar um sistema de arquivos criptografado em repouso usando o console, consulte Como criar o sistema de arquivos do Amazon FSx para Lustre.

> **Note**
>
> A infraestrutura de gerenciamento de AWS chaves usa algoritmos criptográficos aprovados pelo Federal Information Processing Standards (FIPS) 140-2. A infraestrutura é consistente com as recomendações 800-57 do National Institute of Standards and Technology (NIST).

Para obter mais informações sobre como o FSx for AWS KMS Lustre é usado, consulte. Como o Amazon FSx for Lustre usa AWS KMS

Como funciona a criptografia em repouso

Em um sistema de arquivos criptografado, os dados e metadados são criptografados automaticamente antes de serem gravados no sistema de arquivos. De maneira semelhante, à medida que os dados e metadados são lidos, eles são automaticamente descriptografados antes de serem apresentados ao aplicativo. Esses processos são tratados de maneira transparente pelo Amazon FSx para Lustre. Portanto, não é necessário modificar as aplicações.

O Amazon FSx para Lustre usa um algoritmo de criptografia AES-256 padrão do setor para criptografar dados em repouso do sistema de arquivos. Para obter mais informações, consulte Cryptography Basics no Guia do desenvolvedor do AWS Key Management Service .

Como o Amazon FSx for Lustre usa AWS KMS

O Amazon FSx for Lustre criptografa os dados automaticamente antes de serem gravados no sistema de arquivos e os descriptografa automaticamente à medida que são lidos. Os dados são criptografados usando uma cifra de bloco XTS-AES-256. Todos os sistemas de arquivos scratch FSx for Lustre são criptografados em repouso com chaves gerenciadas por. AWS KMS O Amazon FSx for Lustre se AWS KMS integra ao gerenciamento de chaves. As chaves usadas para criptografar sistemas de arquivos transitórios em repouso são exclusivas por sistema de arquivos e são destruídas após a exclusão do sistema de arquivos. Para sistemas de arquivos persistentes, você escolhe a chave KMS usada para criptografar e descriptografar dados. Você especifica qual chave será usada ao criar um sistema de arquivos persistente. É possível habilitar, desabilitar ou revogar as concessões nessa chave do KMS. Essa chave do KMS pode ser de um dos seguintes dois tipos:

- Chave gerenciada pela AWS para Amazon FSx — Essa é a chave KMS padrão. Você não recebe cobranças pela criação e pelo armazenamento de uma chave do KMS, mas existem cobranças de uso. Para obter mais informações, consulte Preços do AWS Key Management Service.
- Chave gerenciada pelo cliente: essa é a chave do KMS mais flexível para usar, pois é possível configurar suas políticas de chaves e concessões para diversos usuários ou serviços. Para obter mais informações sobre a criação de chaves gerenciadas pelo cliente, consulte Criação de chaves no Guia do AWS Key Management Service desenvolvedor.

Se você usar uma chave gerenciada pelo cliente como a chave do KMS para descriptografia e criptografia de dados de arquivos, poderá habilitar a rotação de chaves. Quando você ativa a rotação de chaves, gira AWS KMS automaticamente sua chave uma vez por ano. Além disso, com uma chave gerenciada pelo cliente, é possível escolher quando desabilitar, habilitar novamente, excluir ou revogar o acesso à chave gerenciada pelo cliente a qualquer momento.

> **Important**
>
> O Amazon FSx aceita somente chaves do KMS com criptografia simétrica. Não é possível usar chaves do KMS assimétricas com o Amazon FSx.

Políticas-chave do Amazon FSx para AWS KMS

Políticas de chaves são a principal maneira de controlar o acesso a chaves do KMS. Para obter mais informações sobre as políticas de chaves, consulte Using key policies in AWS KMS no Guia do desenvolvedor do AWS Key Management Service .A lista a seguir descreve todas as permissões relacionadas ao AWS KMS com suporte no Amazon FSx para sistemas de arquivos criptografados em repouso:

- kms:Encrypt: (opcional) criptografa texto simples em texto cifrado. Essa permissão está incluída na política de chaves padrão.
- kms:Decrypt - (Obrigatório) Descriptografa texto cifrado. O texto cifrado é o texto simples que já foi criptografado. Essa permissão está incluída na política de chaves padrão.
- kms: ReEncrypt — (Opcional) Criptografa dados no lado do servidor com uma nova chave KMS, sem expor o texto simples dos dados no lado do cliente. Primeiro os dados são descriptografados e, depois, recriptografados. Essa permissão está incluída na política de chaves padrão.

- kms: GenerateDataKeyWithoutPlaintext — (Obrigatório) Retorna uma chave de criptografia de dados criptografada sob uma chave KMS. Essa permissão está incluída na política de chaves padrão em kms: GenerateDataKey *.
- kms: CreateGrant — (Obrigatório) Adiciona uma concessão a uma chave para especificar quem pode usar a chave e sob quais condições. Concessões são mecanismos de permissão alternativos para políticas de chaves. Para obter mais informações sobre concessões, consulte Using grants no Guia do desenvolvedor do AWS Key Management Service .. Essa permissão está incluída na política de chaves padrão.
- kms: DescribeKey — (Obrigatório) Fornece informações detalhadas sobre a chave KMS especificada. Essa permissão está incluída na política de chaves padrão.
- kms: ListAliases — (Opcional) Lista todos os aliases de chave na conta. Quando você usa o console para criar um sistema de arquivos criptografado, essa permissão preenche a lista para selecionar a chave do KMS. Recomendamos usar essa permissão para proporcionar a melhor experiência do usuário. Essa permissão está incluída na política de chaves padrão.

Criptografia de dados em trânsito

Sistemas de arquivos persistentes e Scratch 2 podem criptografar automaticamente os dados em trânsito. Na tabela a seguir, se houver uma marca de seleção na célula para esse tipo de implantação Região da AWS, os dados serão criptografados em trânsito quando o sistema de arquivos for acessado a partir de instâncias do Amazon EC2 que oferecem suporte à criptografia em trânsito e também para todas as comunicações entre hosts dentro do sistema de arquivos. Para saber quais instâncias do EC2 oferecem suporte à criptografia em trânsito, consulte Criptografia em trânsito no Guia do usuário do Amazon EC2 para instâncias do Linux.

A criptografia de dados em trânsito para sistemas de arquivos Scratch 2 e persistentes está disponível a seguir Regiões da AWS.

Região da AWS	Scratch_2	Persistent_1	Persistent_2
Leste dos EUA (Ohio)	✓	✓	✓
Leste dos EUA (N. da Virgínia)	✓	✓	✓
Oeste dos EUA (Oregon)	✓	✓	✓
Oeste dos EUA (N. da Califórnia) *	✓	✓	

Região da AWS	Scratch_2	Persistent_1	Persistent_2
Oeste dos EUA (Los Angeles)	✓	✓	
AWS GovCloud (Leste dos EUA) *	✓	✓	
AWS GovCloud (Oeste dos EUA)	✓	✓	
Canadá (Central) *	✓	✓	✓
Europa (Irlanda)	✓	✓	✓
Europa (Milão)	✓	✓	
Europa (Frankfurt)	✓	✓	✓
Europa (Paris)	✓	✓	
Europa (Londres)	✓	✓	✓
Europa (Estocolmo) *	✓	✓	✓
Ásia-Pacífico (Seul)	✓		✓
Ásia-Pacífico (Singapura)	✓	✓	✓
Ásia-Pacífico (Tóquio) *	✓	✓	✓
Ásia-Pacífico (Mumbai) *	✓	✓	✓
Ásia-Pacífico (Hong Kong) *	✓	✓	✓
Ásia-Pacífico (Sydney) *	✓	✓	✓
Israel (Tel Aviv) *		✓	
América do Sul (São Paulo) *	✓	✓	

> **Note**
>
> * A criptografia de dados em trânsito está disponível para sistemas de arquivos criados após 11 de abril de 2021.

Privacidade do tráfego entre redes

Este tópico descreve como o Amazon FSx protege conexões do serviço para outros locais.

Tráfego entre o Amazon FSx e os clientes on-premises

Você tem duas opções de conectividade entre sua rede privada e AWS:

- Uma AWS Site-to-Site VPN conexão. Para obter mais informações, consulte O que é AWS Site-to-Site VPN?
- Uma AWS Direct Connect conexão. Para obter mais informações, consulte O que é AWS Direct Connect?

Você pode acessar o FSx for Lustre pela rede para acessar operações de API publicadas AWS para realizar tarefas administrativas e portas Lustre para interagir com o sistema de arquivos.

Criptografia do tráfego da API

Para acessar as operações AWS de API publicadas, os clientes devem oferecer suporte ao Transport Layer Security (TLS) 1.2 ou posterior. Exigimos TLS 1.2 e recomendamos TLS 1.3. Os clientes também devem ter suporte a pacotes de criptografia com sigilo de encaminhamento perfeito (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos. Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Como alternativa, é possível usar o AWS Security Token Service (STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Criptografia do tráfego de dados

A criptografia de dados em trânsito é habilitada usando instâncias do EC2 com suporte que acessam os sistemas de arquivos na Nuvem AWS. Para ter mais informações, consulte Criptografia de dados

em trânsito. O FSx para Lustre não oferece criptografia nativa em trânsito entre clientes on-premises e sistemas de arquivos.

Gerenciamento de identidade e acesso no Amazon FSx para Lustre

O AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda o administrador a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) para utilizar os recursos do Amazon FSx. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

Público

A forma de usar o AWS Identity and Access Management (IAM) varia em função do trabalho realizado no Amazon FSx.

Usuário do serviço: se você usar o serviço do Amazon FSx para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que mais recursos do Amazon FSx forem usados para realizar o trabalho, talvez sejam necessárias permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador.

Se você não puder acessar um recurso no Amazon FSx, consulte Solução de problemas de identidade e acesso do Amazon FSx para Lustre.

Administrador do serviço: se você for o responsável pelos recursos do Amazon FSx em sua empresa, provavelmente terá acesso total ao Amazon FSx. Cabe a você determinar quais funcionalidades e recursos do Amazon FSx os usuários do serviço deverão acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Amazon FSx, consulte Como o Amazon FSx para Lustre funciona com o IAM.

Administrador do IAM: se você for administrador do IAM, talvez deseje saber detalhes sobre como criar políticas para gerenciar o acesso ao Amazon FSx. Para ver exemplos de políticas baseadas em identidade do Amazon FSx que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o Amazon FSx para Lustre.

Autenticando com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. É necessário ser autenticado (fazer login na AWS) como o usuário raiz da Usuário raiz da conta da AWS, como usuário do IAM ou assumindo um perfil do IAM.

É possível fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS IAM Identity Center Os usuários do IAM Identity Center, a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades utilizando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

É possível fazer login no AWS Management Console ou no de acesso da AWS dependendo do tipo de usuário que você é. Para obter mais informações sobre como fazer login na AWS, consulte Conta da AWS Como fazer login na sua no Início de Sessão da AWS Guia do usuário.

Se você acessar a AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface da linha de comando (CLI) para você assinar criptograficamente as solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinar solicitações de API da AWS no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça mais informações de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator (MFA) naAWS no Guia do usuário do IAM.

Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os atributos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não utilizar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da web AWS Directory Service, o , o diretório do Centro de Identidade ou qualquer usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o .AWS IAM Identity Center É possível criar usuários e grupos no Centro de Identidade do IAM ou se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicações. Para obter mais informações sobre o IAM Identity Center, consulte “O que é o IAM Identity Center?” no Guia do usuário do AWS IAM Identity Center.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e

chaves de acesso. No entanto, se você tiver casos de utilização específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível utilizar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar uma função para um provedor de identidade de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, deverá configurar um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário do AWS IAM Identity Center.
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.

- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso no Guia do usuário do IAM.
- Acesso entre serviços: alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou uma função vinculada ao serviço.
  - Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
  - Função vinculada a serviço: uma função vinculada a serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir o perfil de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.
- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de

instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Como gerenciar acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de perfis do AWS Management Console, da AWS CLI ou da API da AWS.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas embutidas ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recurso

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços compatíveis com ACLs. Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS aceita tipos de política menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade

do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, incluindo cada .Usuário raiz da conta da AWS Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) noAWS Organizations Guia do usuário do .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte Lógica da avaliaçãode políticas no Guia do usuário do IAM.

Como o Amazon FSx para Lustre funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Amazon FSx, saiba quais recursos do IAM estão disponíveis para uso com o Amazon FSx.

Atributos do IAM que você pode usar com o Amazon FSx para Lustre

atributo do IAM	Suporte do Amazon FSx
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
atributos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para obter uma visão geral de como o Amazon FSx e outros serviços da AWS funcionam com a maioria dos recursos do IAM, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade do Amazon FSx

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que é possível anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou atributos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil à qual ela está anexado. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para o Amazon FSx

Para ver exemplos de políticas baseadas em identidade do Amazon FSx, consulte Exemplos de políticas baseadas em identidade para o Amazon FSx para Lustre.

Políticas baseadas em recursos no Amazon FSx

Oferece suporte a políticas baseadas em recurso	Não

Ações de políticas para o Amazon FSx

Oferece suporte a ações de políticas	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que é possível usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do Amazon FSx, consulte Ações definidas pelo Amazon FSx para Lustre na Referência de autorização do serviço.

As ações de política no Amazon FSx usam o seguinte prefixo antes da ação:

```
fsx
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Para ver exemplos de políticas baseadas em identidade do Amazon FSx, consulte Exemplos de políticas baseadas em identidade para o Amazon FSx para Lustre.

Recursos de políticas do Amazon FSx

Oferece suporte a atributos de políticas	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política `Resource` JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu Nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um caractere curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do Amazon FSx e seus ARNs, consulte Recursos definidos pelo Amazon FSx para Lustre na Referência de autorização do serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Amazon FSx para Lustre.

Para ver exemplos de políticas baseadas em identidade do Amazon FSx, consulte Exemplos de políticas baseadas em identidade para o Amazon FSx para Lustre.

Chaves de condição de política para o Amazon FSx

Suporta chaves de condição de política específicas de serviço	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou `Condition` bloco de) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam atendentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

É possível também usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as AWS chaves de condição globais da , consulte AWSChaves de contexto de condição globais da no Guia do usuário do IAM.

Para ver uma lista de chaves de condição do Amazon FSx, consulte Chaves de condição do Amazon FSx para Lustre na Referência de autorização do serviço. Para saber com quais ações e recursos é possível usar a chave de condição, consulte Ações definidas pelo Amazon FSx para Lustre.

Para ver exemplos de políticas baseadas em identidade do Amazon FSx, consulte Exemplos de políticas baseadas em identidade para o Amazon FSx para Lustre.

Listas de controle de acesso (ACLs) no Amazon FSx

Oferece suporte a ACLs	Não

Controle de acesso por atributo (ABAC) com o Amazon FSx

Oferece suporte a ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos recursos da AWS. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do atributo que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Para obter mais informações sobre como marcar recursos do Amazon FSx, consulte Marcar os recursos do Amazon FSx.

Para visualizar um exemplo de política baseada em identidade para limitar o acesso a um atributo baseado em tags desse atributo, consulte Como usar tags para controlar o acesso aos seus recursos do Amazon FSx.

Como usar credenciais temporárias com o Amazon FSx

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se faz login no AWS Management Console usando qualquer método, exceto um nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

É possível criar credenciais temporárias manualmente usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar aAWS .AWS A recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para Amazon FSx

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou um perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Perfis de serviço para o Amazon FSx

Oferece suporte a perfis de serviço	Não

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

> **Warning**
>
> A alteração das permissões de um perfil de serviço pode interromper a funcionalidade do Amazon FSx. Só edite os perfis de serviço quando o Amazon FSx fornecer orientação para isso.

Perfis vinculados ao serviço para Amazon FSx

Oferece suporte a perfis vinculados ao serviço	Sim

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir o perfil de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter mais informações sobre como criar e gerenciar perfis vinculados ao serviço do Amazon FSx, consulte Como usar perfis vinculados a serviço no Amazon FSx.

Exemplos de políticas baseadas em identidade para o Amazon FSx para Lustre

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Amazon FSx. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API AWS. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recurso definidos pelo Amazon FSx, incluindo o formato dos ARNs de cada tipo de recurso, consulte Ações, recursos e chaves de condição do Amazon FSx para Lustre na Referência de autorização do serviço.

Tópicos

Melhores práticas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Amazon FSx em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com AWS as políticas gerenciadas pela e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as AWS políticas gerenciadas pela que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. É possível também usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condição no Manual do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Como usar o console do Amazon FSx

Para acessar o console do Amazon FSx para Lustre, você deve ter um conjunto mínimo de permissões. Essas permissões devem deixar que você liste e visualize detalhes sobre os recursos do Amazon FSx em sua Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e perfis ainda possam usar o console do Amazon FSx, anexe também a política `AmazonFSxConsoleReadOnlyAccess` gerenciada pela AWS às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Você pode ver as políticas `AmazonFSxConsoleReadOnlyAccess` e outras políticas de serviço gerenciadas do Amazon FSx em AWS políticas gerenciadas para Amazon FSx.

Permitir que os usuários exibam as próprias permissões

Este exemplo mostra como é possível criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política

inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS políticas gerenciadas para Amazon FSx

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para obter mais informações, consulte AWS Políticas gerenciadas pela no Guia do usuário do IAM.

Amazon F SxServiceRolePolicy

Permite que o Amazon FSx gerencie AWS recursos em seu nome. Para saber mais, consulte Como usar perfis vinculados a serviço no Amazon FSx.

AWS política gerenciada: AmazonF SxDeleteServiceLinkedRoleAccess

Não é possível anexar `AmazonFSxDeleteServiceLinkedRoleAccess` às entidades do IAM. Essa política está vinculada a um serviço e só é usada com o perfil vinculado a esse serviço. Você não pode anexar, desanexar, modificar ou excluir essa política. Para ter mais informações, consulte Como usar perfis vinculados a serviço no Amazon FSx.

Essa política concede permissões administrativas que permitem que o Amazon FSx exclua o perfil vinculado ao serviço para acesso do Amazon S3, usado somente pelo Amazon FSx para Lustre.

Detalhes da permissão

Essa política inclui permissões `iam` para permitir que o Amazon FSx visualize, exclua e visualize o status de exclusão da função vinculada ao serviço FSx para acesso ao Amazon S3.

Para ver as permissões dessa política, consulte a AmazonF SxDeleteServiceLinkedRoleAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonF SxFullAccess

Você pode anexar o AmazonF SxFullAccess às suas entidades do IAM. O Amazon FSx também anexa essa política a um perfil de serviço que permite que o Amazon FSx execute ações em seu nome.

Fornece acesso total ao Amazon FSx e acesso aos serviços relacionados AWS .

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`: permite que as entidades principais tenham acesso total para executar todas as ações do Amazon FSx, exceto `BypassSnaplockEnterpriseRetention`.
- `ds`— Permite que os diretores visualizem informações sobre os AWS Directory Service diretórios.
- `ec2`
  - Permite que os diretores criem tags sob as condições especificadas.
  - Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança que podem ser usados com uma VPC.
- `iam`: permite que as entidades principais criem um perfil vinculado ao serviço do Amazon FSx em nome do usuário. Isso é necessário para que o Amazon FSx possa gerenciar AWS recursos em nome do usuário.
- `logs`: permite que as entidades principais criem grupos de logs, fluxos de logs e gravem eventos nos fluxos de logs. Isso é necessário para que os usuários possam monitorar o acesso ao sistema de arquivos do FSx for Windows File Server enviando registros de acesso de auditoria CloudWatch para o Logs.
- `firehose`— Permite que os diretores gravem registros em um Amazon Data Firehose. Isso é necessário para que os usuários possam monitorar o acesso ao sistema de arquivos FSx for Windows File Server enviando registros de acesso de auditoria para o Firehose.

Para ver as permissões dessa política, consulte a AmazonF SxFullAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonF SxConsoleFullAccess

É possível anexar a política `AmazonFSxConsoleFullAccess` a suas identidades do IAM.

Essa política concede permissões administrativas que permitem acesso total ao Amazon FSx e acesso a AWS serviços relacionados por meio do. AWS Management Console

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`: permite que as entidades principais realizem todas as ações no console de gerenciamento do Amazon FSx, exceto `BypassSnaplockEnterpriseRetention`.
- `cloudwatch`— Permite que os diretores visualizem CloudWatch alarmes e métricas no console de gerenciamento do Amazon FSx.
- `ds`— Permite que os diretores listem informações sobre um AWS Directory Service diretório.
- `ec2`
  - Permite que os diretores criem tags em tabelas de rotas, listem interfaces de rede, tabelas de rotas, grupos de segurança, sub-redes e a VPC associada a um sistema de arquivos Amazon FSx.
  - Permite que os diretores forneçam validação aprimorada do grupo de segurança de todos os grupos de segurança que podem ser usados com uma VPC.
- `kms`— Permite que os diretores listem aliases para AWS Key Management Service chaves.
- `s3`: permite que as entidades principais listem alguns ou todos os objetos em um bucket do Amazon S3 (até mil).
- `iam`: concede permissão para criar um perfil vinculado ao serviço que permite que o Amazon FSx execute ações em nome do usuário.

Para ver as permissões dessa política, consulte a AmazonF SxConsoleFullAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonF SxConsoleReadOnlyAccess

É possível anexar a política `AmazonFSxConsoleReadOnlyAccess` a suas identidades do IAM.

Essa política concede permissões somente de leitura ao Amazon FSx e AWS serviços relacionados para que os usuários possam visualizar informações sobre esses serviços no. AWS Management Console

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`: permite que as entidades principais visualizem informações sobre os sistemas de arquivos do Amazon FSx, incluindo todas as tags, no console de gerenciamento do Amazon FSx.

- `cloudwatch`— Permite que os diretores visualizem CloudWatch alarmes e métricas no Amazon FSx Management Console.
- `ds`— Permite que os diretores visualizem informações sobre um AWS Directory Service diretório no Amazon FSx Management Console.
- `ec2`
  - Permite que os diretores visualizem interfaces de rede, grupos de segurança, sub-redes e a VPC associada a um sistema de arquivos Amazon FSx no Amazon FSx Management Console.
  - Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança que podem ser usados com uma VPC.
- `kms`— Permite que os diretores visualizem aliases para AWS Key Management Service chaves no Amazon FSx Management Console.
- `log`— Permite que os diretores descrevam os grupos de log do Amazon CloudWatch Logs associados à conta que fez a solicitação. Isso é necessário para que as entidades principais possam visualizar a configuração de auditoria de acesso a arquivos existente para um sistema de arquivos do FSx para Windows File Server.
- `firehose`— Permite que os diretores descrevam os fluxos de entrega do Amazon Data Firehose associados à conta que fez a solicitação. Isso é necessário para que as entidades principais possam visualizar a configuração de auditoria de acesso a arquivos existente para um sistema de arquivos do FSx para Windows File Server.

Para ver as permissões dessa política, consulte a AmazonF SxConsoleReadOnlyAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonF SxReadOnlyAccess

É possível anexar a política `AmazonFSxReadOnlyAccess` a suas identidades do IAM.

Esta política inclui as seguintes permissões.

- `fsx`: permite que as entidades principais visualizem informações sobre os sistemas de arquivos do Amazon FSx, incluindo todas as tags, no console de gerenciamento do Amazon FSx.
- `ec2`— Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança que podem ser usados com uma VPC.

Para ver as permissões dessa política, consulte a AmazonF SxReadOnlyAccess no Guia de referência de políticas AWS gerenciadas.

Atualizações do Amazon FSx para AWS políticas gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Amazon FSx desde que esse serviço começou a monitorar essas mudanças. Para receber alertas automáticos sobre alterações nesta página, assine o feed RSS na página Histórico do documento do Amazon FSx.

Alteração	Descrição	Data
AmazonF SxServiceRolePolicy — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	09 de janeiro de 2024
AmazonF SxReadOnlyAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	09 de janeiro de 2024
AmazonF SxConsoleReadOnlyAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	09 de janeiro de 2024

Alteração	Descrição	Data
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	09 de janeiro de 2024
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	09 de janeiro de 2024
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação de dados entre regiões e entre contas para sistemas de arquivos FSx for OpenZFS.	20 de dezembro de 2023
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação de dados entre regiões e entre contas para sistemas de arquivos FSx for OpenZFS.	20 de dezembro de 2023

Alteração	Descrição	Data
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação sob demanda de volumes para sistemas de arquivos FSx for OpenZFS.	26 de novembro de 2023
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação sob demanda de volumes para sistemas de arquivos FSx for OpenZFS.	26 de novembro de 2023
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os usuários visualizem, habilitem e desabilitem o suporte compartilhado de VPC para FSx para sistemas de arquivos ONTAP Multi-AZ.	14 de novembro de 2023
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os usuários visualizem, habilitem e desabilitem o suporte compartilhado de VPC para FSx para sistemas de arquivos ONTAP Multi-AZ.	14 de novembro de 2023

Alteração	Descrição	Data
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que ele gerencie as configurações de rede dos sistemas de arquivos do FSx para OpenZFS com várias AZs.	9 de agosto de 2023
AWS política gerenciada: AmazonF SxServiceRolePolicy — Atualização de uma política existente	O Amazon FSx modificou a `cloudwatch:PutMetricData` permissão existente para que o Amazon FSx publique métricas no namespace. CloudWatch `AWS/FSx`	24 de julho de 2023
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx atualizou a política para remover a permissão `fsx:*` e adicionar ações `fsx` específicas.	13 de julho de 2023
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx atualizou a política para remover a permissão `fsx:*` e adicionar ações `fsx` específicas.	13 de julho de 2023
AmazonF SxConsole ReadOnlyAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os usuários visualizem métricas de performance aprimoradas e ações recomendadas para sistemas de arquivos do FSx para Windows File Server no console do Amazon FSx.	21 de setembro de 2022

Alteração	Descrição	Data
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os usuários visualizem métricas de performance aprimoradas e ações recomendadas para sistemas de arquivos do FSx para Windows File Server no console do Amazon FSx.	21 de setembro de 2022
AmazonF SxReadOnlyAccess — Iniciou a política de rastreamento	Essa política concede acesso somente leitura a todos os recursos do Amazon FSx e a qualquer tag associada a eles.	4 de fevereiro de 2022
AmazonF SxDeleteServiceLinkedRoleAccess — Iniciou a política de rastreamento	Essa política concede permissões administrativas que permitem que o Amazon FSx exclua o perfil vinculado ao serviço para acesso do Amazon S3.	7 de janeiro de 2022
AmazonF SxServiceRolePolicy — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx gerencie configurações de rede para sistemas de arquivos Amazon FSx for ONTAP. NetApp	2 de setembro de 2021

Alteração	Descrição	Data
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx crie tags nas tabelas de rotas do EC2 para chamadas com escopo reduzido.	2 de setembro de 2021
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx crie Amazon FSx para sistemas de arquivos ONTAP Multi-AZ. NetApp	2 de setembro de 2021
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx crie tags nas tabelas de rotas do EC2 para chamadas com escopo reduzido.	2 de setembro de 2021
AmazonF SxServiceRolePolicy — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx descreva e grave em fluxos de log de CloudWatch registros. Isso é necessário para que os usuários possam visualizar os registros de auditoria de acesso a arquivos dos sistemas de arquivos FSx for Windows File Server CloudWatch usando Logs.	8 de junho de 2021

Alteração	Descrição	Data
AmazonF SxServiceRolePolicy — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx descreva e grave nos fluxos de entrega do Amazon Data Firehose. Isso é necessário para que os usuários possam visualizar os registros de auditoria de acesso a arquivos de um sistema de arquivos FSx for Windows File Server usando o Amazon Data Firehose.	8 de junho de 2021
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os diretores descrevam e criem grupos de registros de CloudWatch registros, fluxos de registros e gravem eventos em fluxos de registros. Isso é necessário para que os diretores possam visualizar os registros de auditoria de acesso a arquivos dos sistemas CloudWatch de arquivos FSx for Windows File Server usando Logs.	8 de junho de 2021

Alteração	Descrição	Data
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os diretores descrevam e gravem registros em um Amazon Data Firehose. Isso é necessário para que os usuários possam visualiza r os registros de auditoria de acesso a arquivos de um sistema de arquivos FSx for Windows File Server usando o Amazon Data Firehose.	8 de junho de 2021
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os diretores descrevam os grupos de log do Amazon CloudWatch Logs associados à conta que fez a solicitação. Isso é necessário para que os diretores possam escolher um grupo de registros de CloudWatch registros existente ao configurar a auditoria de acesso a arquivos para um sistema de arquivos FSx for Windows File Server.	8 de junho de 2021

Alteração	Descrição	Data
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os diretores descrevam os fluxos de entrega do Amazon Data Firehose associados à conta que fez a solicitação. Isso é necessário para que os diretores possam escolher um stream de entrega existente do Firehose ao configurar a auditoria de acesso a arquivos para um sistema de arquivos FSx for Windows File Server.	8 de junho de 2021
AmazonF SxConsole ReadOnlyAccess — Atualizaç ão de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os diretores descrevam os grupos de log do Amazon CloudWatch Logs associados à conta que fez a solicitação. Isso é necessário para que as entidades principais possam visualizar a configuração de auditoria de acesso a arquivos existente para um sistema de arquivos do FSx para Windows File Server.	8 de junho de 2021

Alteração	Descrição	Data
AmazonF SxConsole ReadOnlyAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os diretores descrevam os fluxos de entrega do Amazon Data Firehose associados à conta que fez a solicitação. Isso é necessário para que as entidades principais possam visualizar a configuração de auditoria de acesso a arquivos existente para um sistema de arquivos do FSx para Windows File Server.	8 de junho de 2021
Amazon FSx iniciou o rastreamento de alterações	O Amazon FSx começou a monitorar as mudanças em suas políticas AWS gerenciadas.	8 de junho de 2021

Solução de problemas de identidade e acesso do Amazon FSx para Lustre

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Amazon FSx e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Amazon FSx
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus recursos do Amazon FSx

Não tenho autorização para executar uma ação no Amazon FSx

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `fsx:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao atributo *`my-example-widget`* usando a ação `fsx:`*`GetWidget`*.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Caso receba uma mensagem de erro informando que você não tem autorização para executar a ação `iam:PassRole`, as políticas deverão ser atualizadas para permitir a transmissão de um perfil ao Amazon FSx.

Alguns Serviços da AWS permitem que você passe um perfil existente para o serviço, em vez de criar um novo perfil de serviço ou perfil vinculado ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro exemplificado a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Amazon FSx. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS acessem meus recursos do Amazon FSx

É possível criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Amazon FSx oferece suporte a esses recursos, consulte Como o Amazon FSx para Lustre funciona com o IAM.
- Para saber como conceder acesso a seus atributos em todas as Contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para terceiros Contas da AWS, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em atributos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em atributos no Guia do usuário do IAM.

Como usar tags com o Amazon FSx

É possível usar tags para controlar o acesso aos recursos do Amazon FSx e implementar o controle de acesso por atributo (ABAC). Para aplicar tags aos recursos do Amazon FSx durante a criação, os usuários devem ter determinadas permissões do AWS Identity and Access Management (IAM).

Conceder permissão para marcar recursos durante a criação

Com algumas ações de criação de recurso da API do Amazon FSx para Lustre, você poderá especificar tags quando criar o recurso. É possível usar essas tags de recurso para implementar o

controle de acesso por atributo (ABAC). Para obter mais informações, consulte O que é ABAC para AWS? no Guia do usuário do IAM.

Para que os usuários marquem recursos na criação, eles devem ter permissão para usar a ação que cria o recurso, como `fsx:CreateFileSystem`. Se tags forem especificadas na ação de criação do recurso, o IAM executará autorização adicional na ação `fsx:TagResource` para verificar se os usuários têm permissões para criar tags. Portanto, os usuários também precisam ter permissões para usar a ação `fsx:TagResource`.

O exemplo de política a seguir permite que os usuários criem sistemas de arquivos e apliquem tags a eles durante a criação em uma Conta da AWS específica.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*"
      ]
    }
  ]
}
```

Da mesma forma, a política a seguir permite que os usuários criem backups em um sistema de arquivos específico e apliquem qualquer tag ao backup durante a criação do backup.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
            "fsx:TagResource"
        ],
        "Resource": "arn:aws:fsx:region:account-id:backup/*"
      }
    ]
}
```

A ação `fsx:TagResource` só será avaliada se as tags forem aplicadas durante a ação de criação do recurso. Portanto, um usuário que tiver permissões para criar um recurso (supondo que não existam condições de tag) não precisará de permissão para usar a ação `fsx:TagResource` se nenhuma tag for especificada na solicitação. Contudo, se o usuário tentar criar um recurso com tags, haverá falha na solicitação se o usuário não tiver permissão para usar a ação `fsx:TagResource`.

Para obter mais informações sobre como marcar recursos do Amazon FSx, consulte Marcar os recursos do Amazon FSx. Para obter mais informações sobre como usar tags para controlar o acesso aos recursos do Amazon FSx para Lustre, consulte Como usar tags para controlar o acesso aos seus recursos do Amazon FSx.

Como usar tags para controlar o acesso aos seus recursos do Amazon FSx

Para controlar o acesso a recursos e ações do Amazon FSx, você pode usar políticas do IAM baseadas em tags. É possível conceder o controle de duas formas:

- Você pode controlar o acesso aos recursos do Amazon FSx com base nas tags desses recursos.
- Controle quais tags podem ser transmitidas em uma condição de solicitação do IAM.

Para obter informações sobre como usar tags para controlar o acesso aos recursos da AWS, consulte Controle de acesso usando tags no Guia do usuário do IAM. Para obter mais informações sobre como marcar recursos do Amazon FSx no momento da criação, consulte Conceder permissão para marcar recursos durante a criação. Para obter mais informações sobre como marcar recursos, consulte Marcar os recursos do Amazon FSx.

Como controlar o acesso com base em tags em um recurso

Para controlar quais ações um usuário ou um perfil pode executar em um recurso do Amazon FSx, é possível usar tags no recurso. Por exemplo, talvez você queira permitir ou negar operações de API específicas em um recurso do sistema de arquivos com base no par de chave/valor da tag no recurso.

Example Exemplo de política: crie um sistema de arquivos fornecendo uma tag específica

Essa política permite que o usuário só crie um sistema de arquivos quando marcá-lo com um par de chave/valor de tag específico; neste exemplo, `key=Department, value=Finance`.

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example Exemplo de política: só crie backups nos sistemas de arquivos com uma tag específica

Essa política permite que os usuários só criem backups em sistemas de arquivos marcados com o par de chave/valor `key=Department, value=Finance`, e o backup será criado com a tag `Deparment=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example Exemplo de política: crie um sistema de arquivos com uma tag específica usando backups com uma tag específica

Essa política permite que os usuários só criem sistemas de arquivos marcados com `Department=Finance` por meio de backups marcados com `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Exemplo de política: excluir sistemas de arquivos com tags específicas

Essa política só permite que o usuário exclua sistemas de arquivos marcados com `Department=Finance`. Se um backup final for criado, ele deverá ser marcado com `Department=Finance`. Para sistemas de arquivos do Lustre, os usuários precisam ter o privilégio `fsx:CreateBackup` para criar o backup final.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
```

```
        }
    ]
}
```

Example Exemplo de política: crie tarefas de repositório de dados em sistemas de arquivos com tag específica

Essa política permite que os usuários criem tarefas de repositório de dados marcadas com `Department=Finance` e somente em sistemas de arquivos marcados com `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:task/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Como usar perfis vinculados a serviço no Amazon FSx

O Amazon FSx usa funções vinculadas a serviços AWS Identity and Access Management (IAM). Um perfil vinculado ao serviço é um tipo especial de perfil do IAM vinculado diretamente ao Amazon FSx. As funções vinculadas ao serviço são predefinidas pelo Amazon FSx e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Um perfil vinculado ao serviço facilita a configuração do Amazon FSx porque você não precisa adicionar as permissões necessárias manualmente. O Amazon FSx define as permissões dos perfis vinculados ao serviço e, a não ser que esteja definido de outra forma, somente o Amazon FSx poderá assumir os perfis. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus recursos do Amazon FSx, uma vez que você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados ao serviço, consulte serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Perfis vinculados aos serviços. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de perfil vinculado ao serviço para o Amazon FSx

O Amazon FSx usa duas funções vinculadas a serviços nomeadas `AWSServiceRoleForAmazonFSx` e `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`* que executam determinadas ações em sua conta. Exemplos dessas ações são criar interfaces de rede elástica para seus sistemas de arquivos em sua VPC e acessar seu repositório de dados em um bucket do Amazon S3. Para `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`*, esse perfil vinculado ao serviço é criado para cada sistema de arquivos do Amazon FSx para Lustre que você cria e que está vinculado a um bucket do S3.

AWSServiceRoleForAmazonFSx detalhes de permissões

Pois`AWSServiceRoleForAmazonFSx`, a política de permissões de função permite que o Amazon FSx conclua as seguintes ações administrativas em nome do usuário em todos os recursos aplicáveis AWS :

Para atualizações desta política, consulte Amazon F SxServiceRolePolicy

> **Note**
>
> O AWSServiceRoleForAmazonFSx é usado por todos os tipos de sistema de arquivos Amazon FSx; algumas das permissões listadas não são aplicáveis ao FSx for Lustre.

- `ds`— Permite que o Amazon FSx visualize, autorize e não autorize aplicativos em seu diretório. AWS Directory Service
- `ec2`: permite que o Amazon FSx faça o seguinte:
  - Visualizar, criar e desassociar interfaces de rede associadas a um sistema de arquivos do Amazon FSx.
  - Visualizar um ou mais endereços IP elásticos associados a um sistema de arquivos do Amazon FSx.
  - Visualizar Amazon VPCs, grupos de segurança e sub-redes associados a um sistema de arquivos do Amazon FSx.
  - Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança que podem ser usados com uma VPC.
  - Crie uma permissão para que um usuário AWS autorizado realize determinadas operações em uma interface de rede.
- `cloudwatch`— Permite que o Amazon FSx publique pontos de dados métricos CloudWatch sob o namespace AWS /FSx.
- `route53`: permite que o Amazon FSx associe uma Amazon VPC a uma zona hospedada privada.
- `logs`— Permite que o Amazon FSx descreva e grave em fluxos de log de CloudWatch registros. Isso é para que os usuários possam enviar registros de auditoria de acesso a arquivos de um sistema de arquivos FSx for Windows File Server para CloudWatch um stream de registros.
- `firehose`— Permite que o Amazon FSx descreva e grave nos fluxos de entrega do Amazon Data Firehose. Isso é para que os usuários possam publicar os registros de auditoria de acesso a arquivos de um sistema de arquivos FSx for Windows File Server em um stream de distribuição do Amazon Data Firehose.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
```

```
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
```

```
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Todas as atualizações dessa política estão descritas em Atualizações do Amazon FSx para AWS políticas gerenciadas.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado ao serviço. Para obter mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

AWSServiceRoleForFSxS3Access detalhes de permissões

Pois`AWSServiceRoleForFSxS3Access_`*`file-system-id`*, a política de permissões de função permite que o Amazon FSx conclua as seguintes ações em um bucket do Amazon S3 que hospeda o repositório de dados de um sistema de arquivos Amazon FSx for Lustre.

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:Get*`
- `s3:List*`

- `s3:PutBucketNotification`
- `s3:PutObject`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado ao serviço. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM.

Como criar um perfil vinculado ao serviço para o Amazon FSx

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria um sistema de arquivos na AWS Management Console, na ou na AWS API AWS CLI, o Amazon FSx cria a função vinculada ao serviço para você.

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Para saber mais, consulte Uma Nova Função Apareceu na minha Conta do IAM.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você pode usar esse mesmo processo para recriar a função na sua conta. Quando você cria um sistema de arquivos, o Amazon FSx cria o perfil vinculado ao serviço para você novamente.

Edição de um perfil vinculado ao serviço do Amazon FSx

O Amazon FSx não permite que você edite essas funções vinculadas a serviços. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Exclusão de um perfil vinculado ao serviço do Amazon FSx

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve excluir todos os seus sistemas de arquivos e backups para poder excluir manualmente o perfil vinculado ao serviço.

> **Note**
>
> Se o serviço do Amazon FSx estiver usando o perfil quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console, a CLI ou a API do IAM para excluir a função vinculada ao serviço AWSServiceRoleForAmazonFSx. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões com suporte para os perfis vinculados a serviço do Amazon FSx

O Amazon FSx fornece suporte ao uso de perfis vinculados ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

Controle de acesso ao sistema de arquivos com a Amazon VPC

Um sistema de arquivos do Amazon FSx é acessado por meio de uma interface de rede elástica que reside na nuvem privada virtual (VPC) com base no serviço Amazon VPC que você associa ao seu sistema de arquivos. Você acessa seu sistema de arquivos do Amazon FSx por meio do nome DNS, que é mapeado para a interface de rede do sistema de arquivos. Somente recursos dentro da VPC associada, ou de uma VPC emparelhada, podem acessar a interface de rede do seu sistema de arquivos. Para obter mais informações, consulte O que é a Amazon VPC? no Guia do usuário da Amazon VPC.

> **Warning**
>
> Não é permitido modificar nem excluir a interface de rede elástica do Amazon FSx. A modificação ou a exclusão da interface de rede pode causar uma perda permanente de conexão entre a VPC e o sistema de arquivos.

Grupos de segurança da Amazon VPC

Para controlar ainda mais o tráfego de rede que passa pela interface de rede do sistema de arquivos na VPC, use grupos de segurança para limitar o acesso aos sistemas de arquivos. Um grupo de

segurança age como um firewall virtual que controla o tráfego de recursos associados. Nesse caso, o recurso associado é a interface de rede do sistema de arquivos. Você também usa grupos de segurança da VPC para controlar o tráfego de rede para os clientes Lustre.

Controle de acesso usando regras de entrada e saída

Para usar um grupo de segurança para controlar o acesso ao sistema de arquivos do Amazon FSx e aos clientes do Lustre, você adiciona regras de entrada para controlar o tráfego de entrada e regras de saída para controlar o tráfego de saída no sistema de arquivos e nos clientes do Lustre. Verifique se você tem as regras de tráfego de rede corretas em seu grupo de segurança para mapear o compartilhamento de arquivos do sistema de arquivos do Amazon FSx para uma pasta na sua instância de computação com suporte.

Para obter mais informações sobre regras de grupo de segurança, consulte Regras de grupo de segurança no Guia do usuário do Amazon EC2 para instâncias do Linux.

Para criar um grupo de segurança para seu sistema de arquivos Amazon FSx

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2.
2. No painel de navegação, escolha Grupos de segurança.
3. Escolha Create Security Group.
4. Especifique um nome e uma descrição para o grupo de segurança.
5. Para VPC, escolha a VPC associada ao sistema de arquivos do Amazon FSx para criar o grupo de segurança dentro dessa VPC.
6. Escolha Create (Criar) para criar o grupo de segurança.

Em seguida, adicione regras de entrada ao grupo de segurança que você acabou de criar para habilitar o tráfego do Lustre entre os servidores de arquivos do FSx para Lustre.

Adicionar regras de entrada ao grupo de segurança

1. Selecione o grupo de segurança que você acabou de criar, se ele ainda não estiver selecionado. Em Actions (Ações), escolha Edit inbound rules (Editar regras de entrada).
2. Adicione as regras de entrada a seguir.

Tipo	Protocolo	Port Range (Intervalo de portas)	Origem	Descrição
Regra personalizada de TCP	TCP	988	Escolha Personalizado e digite o ID do grupo de segurança que você acabou de criar	Permite o tráfego do Lustre entre servidores de arquivos do FSx para Lustre
Regra personalizada de TCP	TCP	988	Escolha Personalizado e insira os IDs dos grupos de segurança associados aos clientes Lustre	Permite o tráfego do Lustre entre os servidores de arquivos do FSx para Lustre e os clientes Lustre
Regra personalizada de TCP	TCP	1018-1023	Escolha Personalizado e digite o ID do grupo de segurança que você acabou de criar	Permite o tráfego do Lustre entre servidores de arquivos do FSx para Lustre
Regra personalizada de TCP	TCP	1018-1023	Escolha Personalizado e insira os IDs dos grupos de segurança associados aos clientes Lustre	Permite o tráfego do Lustre entre os servidores de arquivos do FSx para Lustre e os clientes Lustre

3. Escolha Salvar para salvar e aplicar as novas regras de entrada.

Por padrão, as regras de grupo de segurança permitem todo tráfego de saída (Todos, 0.0.0.0/0). Se o seu grupo de segurança não permitir todo tráfego de saída, adicione as seguintes regras de saída ao seu grupo de segurança. Essas regras permitem o tráfego entre os servidores de arquivos e os clientes do Lustre, bem como entre os servidores de arquivos do Lustre.

Adicionar regras de saída ao grupo de segurança

1. Escolha o mesmo grupo de segurança ao qual você acabou de adicionar as regras de entrada. Em Ações, escolha Editar regras de saída.
2. Adicione as regras de saída a seguir.

Tipo	Protocolo	Port Range (Intervalo de portas)	Origem	Descrição
Regra personalizada de TCP	TCP	988	Escolha Personalizado e digite o ID do grupo de segurança que você acabou de criar	Permitir o tráfego do Lustre entre os servidores de arquivos do FSx para Lustre
Regra personalizada de TCP	TCP	988	Escolha Personalizado e insira os IDs do grupo de segurança associado aos seus clientes Lustre	Permitir o tráfego do Lustre entre os servidores de arquivos do FSx para Lustre e os clientes Lustre
Regra personalizada de TCP	TCP	1018-1023	Escolha Personalizado e digite o ID do grupo de segurança que	Permite o tráfego do Lustre entre servidores de

Tipo	Protocolo	Port Range (Intervalo de portas)	Origem	Descrição
			você acabou de criar	arquivos do FSx para Lustre
Regra personalizada de TCP	TCP	1018-1023	Escolha Personalizado e insira os IDs dos grupos de segurança associados aos clientes Lustre	Permite o tráfego do Lustre entre os servidores de arquivos do FSx para Lustre e os clientes Lustre

3. Escolha Salvar para salvar e aplicar as novas regras de saída.

Associar um grupo de segurança ao seu sistema de arquivos do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel do console, escolha o sistema de arquivos para ver seus detalhes.
3. Na guia Rede e segurança, escolha os IDs da interface de rede do seu sistema de arquivos (por exemplo, `ENI-01234567890123456`). Isso direciona você para o console do Amazon EC2.
4. Escolha cada ID de interface de rede. Cada ação abre uma nova instância do console do Amazon EC2 em seu navegador. Para cada grupo de segurança, escolha Alterar grupos de segurança para Ações.
5. Na caixa de diálogo Alterar grupos de segurança, escolha os grupos de segurança a serem usados e selecione Salvar.

Regras do grupo de segurança da VPC do cliente Lustre

Use grupos de segurança da VPC para controlar o acesso aos clientes Lustre, adicionando regras de entrada para controlar o tráfego de entrada e regras de saída para controlar o tráfego de saída nos clientes Lustre. Certifique-se de ter as regras de tráfego de rede corretas em seu grupo de segurança para garantir que o tráfego do Lustre possa fluir entre seus clientes Lustre e seus sistemas de arquivos do Amazon FSx.

Adicione as regras de entrada a seguir aos grupos de segurança aplicados aos clientes Lustre.

Tipo	Protocolo	Port Range (Intervalo de portas)	Origem	Descrição
Regra personalizada de TCP	TCP	988	Escolha Personalizado e insira os IDs dos grupos de segurança que são aplicados aos seus clientes Lustre	Permite o tráfego do Lustre entre os clientes Lustre
Regra personalizada de TCP	TCP	988	Escolha Personalizado e insira os IDs dos grupos de segurança associados aos seus sistemas de arquivos do FSx para Lustre	Permite o tráfego do Lustre entre os servidores de arquivos do FSx para Lustre e os clientes Lustre
Regra personalizada de TCP	TCP	1018-1023	Escolha Personalizado e insira os IDs dos grupos de segurança que são aplicados aos seus clientes Lustre	Permite o tráfego do Lustre entre os clientes Lustre
Regra personalizada de TCP	TCP	1018-1023	Escolha Personalizado e insira os IDs dos grupos	Permite o tráfego do Lustre entre os servidores de arquivos do FSx

Tipo	Protocolo	Port Range (Intervalo de portas)	Origem	Descrição
			de segurança associados aos seus sistemas de arquivos do FSx para Lustre	para Lustre e os clientes Lustre

Adicione as regras de saída a seguir aos grupos de segurança aplicados aos clientes Lustre.

Tipo	Protocolo	Port Range (Intervalo de portas)	Origem	Descrição
Regra personalizada de TCP	TCP	988	Escolha Personalizado e insira os IDs dos grupos de segurança que são aplicados aos seus clientes Lustre	Permite o tráfego do Lustre entre os clientes Lustre
Regra personalizada de TCP	TCP	988	Escolha Personalizado e insira os IDs dos grupos de segurança associados aos seus sistemas de arquivos do FSx para Lustre	Permitir o tráfego do Lustre entre os servidores de arquivos do FSx para Lustre e os clientes Lustre
Regra personalizada de TCP	TCP	1018-1023	Escolha Personalizado	Permite o tráfego do Lustre entre

Tipo	Protocolo	Port Range (Intervalo de portas)	Origem	Descrição
			e insira os IDs dos grupos de segurança que são aplicados aos seus clientes Lustre	os clientes Lustre
Regra personalizada de TCP	TCP	1018-1023	Escolha Personalizado e insira os IDs dos grupos de segurança associados aos seus sistemas de arquivos do FSx para Lustre	Permite o tráfego do Lustre entre os servidores de arquivos do FSx para Lustre e os clientes Lustre

ACLs de rede da Amazon VPC

Outra opção para proteger o acesso ao sistema de arquivos em sua VPC é estabelecer listas de controle de acesso à rede (ACLs da rede). As ACLs da rede são diferentes dos grupos de segurança, mas têm funcionalidade semelhante para adicionar outra camada de segurança aos recursos em sua VPC. Para obter mais informações sobre como implementar o controle de acesso usando ACLs de rede, consulte Controlar o tráfego para sub-redes usando ACLs de rede no Guia do usuário da Amazon VPC.

Validação de conformidade para o Amazon FSx para Lustre

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade e selecione o programa de conformidade em que você está interessado. Para obter informações gerais, consulteAWS Programas de conformidade.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Downloading Reports inAWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes atributos para ajudar com a conformidade:

- Guias de referência rápida de conformidade e segurança - estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services): esse estudo técnico descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

  > **Note**
  >
  > Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- atributos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliar atributos com regras no AWS Config Guia do desenvolvedor: o serviço AWS Config avalia como as configurações de atributos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.

- AWS Audit Manager – Esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Amazon FSx para Lustre e endpoints da VPC de interface (AWS PrivateLink)

Você pode aprimorar a postura de segurança da VPC ao configurar o Amazon FSx para usar um endpoint da VPC de interface. Os endpoints da VPC de interface são desenvolvidos pelo AWS PrivateLink, uma tecnologia que possibilita acessar APIs do Amazon FSx de forma privada sem um gateway da Internet, dispositivo NAT, conexão VPN ou conexão do AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para se comunicar com as APIs do Amazon FSx. O tráfego entre a VPC e o Amazon FSx não é realizado de forma externa à rede da AWS.

Cada endpoint da VPC de interface é representado por uma ou mais interfaces de rede elástica em suas sub-redes. Uma interface de rede fornece um endereço IP privado que serve como um ponto de entrada para o tráfego para a API do Amazon FSx.

Considerações sobre endpoints da VPC de interface do Amazon FSx

Antes de configurar um endpoint da VPC de interface para o Amazon FSx, certifique-se de consultar Interface VPC endpoint properties and limitations no Guia do usuário da Amazon VPC.

É possível chamar qualquer uma das operações de API do Amazon FSx usando sua VPC. Por exemplo, você pode criar um sistema de arquivos do FSx para Lustre ao chamar a API CreateFileSystem usando sua VPC. Para obter a lista completa de APIs do Amazon FSx, consulte Actions na referência de APIs do Amazon FSx.

Considerações sobre emparelhamento de VPC

Você pode conectar outras VPCs à VPC com endpoints da VPC de interface usando o emparelhamento de VPC. O emparelhamento de VPC é uma conexão de rede entre duas VPCs. É possível estabelecer uma conexão de emparelhamento da VPC entre suas duas VPCs ou com uma VPC em outra Conta da AWS. As VPCs também podem estar em duas Regiões da AWS diferentes.

O tráfego entre VPCs emparelhadas permanece na rede da AWS e não passa pela Internet pública. Depois que as VPCs são emparelhadas, os recursos, como as instâncias do Amazon Elastic

Compute Cloud (Amazon EC2) em ambas as VPCs, podem acessar a API do Amazon FSx por meio de endpoints da VPC de interface criados em uma das VPCs.

Como criar um endpoint da VPC de interface para a API do Amazon FSx

Você pode criar um endpoint da VPC para a API do Amazon FSx usando o console da Amazon VPC ou a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Creating an interface VPC endpoint no Guia do usuário da Amazon VPC.

Para obter uma lista completa de endpoints do Amazon FSx, consulte Amazon FSx endpoints and quotas na Referência geral da Amazon Web Services.

Para criar um endpoint da VPC de interface para o Amazon FSx, use um dos seguintes:

- **`com.amazonaws.`*`region`*`.fsx`**: cria um endpoint para as operações de API do Amazon FSx.
- **`com.amazonaws.`*`region`*`.fsx-fips`**: cria um endpoint para a API do Amazon FSx que está em conformidade com o padrão Federal Information Processing Standard (FIPS) 140-2.

Para usar a opção de DNS privado, é necessário definir os recursos `enableDnsHostnames` e `enableDnsSupport` da sua VPC. Para obter mais informações, consulte Viewing and updating DNS support for your VPC no Guia do usuário da Amazon VPC.

Ao excluir as Regiões da AWS na China, se você habilitar o DNS privado para o endpoint, poderá realizar solicitações de API ao Amazon FSx com o endpoint da VPC usando o nome DNS padrão para a Região da AWS, por exemplo, `fsx.us-east-1.amazonaws.com`. Para as Regiões da AWS China (Pequim) e China (Ningxia), você pode realizar solicitações de API com o endpoint da VPC usando `fsx-api.cn-north-1.amazonaws.com.cn` e `fsx-api.cn-northwest-1.amazonaws.com.cn`, respectivamente.

Para obter mais informações, consulte Accessing a service through an interface VPC endpoint no Guia do usuário da Amazon VPC.

Como criar uma política de endpoint da VPC para o Amazon FSx

Para controlar ainda mais o acesso à API do Amazon FSx, como opção, é possível anexar uma política do AWS Identity and Access Management (IAM) ao endpoint da VPC. A política especifica o seguinte:

- A entidade principal que pode executar ações.

- As ações que podem ser executadas.
- Os recursos sobre os quais as ações podem ser realizadas.

Para obter mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Cotas

A seguir, descubra mais sobre as cotas para o trabalho com o Amazon FSx para Lustre.

Tópicos

Cotas que podem ser aumentadas

A seguir, são apresentadas as cotas do Amazon FSx para Lustre por conta da AWS, por região da AWS, que você pode aumentar.

Recurso	Padrão	Descrição
Sistemas de arquivos Persistent_1 do Lustre	100	O número máximo de sistemas de arquivos Persistent_1 do Amazon FSx para Lustre que você pode criar nesta conta.
Sistemas de arquivos Persistent_2 do Lustre	100	O número máximo de sistemas de arquivos Persistent_2 do Amazon FSx para Lustre que você pode criar nesta conta.
Capacidade de armazenam ento persistente baseado em HDD do Lustre (por sistema de arquivos)	102000	A quantidade máxima de capacidade de armazenam ento em HDD (em GiB) que você pode configurar para um sistema de arquivos persistente do Amazon FSx para Lustre.

Recurso	Padrão	Descrição
Capacidade de armazenamento de arquivos Persistent_1 do Lustre	100800	A quantidade máxima de capacidade de armazenamento (em GiB) que você pode configurar para todos os sistemas de arquivos Persistent_1 do Amazon FSx para Lustre nesta conta.
Capacidade de armazenamento de arquivos Persistent_2 do Lustre	100800	A quantidade máxima de capacidade de armazenamento (em GiB) que você pode configurar para todos os sistemas de arquivos Persistent_2 do Amazon FSx para Lustre nesta conta.
Sistemas de arquivos transitórios do Lustre	100	O número máximo de sistemas de arquivos transitórios do Amazon FSx para Lustre que você pode criar nesta conta.
Capacidade de armazenamento transitório do Lustre	100800	A quantidade máxima de capacidade de armazenamento (em GiB) que você pode configurar para todos os sistemas de arquivos transitórios do Amazon FSx para Lustre nesta conta.

Recurso	Padrão	Descrição
Backups do Lustre	500	O número máximo de backups iniciados pelo usuário que você pode ter para todos os sistemas de arquivos do Amazon FSx para Lustre nesta conta.

Para solicitar um aumento da cota

1. Abra o console do Service Quotas.
2. No painel de navegação, escolha Serviços da AWS.
3. Escolha Amazon FSx.
4. Escolha uma cota.
5. Escolha Solicitar aumento da cota e siga as instruções para solicitar um aumento da cota.
6. Para visualizar o status da solicitação de cota, escolha Histórico de solicitações de cota no painel de navegação do console.

Para obter mais informações, consulte Solicitando um Aumento de Cota no Guia do Usuário do Service Quotas.

Cotas de recursos para cada sistema de arquivos

A seguir, são apresentados os limites dos recursos do Amazon FSx para Lustre para cada sistema de arquivos em uma região da AWS.

Recurso	Limite por sistema de arquivos
Número máximo de tags	50
Período máximo de retenção para backups automatizados	90 dias

Recurso	Limite por sistema de arquivos
Número máximo de solicitações de cópia de backup em andamento para uma única região de destino por conta.	5
Número de atualizações de arquivos do bucket do S3 vinculado por sistema de arquivos	10 milhões por mês
Capacidade mínima de armazenamento em SSD para sistemas de arquivos	1,2 TiB
Capacidade mínima de armazenamento em HDD para sistemas de arquivos	6 TiB
Throughput mínimo por unidade de armazenamento em SSD	50 MBps
Throughput máximo por unidade de armazenamento em SSD	1.000 MBps
Throughput mínimo por unidade de armazenamento em HDD	12 MBps
Throughput máximo por unidade de armazenamento em HDD	40 MBps

Considerações adicionais

Além disso, observe o seguinte:

- É possível usar cada chave do AWS Key Management Service (AWS KMS) em até 125 sistemas de arquivos do Amazon FSx para Lustre.
- Para obter uma lista de regiões da AWS nas quais você pode criar sistemas de arquivos, consulte Amazon FSx Endpoints and Quotas na Referência geral da AWS.

Solução de problemas

Use as informações a seguir para ajudar a resolver problemas que você possa encontrar ao trabalhar com sistemas de arquivos do Amazon FSx para Lustre.

Se você encontrar problemas não listados a seguir, tente fazer uma pergunta no Fórum do Amazon FSx para Lustre.

Tópicos

A tentativa de criar um sistema de arquivos do FSx para Lustre falha

Há várias causas possíveis para a falha de uma solicitação de criação de sistema de arquivos, conforme descrito nos tópicos a seguir.

Não é possível criar um sistema de arquivos porque o grupo de segurança está configurado incorretamente

A criação de um sistema de arquivos do FSx para Lustre falha com a seguinte mensagem de erro:

```
The file system cannot be created because the default security group in the subnet
 provided
or the provided security groups do not permit Lustre LNET network traffic on port 988
```

Medida a ser tomada

Certifique-se de que o grupo de segurança da VPC que você está usando para a operação de criação esteja configurado conforme descrito em Controle de acesso ao sistema de arquivos com a Amazon VPC. Você deve configurar o grupo de segurança para permitir o tráfego de entrada nas portas 988 e 1018 a 1023 do próprio grupo de segurança ou do CIDR completo da sub-rede, que é necessário para permitir que os hosts do sistema de arquivos se comuniquem entre si.

Não é possível criar um sistema de arquivos vinculado a um bucket do S3

Se a criação de um novo sistema de arquivos vinculado a um bucket do S3 falhar com uma mensagem de erro semelhante à seguinte.

```
User: arn:aws:iam::012345678901:user/username is not authorized to perform:
 iam:PutRolePolicy on resource: resource ARN
```

Esse erro poderá ocorrer se você tentar criar um sistema de arquivos vinculado a um bucket do Amazon S3 sem as permissões necessárias do IAM. As permissões do IAM necessárias oferecem suporte ao perfil vinculado ao serviço Amazon FSx para Lustre que é usado para acessar o bucket especificado do Amazon S3 em seu nome.

Medida a ser tomada

Certifique-se de que sua entidade do IAM (usuário, grupo ou perfil) tenha as permissões apropriadas para criar sistemas de arquivos. Isso inclui adicionar a política de permissões que dá suporte ao perfil vinculado ao serviço Amazon FSx para Lustre. Para obter mais informações, consulte Adição de permissões para usar repositórios de dados no Amazon S3.

Para obter mais informações sobre funções vinculadas ao serviço, consulte Como usar perfis vinculados a serviço no Amazon FSx.

Solução de problemas de montagem do sistema de arquivos

Há várias causas possíveis para a falha no comando de montagem de um sistema de arquivos, conforme descrito nos tópicos a seguir.

A montagem do sistema de arquivos falha imediatamente

O comando de montagem do sistema de arquivos falha imediatamente. O seguinte código mostra um exemplo.

```
mount.lustre: mount fs-0123456789abcdef0.fsx.us-east-1.aws@tcp:/fsx at /lustre
```

```
failed: No such file or directory

Is the MGS specification correct?
Is the filesystem name correct?
```

Esse erro poderá ocorrer se você não estiver usando o valor `mountname` correto ao montar um sistema de arquivos persistent ou scratch 2 usando o comando mount. Você pode obter o valor `mountname` pela resposta do comando describe-file-systems da AWS CLI ou da operação DescribeFileSystems da API.

A montagem do sistema de arquivos trava e depois falha com erro de tempo limite

O comando de montagem do sistema de arquivos trava por um ou dois minutos e, em seguida, falha com um erro de tempo limite.

O seguinte código mostra um exemplo.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx

[2+ minute wait here]
Connection timed out
```

Esse erro pode ocorrer porque os grupos de segurança da instância do Amazon EC2 ou do sistema de arquivos não estão configurados corretamente.

Medida a ser tomada

Certifique-se de que seus grupos de segurança do sistema de arquivos tenham as regras de entrada especificadas em Grupos de segurança da Amazon VPC.

A montagem automática falha e a instância não responde

Em alguns casos, a montagem automática pode falhar em um sistema de arquivos e a instância do Amazon EC2 pode parar de responder.

Esse problema poderá ocorrer se a opção `_netdev` não tiver sido declarada. Se `_netdev` estiver ausente, a instância do Amazon EC2 poderá parar de responder. Isso ocorre porque os sistemas de arquivos de rede precisam ser iniciados depois que a instância de computação inicia suas redes.

Medida a ser tomada

Se esse problema ocorrer, entre em contato com o AWS Support..

A montagem do sistema de arquivos falha durante a inicialização do sistema

A montagem do sistema de arquivos falha durante a inicialização do sistema. A montagem é automatizada usando `/etc/fstab`. Quando o sistema de arquivos não está montado, o seguinte erro é visto no syslog do período de inicialização da instância.

```
LNetError: 3135:0:(lib-socket.c:583:lnet_sock_listen()) Can't create socket: port 988
 already in use
LNetError: 122-1: Can't start acceptor on port 988: port already in use
```

Esse erro pode ocorrer quando a porta 988 não está disponível. Quando a instância está configurada para montar sistemas de arquivos NFS, é possível que as montagens NFS vinculem a porta do cliente à porta 988

Medida a ser tomada

Você pode contornar esse problema ajustando, quando possível, as opções de montagem `noresvport` e `noauto` do cliente NFS.

A montagem do sistema de arquivos usando o nome DNS falha

Nomes DNS configurados incorretamente podem causar falhas na montagem do sistema de arquivos, conforme mostrado nos cenários a seguir.

Cenário 1: uma montagem de sistema de arquivos que está usando um nome DNS falha. O seguinte código mostra um exemplo.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: Can't parse NID
'file_system_dns_name@tcp:/mountname'
```

Medida a ser tomada

Verifique a configuração da nuvem privada virtual (VPC). Em caso de uso de uma VPC personalizada, verifique se as configurações do DNS estão ativadas. Para obter mais informações, consulte Usar DNS com a VPC, no Guia do usuário da Amazon VPC.

Para especificar um nome DNS no comando `mount`, faça o seguinte:

- Certifique-se de que a instância do Amazon EC2 esteja na mesma VPC do sistema de arquivos do Amazon FSx para Lustre.
- Conecte a instância do Amazon EC2 dentro de uma VPC configurada para usar o servidor DNS fornecido pela Amazon. Para obter mais informações, consulte Conjuntos de Opções de DHCP no Manual do Usuário da Amazon VPC.
- Certifique-se de que a Amazon VPC da instância de conexão do Amazon EC2 tenha nomes DNS de host habilitados. Para obter mais informações, consulte Atualização do suporte a DNS para sua VPC no Guia do usuário da Amazon VPC.

Cenário 2: uma montagem de sistema de arquivos que está usando um nome DNS falha. O seguinte código mostra um exemplo.

```
mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: mount file_system_dns_name@tcp:/mountname at /mnt/fsx failed: Input/
output error Is the MGS running?
```

Medida a ser tomada

Certifique-se de que os grupos de segurança da VPC do cliente tenham as regras corretas de tráfego de saída aplicadas. Essa recomendação é válida especialmente quando você não está usando o grupo de segurança padrão ou quando o modificou. Para obter mais informações, consulte Grupos de segurança da Amazon VPC.

Não é possível acessar o sistema de arquivos

Há várias causas possíveis para a impossibilidade de acessar o sistema de arquivos, cada uma com sua própria solução, conforme mostrado a seguir.

O endereço IP elástico anexado à interface de rede elástica do sistema de arquivos foi excluído

O Amazon FSx não é compatível com o acesso a sistemas de arquivos na Internet pública. O Amazon FSx desvincula automaticamente qualquer endereço IP elástico, que é um endereço IP público acessível pela Internet, que é anexado à interface de rede elástica de um sistema de arquivos.

A interface de rede elástica do sistema de arquivos foi modificada ou excluída

Não é permitido modificar nem excluir a interface de rede elástica do sistema de arquivos. A modificação ou a exclusão da interface de rede pode causar uma perda permanente de conexão entre a VPC e o sistema de arquivos. Crie um novo sistema de arquivos e não modifique nem exclua a interface de rede elástica do FSx. Para obter mais informações, consulte Controle de acesso ao sistema de arquivos com a Amazon VPC.

Não é possível validar o acesso a um bucket do S3 ao criar uma associação de repositório de dados

A criação de uma associação de repositório de dados (DRA) a partir do console Amazon FSx ou o uso do comando `create-data-repository-association` CLI CreateDataRepositoryAssociation(é a ação equivalente da API) falha com a seguinte mensagem de erro.

```
Amazon FSx is unable to validate access to the S3 bucket. Ensure the IAM role or user
you are using has s3:Get*, s3:List* and s3:PutObject permissions to the S3 bucket
 prefix.
```

> **Note**
>
> Você também pode obter o erro acima ao criar um sistema de arquivos Scratch 1, Scratch 2 ou Persistent 1 vinculado a um repositório de dados (bucket ou prefixo do S3) usando o console Amazon FSx ou o comando `create-file-system` CLI (CreateFileSystemé a ação equivalente da API).

Medida a ser tomada

Se o sistema de arquivos do FSx para Lustre estiver na mesma conta do bucket do S3, esse erro significará que o perfil do IAM que você usou para a solicitação de criação não tem as permissões necessárias para acessar o bucket do S3. Certifique-se de que o perfil do IAM tenha as permissões listadas na mensagem de erro. Essas permissões oferecem suporte ao perfil vinculado ao serviço do Amazon FSx para Lustre que é usado para acessar o bucket especificado do Amazon S3 em seu nome.

Se o sistema de arquivos do FSx para Lustre estiver em uma conta diferente da conta do bucket do S3 (caso entre contas), além de garantir que o perfil do IAM que você usou tenha as permissões necessárias, a política de bucket do S3 deverá ser configurada para permitir o acesso pela conta na qual o FSx para Lustre foi criado. Veja a seguir um exemplo de política de bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketNotification",
                "s3:ListBucket",
                "s3:PutBucketNotification"
            ],
            "Resource": [
                "arn:aws:s3:::bucket_name",
                "arn:aws:s3:::bucket_name/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::file_system_account_ID:role/aws-service-role/
s3.data-source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fs-*"
                }
            }
        }
    ]
}
```

Para obter mais informações sobre permissões de bucket entre contas do S3, consulte Exemplo 2: proprietário do bucket concedendo permissões de bucket entre contas no Guia do usuário do Amazon Simple Storage Service.

A renomeação de diretórios demora muito tempo

Pergunta

Eu renomeei um diretório em um sistema de arquivos vinculado a um bucket do Amazon S3 e habilitei a exportação automática. Por que os arquivos dentro desse diretório estão demorando muito para serem renomeados no bucket do S3?

Resposta

Quando você renomeia um diretório no sistema de arquivos, o FSx para Lustre cria novos objetos do S3 para todos os arquivos e diretórios dentro do diretório que foi renomeado. O tempo necessário para propagar a renomeação do diretório para o S3 está diretamente correlacionado à quantidade de arquivos e diretórios que são descendentes do diretório que está sendo renomeado.

Solução de problemas de um bucket do S3 vinculado configurado incorretamente

Em alguns casos, um bucket do S3 vinculado do sistema de arquivos do FSx para Lustre pode ter um estado de ciclo de vida do repositório de dados configurado incorretamente.

Possível causa

Esse erro poderá ocorrer se o Amazon FSx não tiver as permissões do AWS Identity and Access Management (IAM) necessárias para acessar o repositório de dados vinculado. As permissões do IAM necessárias oferecem suporte ao perfil vinculado ao serviço Amazon FSx para Lustre que é usado para acessar o bucket especificado do Amazon S3 em seu nome.

Medida a ser tomada

1. Certifique-se de que sua entidade do IAM (usuário, grupo ou perfil) tenha as permissões apropriadas para criar sistemas de arquivos. Isso inclui adicionar a política de permissões que dá suporte ao perfil vinculado ao serviço Amazon FSx para Lustre. Para obter mais informações, consulte Adição de permissões para usar repositórios de dados no Amazon S3.
2. Usando a CLI ou API do Amazon FSx, atualize o sistema de arquivos com o comando `update-file-system` CLI (UpdateFileSystemé `AutoImportPolicy` a ação equivalente da API), da seguinte forma.

```
aws fsx update-file-system \
```

```
--file-system-id fs-0123456789abcdef0 \
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Para obter mais informações sobre funções vinculadas ao serviço, consulte Como usar perfis vinculados a serviço no Amazon FSx.

Possível causa

Esse erro poderá ocorrer se o repositório de dados vinculado do Amazon S3 tiver uma configuração de notificação de eventos existente, com tipos de eventos que se sobrepõem à configuração de notificação de eventos do Amazon FSx (`s3:ObjectCreated:*`, `s3:ObjectRemoved:*`).

Isso também poderá ocorrer se a configuração de notificação de eventos do Amazon FSx no bucket do S3 vinculado for excluída ou modificada.

Medida a ser tomada

1. Remova qualquer notificação de evento existente no bucket do S3 vinculado que usa um ou ambos os tipos de evento que a configuração de evento do FSx usa, `s3:ObjectCreated:*` e `s3:ObjectRemoved:*`.
2. Verifique se há uma configuração de notificação de evento do S3 em seu bucket do S3 vinculado com o nome `FSx`, os tipos de evento `s3:ObjectCreated:*` e `s3:ObjectRemoved:*` e envie para o tópico do SNS com ARN:*topic_arn_returned_in_API_response*.
3. Reaplique a configuração de notificação de evento do FSx no bucket do S3 usando a CLI ou a API do Amazon FSx para atualizar `AutoImportPolicy` do sistema de arquivos. Faça isso com o comando `update-file-system` CLI (UpdateFileSystemé a ação equivalente da API), da seguinte maneira.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Solução de problemas de armazenamento

Em alguns casos, você pode ter problemas de armazenamento com seu sistema de arquivos. Você pode solucionar esses problemas usando comandos `lfs`, como o comando `lfs migrate`.

Erro de gravação devido à falta de espaço no destino de armazenamento

Você pode verificar o uso de armazenamento do seu sistema de arquivos usando o comando `lfs df -h`, conforme descrito em Layout de armazenamento do sistema de arquivos. O campo `filesystem_summary` relata o uso total do armazenamento do sistema de arquivos.

Se o uso do disco do sistema de arquivos estiver em 100%, considere aumentar a capacidade de armazenamento do sistema de arquivos. Para obter mais informações, consulte Como gerenciar a capacidade de armazenamento.

Se o uso do armazenamento do sistema de arquivos não estiver em 100% e você ainda receber erros de gravação, o arquivo no qual você está gravando pode estar distribuído em um OST cheio.

Medida a ser tomada

- Se muitos dos seus OSTs estiverem cheios, aumente a capacidade de armazenamento do seu sistema de arquivos. Verifique se há armazenamento desbalanceado em OSTs seguindo as ações da seção Armazenamento desbalanceado em OSTs.
- Se seus OSTs não estiverem cheios, ajuste o tamanho do buffer da página suja do cliente aplicando o seguinte ajuste a todas as instâncias do seu cliente:

```
sudo lctl set_param osc.*.max_dirty_mb=64
```

Armazenamento desbalanceado em OSTs

O Amazon FSx para Lustre distribui novas faixas de arquivos uniformemente entre os OSTs. No entanto, seu sistema de arquivos ainda pode ficar desbalanceado devido aos padrões de E/S ou ao layout de armazenamento de arquivos. Como resultado, alguns destinos de armazenamento podem ficar cheios, enquanto outros permanecem relativamente vazios.

Você usa o comando `lfs migrate` para mover arquivos ou diretórios de OSTs mais cheios para menos cheios. Você pode usar o comando `lfs migrate` no modo de bloqueio ou sem bloqueio.

- O modo de bloqueio é o modo padrão para o comando `lfs migrate`. Quando executado no modo de bloqueio, o comando `lfs migrate` primeiro adquire um bloqueio de grupo nos arquivos e diretórios antes da migração de dados para evitar modificações nos arquivos e, em seguida, libera o bloqueio quando a migração é concluída. Ao impedir que outros processos modifiquem os arquivos, o modo de bloqueio impede que esses processos interrompam a migração. A

desvantagem é que impedir que uma aplicação modifique um arquivo pode resultar em atrasos ou erros na aplicação.

- O modo sem bloqueio é habilitado para o comando `lfs migrate` com a opção `-n`. Ao executar `lfs migrate` no modo sem bloqueio, outros processos ainda podem modificar os arquivos que estão sendo migrados. Se um processo modificar um arquivo antes que o comando `lfs migrate` conclua a migração, o comando `lfs migrate` falhará na migração desse arquivo, deixando o arquivo com seu layout de faixa original.

Recomendamos que você use o modo sem bloqueio, pois é menos provável que ele interfira na sua aplicação.

Medida a ser tomada

1. Execute uma instância de cliente relativamente grande (como o tipo de instância `c5n.4xlarge` do Amazon EC2) para montagem no sistema de arquivos.
2. Antes de executar o script do modo sem bloqueio ou o script do modo de bloqueio, primeiro execute os seguintes comandos em cada instância do cliente para acelerar o processo:

   ```
   sudo lctl set_param 'mdc.*.max_rpcs_in_flight=60'
   sudo lctl set_param 'mdc.*.max_mod_rpcs_in_flight=59'
   ```

3. Inicie uma sessão de tela e execute o script do modo sem bloqueio ou do modo de bloqueio. Certifique-se de alterar as variáveis apropriadas nos scripts:

   - Script de modo sem bloqueio:

     ```
     #!/bin/bash

     # UNCOMMENT THE FOLLOWING LINES:
     #
     # TRY_COUNT=0
     # MAX_MIGRATE_ATTEMPTS=100
     # OSTS="fsname-OST0000_UUID"
     # DIR_OR_FILE_MIGRATED="/mnt/subdir/"
     # BATCH_SIZE=10
     # PARALLEL_JOBS=16 # up to max-procs processes, set to 16 if client is
      c5n.4xlarge with 16 vcpu
     # LUSTRE_STRIPING_CONFIG="-E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32" #
      should be consistent with the existing striping setup
     #
     ```

```
if [ -z "$TRY_COUNT" -o -z "$MAX_MIGRATE_ATTEMPTS" -o -z "$OSTS" -o -z
 "$DIR_OR_FILE_MIGRATED" -o -z "$BATCH_SIZE" -o -z "$PARALLEL_JOBS" -o -z
 "$LUSTRE_STRIPING_CONFIG" ]; then
    echo "Some variables are not set."
    exit 1
fi

echo "lfs migrate starts"
while true; do
    output=$(sudo lfs find ! -L released --ost $OSTS --print0
 $DIR_OR_FILE_MIGRATED | shuf -z | /bin/xargs -0 -P $PARALLEL_JOBS -n $BATCH_SIZE
 sudo lfs migrate -n $LUSTRE_STRIPING_CONFIG 2>&1)
    if [[ $? -eq 0 ]]; then
        echo "lfs migrate succeeds for $DIR_OR_FILE_MIGRATED at the $TRY_COUNT
 attempt, exiting."
        exit 0
    elif [[ $? -eq 123 ]]; then
        echo "WARN: Target data objects are not located on these OSTs. Skipping
 lfs migrate"
        exit 1
    else
        echo "lfs migrate fails for $DIR_OR_FILE_MIGRATED at the $TRY_COUNT
 attempt, retrying..."
        if (( ++TRY_COUNT >= MAX_MIGRATE_ATTEMPTS )); then
            echo "WARN: Exceeds max retry attempt. Skipping lfs migrate for
 $DIR_OR_FILE_MIGRATED. Failed with the following error"
            echo $output
            exit 1
        fi
    fi
done
```

- Script de modo de bloqueio:
  - Substitua os valores em `OSTS` pelos valores de seus OSTs.
  - Forneça um valor inteiro para `nproc` a fim de definir o número de processos max-procs a serem executados em paralelo. Por exemplo, o tipo de instância `c5n.4xlarge` do Amazon EC2 tem 16 vCPUs; por isso, você pode usar 16 (ou um valor < 16) para `nproc`.
  - Forneça o caminho do diretório de montagem em `mnt_dir_path`.

```
# find all OSTs with usage above a certain threshold; for example, greater than
 or equal to 85% full
```

```
for OST in $(lfs df -h |egrep '( 8[5-9]| 9[0-9]|100)%'|cut -d' ' -f1); do echo
 ${OST};done|tr '\012' ','

# customer can also just pass OST values directly to OSTS variable
OSTS='dzfevbmv-OST0000_UUID,dzfevbmv-OST0002_UUID,dzfevbmv-OST0004_UUID,dzfevbmv-
OST0005_UUID,dzfevbmv-OST0006_UUID,dzfevbmv-OST0008_UUID'

nproc=<Run up to max-procs processes if client is c5n.4xlarge with 16 vcpu, this
 value can be set to 16>

mnt_dir_path=<mount dir, e.g. '/my_mnt'>

lfs find ${mnt_dir_path} --ost ${OSTS}| xargs -P ${nproc} -n2 lfs migrate -E 100M
 -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32
```

Observações

- Se você perceber que há um impacto na performance das leituras do sistema de arquivos, será possível interromper as migrações a qualquer momento usando `ctrl-c` ou `kill -9` e reduzir o número de threads (valor `nproc`) de volta para um número menor (como 8) e continuar a migração dos arquivos.
- O comando `lfs migrate` falhará em um arquivo que também é aberto pela workload do cliente. Isso vai gerar um erro e mover para o próximo arquivo; portanto, é possível que, se houver muitos arquivos sendo acessados, o script não consiga migrar nenhum arquivo e isso será refletido como progresso muito lento da migração.
- Você pode monitorar o uso do OST usando qualquer um dos métodos a seguir
  - Na montagem do cliente, execute o seguinte comando para monitorar o uso do OST e encontrar o OST com uso maior que 85%:

    ```
    lfs df -h |egrep '( 8[5-9]| 9[1-9]|100)%'
    ```

  - Verifique a CloudWatch métrica da Amazon0ST `FreeDataStorageCapacity`, verifique`Minimum`. Se o script estiver encontrando OSTs com mais de 85% cheios, quando a métrica estiver próxima de 15%, use `ctrl-c` ou `kill -9` para interromper a migração.
- Você também pode considerar alterar a configuração de distribuição do seu sistema de arquivos ou de um diretório para que os novos arquivos sejam distribuídos em vários destinos de armazenamento. Para obter mais informações, consulte em Distribuição de dados no sistema de arquivos.

Solução de problemas de driver de CSI do FSx para Lustre

Se você estiver enfrentando problemas com o driver FSx for Lustre CSI para contêineres em execução no Amazon EKS, consulte Solução de problemas do driver CSI (problemas comuns), disponível em. GitHub

Mais informações

Esta seção fornece uma referência de recursos do Amazon FSx com suporte, mas obsoletos.

Tópicos

Como configurar uma programação de backup personalizada

Recomendamos usar o AWS Backup para configurar uma programação de backup personalizada para o sistema de arquivos. As informações fornecidas nesta seção são para fins de referência caso precise programar backups com mais frequência do que é possível ao usar o AWS Backup.

Quando habilitado, o Amazon FSx realiza um backup do sistema de arquivos automaticamente uma vez por dia durante uma janela diária de backup. O Amazon FSx aplica um período de retenção especificado por você para esses backups automáticos. Além disso, ele oferece suporte a backups iniciados pelo usuário, para que você possa realizar backups a qualquer momento.

A seguir, você encontrará os recursos e a configuração para implantar a programação de backup personalizada. A programação de backup personalizada executa backups iniciados pelo usuário em um sistema de arquivos do Amazon FSx para Lustre em uma programação personalizada que é definida por você. Os exemplos de programação podem ser uma vez a cada seis horas, uma vez por semana, e assim por diante. Este script também configura a exclusão de backups anteriores ao período de retenção especificado.

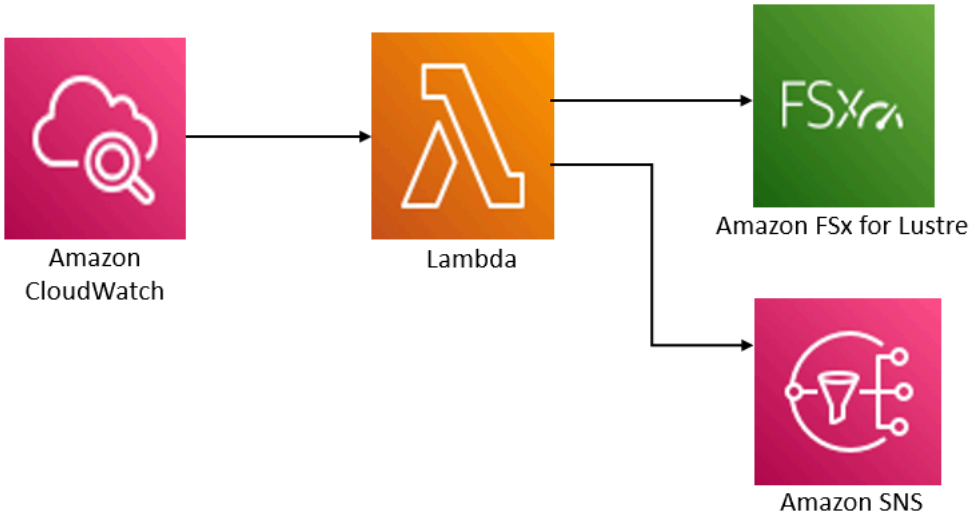
A solução implanta automaticamente todos os componentes necessários e considera os seguintes parâmetros:

- O sistema de arquivos
- Um padrão de programação CRON para realizar backups
- O período de retenção de backups (em dias)
- As tags de nome para backups

Para obter mais informações sobre os padrões de programação do CRON, consulte Expressões de programação para regras no Guia do CloudWatch usuário da Amazon.

Visão geral da arquitetura

A implantação dessa solução cria os recursos apresentados a seguir na Nuvem AWS.



Essa solução faz o seguinte:

1. O AWS CloudFormation modelo implanta um CloudWatch evento, uma função Lambda, uma fila do Amazon SNS e uma função do IAM. O perfil do IAM concede à função do Lambda permissão para invocar as operações de API do Amazon FSx para Lustre.
2. O CloudWatch evento é executado em uma programação que você define como um padrão CRON, durante a implantação inicial. Esse evento invoca a função do Lambda de gerenciador de backup da solução, que invoca a operação de API `CreateBackup` do Amazon FSx para Lustre para iniciar um backup.
3. O gerenciador de backup recupera uma lista de backups existentes que foram iniciados pelo usuário para o sistema de arquivos especificado usando `DescribeBackups`. Em seguida, ele exclui backups anteriores ao período de retenção especificado durante a implantação inicial.
4. O gerenciador de backup envia uma mensagem de notificação para a fila do Amazon SNS em caso de backup com êxito, caso escolha a opção de receber notificação durante a implantação inicial. Uma notificação é sempre enviada em caso de falha.

Modelo do AWS CloudFormation

Esta solução usa o AWS CloudFormation para automatizar a implantação da solução de programação de backup personalizada do Amazon FSx para Lustre. Para usar essa solução, baixe o fsx-scheduled-backupmodelo AWS CloudFormation .template.

Implantação automatizada

O procedimento apresentado a seguir configura e implanta essa solução de programação de backup personalizada. A implantação demora cerca de cinco minutos. Antes de começar, é necessário ter o ID de um sistema de arquivos do Amazon FSx para Lustre em execução em uma Amazon Virtual Private Cloud (Amazon VPC) em sua conta da AWS. Para obter mais informações sobre como criar esses recursos, consulte Conceitos básicos do Amazon FSx para Lustre.

> **Note**
>
> A implementação desta solução incorre em cobranças pelos serviços da AWS associados. Para obter mais informações, consulte as páginas de detalhes de preços desses serviços.

Iniciar a pilha de soluções de backup personalizadas

1. Baixe o fsx-scheduled-backupmodelo AWS CloudFormation .template. Para obter mais informações sobre a criação de uma pilha do AWS CloudFormation, consulte Criar uma pilha no console do AWS CloudFormation no Guia do usuário do AWS CloudFormation.

   > **Note**
   >
   > Por padrão, esse modelo é iniciado na região Leste dos EUA (Norte da Virgínia) da AWS. No momento, o Amazon FSx para Lustre está disponível somente em Regiões da AWS específicas. Você deve iniciar essa solução em uma região da AWS na qual o Amazon FSx para Lustre esteja disponível. Para obter mais informações, consulte a seção do Amazon FSx de Regiões da AWS and Endpoints na Referência geral da AWS.

2. Em Parâmetros, analise os parâmetros para o modelo e modifique-os de acordo com as necessidades do seu sistema de arquivos. Essa solução usa os valores padrão apresentados a seguir.

Parâmetro	Padrão	Descrição
ID do sistema de arquivos do Amazon FSx para Lustre	Nenhum valor padrão	O ID do sistema de arquivos para o sistema de arquivos do qual você deseja realizar o backup.

Parâmetro	Padrão	Descrição
Padrão de programação CRON para backups.	0 0/4 * * ? *	A programação para realizar o CloudWatch evento, acionando um novo backup e excluindo backups antigos fora do período de retenção.
Retenção de backup (dias)	7	O número de dias em que os backups iniciados pelo usuário serão mantidos. A função do Lambda exclui os backups iniciados pelo usuário que têm mais do que esse número de dias.
Nome para backups	Backups programados pelo usuário	O nome desses backups, que aparece na coluna Nome do backup do console de gerenciamento do Amazon FSx para Lustre.
Notificações de backups	Sim	Escolha se deseja receber notificações quando os backups forem iniciados com êxito. Uma notificaç ão sempre será enviada se houver um erro.
Endereço de e-mail	Nenhum valor padrão	O endereço de e-mail para assinar as notificações do SNS.

3. Escolha Próximo.
4. Em Opções, escolha Próximo.
5. Em Análise, analise e confirme as configurações. Você deve selecionar a caixa de seleção confirmando que o modelo cria os recursos do IAM.
6. Selecione Criar para implantar a stack.

Você pode visualizar o status da pilha no console do AWS CloudFormation, na coluna Status. Você deverá visualizar um status CREATE_COMPLETE em cerca de cinco minutos.

Opções adicionais

É possível usar a função do Lambda criada por esta solução para realizar backups programados personalizados de mais de um sistema de arquivos do Amazon FSx para Lustre. O ID do sistema de arquivos é passado para a função Amazon FSx for Lustre no CloudWatch JSON de entrada do evento. O JSON padrão passado para a função do Lambda é semelhante ao apresentado a seguir, no qual os valores para `FileSystemId` e `SuccessNotification` são passados dos parâmetros especificados ao iniciar a pilha do AWS CloudFormation.

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
}
```

Para programar backups para um sistema de arquivos adicional do Amazon FSx for Lustre, CloudWatch crie outra regra de evento. Você faz isso usando a origem do evento Programação, com a função do Lambda criada por essa solução como o destino. Escolha Constante (texto JSON) em Configurar entrada. Na entrada JSON, basta substituir o ID do sistema de arquivos do Amazon FSx para Lustre para fazer backup no lugar de `${FileSystemId}`. Além disso, substitua `Yes` ou `No` no lugar de `${SuccessNotification}` no JSON acima.

Quaisquer regras de CloudWatch eventos adicionais que você crie manualmente não fazem parte da pilha de soluções de backup programadas AWS CloudFormation personalizadas do Amazon FSx for Lustre. Portanto, eles não serão removidos se você excluir a pilha.

Histórico do documento

- Versão da API: 1/3/2018
- Última atualização da documentação: 25 de março de 2024

A tabela a seguir descreve alterações importantes que foram realizadas no Guia do usuário do Amazon FSx para Lustre. Para receber notificações sobre atualizações da documentação, inscreva-se no feed RSS.

Alteração	Descrição	Data
Suporte ao cliente Lustre para Amazon Linux 2023 adicionado	O cliente FSx for Lustre agora oferece suporte a instâncias do Amazon EC2 executando o Amazon Linux 2023. Para obter mais informações, consulte Instalação do cliente Lustre.	25 de março de 2024
Suporte ao cliente Lustre para Centos, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.9 adicionado	O cliente FSx for Lustre agora oferece suporte a instâncias do Amazon EC2 executando o Centos, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.9. Para obter mais informações, consulte Instalação do cliente Lustre.	9 de janeiro de 2024
O Amazon FSx atualizou as políticas gerenciadas do AmazonFSxFullAccess, AmazonF, AmazonFSxConsoleFullAccess, AmazonF e SxReadOnlyAccess AmazonF SxConsole	O Amazon FSx atualizou as políticas AmazonF, AmazonFSxFullAccess, AmazonFSxConsoleFullAccess, AmazonF e AmazonF para SxReadOnlyAccess adicionar a permissãoSxConsole	9 de janeiro de 2024

ReadOnlyAccess SxService RolePolicy AWS	ReadOnlyAccess. SxService RolePolicy `ec2:GetSecurityGroupsForVpc` Para obter mais informações, consulte as atualizações do Amazon FSx para políticas AWS gerenciadas.	
Suporte ao cliente Lustre para Centos, Rocky Linux e Red Hat Enterprise Linux (RHEL) 9.0 e 9.3 adicionado	O cliente FSx for Lustre agora oferece suporte a instâncias do Amazon EC2 executando Centos, Rocky Linux e Red Hat Enterprise Linux (RHEL) 9.0 e 9.3. Para obter mais informações, consulte Instalação do cliente Lustre.	20 de dezembro de 2023
O Amazon FSx for Lustre atualizou as políticas gerenciadas do AmazonF e SxFullAccess do AmazonF SxConsoleFullAccess AWS	O Amazon FSx atualizou as políticas do AmazonF SxFullAccess e do AmazonF para adicionar a açãoSxConsoleFullAccess . `ManageCrossAccountDataReplication` Para obter mais informações, consulte as atualizações do Amazon FSx para políticas AWS gerenciadas.	20 de dezembro de 2023

O Amazon FSx atualizou as políticas gerenciadas do AmazonF SxFullAccess e do AmazonF SxConsoleFullAccess AWS	O Amazon FSx atualizou as políticas do AmazonF SxFullAccess e do AmazonF para adicionar a permissão . SxConsoleFullAccess `fsx:CopySnapshotAndUpdateVolume` Para obter mais informações, consulte as atualizações do Amazon FSx para políticas AWS gerenciadas.	26 de novembro de 2023
Suporte adicionado para a escalabilidade da capacidade de throughput	Agora, é possível modificar a capacidade de throughput para os sistemas de arquivos persistentes existentes e baseados em SSD do FSx para Lustre à medida que seus requisitos de throughput evoluem. Para obter mais informações, consulte Como gerenciar a capacidade de throughput.	16 de novembro de 2023

O Amazon FSx atualizou as políticas gerenciadas do AmazonF SxFullAccess e do AmazonF SxConsoleFullAccess AWS	O Amazon FSx atualizou as SxConsoleFullAccess políticas do AmazonF SxFullAccess e do AmazonF para adicionar as permissões e. `fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` Para obter mais informações, consulte as atualizações do Amazon FSx para políticas AWS gerenciadas.	14 de novembro de 2023
Suporte adicionado para cotas de projetos	Agora, é possível criar cotas de armazenamento para projetos. Uma cota de projeto se aplica a todos os arquivos ou os diretórios associados a um projeto. Para obter mais informações, consulte Cotas de armazenamento.	29 de agosto de 2023
Suporte adicionado para a versão 2.15 do Lustre	Todos os sistemas de arquivos do FSx para Lustre passaram a ser desenvolvidos na versão 2.15 do Lustre quando criados usando o console do Amazon FSx. Para obter mais informações, consulte Etapa 1: criar o sistema de arquivos do Amazon FSx para Lustre.	29 de agosto de 2023

Região da AWS Suporte adicional adicionado para o tipo de implantação Persistent_1	Os sistemas de arquivos Persistent_1 FSx for Lustre agora estão disponíveis em Israel (Tel Aviv). Região da AWS Para obter mais informações, consulte Opções de implantação para sistemas de arquivos do FSx para Lustre.	24 de agosto de 2023
Suporte adicionado para tarefas de repositório de dados de lançamento	Agora, o FSx para Lustre fornece tarefas de repositório de dados de liberação para liberar arquivos arquivados de um sistema de arquivos vinculado a um repositório de dados do S3. A liberação de um arquivo retém a listagem e os metadados do arquivo, mas remove a cópia local do conteúdo desse arquivo. Para obter mais informações, consulte Using data repository tasks to release files.	9 de agosto de 2023
O Amazon FSx atualizou a política gerenciada do SxServiceRolePolicy AWS AmazonF	O Amazon FSx atualizou a `cloudwatch:PutMetricData` permissão no AmazonF. SxServiceRolePolicy Para obter mais informações, consulte as atualizações do Amazon FSx para políticas AWS gerenciadas.	24 de julho de 2023

O Amazon FSx atualizou a política gerenciada do SxFullAccess AWS AmazonF	O Amazon FSx atualizou a SxFullAccess política da AmazonF para remover a `fsx:*` permissão e adicionar ações específicas. `fsx` Para obter mais informações, consulte a política da Amazon SxFullAccess.	13 de julho de 2023
O Amazon FSx atualizou a política gerenciada do SxConsoleFullAccess AWS AmazonF	O Amazon FSx atualizou a SxConsoleFullAccess política da AmazonF para remover a `fsx:*` permissão e adicionar ações específicas. `fsx` Para obter mais informações, consulte a política da Amazon SxConsoleFullAccess.	13 de julho de 2023
Adição de suporte ao cliente Lustre para Centos, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.8	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam Centos, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.8. Para obter mais informações, consulte Instalação do cliente Lustre.	25 de maio de 2023

Support adicionado AutoImport e AutoExport métricas	O FSx for Lustre agora fornece métricas CloudWatch da Amazon que monitoram atualizações automáticas de importação e exportação para sistemas de arquivos vinculados a repositórios de dados. Para obter mais informações, consulte Monitoramento com a Amazon CloudWatch.	31 de março de 2023
Adição de suporte de DRA para os tipos de implantação Persistent_1 e Scratch_2	Agora, é possível criar associações de repositórios de dados para vincular repositórios de dados a sistemas de arquivos do Lustre 2.12 com os tipos de implantação Persistent_1 ou Scratch_2. Para obter mais informações, consulte Using data repositories with Amazon FSx for Lustre.	29 de março de 2023
Adição de suporte ao cliente Lustre para Centos, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.7	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam Centos, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.7. Para obter mais informações, consulte Instalação do cliente Lustre.	5 de dezembro de 2022

Região da AWS Suporte adicional adicionado para o tipo de implantação Persistent_2	A próxima geração de sistemas de arquivos SSD Persistent_2 FSx for Lustre já está disponível na Europa (Estocolmo), Ásia-Pacífico (Hong Kong), Ásia-Pacífico (Mumbai) e Ásia-Pacífico (Seul). Regiões da AWS Para obter mais informações, consulte Opções de implantação para sistemas de arquivos do FSx para Lustre.	10 de novembro de 2022
Adição de suporte ao cliente Lustre para Centos, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.6	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam Centos, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.6. Para obter mais informações, consulte Instalação do cliente Lustre.	8 de setembro de 2022
Adição de suporte ao cliente Lustre para Ubuntu 22	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam o Ubuntu 22.04. Para obter mais informações, consulte Instalação do cliente Lustre.	28 de julho de 2022
Adição de suporte ao cliente Lustre para Rocky Linux	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam o Rocky Linux. Para obter mais informações, consulte Instalação do cliente Lustre.	8 de julho de 2022

Suporte adicionado para Lustre Root Squash	Agora, é possível usar o recurso Lustre Root Squash para restringir o acesso no nível raiz de clientes que tentam acessar o sistema de arquivos do FSx para Lustre como raiz. Para obter mais informações, consulte Lustre Root Squash.	25 de maio de 2022
Região da AWS Suporte adicional adicionado para o tipo de implantação Persistent_2	Os sistemas de arquivos FSx for Lustre SSD Persistent_2 de próxima geração agora estão disponíveis na Europa (Londres), Ásia-Pacífico (Cingapura) e Ásia-Pacífico (Sydney). Regiões da AWS Para obter mais informações, consulte Opções de implantação para sistemas de arquivos do FSx para Lustre.	19 de abril de 2022
Support adicionado AWS DataSync para uso na migração de arquivos para seus sistemas de arquivos Amazon FSx for Lustre.	Agora você pode usar AWS DataSync para migrar arquivos de sistemas de arquivos existentes para sistemas de arquivos FSx for Lustre. Para obter mais informações, consulte Como migrar arquivos existentes para o FSx para Lustre usando o AWS DataSync.	5 de abril de 2022

Support adicionado para AWS PrivateLink endpoints de interface VPC	Agora, é possível usar endpoints da VPC de interface para acessar a API do Amazon FSx usando a VPC sem a necessidade de enviar tráfego pela Internet. Para obter mais informações, consulte Amazon FSx and interface VPC endpoints.	5 de abril de 2022
Suporte adicionado para enfileiramento de DRA do Lustre	Agora, é possível criar uma DRA (associação de repositório de dados) durante a criação de um sistema de arquivos do FSx para Lustre. A solicitação será colocada na fila e a DRA será criada assim que o sistema de arquivos estiver disponível. Para obter mais informações, consulte Linking your file system to an S3 bucket.	28 de fevereiro de 2022
Adição de suporte ao cliente Lustre para Centos e Red Hat Enterprise Linux (RHEL) 8.5	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam Centos e Red Hat Enterprise Linux (RHEL) 8.5. Para obter mais informações, consulte Instalação do cliente Lustre.	20 de dezembro de 2021

Suporte para a exportação de alterações do FSx para Lustre para um repositório de dados vinculado	Agora, é possível configurar o FSx para Lustre para exportar arquivos novos, alterados e excluídos automaticamente do sistema de arquivos para um repositório de dados vinculado do Amazon S3. Você pode usar tarefas de repositór io de dados para exportar alterações de dados e de metadados para o repositór io de dados. Além disso, é possível configurar links para vários repositórios de dados. Para obter mais informações, consulte Exporting changes to the data repository.	30 de novembro de 2021
Suporte adicionado para o registro em log do Lustre	Agora você pode configurar o FSx for Lustre para registrar eventos de erro e aviso para repositórios de dados associados ao seu sistema de arquivos no Amazon Logs. CloudWatch Para obter mais informações, consulte Logging with Amazon CloudWatch Logs.	30 de novembro de 2021

Sistemas de arquivos persistentes baseados em SSD oferecem suporte para maior throughput e menor capacidade de armazenamento	Os sistemas de arquivos Persistent do FSx para Lustre baseados em SSD de última geração têm opções de throughput mais altas e uma capacidade de armazenamento mínima mais baixa. Para obter mais informações, consulte Opções de implantação para sistemas de arquivos do FSx para Lustre.	30 de novembro de 2021
Suporte adicionado para a versão 2.12 do Lustre	Agora, é possível escolher a versão 2.12 do Lustre durante a criação de um sistema de arquivos do FSx para Lustre. Para obter mais informações, consulte Etapa 1: criar o sistema de arquivos do Amazon FSx para Lustre.	5 de outubro de 2021
Adição de suporte ao cliente Lustre para Centos e Red Hat Enterprise Linux (RHEL) 8.4	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam Centos e Red Hat Enterprise Linux (RHEL) 8.4. Para obter mais informações, consulte Instalação do cliente Lustre.	9 de junho de 2021

Suporte adicionado para a compactação de dados	Agora, á possível habilitar a compactação de dados ao criar um sistema de arquivos do FSx para Lustre. Você também pode habilitar ou desabilitar a compactação de dados em um sistema de arquivos do FSx para Lustre existente. Para obter mais informações, consulte Compactação de dados do Lustre.	27 de maio de 2021
Suporte adicionado para cópia de backups	Agora você pode usar o Amazon FSx para copiar backups dentro do mesmo Conta da AWS para outro Região da AWS (cópias entre regiões) ou dentro do mesmo Região da AWS (cópias dentro da região). Para obter mais informações, consulte Copying backups.	12 de abril de 2021
Suporte ao cliente Lustre para conjuntos de arquivos do Lustre	Agora, o cliente do FSx para Lustre oferece suporte ao uso de conjuntos de arquivos para montar somente um subconjunto do namespace do sistema de arquivos. Para obter mais informações, consulte Montagem de conjuntos de arquivos específicos.	18 de março de 2021

Suporte adicionado para acesso de clientes usando endereços IP não privados	É possível acessar os sistemas de arquivos do FSx para Lustre de um cliente on-premises usando endereços IP não privados. Para obter mais informações, consulte Montagem de sistemas de arquivos do Amazon FSx usando uma Amazon VPC on-premises ou emparelhada.	17 de dezembro de 2020
Adição de suporte ao cliente Lustre para Centos 7.9 baseado em ARM	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam o Centos 7.9 baseado em ARM. Para obter mais informações, consulte Instalação do cliente Lustre.	17 de dezembro de 2020
Adição de suporte ao cliente Lustre para Centos e Red Hat Enterprise Linux (RHEL) 8.3	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam Centos e Red Hat Enterprise Linux (RHEL) 8.3. Para obter mais informaçõ es, consulte Instalação do cliente Lustre.	16 de dezembro de 2020

Suporte adicionado para a escalabilidade da capacidade e de throughput e de armazenamento	Agora, é possível ampliar a capacidade de throughput e de armazenamento para os sistemas de arquivos do FSx para Lustre existentes à medida que seus requisitos de armazenamento e de throughput evoluem. Para obter mais informações, consulte Managing storage and throughput capacity.	24 de novembro de 2020
Suporte adicionado para cotas de armazenamento	Agora, é possível criar cotas de armazenamento para usuários e grupos. As cotas de armazenamento limitam a quantidade de espaço no disco e o número de arquivos que um usuário ou um grupo pode consumir no sistema de arquivos do FSx para Lustre. Para obter mais informações, consulte Cotas de armazenamento.	9 de novembro de 2020
O Amazon FSx agora está integrado com AWS Backup	Agora você pode usá-lo AWS Backup para fazer backup e restaurar seus sistemas de arquivos FSx, além de usar os backups nativos do Amazon FSx. Para obter mais informações, consulte Como usar AWS Backup com o Amazon FSx.	9 de novembro de 2020

Suporte adicionado para opções de armazenamento em HDD (unidade de disco rígido)	Agora, além da opção de armazenamento em SSD (unidade de estado sólido), o FSx para Lustre oferece suporte à opção de armazenamento em HDD (unidade de disco rígido). É possível configurar o sistema de arquivos para usar HDD para workloads com alto throughput que, normalmente, têm operações de arquivos grandes e sequenciais. Para obter mais informações, consulte Multiple Storage Options.	12 de agosto de 2020
Suporte para importação de alterações de repositório de dados vinculados para o FSx para Lustre	Agora, é possível configurar o sistema de arquivos do FSx para Lustre com a finalidade de importar automaticamente novos arquivos adicionados e arquivos que foram alterados em um repositório de dados vinculado após a criação do sistema de arquivos. Para obter mais informações, consulte Automatically import updates from the data repository.	23 de julho de 2020

Adição de suporte ao cliente Lustre para SUSE Linux SP4 e SP5	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam o SUSE Linux SP4 e SP5. Para obter mais informações, consulte Instalação do cliente Lustre.	20 de julho de 2020
Adição de suporte ao cliente Lustre para Centos e Red Hat Enterprise Linux (RHEL) 8.2	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam Centos e Red Hat Enterprise Linux (RHEL) 8.2. Para obter mais informaçõ es, consulte Instalação do cliente Lustre.	20 de julho de 2020
Suporte adicionado para backups automáticos e manuais do sistema de arquivos	Agora, é possível efetuar backups diários automátic os e manuais de sistemas de arquivos não vinculado s a um repositório de dados durável do Amazon S3. Para ter mais informações, consulte Trabalhar com backups.	23 de junho de 2020

Liberação de dois novos tipos de implantação para os sistemas de arquivos	Os sistemas de arquivos transitórios são projetados para o armazenamento temporário e para o processamento de dados de curto prazo. Os sistemas de arquivos persistentes são projetados para armazenamento e workloads de longo prazo. Para obter mais informações, consulte Opções de implantação para o FSx para Lustre.	12 de fevereiro de 2020
Suporte adicionado para metadados POSIX	O FSx para Lustre retém metadados POSIX associados ao importar e exportar arquivos para um repositório de dados durável vinculado no Amazon S3. Para obter mais informações, consulte POSIX metadata support for data repositories.	23 de dezembro de 2019
Liberação do novo recurso de tarefas de repositório de dados	Agora, é possível exportar dados alterados e metadados POSIX associados para um repositório de dados durável vinculado no Amazon S3 usando tarefas de repositório de dados. Para obter mais informações, consulte Transferring Data & Metadata Using Data Repository Tasks.	23 de dezembro de 2019

Região da AWS Suporte adicional adicionado	O FSx para Lustre já está disponível na Região da AWS Europa (Londres). Para obter limites específicos relaciona dos à região do FSx para Lustre, consulte Limites.	9 de julho de 2019
Região da AWS Suporte adicional adicionado	O FSx for Lustre agora está disponível na Ásia-Pacífico (Cingapura). Região da AWS Para obter limites específicos relacionados à região do FSx para Lustre, consulte Limites.	26 de junho de 2019
Adição de suporte ao cliente Lustre para Amazon Linux e Amazon Linux 2	Agora, o cliente do FSx para Lustre oferece suporte a instâncias do Amazon EC2 que executam o Amazon Linux e o Amazon Linux 2. Para obter mais informações, consulte Instalação do cliente Lustre.	11 de março de 2019
Suporte adicionado para caminhos de exportação de dados definidos pelos usuários	Agora, os usuários têm a opção de substituir os objetos originais no bucket do Amazon S3 ou gravar os arquivos novos ou alterados em um prefixo especificado por você. Com esta opção, você tem flexibilidade adicional para incorporar o FSx para Lustre em seus fluxos de trabalho de processamento de dados. Para obter mais informaçõ es, consulte Exporting Data to Your Amazon S3 Bucket.	6 de fevereiro de 2019

Aumento do limite do armazenamento total padrão	O armazenamento total padrão para todos os sistemas de arquivos do FSx para Lustre aumentou para 100.800 GiB. Para obter mais informações, consulte Limites.	11 de janeiro de 2019
Amazon FSx para Lustre já está disponível para o público em geral	O Amazon FSx para Lustre é um sistema de arquivos totalmente gerenciado que é otimizado para workloads com uso intensivo de computaçã o, como a computação de alta performance, o machine learning e os fluxos de trabalho de processamento de mídia.	28 de novembro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.