aws

Guia do usuário do ONTAP

FSx para ONTAP

FSx para ONTAP: Guia do usuário do ONTAP

Table of Contents

O que é o Amazon FSx for NetApp ONTAP?

O Amazon FSx for NetApp ONTAP é um serviço totalmente gerenciado que fornece armazenamento de arquivos altamente confiável, escalável, de alto desempenho e rico em recursos, baseado no popular sistema de arquivos ONTAP. NetApp O FSx for ONTAP combina os recursos, o desempenho, os recursos e as operações de API familiares dos sistemas de NetApp arquivos com a agilidade, escalabilidade e simplicidade de um sistema totalmente gerenciado. AWS service (Serviço da AWS)

O FSx for ONTAP fornece armazenamento de arquivos compartilhado rico em recursos, rápido e flexível, amplamente acessível a partir de instâncias de computação Linux, Windows e macOS executadas no local ou no local. AWS O FSx para ONTAP oferece armazenamento de unidade de estado sólido (SSD) de alta performance com latências de submilissegundos. Com o FSx para ONTAP, você pode atingir níveis de performance de SSD para sua workload enquanto paga pelo armazenamento SSD para apenas uma pequena fração de seus dados.

Gerenciar seus dados com o FSx para ONTAP é mais fácil porque você pode capturar, clonar e replicar seus arquivos com o clique de um botão. Além disso, o FSx para ONTAP classifica automaticamente seus dados em camadas em um armazenamento elástico de baixo custo, diminuindo a necessidade de provisionar ou gerenciar a capacidade.

O FSx para ONTAP também fornece armazenamento altamente disponível e durável com backups totalmente gerenciados e suporte para recuperação de desastres entre regiões. Para facilitar a proteção e a segurança de seus dados, o FSx para ONTAP oferece suporte a aplicações populares de segurança de dados e antivírus.

Para clientes que usam o NetApp ONTAP no local, o FSx for ONTAP é a solução ideal para migrar, fazer backup ou explodir seus aplicativos baseados em arquivos do local para AWS sem a necessidade de alterar o código do aplicativo ou a forma como você gerencia seus dados.

Como um serviço totalmente gerenciado, o FSx para ONTAP facilita executar e escalar um armazenamento de arquivos compartilhado confiável, de alta performance e seguro na nuvem. Com o FSx para ONTAP, você não precisa mais se preocupar com:

- Configurar e provisionar servidores de arquivos e volumes de armazenamento
- Replicar dados
- Instalar e aplicar patches no software do servidor de arquivos

- Detectar e resolver falhas de hardware
- Como gerenciar o failover e o failback
- Executar backups manualmente

O FSx for ONTAP também fornece uma integração avançada com outros AWS serviços, como AWS Identity and Access Management (IAM), Amazon WorkSpaces, AWS Key Management Service (AWS KMS) e. AWS CloudTrail

Tópicos

Recursos do FSx para ONTAP

Com o FSx para ONTAP, você obtém uma solução de armazenamento de arquivos totalmente gerenciada com:

- Suporte para conjuntos de dados em escala de petabytes em um único namespace
- Até dezenas de gigabytes por segundo (GBps) de taxa de transferência por sistema de arquivos
- Acesso multiprotocolo aos dados usando os protocolos Network File System (NFS), Server Message Block (SMB) e Internet Small Computer Systems Interface (iSCSI)
- Opções de implantação multi-AZ e single-AZ altamente disponíveis e duráveis
- Classificação automática de dados em camadas que reduz os custos de armazenamento ao fazer a transição automática de dados acessados com pouca frequência para um nível de armazenamento de menor custo com base em seus padrões de acesso
- Compressão, eliminação de duplicação e compactação de dados para reduzir o consumo de armazenamento
- Support for NetApp's, recurso de SnapMirror replicação
- Support para soluções NetApp de armazenamento em cache local: NetApp Global File Cache e FlexCache

- Support para acesso e gerenciamento usando NetApp ferramentas nativas AWS ou operações de API
  - AWS Management Console, AWS Command Line Interface (AWS CLI) e SDKs
  - NetApp CLI do ONTAP, API REST e BlueXP
- Suporte para os seguintes recursos de proteção e segurança de dados:
  - Criptografia de dados do sistema de arquivos e backups em repouso usando AWS KMS keys
  - Criptografia de dados em trânsito usando chaves de sessão do SMB do Kerberos
  - Verificação antivírus sob demanda
  - Autenticação e autorização usando o Microsoft Active Directory
  - Auditoria de acesso a arquivos
  - NetAppSnapLockRecurso WORM com suporte para volumes corporativos e de conformidade

Segurança e proteção de dados

O Amazon FSx fornece vários níveis de segurança e conformidade para facilitar a proteção de seus dados. Ele criptografa automaticamente os dados em repouso em sistemas de arquivos e backups usando chaves que você gerencia em AWS Key Management Service (AWS KMS). Você também pode criptografar dados em trânsito usando o Kerberos para clientes NFS e SMB.

O Amazon FSx foi avaliado para estar em conformidade com os seguintes padrões:

- International Standards Organization (ISO)
- Padrão de segurança de dados do setor de cartão de pagamento (PCI DSS – Payment Card Industry Data Security Standard)
- Certificações SOC (Controles do Sistema e da Organização)
- Lei de Portabilidade e Responsabilidade de Seguros de Saúde de 1996 (HIPAA)

Para ter mais informações, consulte Proteção de dados no Amazon FSx for ONTAP NetApp .

O Amazon FSx também fornece os seguintes níveis de controle de acesso:

- No nível do sistema de arquivos, o Amazon FSx fornece controle de acesso usando grupos de segurança da Amazon Virtual Private Cloud (Amazon VPC).
- No nível da API, o Amazon FSx fornece controle de acesso usando políticas de acesso AWS Identity and Access Management (IAM).

- Para fornecer controle de acesso em nível de arquivo e pasta, o Amazon FSx é compatível com permissões Unix, listas de controle de acesso (ACLs) NFS e ACLs NTFS. Quando você associa o Amazon FSx a um Active Directory, os usuários que estão acessando sistemas de arquivos podem se autenticar usando suas credenciais do Active Directory.

Para que você possa ver as ações realizadas pelos usuários em seus recursos do Amazon FSx, o Amazon FSx se integra AWS CloudTrail para monitorar e registrar suas chamadas de API do Amazon FSx. Para ter mais informações, consulte Registro em log de chamadas de API do FSx para ONTAP com AWS CloudTrail.

Além disso, o Amazon FSx protege seus dados com backups de sistemas de arquivos altamente duráveis. O Amazon FSx realiza backups diários automáticos, e você pode fazer backups adicionais a qualquer momento. Para ter mais informações, consulte Como proteger seus dados.

Preços do FSx para ONTAP

Você é cobrado pelos sistemas de arquivos com base nas seguintes categorias:

- Capacidade de armazenamento SSD (por gigabyte-mês ou GB/mês)
- IOPS de SSD que você provisiona acima de três IOPS/GB (por IOPS/mês)
- Capacidade de throughput (por megabytes por segundo [MBps]/mês)
- Consumo de armazenamento do pool de capacidade (por GB/mês)
- Solicitações de pool de capacidade (por leitura e gravação)
- Consumo de armazenamento de backup (por GB/mês)

Para obter mais informações sobre preços e taxas associados ao serviço, consulte os preços do Amazon FSx for NetApp ONTAP.

Fóruns do FSx para ONTAP

Se você detectar problemas ao usar o Amazon FSx, use os fóruns de discussão do FSx para ONTAP para obter respostas.

Você é um usuário iniciante do Amazon FSx?

Se estiver usando o Amazon FSx pela primeira vez, recomendamos que leia as seguintes seções na ordem:

1. Se você é novo em AWS, veja como Configurar o FSx para ONTAP configurar um Conta da AWS.
2. Se você estiver pronto para criar seu primeiro sistema de arquivos do Amazon FSx, siga as instruções em Introdução ao Amazon FSx for ONTAP NetApp .
3. Para obter mais informações sobre performance, consulte Amazon FSx para NetApp desempenho de ONTAP.
4. Para obter detalhes de segurança do Amazon FSx, consulte Segurança no Amazon FSx for ONTAP NetApp .
5. Para obter mais informações sobre a API do Amazon FSx, consulte Amazon FSx API Reference.

Como o Amazon FSx for NetApp ONTAP funciona

Este tópico apresenta os principais recursos dos sistemas de arquivos Amazon FSx NetApp for ONTAP e como eles funcionam, com links para seções com descrições detalhadas, detalhes importantes de implementação e procedimentos de configuração. step-by-step

Tópicos

Sistemas de arquivos do FSx para ONTAP

Um sistema de arquivos é o principal recurso FSx for ONTAP, análogo a um cluster ONTAP local. NetApp Você especifica a capacidade de armazenamento da unidade de estado sólido (SSD) e a capacidade de throughput do sistema de arquivos, além de escolher uma Amazon Virtual Private Cloud (VPC) na qual seu sistema de arquivos será criado. Para ter mais informações, consulte Como gerenciar sistemas de arquivos do FSx para ONTAP.

Seu sistema de arquivos pode ter de um a 12 pares de alta disponibilidade (HA), dependendo da configuração. Um par de HA é composto por dois servidores de arquivos em uma configuração de espera ativa. Os sistemas de arquivos com um único par de HA são chamados de sistemas de arquivos escaláveis. Os sistemas de arquivos com vários pares de HA são chamados de sistemas de arquivos escaláveis. Para ter mais informações, consulte Pares de alta disponibilidade (HA).

Máquinas virtuais de armazenamento

Uma máquina virtual de armazenamento (SVM) é um servidor de arquivos isolado com seus próprios endpoints administrativos e de acesso a dados, para fins de administrar e acessar dados. Ao acessar dados no sistema de arquivos do FSx para ONTAP, seus clientes e estações de trabalho interagem

com uma SVM usando o endereço IP do endpoint da SVM. Para ter mais informações, consulte Como gerenciar SVMs.

Você pode associar as SVMs a um Microsoft Active Directory para a autenticação e a autorização de acesso a arquivos. Para ter mais informações, consulte Trabalhar com o Microsoft Active Directory no FSx para ONTAP.

Volumes

Os volumes do FSx para ONTAP são recursos virtuais usados para organizar e agrupar seus dados. Os volumes são contêineres lógicos hospedados em SVMs, e os dados armazenados neles consomem a capacidade de armazenamento físico em seu sistema de arquivos.

Ao criar um volume, você define seu tamanho, o que determina a quantidade de dados físicos que você pode armazenar nele, independentemente do nível de armazenamento em que os dados estão armazenados. Você também define o tipo de volume, RW (leitura-gravável) ou DP (proteção de dados). Um volume DP é somente para leitura e pode ser usado como destino em um NetApp SnapMirror relacionamento. SnapVault

Os volumes FSx for ONTAP têm provisionamento reduzido, o que significa que eles só consomem capacidade de armazenamento para os dados armazenados neles. Com volumes de provisionamento reduzido, a capacidade de armazenamento não é reservada com antecedência. Em vez disso, o armazenamento é alocado dinamicamente, conforme necessário. O espaço livre é liberado de volta para o sistema de arquivos quando os dados no volume ou no LUN são excluídos. Por exemplo, você pode criar três volumes de 10 TiB em um sistema de arquivos configurado com 10 TiB de capacidade de armazenamento livre, desde que a quantidade total de dados armazenados nos três volumes não exceda 10 TiB em nenhum momento. A quantidade de dados armazenados fisicamente em um volume conta para o consumo geral da capacidade de armazenamento. Para ter mais informações, consulte Como gerenciar volumes do FSx para ONTAP.

Níveis de armazenamento

Um sistema de arquivos do FSx para ONTAP tem dois níveis de armazenamento: o armazenamento principal e o armazenamento do grupo de capacidade. O armazenamento principal é um armazenamento SSD provisionado, escalável e de alta performance, criado especificamente para a parte ativa do seu conjunto de dados. O armazenamento do grupo de capacidade é um nível de armazenamento totalmente elástico cujo tamanho pode ser escalado para petabytes, sendo otimizado em termos de custo para dados acessados com pouca frequência. Os dados gravados nos

volumes consomem capacidade nos níveis de armazenamento. Para ter mais informações, consulte Níveis de armazenamento do FSx para ONTAP.

Hierarquização de dados

A classificação por níveis de dados é o processo pelo qual o Amazon FSx NetApp for ONTAP move automaticamente os dados entre o SSD e os níveis de armazenamento do pool de capacidade. Cada volume tem uma política de classificação por níveis que controla se os dados são movidos para o nível de capacidade quando ficam inativos (frios). O período de resfriamento da política de hierarquização de um volume determina quando os dados se tornam inativos (frios). Para ter mais informações, consulte Divisão de dados em níveis no volume.

Eficiência de armazenamento

O Amazon FSx for NetApp ONTAP oferece suporte aos recursos de eficiência de armazenamento em nível de bloco do ONTAP — compactação, compactação e desduplicação — para reduzir a capacidade de armazenamento que seus dados consomem. Os recursos de eficiência de armazenamento podem reduzir o espaço ocupado pelos dados no armazenamento SSD, no armazenamento do grupo de capacidade e nos backups. A economia típica da capacidade de armazenamento das workloads de compartilhamento de arquivos de uso geral, sem sacrificar a performance, é de 65% com compressão, eliminação de duplicação e compactação, tanto nos níveis de armazenamento SSD quanto no grupo de capacidade. Para ter mais informações, consulte Eficiência de armazenamento do FSx para ONTAP.

Acessar dados armazenados nos sistemas de arquivos do FSx para ONTAP

Você pode acessar seus dados nos volumes do FSx para ONTAP de vários clientes Linux, Windows ou macOS simultaneamente por meio dos protocolos NFS (v3, v4, v4.1, v4.2) e SMB. Também é possível acessar os dados usando o protocolo iSCSI (blocos). Para ter mais informações, consulte Acesso a dados do .

Como gerenciar recursos do FSx para ONTAP

Existem várias maneiras de interagir com o sistema de arquivos do FSx para ONTAP e gerenciar os recursos. Você pode gerenciar seus recursos FSx for ONTAP usando ambas as ferramentas de gerenciamento AWS e NetApp ONTAP:

- AWS ferramentas de gerenciamento
  - O AWS Management Console
  - O AWS Command Line Interface (AWS CLI)
  - A API e os SDKs do Amazon FSx
  - AWS CloudFormation
- NetApp ferramentas de gerenciamento:
  - NetApp BlueXP
  - O NetApp ONTAP CLI
  - A API NetApp REST ONTAP

Para ter mais informações, consulte Administração de recursos.

Configurar o FSx para ONTAP

Antes de usar o Amazon FSx pela primeira vez, conclua as seguintes tarefas:

1. Inscreva-se para um Conta da AWS
2. Criar um usuário com acesso administrativo

Tópicos

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

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

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

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como uma prática recomendada de segurança, atribua o acesso administrativo para um usuário e use somente o usuário-raiz para executar tarefas que requerem o acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. 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 com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

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

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso 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 para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso para usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Próxima etapa

Para começar a usar o FSx para ONTAP, consulte Introdução ao Amazon FSx for ONTAP NetApp para obter instruções de como criar seus recursos do Amazon FSx.

Introdução ao Amazon FSx for ONTAP NetApp

Saiba como começar a usar o Amazon FSx for NetApp ONTAP. Este exercício sobre os conceitos básicos inclui as etapas apresentadas a seguir.

Tópicos

Etapa 1: Criar um sistema de arquivos Amazon FSx for NetApp ONTAP

O console do Amazon FSx tem duas opções para criar um sistema de arquivos: Criação rápida e Criação padrão. Para criar de forma rápida e fácil um sistema de arquivos Amazon FSx for NetApp ONTAP com a configuração recomendada do serviço, use a opção de criação rápida.

A opção de criação rápida cria um sistema de arquivos com um único par de alta disponibilidade (HA), uma única máquina virtual de armazenamento (SVM) e um único volume. A opção Criação rápida configura esse sistema de arquivos para permitir o acesso a dados das instâncias do Linux pelo protocolo Network File System (NFS). Depois que seu sistema de arquivos for criado, você poderá criar SVMs e volumes adicionais conforme necessário, incluindo uma SVM associada a um Active Directory para permitir o acesso de clientes Windows e macOS pelo protocolo Server Message Block (SMB).

Para obter informações sobre como usar a opção de criação padrão para criar um sistema de arquivos com uma configuração personalizada e para usar a API AWS CLI e, consulteComo criar sistemas de arquivos do FSx para ONTAP.

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 Create file system (Criar sistema de arquivos) para iniciar o assistente de criação de sistemas de arquivos.
3. Na página Selecionar tipo de sistema de arquivos, escolha Amazon FSx for NetApp ONTAP e, em seguida, escolha Avançar. A página Criar sistema de arquivos ONTAP é exibida.

4. Para Método de criação, escolha Criação rápida.
5. Na seção Configuração rápida, em Nome do sistema de arquivos: opcional, insira um nome para seu sistema de arquivos. É mais fácil encontrar e gerenciar seus sistemas de arquivos quando você define um nome para eles. Você pode usar no máximo 256 letras Unicode, espaço em branco e números, além destes caracteres especiais: + - (hífen) = . _ (sublinhado) : /
6. Em Tipo de implantação, escolha Multi-AZ ou Single-AZ.

   - Os sistemas de arquivos Multi-AZ replicam dados e oferecem suporte ao failover em várias zonas de disponibilidade dentro da mesma Região da AWS.
   - Os sistemas de arquivos single-AZ replicam os dados e oferecem failover automático em uma única zona de disponibilidade.

   Para ter mais informações, consulte Disponibilidade e durabilidade.
7. Para capacidade de armazenamento SSD, especifique a capacidade de armazenamento do seu sistema de arquivos, em gibibytes (GiB). Digite qualquer número inteiro no intervalo de 1.024 a 196.608. Se precisar de mais capacidade de armazenamento SSD, você pode usar a criação padrão. Para ter mais informações, consulte Criar um sistema de arquivos (console).

   Você pode aumentar a capacidade de armazenamento, conforme necessário, a qualquer momento após a criação do sistema de arquivos. Para ter mais informações, consulte Como gerenciar a capacidade de armazenamento.
8. Para a capacidade de transferência, o Amazon FSx fornece automaticamente uma capacidade de taxa de transferência recomendada com base no seu armazenamento SSD. Você também pode escolher a taxa de transferência do seu sistema de arquivos (até 4.096 MBps). Se precisar de mais capacidade de processamento, você pode usar a criação padrão.
9. Em Nuvem privada virtual (VPC), escolha a Amazon VPC que você deseja associar ao seu sistema de arquivos.
10. Em Eficiência do armazenamento, escolha Habilitado para ativar os recursos de eficiência do armazenamento do ONTAP (eliminação da duplicação, compressão e compactação) ou selecione Desabilitado para desativar esses recursos.
11. (Somente Multi-AZ) Intervalo de endereços IP do endpoint especifica o intervalo de endereços IP no qual são criados os endpoints para acessar o sistema de arquivos.

    Escolha uma opção de criação rápida para o intervalo de endereços IP do endpoint:

- Intervalo de endereços IP não alocados da VPC: escolha essa opção para que o Amazon FSx use os últimos 64 endereços IP do intervalo CIDR primário da VPC como intervalo de endereços IP do endpoint para o sistema de arquivos. Observe que esse intervalo será compartilhado entre vários sistemas de arquivos se você escolher essa opção várias vezes.

  > **Note**
  >
  > - Cada sistema de arquivos que você cria consome dois endereços IP desse intervalo, um para o cluster e outro para a primeira SVM. O primeiro e o último endereço IP também são reservados. Para cada SVM adicional, o sistema de arquivos consome outro endereço IP. Por exemplo, um sistema de arquivos que hospeda 10 SVMs usa 11 endereços IP. Sistemas de arquivos adicionais funcionam da mesma maneira. Eles consomem os dois endereços IP iniciais, mais um para cada SVM adicional. O número máximo de sistemas de arquivos usando o mesmo intervalo de endereços IP, cada um com uma única SVM, é 31.
  > - Essa opção ficará desabilitada se algum dos últimos 64 endereços IP no intervalo CIDR primário de uma VPC estiver sendo usado por uma sub-rede.

- Intervalo de endereços IP flutuante fora da VPC: escolha essa opção para que o Amazon FSx use um intervalo de endereços 198.19.x.0/24 que ainda não é usado por nenhum outro sistema de arquivos com a mesma VPC e as mesmas tabelas de rotas.

  Você também pode especificar seu próprio intervalo de endereços IP na opção Criação padrão.

12. Escolha Avançar e verifique a configuração do sistema de arquivos na página Criar sistema de arquivos ONTAP. Anote quais configurações do sistema de arquivos você pode modificar após a criação do sistema de arquivos.
13. Escolha Create file system (Criar sistema de arquivos).

A Criação rápida cria um sistema de arquivos com uma SVM (chamada `fsx`) e um volume (chamado `vol1`). O volume tem um caminho de junção `/vol1` e uma política de camadas do grupo de capacidade Automática (que vinculará automaticamente todos os dados que não foram acessados por 31 dias a um armazenamento de grupo de capacidade de menor custo). A política de snapshot padrão é atribuída ao volume padrão. Os dados do sistema de arquivos são criptografados em repouso usando sua AWS KMS chave gerenciada de serviço padrão.

Etapa 2: montar o sistema de arquivos usando uma instância do Linux do Amazon ECS

É possível montar o sistema de arquivos usando uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Esse procedimento usa uma instância que está executando o Amazon Linux 2.

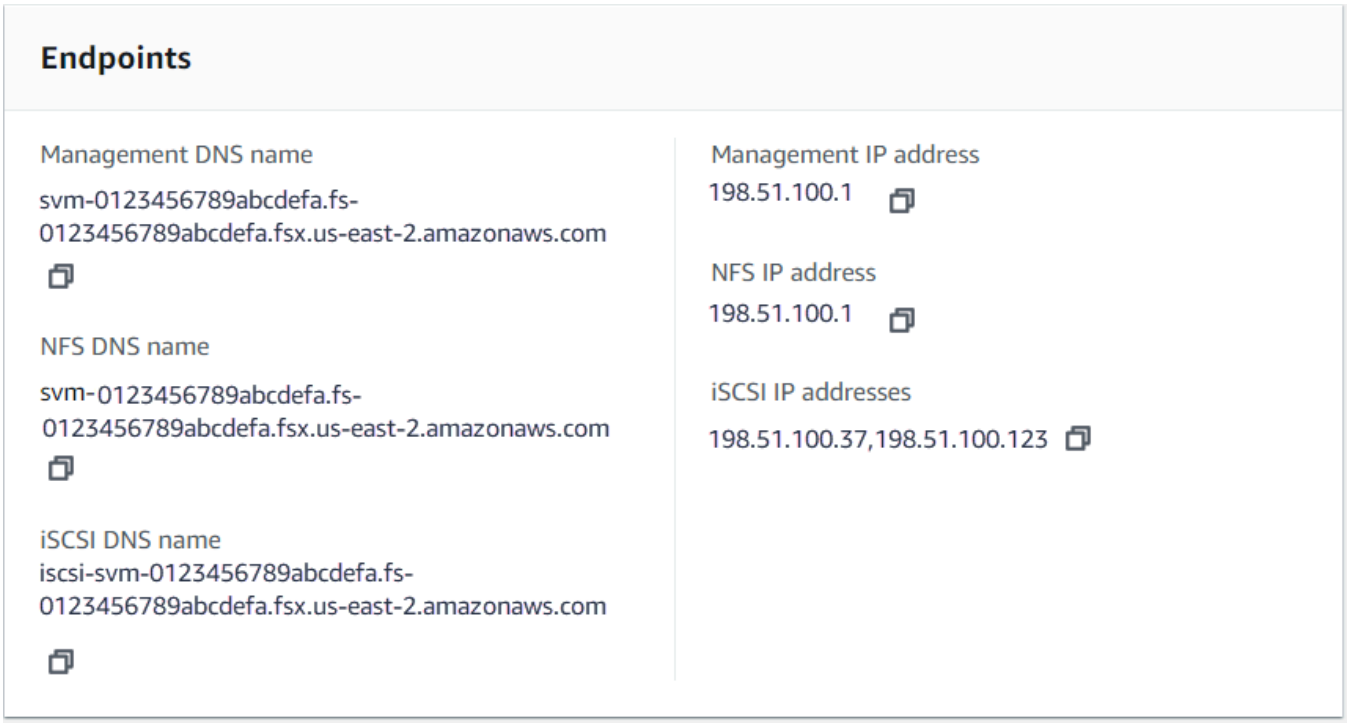
Montar o sistema de arquivos usando o Amazon EC2

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Crie ou selecione uma instância do Amazon EC2 executando o Amazon Linux 2 que esteja na mesma nuvem privada virtual (VPC) que o sistema de arquivos. Para obter mais informações sobre o lançamento de uma instância, consulte Etapa 1: Executar uma instância no Guia do usuário do Amazon EC2.
3. Conecte-se à sua instância do Linux do Amazon EC2. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
4. Abra um terminal na instância do Amazon EC2 usando Secure Shell (SSH) e faça login com as credenciais apropriadas.
5. Crie um diretório na instância do Amazon EC2 para uso como ponto de montagem do volume com o comando a seguir. No exemplo a seguir, substitua *mount-point* por suas próprias informações.

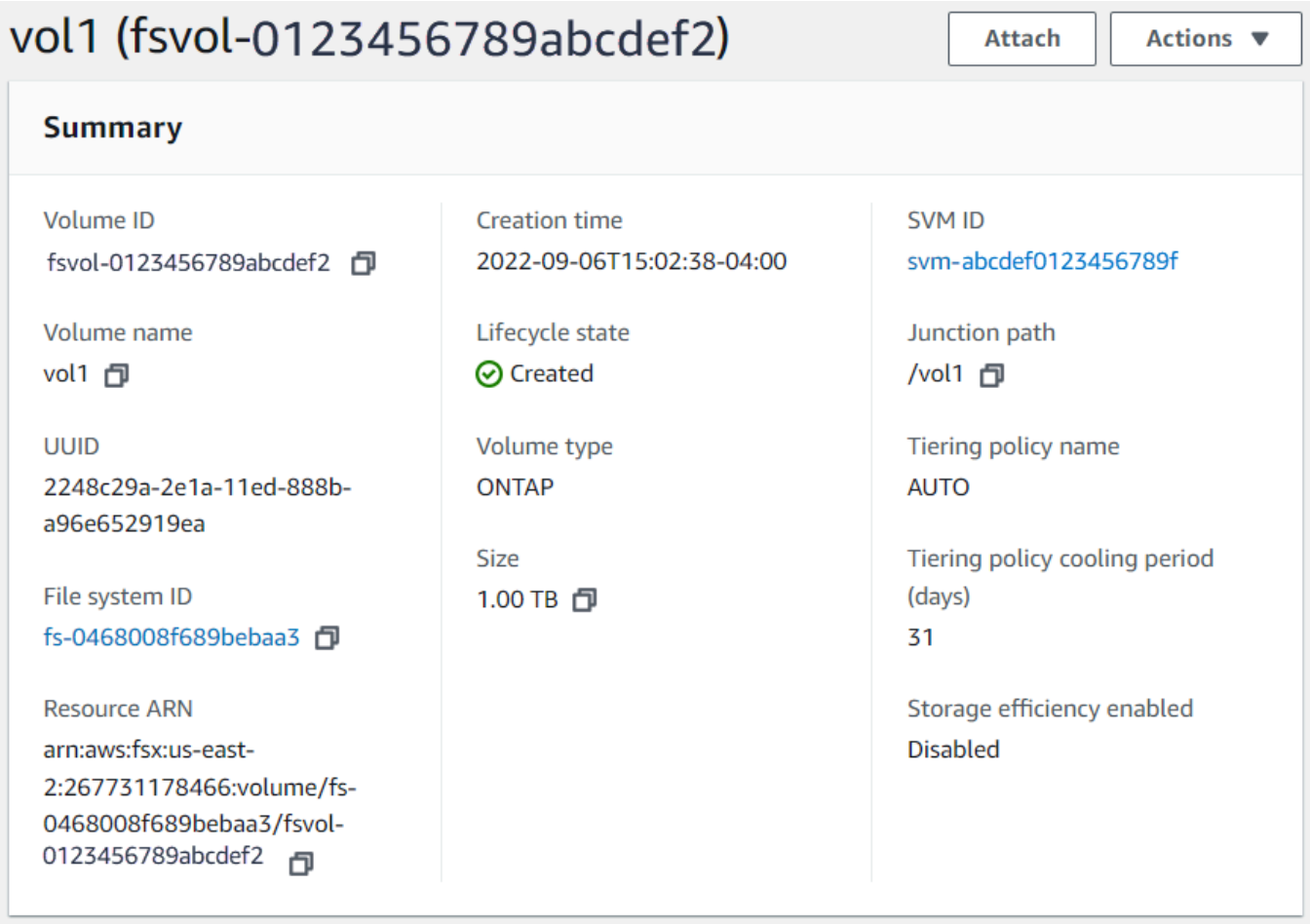
   ```
   $ sudo mkdir /mount-point
   ```

6. Monte seu sistema de arquivos Amazon FSx for NetApp ONTAP no diretório que você criou. Execute um comando `mount` semelhante ao seguinte exemplo: No exemplo a seguir, substitua os valores dos espaços reservados por suas próprias informações.

   - *nfs_version*: a versão do NFS que você está usando; o FSx para ONTAP oferece suporte às versões 3, 4.0, 4.1 e 4.2.
   - *nfs-dns-name*: o nome DNS do NFS da máquina virtual de armazenamento (SVM) na qual o volume que você está montando existe. Você pode encontrar o nome DNS do NFS no console do Amazon FSx escolhendo Máquinas virtuais de armazenamento e, em seguida, escolhendo a SVM na qual o volume que você está montando existe. O nome DNS do NFS é encontrado no painel Endpoints, mostrado na imagem a seguir.



- *`volume-junction-path`*: o caminho de junção do volume que você está montando. Você pode encontrar o caminho de junção de um volume no console do Amazon FSx no painel Resumo da página de detalhes do volume, mostrada na imagem a seguir.



- *`mount-point`*: o nome do diretório que você criou na instância do EC2 para o ponto de montagem do volume.

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

O comando a seguir usa exemplo de valores.

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

Se você tiver problemas com sua instância do Amazon EC2 (como o tempo limite de conexões), consulte Solucionar problemas de instâncias do EC2 no Guia do usuário do Amazon EC2.

Etapa 3: Limpar os recursos

Após concluir este exercício, siga estas etapas para limpar os recursos e proteger sua Conta da AWS.

Como limpar recursos

1. No console do Amazon EC2, encerre sua instância. Para obter mais informações, consulte Encerre sua instância no Guia do usuário do Amazon EC2.
2. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
3. No console do Amazon FSx, exclua todos os volumes do FSx para ONTAP que não sejam volumes raiz da SVM. Para ter mais informações, consulte Excluir um volume.
4. Exclua todos as SVMs do FSx para ONTAP. Para ter mais informações, consulte Excluir uma máquina virtual de armazenamento (SVM).
5. No console do Amazon FSx, exclua o sistema de arquivos. Quando você exclui um sistema de arquivos, todos os backups automáticos são excluídos automaticamente. No entanto, você ainda precisa excluir os backups criados manualmente. As seguintes etapas resumem o processo:

    a. No painel do console, escolha o nome do sistema de arquivos que você criou para este exercício.

    b. Para Ações, escolha Excluir sistema de arquivos.

    c. Na caixa de diálogo Excluir sistema de arquivos, digite o ID do sistema de arquivos que você deseja excluir, na caixa ID do sistema de arquivos.

    d. Escolha Excluir sistema de arquivos.

    e. Enquanto o Amazon FSx exclui o sistema de arquivos, seu status no painel muda para EXCLUINDO. Uma vez excluído, o sistema de arquivos não é exibido mais no painel. Todos os backups automáticos são excluídos com o sistema de arquivos.

    f. Agora você pode excluir todos os backups criados manualmente para o sistema de arquivos. No painel de navegação esquerdo, escolha Backups.

    g. No painel, escolha os backups que têm o mesmo ID de sistema de arquivos do sistema de arquivos que você excluiu e escolha Excluir backup. Certifique-se de manter o backup final, caso tenha criado um.

    h. A caixa de diálogo Excluir backups é aberta. Mantenha a caixa de seleção marcada para os IDs dos backups que você deseja excluir e escolha Excluir backups.

Seu sistema de arquivos do Amazon FSx e todos os backups automáticos relacionados agora estão excluídos, com todos os backups manuais que você optou por excluir.

Acesso a dados do

Você pode acessar seus sistemas de arquivos Amazon FSx usando uma variedade de clientes e métodos compatíveis, tanto no ambiente interno Nuvem AWS quanto no local.

Cada SVM tem quatro endpoints que são usados para acessar dados ou gerenciar o SVM usando a NetApp CLI do ONTAP ou a API REST:

- `Nfs`: para se conectar usando o protocolo Network File System (NFS)
- `Smb`: para se conectar usando o protocolo Service Message Block (SMB) (se a SVM estiver associada a um Active Directory ou se estiver usando um grupo de trabalho).
- `Iscsi`— Para conexão usando o protocolo Internet Small Computer Systems Interface (iSCSI) (somente para sistemas de arquivos escaláveis).
- `Management`— Para gerenciar SVMs usando a NetApp CLI ou API ONTAP, ou BlueXP NetApp

Tópicos

Clientes compatíveis

Os sistemas de arquivos do FSx para ONTAP oferecem suporte ao acesso a dados de uma ampla variedade de instâncias computacionais e sistemas operacionais. Isso é feito oferecendo suporte ao acesso com o protocolo Network File System (NFS) (v3, v4.0, v4.1 e v4.2), todas as versões do protocolo Server Message Block (SMB) (incluindo 2.0, 3.0 e 3.1.1) e o protocolo Internet Small Computer Systems Interface (iSCSI).

> **Important**
>
> 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.

As seguintes instâncias de AWS computação são suportadas para uso com FSx for ONTAP:

- Instâncias do Amazon Elastic Compute Cloud (Amazon EC2) executando Linux com suporte a NFS ou SMB, Microsoft Windows e macOS. Para ter mais informações, consulte Montagem de volumes.
- Contêineres do Docker do Amazon Elastic Container Service (Amazon ECS) em instâncias do Windows e do Linux do Amazon EC2. Para ter mais informações, consulte Como usar o Amazon Elastic Container Service com o FSx para ONTAP.
- Amazon Elastic Kubernetes Service — Para saber mais, consulte o driver CSI do Amazon FSx for NetApp ONTAP no Guia do usuário do Amazon EKS.
- Red Hat OpenShift Service on AWS (ROSA) — Para saber mais, consulte What is Red Hat OpenShift Service on AWS? no Guia do AWS Usuário do Red Hat OpenShift Service on.
- WorkSpaces Instâncias da Amazon. Para ter mais informações, consulte Usando a Amazon WorkSpaces com FSx for ONTAP.
- Instâncias da Amazon AppStream 2.0.
- AWS Lambda — Para obter mais informações, consulte a postagem do AWS blog Habilitando o acesso de pequenas e médias empresas para cargas de trabalho sem servidor com o Amazon FSx.
- Máquinas virtuais (VMs) em execução no VMware Cloud em ambientes. AWS Para obter mais informações, consulte Configurar o Amazon FSx for NetApp ONTAP como armazenamento externo e o Guia de implantação do VMware Cloud on with AWS Amazon FSx for ONTAP. NetApp

Depois de montados, os sistemas de arquivos do FSx para ONTAP aparecem como um diretório local ou letra da unidade em NFS e SMB, fornecendo armazenamento de arquivos em rede totalmente gerenciado e compartilhado que pode ser acessado simultaneamente por até milhares de clientes. Os LUNS de iSCSI são acessíveis como dispositivos de blocos quando montados em iSCSI.

Acessando dados de dentro AWS

Cada sistema de arquivos do Amazon FSx está associado a uma nuvem privada virtual (VPC). Você pode acessar o sistema de arquivos do FSx para ONTAP de qualquer lugar na VPC do sistema

de arquivos, independentemente da zona de disponibilidade. Você também pode acessar seu sistema de arquivos de outras VPCs que podem estar em AWS contas diferentes ou Regiões da AWS. Além dos requisitos descritos nas próximas seções para acessar os recursos do FSx para ONTAP, você também precisa garantir que o grupo de segurança da VPC do sistema de arquivos esteja configurado de modo que o tráfego de dados e gerenciamento possa fluir entre o sistema de arquivos e os clientes. Para obter mais informações sobre a configuração de grupos de segurança com as portas necessárias, consulte Grupos de segurança da Amazon VPC.

Tópicos

Acesso a dados de dentro da mesma VPC

Ao criar seu sistema de arquivos Amazon FSx for NetApp ONTAP, você seleciona a Amazon VPC na qual ele está localizado. Todas as SVMs e volumes associados ao sistema de arquivos Amazon FSx NetApp for ONTAP também estão localizados na mesma VPC. Ao montar um volume, se o sistema de arquivos e o cliente que monta o volume estiverem localizados na mesma VPC Conta da AWS, você poderá usar o nome DNS e a junção de volume ou o compartilhamento SMB do SVM, dependendo do cliente. Para ter mais informações, consulte Montagem de volumes.

Você pode obter uma performance ideal se o cliente e o volume estiverem localizados na mesma zona de disponibilidade da sub-rede do sistema de arquivos ou na sub-rede preferencial dos sistemas de arquivos multi-AZ. Para identificar a sub-rede ou sub-rede preferencial de um sistema de arquivos, no console do Amazon FSx, escolha Sistemas de arquivos e selecione o sistema de arquivos do ONTAP cujo volume você está montando. A sub-rede ou sub-rede preferencial (multi-AZ) é exibida no painel Sub-rede ou Sub-rede preferencial.

Acesso a dados de fora da VPC de implantação

Esta seção descreve como acessar um FSx para endpoints do sistema de arquivos ONTAP a partir de AWS locais fora da VPC de implantação do sistema de arquivos.

Acesso a endpoints NFS, SMB e de gerenciamento do ONTAP em sistemas de arquivos multi-AZ

Os endpoints de gerenciamento NFS, SMB e ONTAP nos sistemas de arquivos Amazon FSx NetApp for ONTAP Multi-AZ usam endereços de protocolo de internet (IP) flutuantes para que os

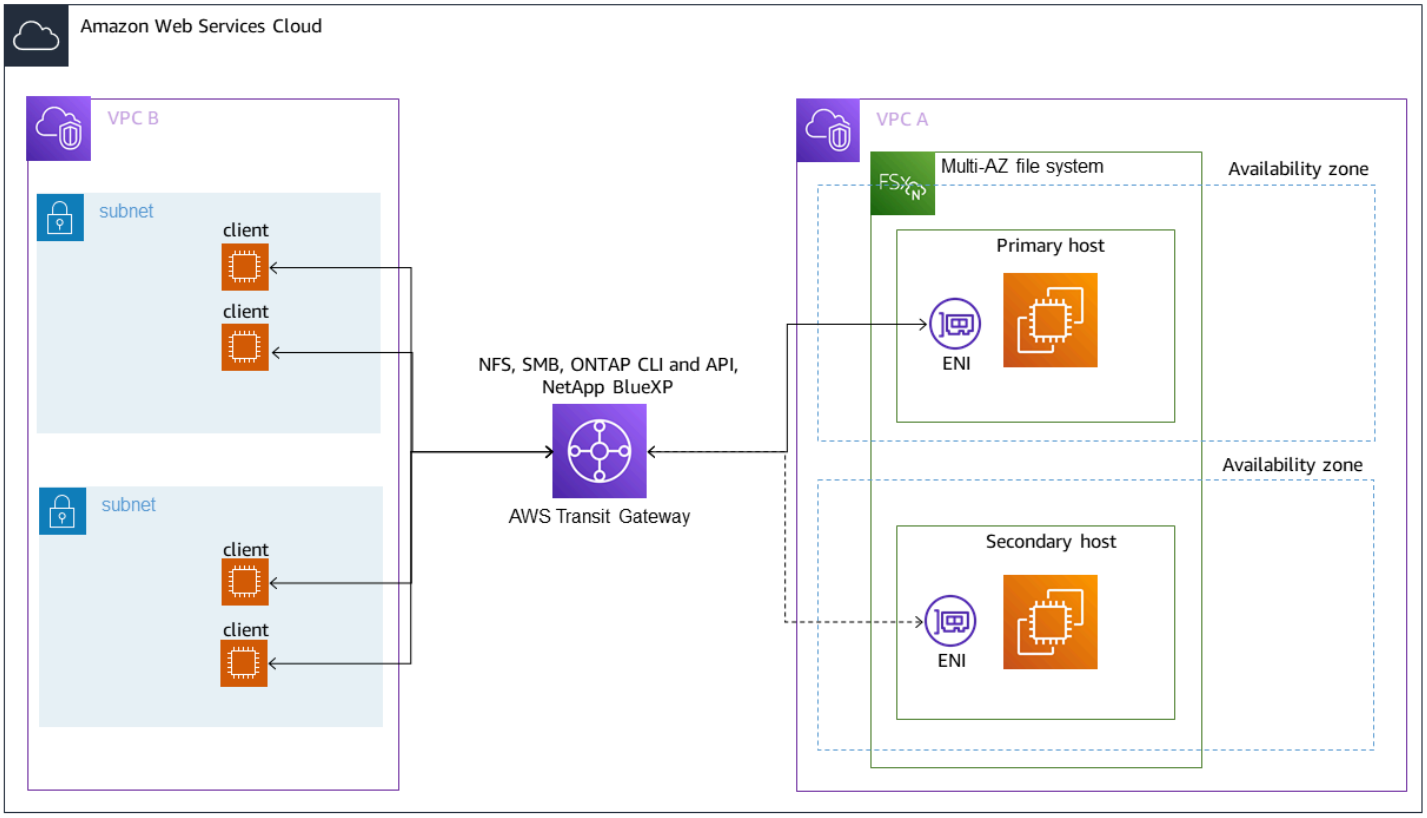
clientes conectados façam uma transição perfeita entre os servidores de arquivos preferenciais e os de espera durante um evento de failover. Para obter mais informações sobre failovers, consulte Processo de failover do FSx para ONTAP.

Esses endereços IP flutuantes são criados nas tabelas de rotas da VPC associadas ao sistema de arquivos, estando dentro do `EndpointIpAddressRange` do sistema de arquivos que você pode especificar durante a criação. O `EndpointIpAddressRange` usa os intervalos de endereços a seguir, dependendo de como um sistema de arquivos é criado.

- Os sistemas de arquivos multi-AZ criados com o console do Amazon FSx usam, por padrão, os últimos 64 endereços IP no intervalo CIDR principal da VPC para o `EndpointIpAddressRange` do sistema de arquivos.
- Os sistemas de arquivos Multi-AZ criados usando a API AWS CLI ou Amazon FSx usam um intervalo de endereços IP dentro `198.19.0.0/16` do bloco de endereços para o, por padrão`EndpointIpAddressRange`.

Somente AWS Transit Gateway oferece suporte ao roteamento para endereços IP flutuantes, também conhecido como emparelhamento transitivo. Peering de VPC, AWS Direct Connect, e AWS VPN não oferecem suporte ao peering transitivo. Portanto, é necessário usar o Transit Gateway para acessar essas interfaces de redes que estão fora da VPC do sistema de arquivos.

O diagrama a seguir ilustra o uso do Transit Gateway para NFS, SMB ou acesso de gerenciamento a um sistema de arquivos multi-AZ que está em uma VPC diferente da dos clientes que o estão acessando.



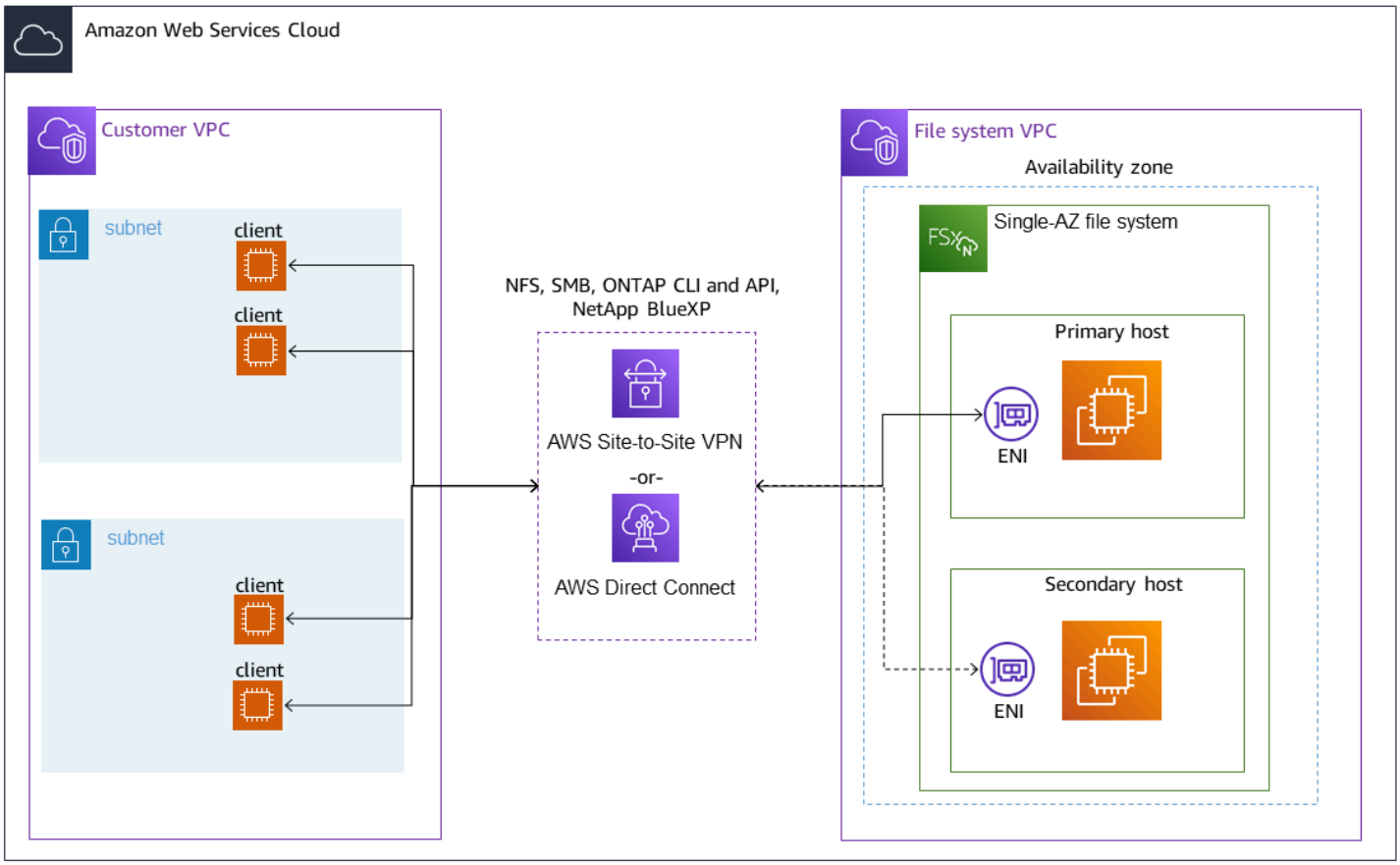
> **Note**
>
> Certifique-se de que todas as tabelas de rotas usadas estejam associadas ao seu sistema de arquivos multi-AZ. Isso ajuda a evitar a indisponibilidade durante um failover. Para obter informações sobre como associar suas tabelas de rotas da Amazon VPC ao sistema de arquivos, consulte Atualização de um sistema de arquivos.

Para obter informações sobre quando é necessário usar o Transit Gateway para acessar o sistema de arquivos do FSx para ONTAP, consulte Quando o Transit Gateway é necessário?.

Acesso a NFS, SMB ou a CLI e API do ONTAP para sistemas de arquivos single-AZ

Os endpoints usados para acessar os sistemas de arquivos single-AZ do FSx para ONTAP por meio de NFS ou SMB e para administrar sistemas de arquivos usando a CLI ou a API REST do ONTAP são endereços IP secundários na ENI do servidor de arquivos ativo. Os endereços IP secundários estão dentro do intervalo CIDR da VPC, então os clientes podem acessar dados e portas de gerenciamento usando o VPC Peering ou sem necessidade. AWS Direct Connect AWS VPN AWS Transit Gateway

O diagrama a seguir ilustra como usar AWS VPN ou AWS Direct Connect para NFS, SMB ou acesso de gerenciamento a um sistema de arquivos Single-AZ que está em uma VPC diferente da dos clientes que o acessam.



Quando o Transit Gateway é necessário?

Se o Transit Gateway é necessário ou não para os sistemas de arquivos multi-AZ depende do método usado para acessar os dados do sistema de arquivos. Os sistemas de arquivos single-AZ não exigem o Transit Gateway. A tabela a seguir descreve quando você precisará usar o AWS Transit Gateway para acessar sistemas de arquivos multi-AZ.

Acesso aos dados	Requer o Transit Gateway?
Acessando FSx por NFS, SMB ou API NetApp REST, CLI ou BlueXP do ONTAP	Somente se: • Acessar de uma rede emparelhada (on-premi ses, por exemplo) e

Acesso aos dados	Requer o Transit Gateway?
	• Você não está acessando o FSx por meio de uma instância NetApp FlexCache ou do Global File Cache
Acessar dados por meio de iSCSI	Não
Associar uma SVM a um Active Directory	Não
SnapMirror	Não
FlexCache Armazenamento em cache	Não
Global File Cache	Não

Como configurar o roteamento usando o AWS Transit Gateway

Se você tiver um sistema de arquivos Multi-AZ `EndpointIPAddressRange` que esteja fora do intervalo CIDR da sua VPC, precisará configurar um roteamento adicional para acessar seu sistema de arquivos AWS Transit Gateway a partir de redes locais ou com peering.

Important

Para acessar um sistema de arquivos multi-AZ usando um Transit Gateway, cada um dos anexos do Transit Gateway deve ser criado em uma sub-rede cuja tabela de rotas esteja associada ao sistema de arquivos.

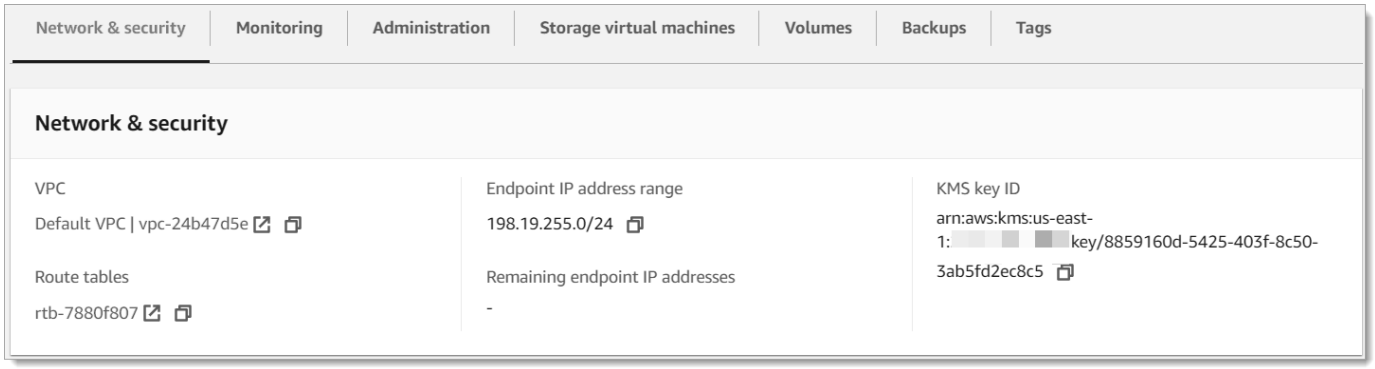
Note

Nenhuma configuração adicional do Transit Gateway é necessária para sistemas de arquivos single-AZ ou sistemas de arquivos multi-AZ com um `EndpointIPAddressRange` que esteja dentro da faixa de endereços IP da sua VPC.

Para configurar o roteamento usando AWS Transit Gateway

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

2. Escolha o sistema de arquivos do FSx para ONTAP para o qual você está configurando o acesso de uma rede emparelhada.
3. Em Rede e segurança, copie o Intervalo de endereços IP do endpoint.



4. Adicione uma rota ao Transit Gateway que roteie o tráfego destinado a esse intervalo de endereços IP para a VPC do sistema de arquivos. Para obter mais informações, consulte Trabalhar com gateways de trânsito em Gateways de trânsito da Amazon VPC.
5. Confirme se consegue acessar seu sistema de arquivos do FSx para ONTAP usando a rede emparelhada.

Para adicionar a tabela de rotas ao sistema de arquivos, consulte Atualização de um sistema de arquivos.

> **Note**
>
> Os registros DNS dos endpoints de gerenciamento, NFS e SMB só podem ser resolvidos na mesma VPC do sistema de arquivos. Para montar um volume ou conectar-se a uma porta de gerenciamento de outra rede, é necessário usar o endereço IP do endpoint. Esses endereços IP não mudam com o tempo.

Acessar endpoints iSCSI ou entre clusters fora da VPC de implantação

Você pode usar o emparelhamento de VPC ou AWS Transit Gateway acessar os endpoints iSCSI ou entre clusters do seu sistema de arquivos de fora da VPC de implantação do sistema de arquivos. Use o emparelhamento da VPC para rotear o tráfego iSCSI e entre clusters entre as VPCs. Conexão de emparelhamento da VPC é uma conexão de redes entre duas VPCs, usada para rotear o tráfego entre elas usando endereços IPv4 privados. Você pode usar o emparelhamento de VPC para conectar VPCs dentro da mesma Região da AWS ou entre diferentes. Regiões da AWS Para obter

mais informações sobre o emparelhamento da VPC, consulte O que é emparelhamento de VPC? no Guia de emparelhamento da Amazon VPC.

Acesso a dados de sistemas on-premises

Você pode acessar os sistemas de arquivos do FSx para ONTAP de on-premises usando o AWS VPN e o AWS Direct Connect. Diretrizes de casos de uso mais específicas estão disponíveis nas próximas seções. Além dos requisitos listados abaixo para acessar diferentes recursos do FSx para ONTAP on-premises, você também precisa garantir que o grupo de segurança da VPC do seu sistema de arquivos permita que os dados fluam entre o sistema de arquivos e os clientes. Para obter uma lista das portas necessárias, consulte Amazon VPC security groups.

Acessar endpoints NFS, SMB ou da CLI ou API REST do ONTAP de sistemas on-premises

Esta seção descreve como acessar as portas NFS, SMB e de gerenciamento do ONTAP em sistemas de arquivos do FSx para ONTAP usando redes on-premises.

Acesso a sistemas de arquivos multi-AZ

O Amazon FSx exige que você use AWS Transit Gateway ou configure o NetApp Global File Cache remoto ou acesse sistemas de arquivos Multi-AZ NetApp FlexCache a partir de uma rede local. Para oferecer suporte ao failover entre AZs para sistemas de arquivos multi-AZ, o Amazon FSx usa endereços IP flutuantes para as interfaces usadas em endpoints NFS, SMB e de gerenciamento do ONTAP. Como os endpoints NFS, SMB e de gerenciamento usam IPs flutuantes, você deve usar AWS Transit Gatewayem conjunto com AWS Direct Connect ou AWS VPN para acessar essas interfaces a partir de uma rede local. Os endereços IP flutuantes usados nessas interfaces estão dentro do `EndpointIpAddressRange` que você especifica ao criar o sistema de arquivos multi-AZ. Por padrão, se você criar o sistema de arquivos no console do Amazon FSx, o Amazon FSx escolhe os últimos 64 endereços IP do intervalo CIDR principal da VPC para usar como o intervalo de endereços IP do endpoint para o sistema de arquivos. Se você criar seu sistema de arquivos a partir da API AWS CLI ou do Amazon FSx, por padrão, o Amazon FSx escolherá um intervalo de endereços IP dentro do intervalo de endereços IP. `198.19.0.0/16` Os endereços IP flutuantes são usados para permitir uma transição sem interrupções dos clientes para o sistema de arquivos em espera, caso seja necessário um failover. Para ter mais informações, consulte Processo de failover do FSx para ONTAP.

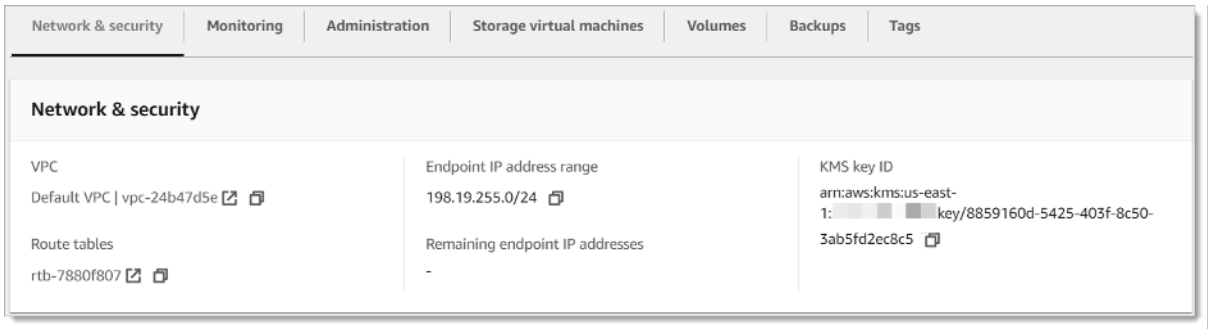
> **Important**
>
> Para acessar um sistema de arquivos multi-AZ usando um Transit Gateway, cada um dos anexos do Transit Gateway deve ser criado em uma sub-rede cuja tabela de rotas esteja associada ao sistema de arquivos.

AWS Transit Gateway Para configurar o acesso de fora da sua VPC

Se você tiver um sistema de arquivos Multi-AZ `EndpointIPAddressRange` que esteja fora do intervalo CIDR da sua VPC, precisará configurar um roteamento adicional para acessar seu sistema de arquivos AWS Transit Gateway a partir de redes locais ou com peering.

> **Note**
>
> Nenhuma configuração adicional do Transit Gateway é necessária para sistemas de arquivos single-AZ ou sistemas de arquivos multi-AZ com um `EndpointIPAddressRange` que esteja dentro da faixa de endereços IP da sua VPC.

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha o sistema de arquivos do FSx para ONTAP para o qual você está configurando o acesso de uma rede emparelhada.
3. Em Rede e segurança, copie o Intervalo de endereços IP do endpoint.



4. Adicione uma rota ao Transit Gateway que roteie o tráfego destinado a esse intervalo de endereços IP para a VPC do seu sistema de arquivos. Para obter mais informações, consulte Trabalhar com gateways de trânsito no Guia do usuário do Amazon VPC Transit Gateway.
5. Confirme se consegue acessar seu sistema de arquivos do FSx para ONTAP usando a rede emparelhada.

> **Important**
>
> Para acessar um sistema de arquivos multi-AZ usando um Transit Gateway, cada um dos anexos do Transit Gateway deve ser criado em uma sub-rede cuja tabela de rotas esteja associada ao sistema de arquivos.

Para adicionar uma tabela de rotas ao sistema de arquivos, consulte Atualização de um sistema de arquivos.

Acesso a sistemas de arquivos single-AZ

O requisito de uso AWS Transit Gateway para acessar dados de uma rede local não existe para sistemas de arquivos Single-AZ. Os sistemas de arquivos single-AZ são implantados em uma única sub-rede, e um endereço IP flutuante não é necessário para fornecer failover entre os nós. Em vez disso, os endereços IP que você acessa nos sistemas de arquivos single-AZ são implementados como endereços IP secundários dentro do intervalo CIDR da VPC do sistema de arquivos, permitindo que você acesse seus dados de outra rede sem precisar do AWS Transit Gateway.

Acesso a endpoints entre clusters de sistemas on-premises

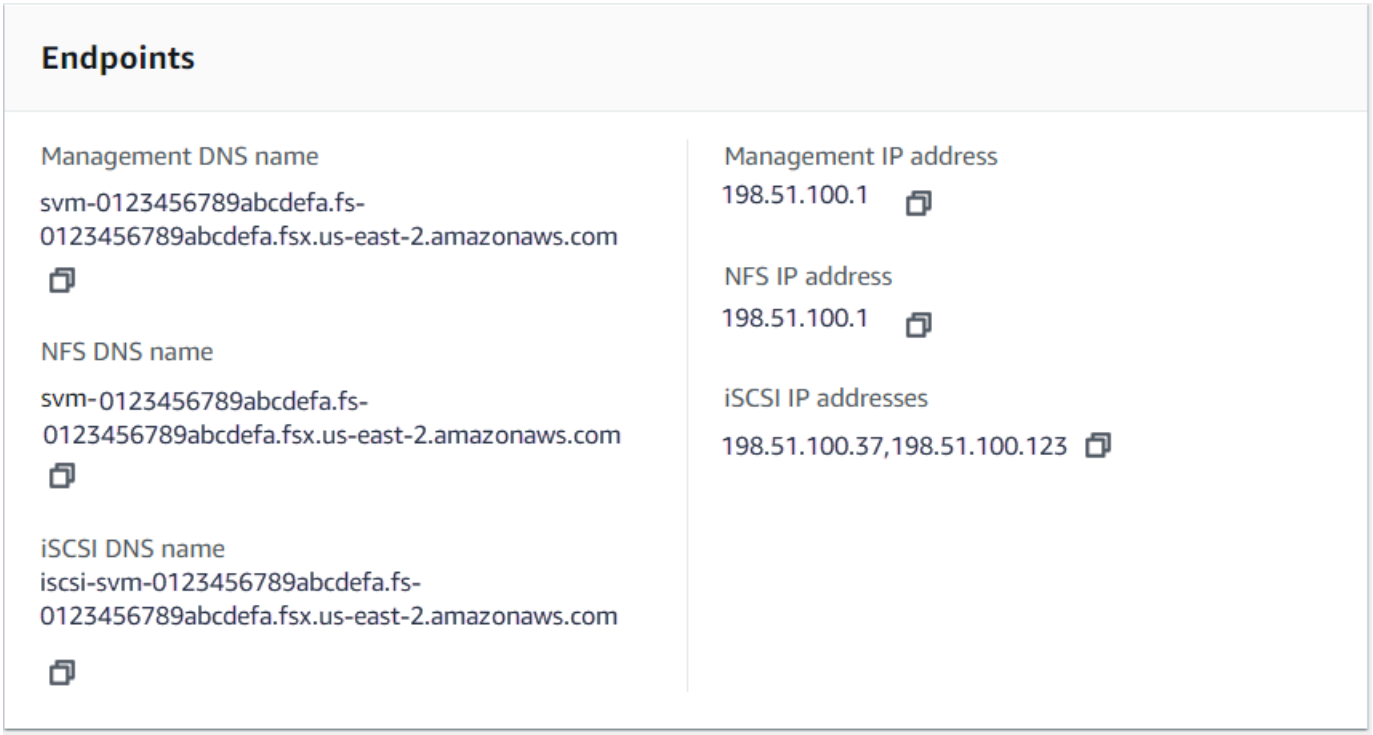
Os endpoints entre clusters do FSx for ONTAP são dedicados ao tráfego de replicação entre os sistemas de arquivos NetApp ONTAP, inclusive entre implantações locais e o FSx for ONTAP. NetApp O tráfego de replicação inclui SnapMirror FlexCache, e FlexClone relacionamentos entre máquinas virtuais de armazenamento (SVMs) e volumes em diferentes sistemas de arquivos e o NetApp Global File Cache. Os endpoints entre clusters também são usados para o tráfego do Active Directory.

Como os endpoints entre clusters de um sistema de arquivos usam endereços IP que estão dentro do intervalo CIDR da VPC fornecido ao criar o sistema de arquivos do FSx para ONTAP, você não precisa usar um Transit Gateway para rotear o tráfego entre clusters entre o sistema on-premises e a Nuvem AWS. No entanto, os clientes locais ainda precisam usar AWS VPN ou AWS Direct Connect estabelecer uma conexão segura com sua VPC.

Montagem de volumes

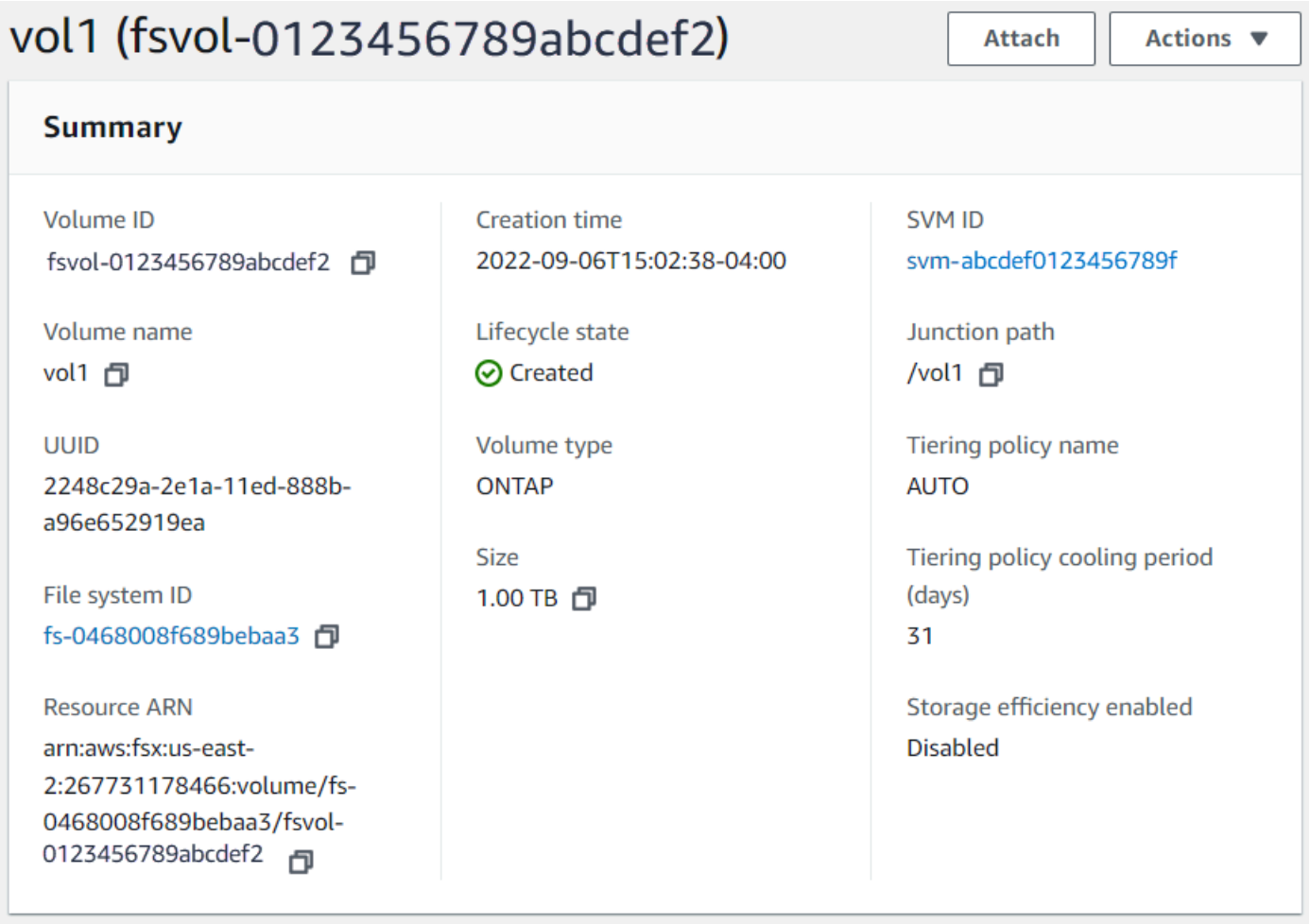
Acesse os dados no FSx para ONTAP montando um volume no seu cliente. Os comandos nesta seção usam o nome DNS ou o endereço IP da SVM na qual o volume é criado para montar ou

anexar um volume. Você encontra o nome DNS e o endereço IP da SVM no console do Amazon FSx, escolhendo ONTAP > Máquinas virtuais de armazenamento, ou na guia Máquina virtual de armazenamento, na página Detalhes do sistema de arquivos do sistema de arquivos, mostrada na imagem a seguir.



Ou você pode encontrá-los na resposta da operação da DescribeStorageVirtualMachinesAPI.

Você pode encontrar o caminho de junção de um volume no console do Amazon FSx no painel Resumo da página de detalhes do volume, mostrada na imagem a seguir.



Tópicos

- Montagem em clientes Linux
- Montagem em clientes Microsoft Windows
- Montagem em clientes macOS

Montagem em clientes Linux

Recomendamos que os volumes da SVM aos quais você está anexando clientes Linux tenham uma configuração de estilo de segurança de `UNIX` ou `mixed`. Para ter mais informações, consulte Como gerenciar volumes do FSx para ONTAP.

> **Note**
>
> Por padrão, as montagens NFS do FSx para ONTAP são `hard`. Para garantir um failover tranquilo caso ocorra, recomendamos que use a opção de montagem `hard` padrão.

Montar um volume do ONTAP em um cliente Linux

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Crie ou selecione uma instância do Amazon EC2 executando o Amazon Linux 2 na mesma VPC do sistema de arquivos.

   Para obter mais informações sobre o lançamento de uma instância Linux do EC2, consulte Etapa 1: Iniciar uma instância no Guia do usuário do Amazon EC2.
3. Conecte-se à sua instância do Linux do Amazon EC2. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
4. Abra um terminal na instância do EC2 usando o secure shell (SSH) e faça login com as credenciais apropriadas.
5. Crie um diretório na instância do EC2 para montar o volume da SVM da seguinte forma:

   ```
   sudo mkdir /fsx
   ```
6. Monte o volume no diretório que acabou de criar usando o seguinte comando:

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   O exemplo a seguir usa valores de amostra.

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   Você também pode usar o endereço IP da SVM em vez do nome DNS. Recomendamos usar o nome DNS para montar clientes em sistemas de arquivos escaláveis, pois isso ajuda a garantir que seus clientes sejam balanceados entre os pares de alta disponibilidade (HA) do sistema de arquivos.

   ```
   sudo mount -t nfs 198.51.100.1:/vol1 /fsx
   ```

> **Note**
>
> Para sistemas de arquivos escaláveis, o protocolo NFS paralelo (pNFS) é habilitado por padrão e é usado por padrão para qualquer cliente que monte volumes com NFS v4.1 ou superior.

Como usar /etc/fstab para montar automaticamente na reinicialização da instância

Para remontar automaticamente o volume do FSx para ONTAP quando uma instância de Linux do Amazon EC2 for reinicializada, use o arquivo `/etc/fstab`. O arquivo `/etc/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 em `/etc/fstab`.

> **Note**
>
> Os sistemas de arquivos do FSx para ONTAP não oferecem suporte à montagem automática usando `/etc/fstab` em instâncias de Mac do Amazon EC2.

> **Note**
>
> Antes de atualizar o arquivo `/etc/fstab` da instância do EC2, verifique se já criou o sistema de arquivos do FSx para ONTAP. Para ter mais informações, consulte Como criar sistemas de arquivos do FSx para ONTAP.

Como atualizar o arquivo /etc/fstab na instância do EC2

1. Conecte-se à sua instância do EC2:
   - Para se conectar à instância em um computador com macOS ou Linux, especifique o arquivo .pem para o comando SSH. Para fazer isso, use a opção `-i` e o caminho para sua chave privada.
   - Para se conectar à sua instância a partir de um computador executando o Windows, você pode usar o PuTTY MindTerm ou o PuTTY. Para usar o PuTTY, instale-o e converta o arquivo .pem para um arquivo .ppk.

Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do Amazon EC2:

- Conectar à sua instância do Linux usando SSH
- Conectar à instância do Linux a partir do Windows usando PuTTY

2. Crie um diretório local que será usado para montar o volume da SVM.

```
sudo mkdir /fsx
```

3. Abra o arquivo `/etc/fstab` com seu editor de preferência.
4. Adicione a linha a seguir ao arquivo `/etc/fstab`. Insira um caractere de tabulação entre cada parâmetro. Deve aparecer como uma linha sem quebras de linha.

```
svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
```

Também é possível usar o endereço IP da SVM do volume. Os três últimos parâmetros indicam opções de NFS (que definimos como padrão), despejo do sistema de arquivos e verificação do sistema de arquivos (normalmente não são usados, então os definimos como 0).

5. Salve a alteração no arquivo.
6. Agora, monte o compartilhamento de arquivos usando o comando a seguir. Na próxima vez em que o sistema for iniciado, a pasta será montada automaticamente.

```
sudo mount /fsx
sudo mount svm-dns-name:volume-junction-path
```

Sua instância do EC2 já está configurada para montar o volume do ONTAP sempre que ele for reiniciado.

Montagem em clientes Microsoft Windows

Esta seção descreve como acessar dados no sistema de arquivos do FSx para ONTAP com clientes executando o sistema operacional Microsoft Windows. Analise os requisitos a seguir, independentemente do tipo de cliente que está usando.

Este procedimento pressupõe que o cliente e o sistema de arquivos estejam localizados na mesma VPC e Conta da AWS. Se o cliente estiver localizado no local ou em uma VPC diferente, ou Conta da AWS Região da AWS, esse procedimento também pressupõe que você tenha configurado ou uma

conexão de rede dedicada usando AWS Transit Gateway AWS Direct Connect ou usando um túnel privado e seguro. AWS Virtual Private Network Para ter mais informações, consulte Acesso a dados de fora da VPC de implantação.

Recomendamos que você anexe volumes aos clientes Windows usando o protocolo SMB.

Pré-requisitos

Para acessar um volume de armazenamento do ONTAP usando um cliente Microsoft Windows, é necessário atender aos pré-requisitos a seguir.

- A SVM do volume que você está anexando deve estar associada ao Active Directory da sua organização ou você deve estar usando um grupo de trabalho. Para obter mais informações sobre como associar a SVM a um Active Directory, consulte Como gerenciar máquinas virtuais de armazenamento do FSx para ONTAP. Para obter mais informações sobre o uso de grupos de trabalho, consulte Configurar um servidor SMB em uma visão geral do grupo de trabalho no NetApp Centro de Documentação.
- O volume que você está anexando tem uma configuração de estilo de segurança de `NTFS` ou `mixed`. Para ter mais informações, consulte Como gerenciar volumes do FSx para ONTAP.

Anexar um volume do ONTAP em um cliente Windows usando o Active Directory e SMB

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Crie ou selecione uma instância do Amazon EC2 executando um Microsoft Windows que esteja na mesma VPC do sistema de arquivos e associada ao mesmo Microsoft Active Directory da SVM do volume.

   Para obter mais informações sobre como iniciar uma instância, consulte Etapa 1: Executar uma instância no Guia do usuário do Amazon EC2.

   Para obter mais informações sobre como associar uma SVM a um Active Directory, consulte Como gerenciar máquinas virtuais de armazenamento do FSx para ONTAP.
3. Conecte-se à instância do Windows do Amazon EC2. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
4. Abra um prompt de comando.
5. Execute o seguinte comando . Substitua o seguinte:

   - Substitua `Z:` por qualquer letra de unidade disponível.

- Substitua `DNS_NAME` pelo nome DNS ou pelo endereço IP do endpoint SMB da SVM do volume.
- `SHARE_NAME`Substitua pelo nome de um compartilhamento SMB. `C$`é o compartilhamento SMB padrão na raiz do namespace do SVM, mas você não deve montá-lo, pois isso expõe o armazenamento ao volume raiz e pode causar interrupções na segurança e no serviço. Você deve fornecer um nome de compartilhamento SMB para montar em vez de`C$`. Para obter mais informações sobre como criar compartilhamentos SMB, consulte Como gerenciar compartilhamentos de SMB.

```
net use Z: \\DNS_NAME\SHARE_NAME
```

O exemplo a seguir usa valores de amostra.

```
net use Z: \\corp.example.com\group_share
```

Você também pode usar o endereço IP da SVM em vez do nome DNS. Recomendamos usar o nome DNS para montar clientes em sistemas de arquivos escaláveis, pois isso ajuda a garantir que seus clientes sejam balanceados entre os pares de alta disponibilidade (HA) do sistema de arquivos.

```
net use Z: \\198.51.100.5\group_share
```

Montagem em clientes macOS

Esta seção descreve como acessar dados no sistema de arquivos do FSx para ONTAP com clientes executando o sistema operacional macOS. Analise os requisitos a seguir, independentemente do tipo de cliente que está usando.

Este procedimento pressupõe que o cliente e o sistema de arquivos estejam localizados na mesma VPC e Conta da AWS. Se o cliente estiver localizado no local ou em uma VPC diferente Região da AWS, Conta da AWS ou se você tiver configurado uma conexão de rede dedicada usando AWS Transit Gateway AWS Direct Connect ou usando um túnel privado e seguro. AWS Virtual Private Network Para ter mais informações, consulte Acesso a dados de fora da VPC de implantação.

Recomendamos que você anexe volumes aos seus clientes Mac usando o protocolo SMB.

Montar um volume do ONTAP em um cliente macOS usando SMB

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Crie ou selecione uma instância de Mac do Amazon EC2 executando o macOS que esteja na mesma VPC do sistema de arquivos.

   Para obter mais informações sobre como iniciar uma instância, consulte Etapa 1: Executar uma instância no Guia do usuário do Amazon EC2.
3. Conecte-se à instância de Mac do Amazon EC2. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
4. Abra um terminal na instância do EC2 usando o secure shell (SSH) e faça login com as credenciais apropriadas.
5. Crie um diretório na instância do EC2 para montar o volume da seguinte maneira:

   ```
   sudo mkdir /fsx
   ```
6. Monte o volume usando o comando a seguir.

   ```
   sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
   ```

   O exemplo a seguir usa valores de amostra.

   ```
   sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-
   east-1.amazonaws.com:/C$ /fsx
   ```

   Você também pode usar o endereço IP da SVM em vez do nome DNS. Recomendamos usar o nome DNS para montar clientes em sistemas de arquivos escaláveis, pois isso ajuda a garantir que seus clientes sejam balanceados entre os pares de alta disponibilidade (HA) do sistema de arquivos.

   ```
   sudo mount -t smbfs 198.51.100.10:/C$ /fsx
   ```

   `C$` é o compartilhamento SMB padrão que você pode montar para ver a raiz do namespace da SVM. Se você criou algum compartilhamento Server Message Block (SMB) na SVM, forneça os nomes dos compartilhamentos SMB em vez de `C$`. Para obter mais informações sobre como criar compartilhamentos SMB, consulte Como gerenciar compartilhamentos de SMB.

Montar um volume do ONTAP em um cliente macOS usando NFS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Crie ou selecione uma instância do Amazon EC2 executando o Amazon Linux 2 na mesma VPC do sistema de arquivos.

   Para obter mais informações sobre o lançamento de uma instância Linux do EC2, consulte Etapa 1: Iniciar uma instância no Guia do usuário do Amazon EC2.
3. Conecte-se à sua instância do Linux do Amazon EC2. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
4. Monte o volume do FSx para ONTAP na instância de Linux do EC2 usando um script de dados do usuário durante a execução da instância ou executando os seguintes comandos:

   ```
   sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-point
   ```

   O exemplo a seguir usa valores de amostra.

   ```
   sudo mount -t nfs -o nfsvers=4.1
    svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

   Você também pode usar o endereço IP da SVM em vez do nome DNS. Recomendamos usar o nome DNS para montar clientes em sistemas de arquivos escaláveis, pois isso ajuda a garantir que seus clientes estejam equilibrados entre os pares de HA do sistema de arquivos.

   ```
   sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
   ```
5. Monte o volume no diretório que acabou de criar usando o comando a seguir.

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   O exemplo a seguir usa valores de amostra.

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

Você também pode usar o endereço IP da SVM em vez do nome DNS. Recomendamos usar o nome DNS para montar clientes em sistemas de arquivos escaláveis, pois isso ajuda a garantir que seus clientes sejam balanceados entre os pares de alta disponibilidade (HA) do sistema de arquivos.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

Montar LUNs de iSCSI

O Amazon FSx for NetApp ONTAP fornece suporte de armazenamento em bloco compartilhado por meio do protocolo iSCSI (Internet Small Computer Systems Interface). É possível habilitar o armazenamento iSCSI provisionando LUNs (número de unidade lógica) e mapeando-os para grupos de iniciadores (igroups), expondo o armazenamento em blocos aos hosts do Linux e do Windows.

> **Note**
>
> O protocolo iSCSI não é suportado pelos sistemas de arquivos escaláveis FSx for ONTAP, que são sistemas de arquivos com mais de um par de servidores de arquivos de alta disponibilidade (HA).

Tópicos

Montar LUNs de iSCSI em um cliente Linux

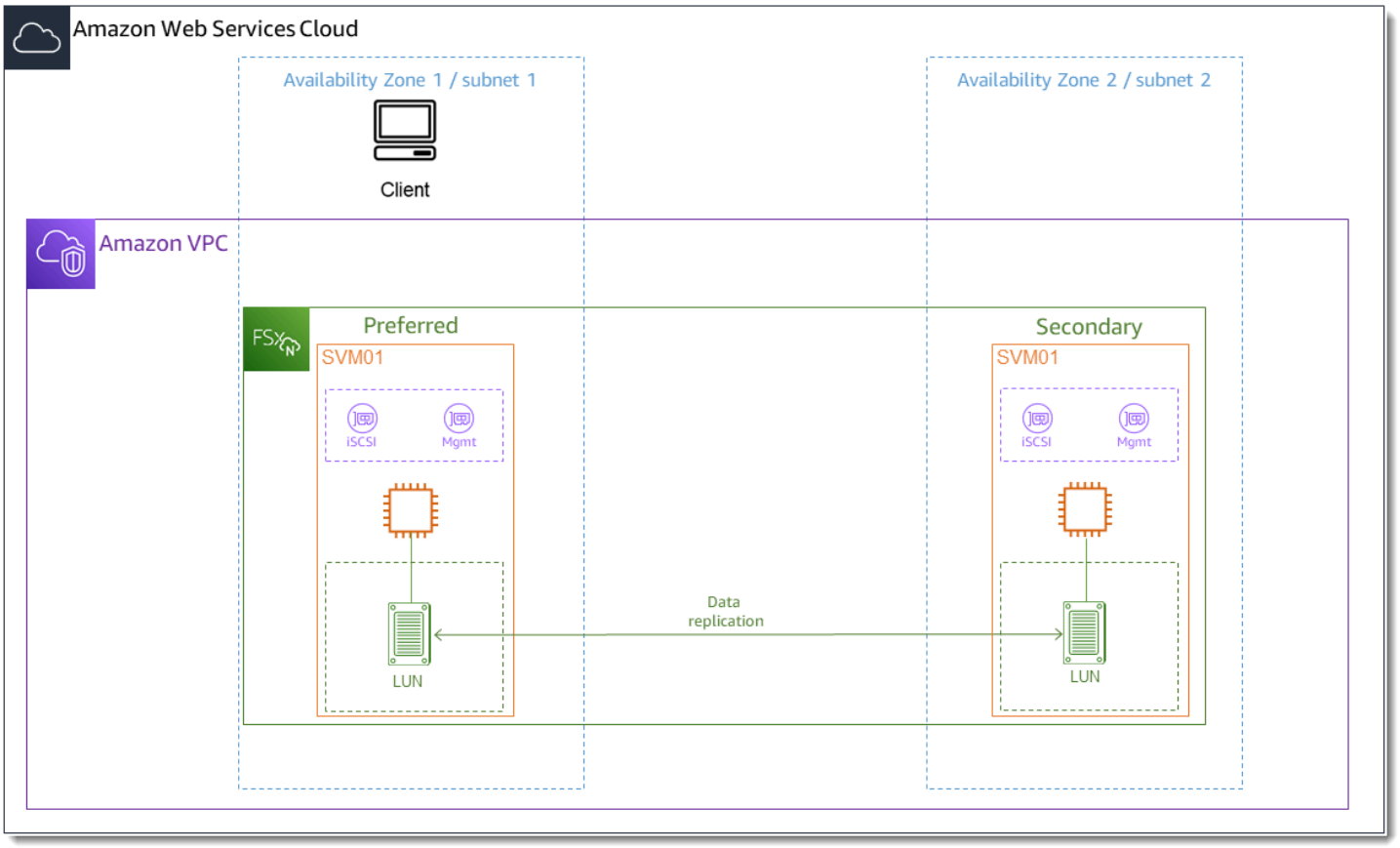
Os exemplos apresentados nestes procedimentos usam a seguinte configuração:

- O LUN do iSCSI que está sendo montado no host do Linux já foi criado. Para ter mais informações, consulte Como criar um LUN de iSCSI.
- O host do Linux que está montando o LUN do iSCSI é uma instância do Amazon EC2 executando a imagem de máquina da Amazon (AMI) do Amazon Linux 2. Ele tem grupos de segurança de VPC configurados para permitir tráfego de entrada e saída, conforme descrito em Controle de acesso ao sistema de arquivos com a Amazon VPC.

- O host do Linux e o sistema de arquivos do FSx para ONTAP estão localizados na mesma VPC e Conta da AWS. Se o host estiver localizado em outra VPC, você poderá usar o emparelhamento de VPC ou conceder a outras VPCs acesso AWS Transit Gateway aos endpoints iSCSI do volume. Para ter mais informações, consulte Acesso a dados de fora da VPC de implantação.

  Se estiver usando uma instância do EC2 executando uma AMI do Linux diferente, alguns dos utilitários instalados no host podem estar pré-instalados e você pode usar comandos diferentes para instalar os pacotes necessários. Além de instalar pacotes, os comandos usados nesta seção são válidos para outras AMIs do Linux do EC2.

  Recomendamos que a instância do EC2 esteja na mesma zona de disponibilidade da sub-rede preferencial do seu sistema de arquivos, conforme mostrado no gráfico a seguir.



Tópicos

- Instalar e configurar iSCSI no cliente Linux
- Configurar o iSCSI no sistema de arquivos do FSx para ONTAP
- Montar um LUN de iSCSI no cliente Linux

Instalar e configurar iSCSI no cliente Linux

Instalar o cliente iSCSI

1. Confirme se `iscsi-initiator-utils` e `device-mapper-multipath` estão instalados no seu dispositivo Linux. Conecte-se à instância do Linux usando um cliente SSH. Para obter mais informações, consulte Connect to your Linux instance using SSH.
2. Instale `multipath` e o cliente iSCSI usando o comando a seguir. A instalação de `multipath` é necessária se quiser fazer o failover automático entre os servidores de arquivos.

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. Para facilitar uma resposta mais rápida ao fazer o failover automático entre servidores de arquivos ao usar `multipath`, defina o valor do tempo limite de substituição no arquivo `/etc/iscsi/iscsid.conf` como um valor de `5` em vez de usar o valor padrão de `120`.

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/
node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/
iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. Inicie o serviço iSCSI.

```
~$ sudo service iscsid start
```

   Observe que, dependendo da sua versão do Linux, talvez precise usar este comando:

```
~$ sudo systemctl start iscsid
```

5. Confirme se o serviço está em execução usando o comando a seguir.

```
~$ sudo systemctl status iscsid.service
```

   O sistema responde com a seguinte saída:

```
iscsid.service - Open-iSCSI
    Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor
 preset: disabled)
    Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
    Docs: man:iscsid(8)
    man:iscsiadm(8)
```

```
    Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
    CGroup: /system.slice/iscsid.service
    ##14659 /usr/sbin/iscsid
    ##14660 /usr/sbin/iscsid
```

Configurar o iSCSI no seu cliente Linux

1. Para permitir que seus clientes façam o failover automático entre os servidores de arquivos, é necessário configurar múltiplos caminhos. Use o seguinte comando:

   ```
   ~$ sudo mpathconf --enable --with_multipathd y
   ```

2. Determine o nome do iniciador do host do Linux usando o comando a seguir. A localização do nome do iniciador depende do utilitário do iSCSI. Se estiver usando `iscsi-initiator-utils`, o nome do iniciador está localizado no arquivo `/etc/iscsi/initiatorname.iscsi`.

   ```
   ~$ sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   O sistema responde com o nome do iniciador.

   ```
   InitiatorName=iqn.1994-05.com.redhat:abcdef12345
   ```

Configurar o iSCSI no sistema de arquivos do FSx para ONTAP

1. Conecte-se à CLI do NetApp ONTAP no sistema de arquivos FSx for ONTAP no qual você criou o LUN iSCSI usando o comando a seguir. Para ter mais informações, consulte Usar a CLI do NetApp ONTAP.

   ```
   ~$ ssh fsxadmin@your_management_endpoint_ip
   ```

2. Crie o grupo iniciador (`igroup`) usando o comando NetApp ONTAP CLI. lun igroup create Um grupo de iniciadores mapeia para LUNs de iSCSI e controla quais iniciadores (clientes) têm acesso aos LUNs. Substitua `host_initiator_name` pelo nome do iniciador do host do Linux que você recuperou no procedimento anterior.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype linux
```

Se quiser disponibilizar os LUNs mapeados para esse igroup para vários hosts, você pode especificar vários nomes de iniciadores separados por uma vírgula. Para obter mais informações, consulte lun igroup create no Centro de Documentação do NetApp ONTAP.

3. Confirme se o `igroup` existe usando o comando lun igroup show:

```
::> lun igroup show
```

O sistema responde com a seguinte saída:

```
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
svm_name  igroup_name  iscsi    linux    iqn.1994-05.com.redhat:abcdef12345
```

4. Esta etapa pressupõe que você já tenha criado um LUN de iSCSI. Se você não tiver, consulte step-by-step as instruções Como criar um LUN de iSCSI para fazer isso.

Crie um mapeamento do LUN criado para o igroup que você criou, usando o lun mapping create, especificando os atributos a seguir.

- *svm_name*: o nome da máquina virtual de armazenamento que fornece o destino iSCSI. O host usa esse valor para acessar o LUN.
- *vol_name*: o nome do volume que hospeda o LUN.
- *lun_name*: o nome que você atribuiu ao LUN.
- *igroup_name*: o nome do grupo de iniciadores.
- *lun_id*: o número inteiro do ID do LUN é específico do mapeamento e não do LUN em si. Isso é usado pelos iniciadores no igroup, pois o número da unidade lógica usa esse valor para o iniciador ao acessar o armazenamento.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Use o comando `lun show -path` para confirmar se o LUN foi criado, on-line e mapeado.

```
::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
```

O sistema responde com a seguinte saída:

```
 Vserver    Path                            serial-hex               state    mapped
 --------- ------------------------------- ------------------------ --------
 --------
 svm_name  /vol/vol_name/lun_name          6c5742314e5d52766e796150 online   mapped
```

Salve o valor `serial_hex` (neste exemplo, é `6c5742314e5d52766e796150`). Você o usará em uma etapa posterior para criar um nome fácil para o dispositivo de blocos.

6. Use o comando `network interface show -vserver` para recuperar os endereços das interfaces `iscsi_1` e `iscsi_2` e da SVM na qual você criou o LUN do iSCSI.

```
::> network interface show -vserver svm_name
```

O sistema responde com a seguinte saída:

```
            Logical               Status     Network            Current
        Current Is
Vserver     Interface             Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------            ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.0.143/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.21.81/20
 FSxId0123456789abcdef8-02  e0e     true
            nfs_smb_management_1
                                  up/up      198.19.250.177/20
 FSxId0123456789abcdef8-01  e0e     true
3 entries were displayed.
```

Neste exemplo, o endereço IP de `iscsi_1` é `172.31.0.143` e `iscsi_2` é `172.31.21.81`.

Montar um LUN de iSCSI no cliente Linux

1. No cliente Linux, use o comando a seguir para descobrir os nós do iSCSI de destino usando o endereço IP de `iscsi_1` *`iscsi_1_IP`*.

```
~$ sudo iscsiadm --mode discovery --op update --type sendtargets --
portal iscsi_1_IP
```

```
172.31.0.143:3260,1029
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
172.31.21.81:3260,1028
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

   Neste exemplo, `iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3` corresponde ao `target_initiator` para o LUN do iSCSI na zona de disponibilidade preferencial.

2. (Opcional) Você pode estabelecer sessões adicionais com o `target_initiator`. O Amazon EC2 tem um limite de largura de banda de 5 GB/s (cerca de 625 MB/s) para tráfego de fluxo único, mas você pode criar várias sessões a fim de gerar níveis mais altos de throughput para o sistema de arquivos usando um único cliente. Para obter mais informações, consulte Largura de banda da rede de instâncias do Amazon EC2 no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux.

   O comando a seguir estabelece oito sessões por iniciador por nó do ONTAP em cada zona de disponibilidade, permitindo que o cliente gere até 40 GB/s (5.000 MB/s) de throughput agregado para o LUN de iSCSI.

```
~$ sudo iscsiadm --mode node -T target_initiator --op update -n
 node.session.nr_sessions -v 8
```

3. Faça login nos iniciadores de destino. Seus LUNs de iSCSI são apresentados como discos disponíveis.

```
~$ sudo iscsiadm --mode node -T target_initiator --login
```

```
Logging in to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] (multiple)
Login to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] successful.
```

A saída acima está truncada; você deve ver uma resposta `Logging in` e uma resposta `Login successful` para cada sessão em cada servidor de arquivos. No caso de quatro sessões por nó, haverá 8 respostas `Logging in` e 8 respostas `Login successful`.

4. Use o comando a seguir para verificar se `dm-multipath` identificou e mesclou as sessões de iSCSI mostrando um único LUN com várias políticas. Deve haver um número igual de dispositivos listados como `active` e aqueles listados como `enabled`.

```
~$ sudo multipath -ll
```

Na saída, o nome do disco é formatado como `dm-xyz`, onde `xyz` é um número inteiro. Se não houver outros discos de múltiplos caminhos, o valor será `dm-0`.

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
 hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda     8:0   active ready running
| |- 1:0:0:1 sdc     8:32  active ready running
| |- 3:0:0:1 sdg     8:96  active ready running
| `- 4:0:0:1 sdh     8:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb     8:16  active ready running
  |- 7:0:0:1 sdf     8:80  active ready running
  |- 6:0:0:1 sde     8:64  active ready running
  `- 5:0:0:1 sdd     8:48  active ready running
```

Seu dispositivo de blocos agora está conectado ao cliente Linux. Ele está localizado sob o caminho `/dev/dm-xyz`. Você não deve usar esse caminho para fins administrativos; em vez disso, use o link simbólico que está sob o caminho `/dev/mapper/wwid`, onde `wwid` é um identificador exclusivo do seu LUN que é consistente em todos os dispositivos. Na próxima

etapa, você fornecerá um nome fácil para *wwid*, de modo que possa diferenciá-lo de outros discos com múltiplos caminhos.

Dar um nome amigável para o dispositivo de blocos

1. Para fornecer um nome fácil ao dispositivo, crie um alias no arquivo `/etc/multipath.conf`. Para isso, adicione a seguinte entrada ao arquivo usando seu editor de texto preferencial, substituindo os seguintes espaços reservados:

   - Substitua `serial_hex` pelo valor salvo no procedimento Configurar o iSCSI no sistema de arquivos do FSx para ONTAP.
   - Adicione o prefixo `3600a0980` ao valor `serial_hex` conforme mostrado no exemplo. Este é um preâmbulo exclusivo para a distribuição NetApp ONTAP que o Amazon FSx for ONTAP usa. NetApp
   - Substitua `device_name` pelo nome fácil que deseja usar no seu dispositivo.

   ```
   multipaths {
       multipath {
           wwid 3600a0980serial_hex
           alias device_name
       }
   }
   ```

   Como alternativa, você pode copiar e salvar o script a seguir como um arquivo bash, como `multipath_alias.sh`. Você pode executar o script com privilégios sudo, substituindo *serial_hex* (sem o prefixo 3600a0980) e *device_name* pelo seu respectivo número de série e pelo nome desejado. Esse script busca uma seção `multipaths` não comentada no arquivo `/etc/multipath.conf`. Se a seção existir, ele anexa uma entrada `multipath` a essa seção; caso contrário, ele criará uma seção `multipaths` com uma entrada `multipath` para o seu dispositivo de blocos.

   ```
   #!/bin/bash
   SN=serial_hex
   ALIAS=device_name
   CONF=/etc/multipath.conf
   grep -q '^multipaths {' $CONF
   UNCOMMENTED=$?
   if [ $UNCOMMENTED -eq 0 ]
   ```

```
then
        sed -i '/^multipaths {/a\\tmultipath {\n\t\twwid 3600a0980'"${SN}"'\n\t
\talias '"${ALIAS}"'\n\t}\n' $CONF
else
        printf "multipaths {\n\tmultipath {\n\t\twwid 3600a0980$SN\n\t\talias
 $ALIAS\n\t}\n}" >> $CONF
fi
```

2. Reinicie o serviço `multipathd` para que as alterações em `/etc/multipathd.conf` entrem em vigor.

```
~$ systemctl restart multipathd.service
```

Particionar o LUN

A próxima etapa é formatar e particionar o LUN usando `fdisk`.

1. Use o comando a seguir para verificar se o caminho para `device_name` está presente.

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. Particione o disco usando `fdisk`. Você inserirá um prompt interativo. Insira as opções na ordem mostrada. Observe que o valor de `Last sector` terá variações, dependendo do tamanho do LUN de iSCSI (10 GB, neste exemplo). Você pode criar várias partições usando um valor menor que o último setor (`20971519`, neste exemplo).

```
~$ sudo fdisk /dev/mapper/device_name
```

O prompt interativo `fsdisk` é iniciado.

```
Welcome to fdisk (util-linux 2.30.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.
```

```
Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
 20971519): 20971519

Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

Após inserir `w`, sua nova partição `/dev/mapper/partition_name` fica disponível. O *partition_name* tem o formato *<device_name><partition_number>*. 1 foi usado como o número da partição utilizada no comando `fdisk` na etapa anterior.

3. Crie seu sistema de arquivos usando `/dev/mapper/partition_name` como caminho.

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

O sistema responde com a seguinte saída:

```
mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
```

```
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Montar o LUN no cliente Linux

1. Crie um diretório *directory_path* como ponto de montagem do sistema de arquivos.

```
~$ sudo mkdir /directory_path/mount_point
```

2. Monte o sistema de arquivos usando o comando a seguir.

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. (Opcional) Você pode alterar a propriedade do diretório de montagem para o seu usuário. Substitua *username* pelo seu nome do usuário.

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (Opcional) Verifique se pode ler e gravar dados no sistema de arquivos.

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

Você criou e montou com êxito um LUN de iSCSI no cliente Linux.

Montar LUNs de iSCSI em um cliente Windows

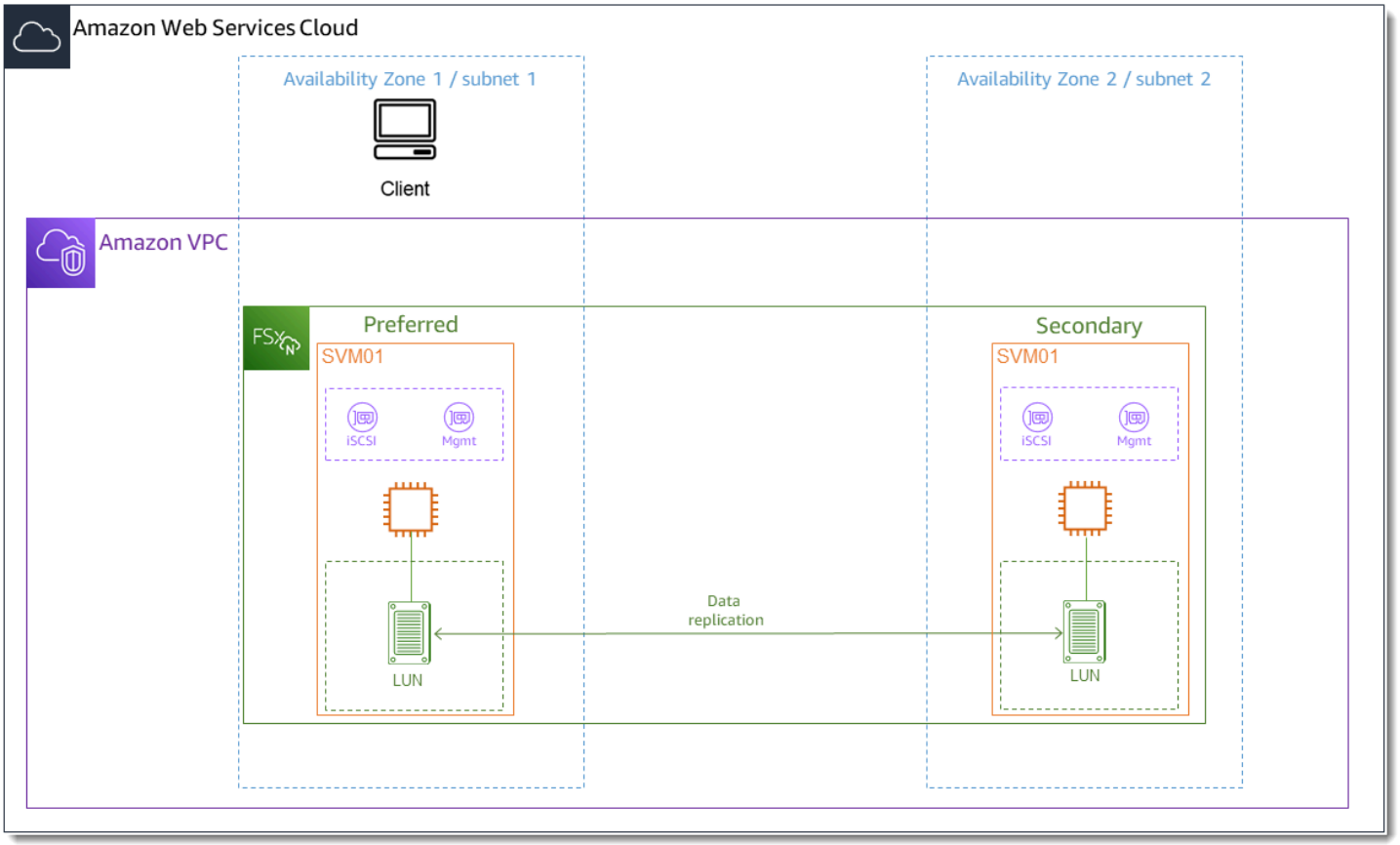
Os exemplos apresentados nestes procedimentos usam a seguinte configuração:

- O LUN do iSCSI que está sendo montado em um host do Windows já foi criado. Para ter mais informações, consulte Como criar um LUN de iSCSI.
- O host do Microsoft Windows que está montando o LUN do iSCSI é uma instância do Amazon EC2 executando uma imagem de máquina da Amazon (AMI) do Microsoft Windows Server 2019. Ele tem grupos de segurança de VPC configurados para permitir tráfego de entrada e saída, conforme descrito em Controle de acesso ao sistema de arquivos com a Amazon VPC.

Você pode estar usando uma AMI diferente do Microsoft Windows na configuração.

- O cliente e o sistema de arquivos estão localizados na mesma VPC e Conta da AWS. Se o cliente estiver localizado em outra VPC, você poderá usar o emparelhamento de VPC ou conceder a outras VPCs acesso AWS Transit Gateway aos endpoints iSCSI. Para ter mais informações, consulte Acesso a dados de fora da VPC de implantação.

  Recomendamos que a instância do EC2 esteja na mesma zona de disponibilidade da sub-rede preferencial do seu sistema de arquivos, conforme mostrado no gráfico a seguir.



Tópicos

- Configurar o iSCSI no cliente Windows
- Configurar o iSCSI no sistema de arquivos do FSx para ONTAP
- Monte um LUN de iSCSI no cliente Windows
- Validando sua configuração iSCSI

Configurar o iSCSI no cliente Windows

1. Use a Área de Trabalho Remota do Windows para se conectar ao cliente Windows no qual você deseja montar o LUN de iSCSI. Para obter mais informações, consulte Conectar-se à sua instância baseada no Windows usando RDP no Guia do usuário do Amazon Elastic Compute Cloud.
2. Abra um Windows PowerShell como administrador. Use os comandos a seguir para habilitar o iSCSI na sua instância do Windows e configurar o serviço de iSCSI para iniciar automaticamente.

```
PS C:\> Start-Service MSiSCSI
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. Recupere o nome do iniciador da instância do Windows. Você usará esse valor na configuração do iSCSI em seu sistema de arquivos FSx for ONTAP usando a CLI ONTAP. NetApp

```
PS C:\> (Get-InitiatorPort).NodeAddress
```

   O sistema responde com a porta do iniciador:

```
iqn.1991-05.com.microsoft:ec2amaz-abc123d
```

4. Para permitir que seus clientes façam o failover automático entre os servidores de arquivos, é necessário instalar `Multipath-IO` (MPIO) na instância do Windows. Use o seguinte comando:

```
PS C:\> Install-WindowsFeature Multipath-IO
```

5. Reinicie a instância do Windows após concluir a instalação de `Multipath-IO`. Mantenha a instância do Windows aberta para executar as etapas de montagem do LUN de iSCSI na seção a seguir.

Configurar o iSCSI no sistema de arquivos do FSx para ONTAP

1. Conecte-se à CLI do NetApp ONTAP no sistema de arquivos FSx for ONTAP no qual você criou o LUN iSCSI usando o comando a seguir. Para ter mais informações, consulte Usar a CLI do NetApp ONTAP.

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. Usando a lun igroup createCLI do NetApp ONTAP, crie o grupo de iniciadores ou. `igroup` Um grupo de iniciadores mapeia para LUNs de iSCSI e controla quais iniciadores (clientes) têm acesso aos LUNs. Substitua `host_initiator_name` pelo nome do iniciador do host do Windows recuperado no procedimento anterior.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype windows
```

Se quiser disponibilizar os LUNs mapeados para esse `igroup` para vários hosts, você pode especificar vários nomes de iniciadores separados por vírgula. Para obter mais informações, consulte o Centro *lun igroup create*de Documentação do NetApp ONTAP.

3. Confirme se o `igroup` foi criado com êxito usando o seguinte comando:

```
::> lun igroup show
```

O sistema responde com a seguinte saída:

```
Vserver    Igroup        Protocol OS Type  Initiators
---------  ------------  -------- -------- ------------------------------------
svm_name   igroup_name   iscsi    windows  iqn.1994-05.com.windows:abcdef12345
```

Com o `igroup` criado, você já pode criar LUNs e mapeá-los para o `igroup`.

4. Esta etapa pressupõe que você já tenha criado um LUN de iSCSI. Se você não tiver, consulte step-by-step as instruções Como criar um LUN de iSCSI para fazer isso.

Crie um mapeamento de LUN do LUN para o seu novo `igroup`.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Confirme se o LUN foi criado on-line e mapeado com o seguinte comando:

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

Agora, você já pode adicionar o destino iSCSI na sua instância do Windows.

6. Recupere os endereços IP das interfaces `iscsi_1` e `iscsi_2` da SVM usando o seguinte comando:

```
::> network interface show -vserver svm_name
```

```
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
svm_name
            iscsi_1    up/up      172.31.0.143/20    FSxId0123456789abcdef8-01
                                                                   e0e     true
            iscsi_2    up/up      172.31.21.81/20    FSxId0123456789abcdef8-02
                                                                   e0e     true
            nfs_smb_management_1
                       up/up      198.19.250.177/20  FSxId0123456789abcdef8-01
                                                                   e0e     true
3 entries were displayed.
```

Neste exemplo, o endereço IP de `iscsi_1` é `172.31.0.143` e `iscsi_2` é `172.31.21.81`.

Monte um LUN de iSCSI no cliente Windows

1. Na sua instância do Windows, abra um PowerShell terminal como administrador.
2. Você criará um script `.ps1` que faça o seguinte:

   - Conecta-se a cada uma das interfaces de iSCSI do seu sistema de arquivos.
   - Adiciona e configura o MPIO para o iSCSI.
   - Estabelece oito sessões para cada conexão de iSCSI, o que permite ao cliente gerar até 40 GB/s (5.000 MB/s) de throughput agregado para o LUN do iSCSI. Ter oito sessões garante que um único cliente possa impulsionar a capacidade de throughput total de 4.000 MB/s para a capacidade de throughput do FSx para ONTAP de mais alto nível. Opcionalmente, você pode alterar o número de sessões para um número maior ou menor (cada sessão fornece até 625 MB/s de throughput) modificando o for-loop do script na etapa `#Establish iSCSI connection` de `1..8` até outro limite superior. Para obter mais informações, consulte Largura de banda da rede de instâncias do Amazon EC2 no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Windows.

Copie o conjunto de comandos a seguir em um arquivo para criar o script `.psl`.

- Substitua `iscsi_1` e `iscsi_2` pelos endereços IP recuperados na etapa anterior.
- Substitua `ec2_ip` pelo endereço IP da instância do Windows.

```
#iSCSI IP addresses for Preferred and Standby subnets
$TargetPortalAddresses = @("iscsi_1","iscsi_2")

#iSCSI Initator IP Address (Local node IP address)
$LocaliSCSIAddress = "ec2_ip"

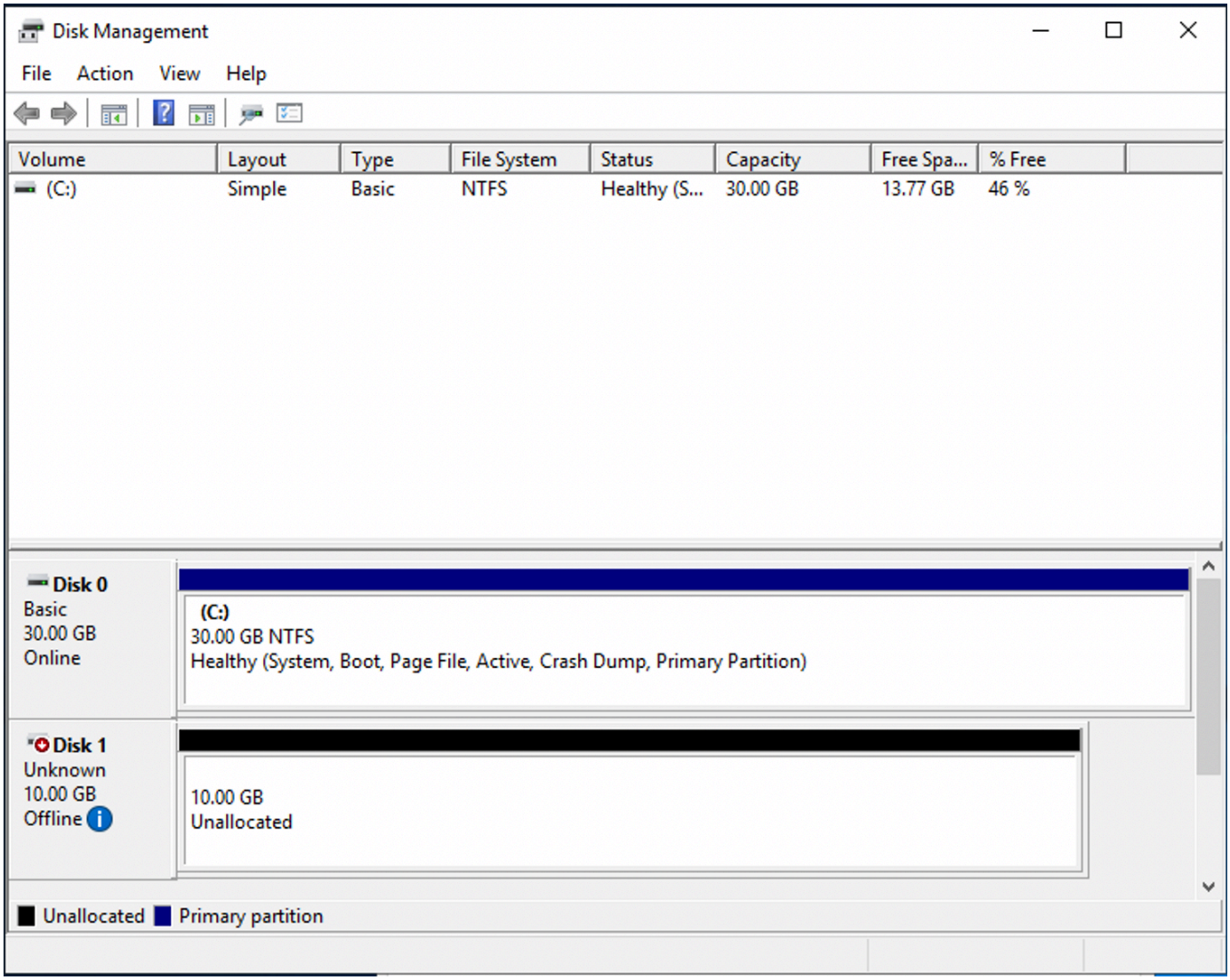
#Connect to FSx for NetApp ONTAP file system
Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

#Add MPIO support for iSCSI
New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

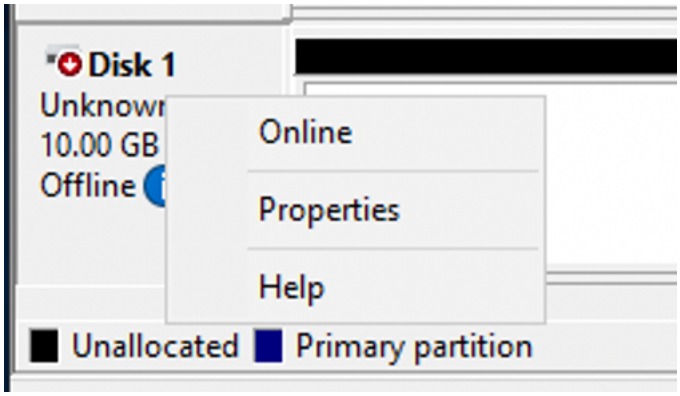
#Establish iSCSI connection
1..8 | %{Foreach($TargetPortalAddress in $TargetPortalAddresses)
{Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true}}

#Set the MPIO Policy to Round Robin
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

3. Inicie a aplicação Gerenciamento de Disco do Windows. Abra a caixa de diálogo Run do Windows, insira `diskmgmt.msc` e pressione Enter. A aplicação Gerenciamento de Disco se abre.



4. Localize o disco não alocado. Esse é o LUN de iSCSI. No exemplo, Disk 1 é o disco iSCSI. Está off-line.



Coloque o volume on-line posicionando o cursor sobre Disk 1, clique com o botão direito do mouse e escolha On-line.

> **Note**
>
> Você pode modificar a política da rede de área do armazenamento (SAN) para que novos volumes sejam automaticamente colocados on-line. Para obter mais informações, consulte as políticas da SAN na Microsoft Windows Server Command Reference.

5. Para inicializar o disco, coloque o cursor sobre Disk 1, clique com o botão direito do mouse e escolha Inicializar. A caixa de diálogo Inicializar é exibida. Escolha OK para inicializar o disco.
6. Formate o disco como você faria normalmente. Depois que a formatação estiver concluída, o drive do iSCSI aparecerá como um drive utilizável no cliente Windows.

Validando sua configuração iSCSI

Fornecemos um script para verificar se a configuração do iSCSI está configurada corretamente. O script examina parâmetros como contagem de sessões, distribuição de nós e status do Multipath I/O (MPIO). A tarefa a seguir explica como instalar e usar o script.

Para validar sua configuração iSCSI

1. Abra uma PowerShell janela do Windows.
2. Faça o download do script usando o comando a seguir.

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/
samples/CheckiSCSI.zip" -OutFile "CheckiSCSI.zip"
```

3. Expanda o arquivo zip usando o comando a seguir.

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

4. Execute o script usando o comando a seguir.

```
PS C:\> ./CheckiSCSI.ps1
```

5. Revise a saída para entender o estado atual da sua configuração. O exemplo a seguir demonstra uma configuração de iSCSI bem-sucedida.

```
PS C:\> ./CheckiSCSI.ps1
```

```
This script checks the iSCSI configuration on the local instance.
It will provide information about the number of connected sessions, connected file
 servers, and MPIO status.

MPIO is installed on this server.

Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'
has 16 total sessions (16 active, 0 non-active)
spread across 2 node(s).
MPIO: Yes
```

Como usar o FSx para ONTAP com outros serviços da AWS

Além do Amazon EC2, você pode usar outros AWS serviços com seus volumes para acessar seus dados.

Tópicos

- Usando a Amazon WorkSpaces com FSx for ONTAP
- Como usar o Amazon Elastic Container Service com o FSx para ONTAP
- Como usar o VMware Cloud com o FSx para ONTAP

Usando a Amazon WorkSpaces com FSx for ONTAP

O FSx for ONTAP pode ser usado com WorkSpaces a Amazon para fornecer armazenamento conectado à rede (NAS) compartilhado ou para armazenar perfis de roaming para contas da Amazon. WorkSpaces Depois de se conectar a um compartilhamento de arquivos SMB com uma WorkSpaces instância, o usuário pode criar e editar arquivos no compartilhamento de arquivos.

Os procedimentos a seguir mostram como usar o Amazon FSx com WorkSpaces a Amazon para fornecer ao perfil de roaming e ao acesso à pasta inicial uma experiência consistente e fornecer uma pasta de equipe compartilhada para usuários de Windows e Linux. WorkSpaces Se você é novo na Amazon WorkSpaces, pode criar seu primeiro WorkSpaces ambiente Amazon com as instruções em Comece com a Configuração WorkSpaces Rápida no Guia de WorkSpaces Administração da Amazon.

Tópicos

Fornecer suporte ao perfil de roaming

Você pode usar o Amazon FSx para fornecer suporte ao perfil de roaming a usuários na sua organização. Um usuário terá permissões para acessar somente seu perfil de roaming. A pasta será conectada automaticamente usando as políticas de grupo do Active Directory. Com um perfil de roaming, os dados e as configurações de desktop dos usuários são salvos quando eles se desconectam de um compartilhamento de arquivos do Amazon FSx, permitindo que documentos e configurações sejam compartilhados entre diferentes WorkSpaces instâncias, e o backup automático é feito automaticamente usando backups automáticos diários do Amazon FSx.

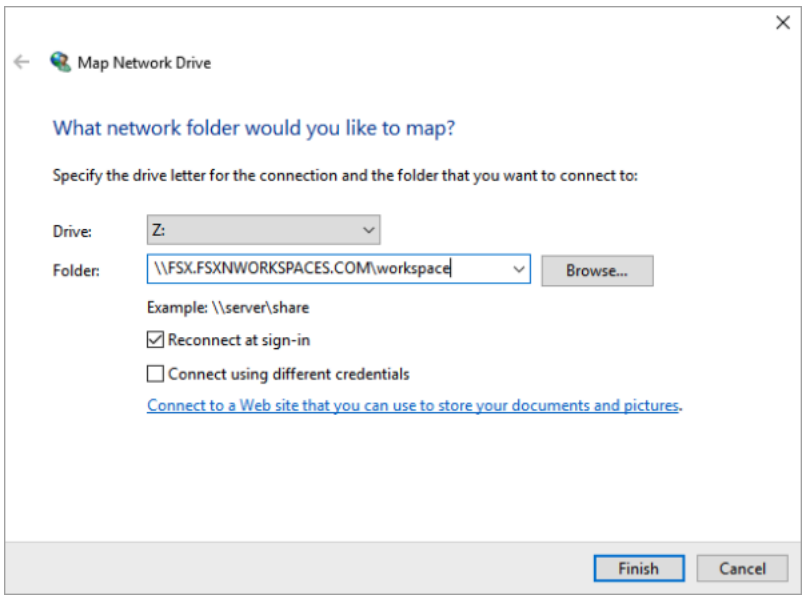
Etapa 1: criar um local de pasta de perfil para usuários de domínio usando o Amazon FSx

1. Crie um sistema de arquivos do FSx para ONTAP usando o console do Amazon FSx. Para obter mais informações, consulte Criar um sistema de arquivos (console).

   > **Important**
   >
   > Cada sistema de arquivos do FSx para ONTAP tem um intervalo de endereços IP do endpoint no qual os endpoints associados ao sistema de arquivos são criados. Para sistemas de arquivos multi-AZ, o FSx para ONTAP escolhe um intervalo de endereços IP padrão não utilizado de 198.19.0.0/16 como o intervalo de endereços IP do endpoint. Esse intervalo de endereços IP também é usado WorkSpaces para gerenciar o intervalo de tráfego, conforme descrito nos requisitos de endereço IP e porta do Amazon WorkSpaces Administration Guide. WorkSpaces Como resultado, para acessar seu sistema de arquivos Multi-AZ FSx for ONTAP a WorkSpaces partir de, você deve selecionar um intervalo de endereços IP de endpoint que não se sobreponha ao 198.19.0.0/16.

2. Se você ainda não tiver uma máquina virtual de armazenamento (SVM) associada a um Active Directory, crie uma agora. Por exemplo, você pode provisionar uma SVM chamada `fsx` e definir o estilo de segurança como NTFS. Para obter mais informações, consulte Criar uma máquina virtual de armazenamento (console).

3. Crie um volume para sua SVM. Por exemplo, você pode criar um volume chamado `fsx-vol` que herda o estilo de segurança do volume raiz da SVM. Para obter mais informações, consulte Para criar um FlexVol volume (console).
4. Crie um compartilhamento SMB em seu volume. Por exemplo, você pode criar um compartilhamento chamado `workspace` em seu volume chamado `fsx-vol`, no qual você cria uma pasta chamada `profiles`. Para obter mais informações, consulte Como gerenciar compartilhamentos de SMB.
5. Acesse seu Amazon FSx SVM a partir de uma instância do Amazon EC2 executando o Windows Server ou de um. WorkSpace Para obter mais informações, consulte Acesso a dados do .
6. Você mapeia seu compartilhamento para `Z:\` na sua WorkSpaces instância do Windows:



Etapa 2: vincular o compartilhamento de arquivos do FSx para ONTAP às contas de usuário

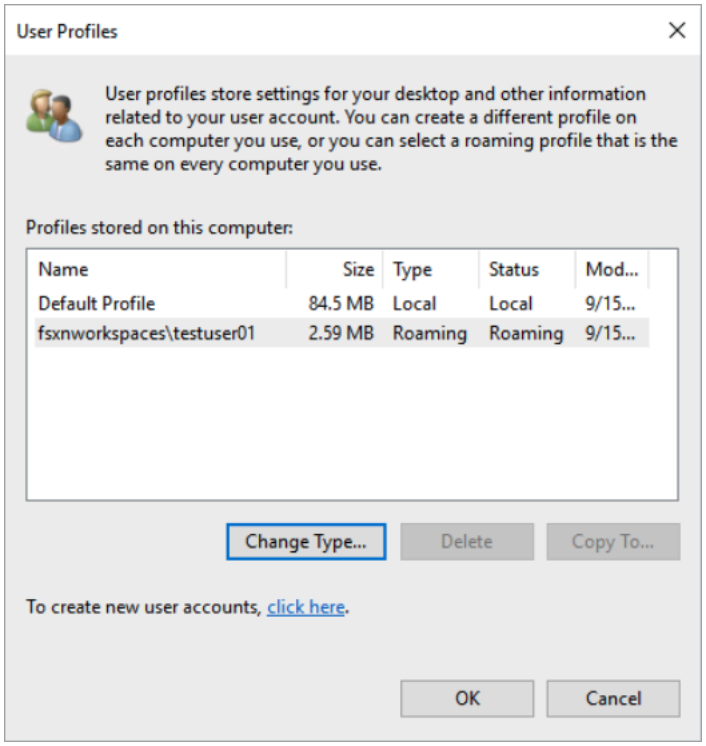
1. No seu usuário de teste WorkSpace, escolha Windows > Sistema > Configurações avançadas do sistema.
2. Em Propriedades do sistema, selecione a guia Avançado e pressione o botão Configurações na seção Perfis de usuário. O usuário conectado terá um tipo de perfil de `Local`.
3. Desconecte o usuário de teste do WorkSpace.
4. Configure o usuário de teste para ter um perfil de roaming localizado no seu sistema de arquivos do Amazon FSx. No seu administrador WorkSpaces, abra um PowerShell console e use um comando semelhante ao exemplo a seguir (que usa a `profiles` pasta que você criou anteriormente na Etapa 1):

```
Set-ADUser username -ProfilePath \\filesystem-dns-
name\sharename\foldername\username
```

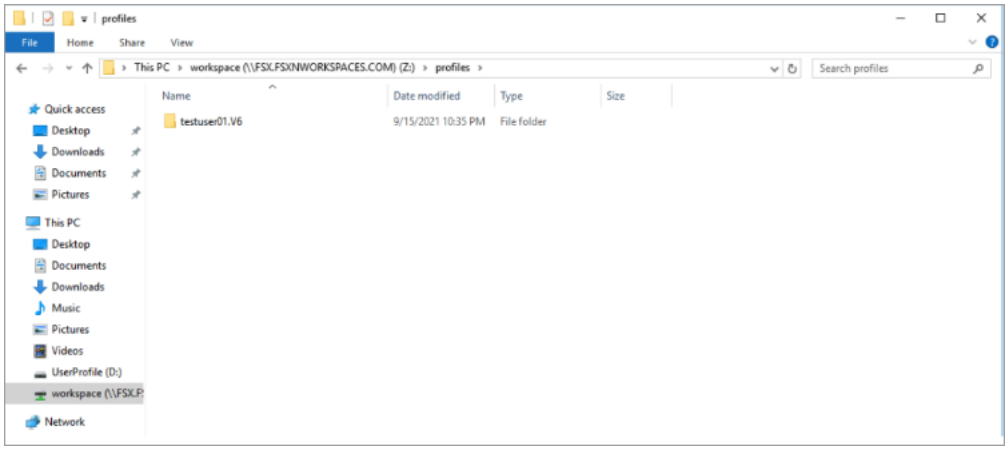
Por exemplo: .

```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxnworkspaces.com\workspace\profiles
\testuser01
```

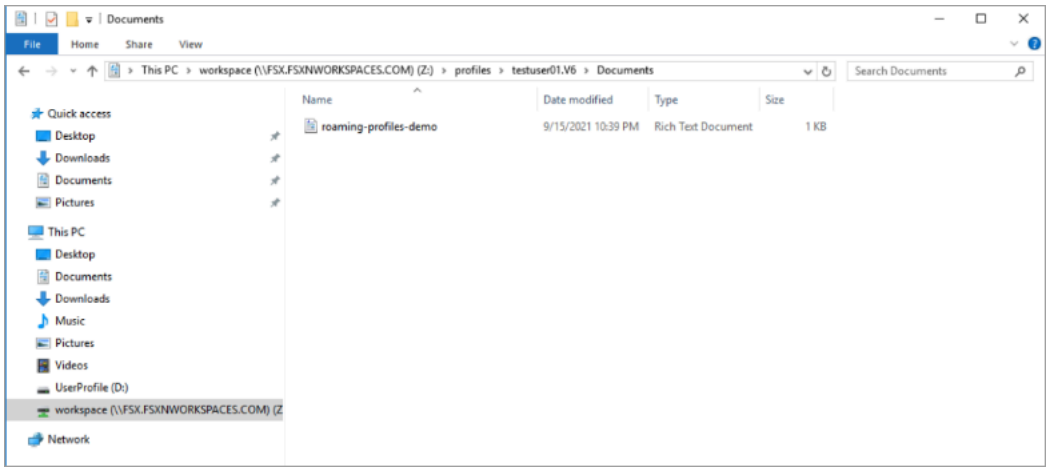
5. Faça login com o usuário de teste WorkSpace.
6. Em Propriedades do sistema, selecione a guia Avançado e pressione o botão Configurações na seção Perfis de usuário. O usuário conectado terá um tipo de perfil de `Roaming`.



7. Procure a pasta compartilhada do FSx para ONTAP. Na pasta `profiles`, você verá uma pasta para o usuário.



8. Criar um documento na pasta `Documents` do usuário de teste
9. Desconecte o usuário de teste do seu WorkSpace.
10. Se você se conectar novamente como usuário de teste e navegar até o armazenamento de perfis, verá o documento que criou.



Fornecer uma pasta compartilhada para acessar arquivos comuns

Você pode usar o Amazon FSx para fornecer uma pasta compartilhada a usuários na sua organização. Uma pasta compartilhada pode ser usada para armazenar arquivos usados pela sua comunidade de usuários, como arquivos de demonstração, exemplos de código e manuais de instruções necessários para todos os usuários. Normalmente, você tem unidades mapeadas para pastas compartilhadas; no entanto, como as unidades mapeadas usam letras, há um limite para o número de compartilhamentos que você pode ter. Esse procedimento cria uma pasta compartilhada do Amazon FSx que está disponível sem uma letra da unidade, oferecendo maior flexibilidade na atribuição de compartilhamentos às equipes.

Para montar uma pasta compartilhada para acesso multiplataforma do Linux e do Windows WorkSpaces

1. Na barra de tarefas, escolha Locais > Conectar ao servidor.

   a. Em Server (Servidor), insira*`file-system-dns-name`*.

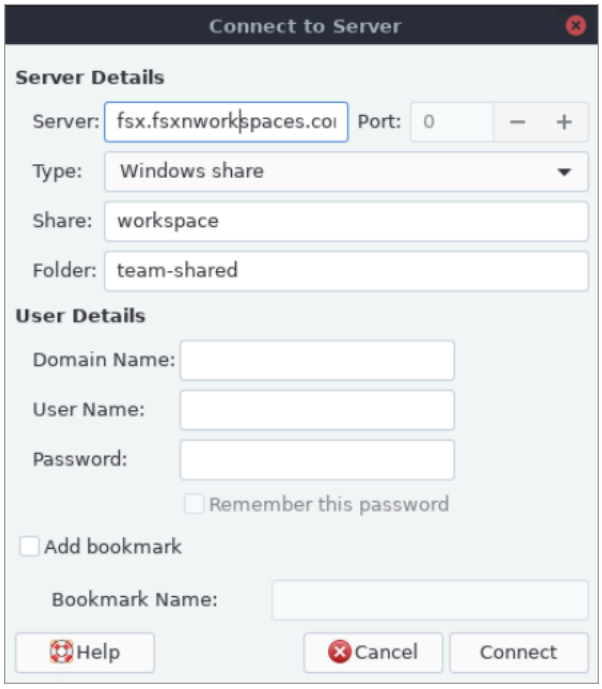
   b. Defina Tipo como `Windows share`.

   c. Defina Compartilhar para o nome do compartilhamento SMB, como `workspace`.

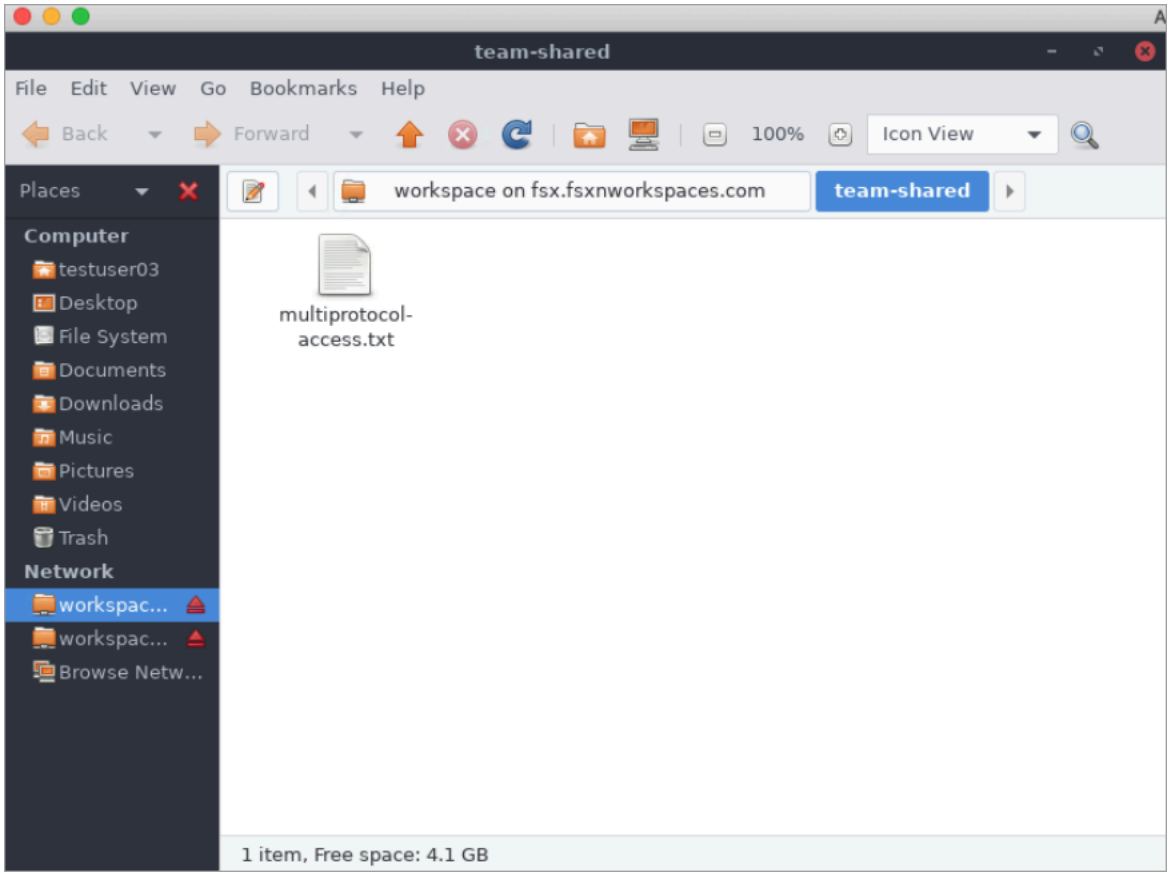
   d. Você pode deixar a Pasta como `/` ou defini-la como uma pasta, como uma pasta chamada `team-shared`.

   e. Para um Linux WorkSpace, você não precisa inserir seus detalhes de usuário se o Linux WorkSpace estiver no mesmo domínio do compartilhamento Amazon FSx.

   f. Selecione Conectar.



2. Depois que a conexão for estabelecida, você poderá ver a pasta compartilhada (denominada `team-shared` neste exemplo) no compartilhamento SMB denominado `workspace`.



Como usar o Amazon Elastic Container Service com o FSx para ONTAP

Você pode acessar seus sistemas de arquivos Amazon FSx for NetApp ONTAP a partir de um contêiner Docker do Amazon Elastic Container Service (Amazon ECS) em uma instância Linux ou Windows do Amazon EC2.

Montagem em um contêiner do Linux do Amazon ECS

1. Crie um cluster do ECS usando o modelo de cluster EC2 Linux + Networking para os contêineres do Linux. Para obter mais informações, consulte Creating a cluster no Guia do desenvolvedor do Amazon Elastic Container Service.
2. Crie um diretório na instância do EC2 para montar o volume da SVM da seguinte forma:

```
sudo mkdir /fsxontap
```

3. Monte o volume do FSx para ONTAP na instância de Linux do EC2 usando um script de dados do usuário durante a execução da instância ou executando os seguintes comandos:

```
sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
```

4. Monte o volume usando o seguinte comando:

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /
fsxontap
```

O exemplo a seguir usa valores de amostra.

```
sudo mount -t nfs -o nfsvers=4.1
 svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
fsxontap
```

Você também pode usar o endereço IP da SVM em vez do nome DNS.

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. Ao criar suas definições de tarefas do Amazon ECS, adicione as propriedades de contêiner `volumes` e `mountPoints` a seguir na definição do contêiner JSON. Substitua `sourcePath` pelo ponto de montagem e pelo diretório no sistema de arquivos do FSx para ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Montagem em um contêiner do Windows do Amazon ECS

1. Crie um cluster do ECS usando o modelo de cluster EC2 Windows + Networking para os contêineres do Windows. Para obter mais informações, consulte Creating a cluster no Guia do desenvolvedor do Amazon Elastic Container Service.
2. Adicione a instância do EC2 para Windows associada a um domínio ao cluster do Windows para ECS e mapeie um compartilhamento SMB.

   Execute uma instância do EC2 para Windows otimizada para ECS que esteja associada ao seu domínio do Active Directory e inicialize o agente do ECS executando o comando a seguir.

   ```
   PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
   EnableTaskIAMRole
   ```

   Você também pode passar as informações em um script para o campo de texto de dados do usuário da forma a seguir.

   ```
   <powershell>
   Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
   </powershell>
   ```
3. Crie um mapeamento global SMB na instância do EC2 para que você possa mapear o compartilhamento SMB em uma unidade. Substitua os valores abaixo do nome NetBIOS ou DNS pelo seu sistema de arquivos do FSx e nome do compartilhamento. O volume NFS vol1 montado na instância do EC2 para Linux está configurado como um compartilhamento CIFS fsxontap no sistema de arquivos do FSx.

   ```
   vserver cifs share show -vserver svm08 -share-name fsxontap


                                   Vserver: svm08
                                     Share: fsxontap
                   CIFS Server NetBIOS Name: FSXONTAPDEMO
                                     Path: /vol1
                            Share Properties: oplocks
                                              browsable
                                              changenotify
                                              show-previous-versions
                                 Symlink Properties: symlinks
                          File Mode Creation Mask: -
   ```

```
                 Directory Mode Creation Mask: -
                               Share Comment: -
                                   Share ACL: Everyone / Full Control
               File Attribute Cache Lifetime: -
                                 Volume Name: vol1
                               Offline Files: manual
           Vscan File-Operations Profile: standard
         Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -
```

4. Crie o mapeamento global SMB na instância do EC2 usando o seguinte comando:

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. Ao criar suas definições de tarefas do Amazon ECS, adicione as propriedades de contêiner `volumes` e `mountPoints` a seguir na definição do contêiner JSON. Substitua `sourcePath` pelo ponto de montagem e pelo diretório no sistema de arquivos do FSx para ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Como usar o VMware Cloud com o FSx para ONTAP

Você pode usar o FSx for ONTAP como um armazenamento de dados externo para o VMware Cloud on AWS Software-Defined Data Centers (SDDCs). Para obter mais informações, consulte Configurar o Amazon FSx for NetApp ONTAP como armazenamento externo e o Guia de implantação do VMware Cloud on with AWS Amazon FSx for ONTAP. NetApp

Disponibilidade e durabilidade

O Amazon FSx for NetApp ONTAP usa dois tipos de implantação, Single-AZ e Multi-AZ, que oferecem diferentes níveis de disponibilidade e durabilidade. Este tópico descreve os recursos de disponibilidade e durabilidade de cada tipo de implantação para ajudar você a escolher o mais adequado às suas workloads. Para obter informações sobre o SLA (Acordo de Nível de Serviço) de disponibilidade do serviço, consulte Amazon FSx Service Level Agreement.

Tópicos

Escolher um tipo de implantação do sistema de arquivos

Os recursos de disponibilidade e durabilidade dos tipos de implantação single-AZ e multi-AZ do sistema de arquivos são descritos nas seções a seguir.

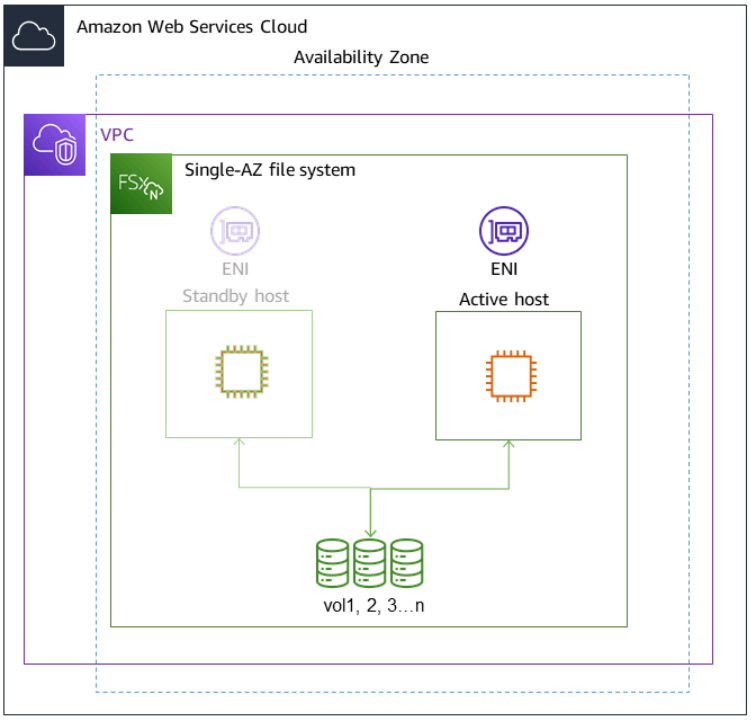
Tipo de implantação single-AZ

Quando você cria um sistema de arquivos Single-AZ, o Amazon FSx provisiona automaticamente de um a doze pares de servidores de arquivos em uma configuração ativa em espera, com os servidores de arquivos ativos e em espera em cada par localizados em domínios de falha separados em uma única zona de disponibilidade no. Região da AWS Durante a manutenção planejada do sistema de arquivos ou uma interrupção não planejada do serviço de qualquer servidor de arquivos ativo, o Amazon FSx transfere automaticamente e de forma independente esse par de alta disponibilidade (HA) para o servidor de arquivos em espera, normalmente em alguns segundos. Durante um failover, você continua tendo acesso aos seus dados sem intervenção manual.

Para garantir a alta disponibilidade, o Amazon FSx monitora continuamente as falhas de hardware e substitui automaticamente os componentes da infraestrutura em caso de falha. Para obter alta durabilidade, o Amazon FSx replica automaticamente seus dados dentro de uma zona de disponibilidade para protegê-los contra falhas de componentes. Além disso, você tem a opção de configurar backups diários automáticos dos dados do sistema de arquivos. Esses backups são armazenados em várias zonas de disponibilidade para fornecer resiliência multi-AZ a todos os dados de backup.

Os sistemas de arquivos single-AZ são projetados para casos de uso que não exigem o modelo de resiliência de dados de um sistema de arquivos multi-AZ. Eles fornecem uma solução econômica para casos de uso, como ambientes de desenvolvimento e teste, ou armazenamento de cópias secundárias de dados que já estão armazenados no local ou em outros ambientes Regiões da AWS, replicando dados somente em uma única zona de disponibilidade.

O diagrama a seguir ilustra a arquitetura de um sistema de arquivos single-AZ do FSx para ONTAP.

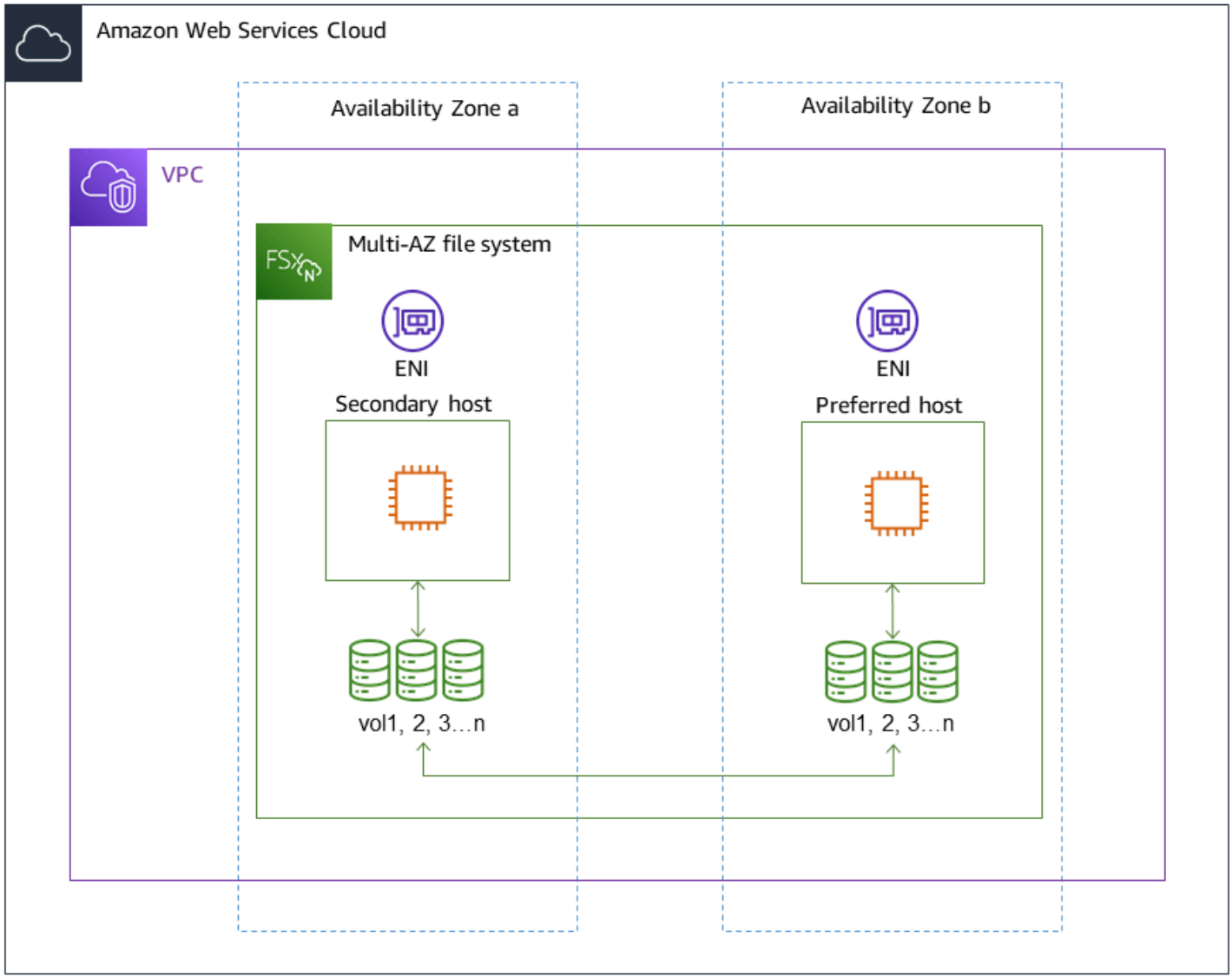


Tipo de implantação multi-AZ

Os sistemas de arquivos multi-AZ oferecem suporte a todos os recursos de disponibilidade e durabilidade dos sistemas de arquivos single-AZ. Além disso, eles são projetados para fornecer disponibilidade contínua aos dados, mesmo quando uma zona de disponibilidade não estiver disponível. As implantações Multi-AZ têm um único par de servidores de arquivos HA; o servidor de arquivos em espera é implantado em uma zona de disponibilidade diferente do servidor de arquivos ativo na mesma. Região da AWS Todas as alterações gravadas no sistema de arquivos são replicadas de forma síncrona nas zonas de disponibilidade para o modo de espera.

Os sistemas de arquivos multi-AZ são projetados para casos de uso, como workloads de produção essenciais para os negócios, que exigem alta disponibilidade para dados de arquivos compartilhados do ONTAP e precisam de armazenamento com replicação integrada em todas as zonas de

disponibilidade. O diagrama a seguir ilustra a arquitetura de um sistema de arquivos multi-AZ do FSx para ONTAP.



Processo de failover do FSx para ONTAP

Os sistemas de arquivos Single-AZ e Multi-AZ automaticamente transferem um determinado par de HA do servidor de arquivos preferencial ou ativo para o servidor de arquivos em espera se alguma das seguintes condições ocorrer:

- O servidor de arquivos preferencial ou ativo fica indisponível
- A capacidade de throughput do sistema de arquivos é alterada
- O servidor de arquivos preferencial ou ativo passa por uma manutenção planejada

- Ocorre uma interrupção na zona de disponibilidade (somente sistemas de arquivos multi-AZ)

> **Note**
>
> Para sistemas de arquivos escaláveis, o comportamento de failover de cada par de HA é independente. Se o servidor de arquivos preferencial para um par de HA não estiver disponível, somente esse par de HA fará o failover para seu servidor de arquivos em espera.

Ao fazer o failover de um servidor de arquivos para outro, o novo servidor de arquivos ativo começa automaticamente a atender todas as solicitações de leitura e gravação do sistema de arquivos para esse par de HA. Para sistemas de arquivos multi-AZ, quando o servidor de arquivos preferencial é totalmente recuperado e fica disponível, o Amazon FSx faz o failback automático a ele, com o failback geralmente concluído em menos de 60 segundos. Para sistemas de arquivos single-AZ e multi-AZ, um failover geralmente é concluído em menos de 60 segundos, desde a detecção da falha no servidor de arquivos ativo até a promoção do servidor de arquivos em espera para o status ativo. Como o endereço IP do endpoint que os clientes usam para acessar dados por NFS ou SMB permanece o mesmo, os failovers são transparentes para aplicações do Linux, Windows e macOS, que retomam as operações do sistema de arquivos sem intervenção manual.

Para garantir que failovers sejam transparentes aos clientes conectados aos sistemas de arquivos single-AZ e multi-AZ do FSx para ONTAP, consulte Acessando dados de dentro AWS.

Como testar o failover em um sistema de arquivos

Você pode testar o failover em seu sistema de arquivos escalável modificando sua capacidade de taxa de transferência. Ao modificar a capacidade de throughput do sistema de arquivos, o Amazon FSx desativa os servidores de arquivos do sistema de arquivos em série. Os sistemas de arquivos fazem o failover automático para o servidor secundário, enquanto o Amazon FSx substitui primeiro o servidor de arquivos preferencial. Depois de atualizado, o sistema de arquivos faz o failback automático para o novo servidor primário e o Amazon FSx substitui o servidor de arquivos secundário.

Você pode monitorar o progresso da solicitação de atualização da capacidade de throughput no console do Amazon FSx, na CLI e na API. Para obter mais informações sobre como modificar a capacidade de throughput do sistema de arquivos e monitorar o progresso da solicitação, consulte Como gerenciar a capacidade de throughput.

Recursos da rede

Esta seção descreve os recursos de rede consumidos pelos sistemas de arquivos single-AZ e multi-AZ.

Subredes

Ao criar um sistema de arquivos single-AZ, você especifica uma única sub-rede para o sistema de arquivos. A sub-rede escolhida define a zona de disponibilidade na qual o sistema de arquivos é criado. Ao criar um sistema de arquivos multi-AZ, você especifica duas sub-redes, uma para o servidor de arquivos preferencial e outra para o servidor de arquivos em espera. As duas sub-redes escolhidas devem estar em zonas de disponibilidade diferentes na mesma Região da AWS. Para obter mais informações sobre a Amazon VPC, consulte O que é Amazon VPC? no Guia do usuário da Amazon Virtual Private Cloud.

> **Note**
>
> Independentemente da sub-rede especificada, você pode acessar seu sistema de arquivos de qualquer sub-rede dentro da VPC do sistema de arquivos.

Interfaces de rede elástica do sistema de arquivos

Para sistemas de arquivos single-AZ, o Amazon FSx provisiona duas interfaces de rede elástica (ENI) na sub-rede associada ao sistema de arquivos. Para sistemas de arquivos multi-AZ, o Amazon FSx também provisiona duas ENIs, uma em cada uma das sub-redes associadas ao sistema de arquivos. Os clientes se comunicam com o seu sistema de arquivos do Amazon FSx usando a interface de rede elástica. Considera-se que as interfaces de rede estão dentro do escopo de serviço do Amazon FSx, apesar de fazerem parte da VPC da sua conta. Os sistemas de arquivos Multi-AZ usam endereços de protocolo de Internet (IP) flutuantes para que os clientes conectados façam uma transição perfeita entre os servidores de arquivos preferenciais e os de espera durante um evento de failover.

> **Warning**
>
> - Você não deve modificar ou excluir as interfaces de rede elástica associadas ao seu 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.

- As interfaces de rede elástica associadas ao sistema de arquivos terão rotas criadas automaticamente e adicionadas às tabelas de rotas da sub-rede e da VPC padrão. Modificar ou excluir essas rotas pode causar perda temporária ou permanente de conectividade para os clientes do sistema de arquivos.

A seguinte tabela resume os recursos de sub-rede, interface de rede elástica e endereço IP para cada um dos tipos de implantação do sistema de arquivos do FSx para ONTAP:

	Single-AZ (aumento de escala)	Single-AZ (expansão horizontal)	Multi-AZ (aumento de escala)
Número de sub-redes	1	1	2
Número de interfaces de rede elástica	2	2 por par de HA	2
Número de endereços IP por ENI	1 + o número de SVMs no sistema de arquivos	Contagem de pares HA + contagem de pares HA multiplicada pelo número de SVMs no sistema de arquivos	1 + o número de SVMs no sistema de arquivos
Número de rotas da tabela de rotas da VPC	N/D	N/D	1 + o número de SVMs no sistema de arquivos

Depois que um sistema de arquivos ou uma SVM são criados, os endereços IP não mudam até que o sistema de arquivos seja excluído.

Important

O Amazon FSx não é compatível com o acesso a sistemas de arquivos ou com a exposição dos sistemas de arquivos à 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.

Como gerenciar a capacidade de armazenamento

O Amazon FSx for NetApp ONTAP fornece vários recursos relacionados ao armazenamento que você pode usar para gerenciar a capacidade de armazenamento em seu sistema de arquivos.

Tópicos

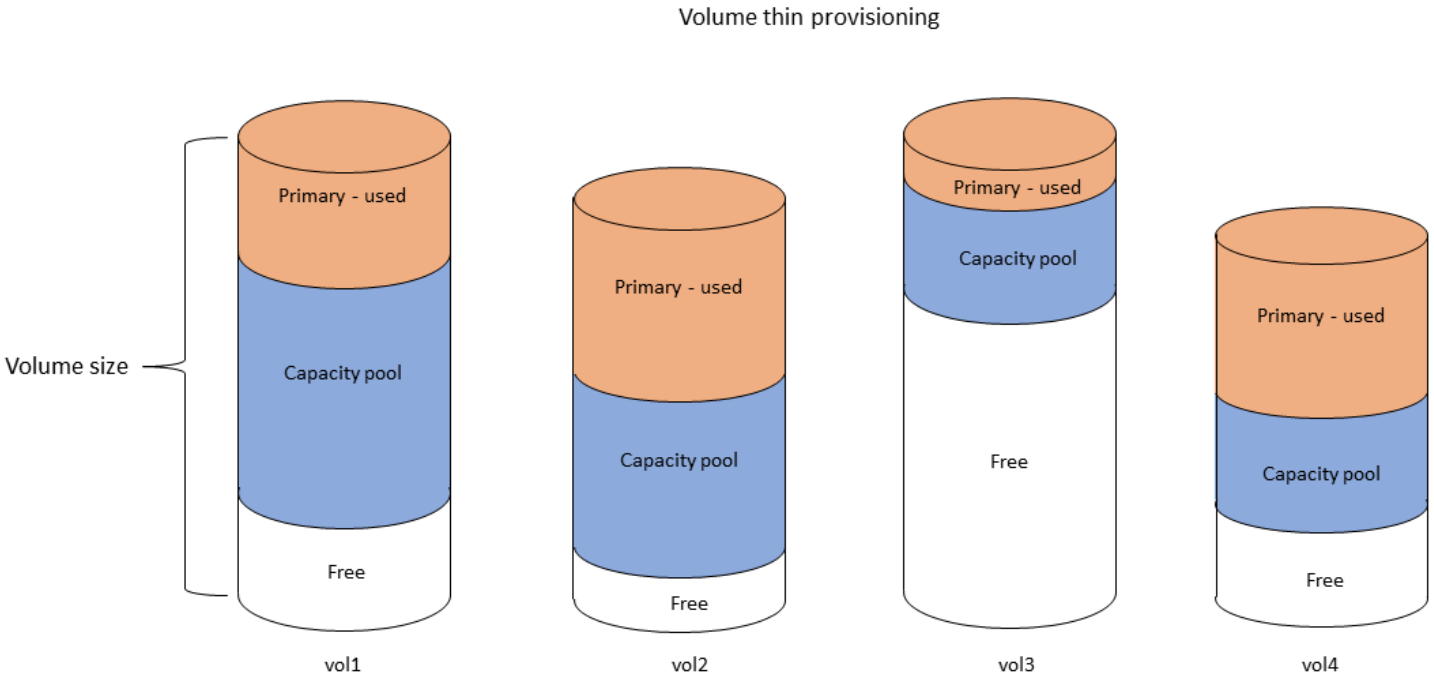
Níveis de armazenamento do FSx para ONTAP

Os níveis de armazenamento são a mídia física de armazenamento de um sistema de arquivos Amazon FSx NetApp for ONTAP. O FSx para ONTAP oferece os seguintes níveis de armazenamento:

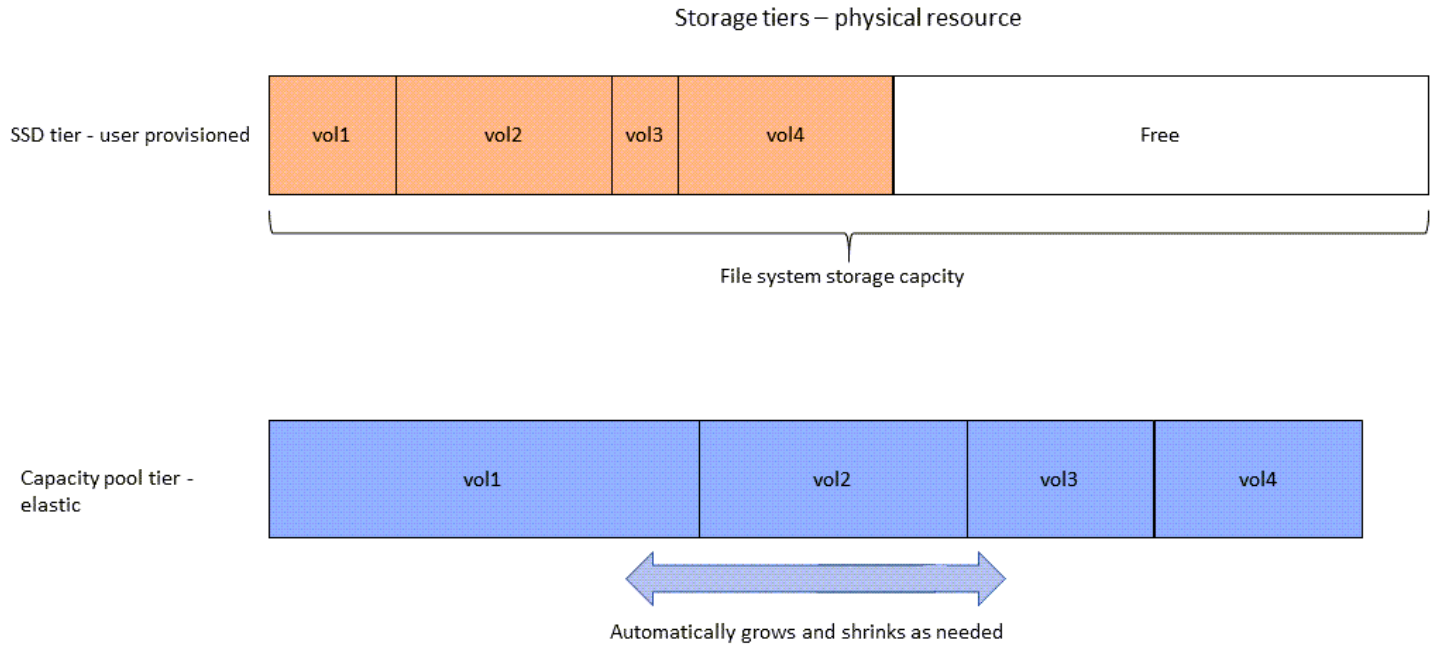
- Nível SSD: o armazenamento em unidade de estado sólido (SSD) de alta performance e provisionado pelo usuário, criado especificamente para a parte ativa do seu conjunto de dados.
- Nível do grupo de capacidade: armazenamento totalmente elástico cujo tamanho é escalado automaticamente para petabytes, sendo otimizado em termos de custo para os dados acessados com pouca frequência.

Um volume do FSx para ONTAP é um recurso virtual que, de modo semelhante às pastas, não consome capacidade de armazenamento. Os dados armazenados, que consomem armazenamento físico, residem em volumes. Ao criar um volume, você especifica o tamanho, que pode ser modificado depois. Os volumes do FSx para ONTAP têm provisionamento reduzido e o armazenamento do sistema de arquivos não é reservado com antecedência. Em vez disso, o armazenamento SSD e do grupo de capacidade são alocados dinamicamente, conforme necessário. Uma política de divisão em níveis, configurada no nível do volume, determina se e quando os dados armazenados no nível SSD fazem a transição para o nível do grupo de capacidade.

O diagrama a seguir ilustra um exemplo de dados dispostos em vários volumes do FSx para ONTAP em um sistema de arquivos.



O diagrama a seguir ilustra como a capacidade de armazenamento físico do sistema de arquivos é consumida pelos dados nos quatro volumes do diagrama anterior.



Você pode reduzir seus custos de armazenamento escolhendo a política de divisão em níveis que melhor atenda aos requisitos de cada volume no sistema de arquivos. Para ter mais informações, consulte Divisão de dados em níveis no volume.

Escolhendo a quantidade certa de armazenamento SSD do sistema de arquivos

Ao escolher a quantidade de capacidade de armazenamento SSD para o sistema de arquivos do FSx para ONTAP, é necessário considerar os seguintes itens que afetam a quantidade de armazenamento SSD disponível para armazenar seus dados:

- Capacidade de armazenamento reservada para a sobrecarga do software NetApp ONTAP.
- Metadados de arquivo
- Dados gravados recentemente
- Arquivos que você pretende armazenar no armazenamento SSD, sejam eles dados que não atingiram o período de resfriamento ou dados lidos recentemente e que foram recuperados no SSD.

Como o armazenamento SSD é usado

O armazenamento SSD do seu sistema de arquivos é usado para uma combinação do software NetApp ONTAP (sobrecarga), metadados de arquivos e seus dados.

NetApp Sobrecarga do software ONTAP

Como outros sistemas de arquivos NetApp ONTAP, até 16% da capacidade de armazenamento SSD de um sistema de arquivos é reservada para a sobrecarga do ONTAP, o que significa que ele não está disponível para armazenar seus arquivos. A sobrecarga do ONTAP é alocada da seguinte forma:

- 11% é reservado para o software NetApp ONTAP. Para sistemas de arquivos com mais de 30 tebibytes (TiB) de capacidade de armazenamento SSD, 6% são reservados.
- 5% são reservados para snapshots agregados, necessários na sincronização de dados entre os dois servidores de arquivos do sistema de arquivos.

Metadados de arquivo

Os metadados de arquivos normalmente consomem de 3 a 7% da capacidade de armazenamento consumida pelos arquivos. Essa porcentagem depende do tamanho médio do arquivo (um tamanho

médio de arquivo menor requer mais metadados) e da quantidade de economia com a eficiência de armazenamento obtida nos arquivos. Observe que os metadados do arquivo não se beneficiam da economia com a eficiência de armazenamento. Você pode usar as diretrizes a seguir para estimar a quantidade de armazenamento SSD usada para os metadados no sistema de arquivos.

Tamanho médio do arquivo	Tamanho dos metadados como porcentagem dos dados do arquivo
4 KB	7%
8 KB	3,5%
32 KB ou maior	1-3%

Ao dimensionar a quantidade de capacidade de armazenamento SSD necessária para os metadados dos arquivos que planeja armazenar no nível do grupo de capacidade, recomendamos usar uma proporção conservadora de 1 GiB de armazenamento SSD para cada 10 GiB de dados que planeja armazenar no nível do grupo de capacidade.

Dados de arquivos armazenados no nível SSD

Além do conjunto de dados ativo e de todos os metadados do arquivo, todos os dados gravados no sistema de arquivos são inicialmente gravados no nível SSD antes de serem divididos em níveis para o armazenamento do grupo de capacidade. Isso é verdade independentemente da política de classificação por níveis do volume, com exceção da transferência de dados SnapMirror para um volume configurado com uma política de todos os dados em camadas.

As leituras aleatórias do nível do grupo de capacidade são armazenadas em cache no nível SSD, desde que ele esteja abaixo de 90% de utilização. Para ter mais informações, consulte Divisão de dados em níveis no volume.

Utilização recomendada da capacidade do SSD

Recomendamos que você não exceda 80% de utilização do nível de armazenamento SSD de forma contínua. Para sistemas de arquivos escaláveis, também recomendamos que você não exceda 80% de utilização contínua de nenhum dos agregados do seu sistema de arquivos. Essas recomendações são consistentes com NetApp a recomendação do ONTAP. Como o nível SSD do sistema de arquivos também é usado para preparar gravações e leituras aleatórias do nível do grupo

de capacidade, qualquer mudança repentina nos padrões de acesso pode fazer com que a utilização do nível SSD aumente rapidamente.

Com 90% de utilização do SSD, os dados lidos do nível do grupo de capacidade não são mais armazenados em cache no nível SSD, de modo que a capacidade restante do SSD seja preservada para quaisquer novos dados gravados no sistema de arquivos. Isso faz com que as leituras repetidas dos mesmos dados do nível do grupo de capacidade sejam lidas no armazenamento do grupo de capacidade em vez de serem armazenadas em cache e lidas no nível SSD, o que pode afetar a capacidade de throughput do sistema de arquivos.

Toda a funcionalidade de divisão em níveis é interrompida quando o nível SSD atinge ou ultrapassa 98% de utilização. Para ter mais informações, consulte Limites de divisão em níveis.

Eficiência de armazenamento do FSx para ONTAP

NetApp O ONTAP oferece recursos de eficiência de armazenamento em nível de bloco, incluindo compactação, compactação e desduplicação, que podem economizar até 65% na capacidade de armazenamento para compartilhamentos gerais de arquivos, sem sacrificar o desempenho.

O Amazon FSx for NetApp ONTAP também oferece suporte a outros recursos do ONTAP que economizam espaço, incluindo snapshots, provisionamento reduzido e volumes. FlexClone

Os recursos de eficiência de armazenamento não estão habilitados por padrão. É possível habilitá-los dos modos a seguir.

- No volume raiz de uma SVM, ao criar um sistema de arquivos.
- Ao criar um volume.
- Ao modificar um volume existente.

Para ver a quantidade de economia de armazenamento em um sistema de arquivos com a eficiência de armazenamento ativada, consulteVisualizando a economia de eficiência de armazenamento.

Calculando a economia de eficiência de armazenamento

Você pode usar as métricas do sistema de CloudWatch arquivos `LogicalDataStored` e `StorageUsed` FSx for ONTAP para calcular a economia de armazenamento com compactação, desduplicação, compactação, instantâneos e. FlexClones Essas métricas têm `FileSystemId` como única dimensão. Para ter mais informações, consulte Métricas do sistema de arquivos.

- Para computar a economia com a eficiência de armazenamento em bytes, pegue a média de `StorageUsed` em um determinado período e subtraia da média de `LogicalDataStored` do mesmo período.
- Para computar a economia com a eficiência do armazenamento como uma porcentagem do tamanho lógico total dos dados, pegue a `Average` de `StorageUsed` em um determinado período e subtraia da `Average` de `LogicalDataStored` no mesmo período. Em seguida, divida a diferença pela `Average` de `LogicalDataStored` no mesmo período.

Exemplo de dimensionamento do SSD

Suponha que você queira armazenar 100 TiB de dados para uma aplicação em que 80% dos dados são acessados com pouca frequência. Nesse cenário, 80% (80 TB) dos seus dados são automaticamente divididos em níveis no nível do grupo de capacidade e os 20% restantes (20 TB) permanecem no armazenamento SSD. Com base na economia típica de 65% com a eficiência de armazenamento para workloads de compartilhamento de arquivos de uso geral, isso equivale a 7 TiB de dados. Para manter uma taxa de utilização de 80% do SSD, você precisa de 8,75 TiB de capacidade de armazenamento SSD para os 20 TiB de dados acessados ativamente. A quantidade provisionada de armazenamento SSD também precisa considerar a sobrecarga de 16% de armazenamento do software ONTAP, conforme mostrado no cálculo a seguir.

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

Portanto, neste exemplo, é necessário provisionar pelo menos 10,42 TiB de armazenamento SSD. Você também usará 28 TiB de armazenamento do grupo de capacidade para os 80 TiB restantes de dados acessados com pouca frequência.

Capacidade de armazenamento do sistema de arquivos e IOPS

Ao criar um sistema de arquivos do FSx para ONTAP, você especifica a capacidade de armazenamento do nível SSD. Para sistemas de arquivos escaláveis, a capacidade de armazenamento especificada é distribuída uniformemente entre os pools de armazenamento de cada par de alta disponibilidade (HA); esses pools de armazenamento são chamados de agregados.

Para cada GiB de armazenamento provisionado do SSD, o Amazon FSx provisiona automaticamente três operações de entrada e saída por segundo (IOPS) para o sistema de arquivos, até um máximo

de 160.000 IOPS de SSD por sistema de arquivos. Para sistemas de arquivos escaláveis, suas IOPS de SSD são distribuídas uniformemente em cada um dos agregados do seu sistema de arquivos. Você tem a opção de especificar um nível de IOPS de SSD provisionado acima das três IOPS de SSD automáticos por GiB. Para obter mais informações sobre o número máximo de IOPS de SSD que você pode provisionar para o sistema de arquivos do FSx para ONTAP, consulte Impacto da capacidade de throughput na performance.

Tópicos

Atualizando o armazenamento SSD e o IOPS do sistema de arquivos

Quando precisar de armazenamento adicional para a parte ativa do seu conjunto de dados, você pode aumentar a capacidade de armazenamento SSD do seu sistema de arquivos Amazon FSx NetApp for ONTAP. Use o console Amazon FSx, a API Amazon FSx ou AWS Command Line Interface (AWS CLI) para aumentar a capacidade de armazenamento SSD. Para ter mais informações, consulte Modificando a capacidade de armazenamento SSD e o IOPS provisionado.

Ao aumentar a capacidade de armazenamento SSD do sistema de arquivos do Amazon FSx, a nova capacidade normalmente fica disponível para uso em minutos. Será gerada uma cobrança pela nova capacidade de armazenamento SSD depois que ela estiver disponível para você. Para obter mais informações sobre preços, consulte Amazon FSx for NetApp ONTAP Pricing.

Depois de aumentar sua capacidade de armazenamento, o Amazon FSx executa um processo de otimização de armazenamento em segundo plano para reequilibrar seus dados. Na maioria dos sistemas de arquivos, a otimização do armazenamento leva algumas horas, com um impacto mínimo perceptível na performance da workload.

Acompanhe o progresso do processo de otimização do armazenamento a qualquer momento usando o console do Amazon FSx, a CLI e a API. Para ter mais informações, consulte Monitorar as atualizações da capacidade de armazenamento e das IOPS.

Considerações

Aqui estão alguns itens importantes a serem considerados ao modificar a capacidade de armazenamento SSD e as IOPS provisionadas de um sistema de arquivos:

- Somente o aumento da capacidade de armazenamento: só é possível aumentar a quantidade da capacidade de armazenamento SSD de um sistema de arquivos; não é possível diminuir a capacidade de armazenamento.
- Aumento mínimo da capacidade de armazenamento — Cada aumento na capacidade de armazenamento SSD deve ser no mínimo 10% da capacidade atual de armazenamento SSD do sistema de arquivos, até a capacidade máxima de armazenamento SSD para a configuração do seu sistema de arquivos.
- (Somente expansão horizontal) Distribuição da capacidade de armazenamento — A nova capacidade de armazenamento ou SSD IOPS que você seleciona para seu sistema de arquivos é distribuída uniformemente em cada um dos agregados do sistema de arquivos.
- Tempo entre aumentos: após modificar a capacidade de armazenamento SSD, as IOPS provisionadas ou a capacidade de throughput em um sistema de arquivos, aguarde pelo menos seis horas antes de modificar qualquer uma dessas configurações no mesmo sistema de arquivos novamente. Às vezes isso é referenciado como período de desaquecimento.
- Modos de IOPS provisionadas: para uma alteração das IOPS provisionadas, especifique um dos dois modos de IOPS a seguir.
  - Modo automático — O Amazon FSx escala automaticamente suas IOPS de SSD para manter 3 IOPS de SSD provisionadas por GiB de capacidade de armazenamento de SSD, até o máximo de IOPS de SSD para sua configuração de sistema de arquivos.

    > **Note**
    >
    > Para obter mais informações sobre o número máximo de IOPS de SSD que você pode provisionar para o sistema de arquivos do FSx para ONTAP, consulte Impacto da capacidade de throughput na performance.

  - Modo provisionado pelo usuário: você especifica o número de IOPS de SSD, que deve ser maior ou igual a três IOPS por GiB de capacidade de armazenamento SSD. Se você optar por provisionar um nível mais alto de IOPS, pagará pela média de IOPS provisionadas acima da taxa incluída no mês, medida em meses de IOPS.

Para obter mais informações sobre preços, consulte Amazon FSx for NetApp ONTAP Pricing.

Quando aumentar a capacidade de armazenamento SSD

Se você estiver ficando sem armazenamento de nível SSD disponível, recomendamos aumentar a capacidade de armazenamento do sistema de arquivos. A falta de armazenamento indica que seu nível SSD está subdimensionado para a parte ativa do seu conjunto de dados.

Para monitorar a quantidade de armazenamento gratuito disponível no sistema de arquivos, use o nível do sistema de arquivos e as métricas `StorageCapacity` da `StorageUsed` Amazon CloudWatch . Você pode criar um CloudWatch alarme em uma métrica e ser notificado quando ela cair abaixo de um limite específico. Para ter mais informações, consulte Monitoramento com a Amazon CloudWatch.

> **Note**
>
> Recomendamos que você não exceda 80% de utilização da capacidade de armazenamento SSD, para garantir que a divisão de dados em níveis, a escalabilidade do throughput e outras atividades de manutenção funcionem adequadamente, além de que haja capacidade disponível para dados adicionais. Para sistemas de arquivos escaláveis, essa recomendação se aplica tanto à utilização média em todos os agregados do seu sistema de arquivos quanto a cada agregado individual.

Para obter mais informações sobre como o armazenamento SSD de um sistema de arquivos é usado e a quantidade de armazenamento SSD reservada para metadados de arquivos e software operacional, consulte Escolhendo a quantidade certa de armazenamento SSD do sistema de arquivos.

Monitorando a utilização do armazenamento SSD

Você pode monitorar a utilização da capacidade de armazenamento SSD do seu sistema de arquivos usando uma variedade de ferramentas AWS . NetApp Usando a Amazon, CloudWatch você pode monitorar a utilização da capacidade de armazenamento e definir alarmes para alertá-lo quando a utilização da capacidade de armazenamento atingir um limite personalizável.

> **Note**
>
> Recomendamos que você não exceda 80% da utilização da capacidade de armazenamento do seu nível de armazenamento SSD. Isso garante que a divisão em níveis funcione adequadamente e fornece sobrecarga para novos dados. Se nível de armazenamento SSD estiver consistentemente acima de 80% de utilização da capacidade de armazenamento, você poderá aumentar a capacidade do nível de armazenamento SSD. Para ter mais informações, consulte Atualizando o armazenamento SSD e o IOPS do sistema de arquivos.

Você pode ver o armazenamento SSD disponível em um sistema de arquivos e a distribuição geral do armazenamento no console do Amazon FSx. O gráfico Capacidade de armazenamento SSD disponível exibe a quantidade de capacidade de armazenamento baseada em SSD disponível em um sistema de arquivos ao longo do tempo. O gráfico Distribuição de armazenamento mostra como a capacidade geral de armazenamento de um sistema de arquivos está atualmente distribuída em três categorias:

- Nível do grupo de capacidade
- Nível SSD disponível
- Nível SSD usado

Você pode monitorar a utilização da capacidade de armazenamento SSD do seu sistema de arquivos no AWS Management Console, usando o procedimento a seguir.

Para monitorar a capacidade de armazenamento de nível SSD disponível no sistema de arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha Sistemas de arquivos na coluna de navegação à esquerda e, em seguida, escolha o sistema de ONTAP arquivos do qual você deseja visualizar as informações de capacidade de armazenamento. A página de detalhes do sistema de arquivos é exibida.
3. No segundo painel, escolha a guia Monitoramento e desempenho e, em seguida, escolha Armazenamento. Os gráficos de capacidade de armazenamento primário disponível e Utilização da capacidade de armazenamento por agregado são exibidos.

Criando um alarme de utilização da capacidade de armazenamento do sistema de arquivos

Recomendamos que você não exceda, de forma contínua, uma utilização média de 80% da capacidade de armazenamento SSD. Picos ocasionais de utilização do armazenamento SSD acima de 80% são aceitáveis. Manter uma utilização média abaixo de 80% fornece capacidade suficiente para aumentar seu armazenamento sem encontrar problemas. O procedimento a seguir mostra como criar um CloudWatch alarme que alerta quando a utilização do armazenamento SSD do seu sistema de arquivos está se aproximando de 80%.

Para criar um alarme SCU do sistema de arquivos

Você pode usar a `StorageCapacityUtilization` métrica para criar um alarme que é acionado quando um ou mais de seus sistemas de arquivos FSx for ONTAP atingem um limite de utilização de armazenamento.

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação esquerdo, em Alarmes, escolha Todos os alarmes. Em seguida, escolha Criar alarme. No assistente de criação de alarme, escolha Selecionar métrica.
3. No explorador de gráficos, escolha a guia Consulta de várias fontes.
4. No criador de consultas, escolha o seguinte:
   - Para Namespace, selecione AWS/FSX > Métricas detalhadas do sistema de arquivos.
   - Em Nome da métrica, selecione MAX (StorageCapacityUtilization).
   - Em Filtrar por, você pode, opcionalmente, incluir ou excluir sistemas de arquivos específicos por sua ID. Se você deixar Filtrar por vazio, seu alarme será acionado quando qualquer um dos seus sistemas de arquivos exceder o limite de utilização da capacidade de armazenamento do alarme.
   - Deixe o resto das opções vazias e escolha Consulta gráfica.
5. Escolha Selecionar métrica. De volta ao assistente, na seção Métrica, atribua um rótulo à sua métrica. Recomendamos manter o Período em 5 minutos.
6. Em Condições, escolha o tipo de limite estático, sempre que sua métrica for Maior/Igual a 80.
7. Escolha Avançar para ir até a página Configurar ações.

Para configurar ações de alarme

Você pode configurar uma variedade de ações para que seu alarme seja acionado quando atingir o limite que você configurou. Neste exemplo, escolhemos um tópico do Simple Notification Service (SNS), mas você pode aprender sobre outras ações em Usando CloudWatch alarmes da Amazon no Guia do usuário da Amazon. CloudWatch

1. Na seção Notificação, escolha um tópico do SNS para notificar quando o alarme estiver no `ALARM` estado. Você pode escolher um tópico existente ou criar um novo. Você receberá uma notificação de assinatura que precisa confirmar antes de receber notificações de alarme no endereço de e-mail.
2. Escolha Próximo.

Para finalizar o alarme

Siga estas instruções para concluir o processo de criação do CloudWatch alarme.

1. Na página Adicionar nome e descrição, dê um nome ao alarme e, opcionalmente, uma descrição e escolha Avançar.
2. Revise tudo o que você configurou na página Visualizar e criar e, em seguida, escolha Criar alarme.

Visualizando a economia de eficiência de armazenamento

Quando ativado, você pode ver quanta capacidade de armazenamento está economizando no console Amazon FSx, no console da Amazon e na CloudWatch CLI do ONTAP.

Para ver a economia de eficiência de armazenamento (console)

A economia de eficiência de armazenamento exibida no console Amazon FSx para um sistema de arquivos FSx for ONTAP inclui a economia de e. FlexClones SnapShots

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha o sistema de arquivos do FSx para ONTAP para o qual deseja visualizar a economia com a eficiência de armazenamento na lista de Sistemas de arquivos.
3. Escolha Resumo na guia Monitoramento e desempenho no segundo painel na página de detalhes do sistema de arquivos.

4. O gráfico Economia com a eficiência de armazenamento mostra quanto espaço está sendo economizado como uma porcentagem do tamanho lógico dos dados e em bytes físicos.

Para ver a economia de eficiência de armazenamento (ONTAPCLI)

Você pode ver a economia de eficiência de armazenamento decorrente apenas da compactação, compactação e desduplicação — sem os efeitos dos instantâneos FlexClones — executando o comando `storage aggregate show-efficiency` usando a CLI. ONTAP Para obter mais informações, consulte a demonstração de eficiência agregada de armazenamento no Centro de Documentação. NetApp ONTAP

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.
2. O storage aggregate show-efficiency comando exibe informações sobre a eficiência de armazenamento de todos os agregados. A eficiência do armazenamento é exibida em quatro níveis diferentes:

   - Total
   - Agregar
   - Volume
   - Instantâneo e volume FlexClone

   ```
   ::*> aggr show-efficiency

   Aggregate: aggr1
        Node: node1

   Total Data Reduction Efficiency Ratio:  3.29:1
   Total Storage Efficiency Ratio:         4.29:1
   Aggregate: aggr2
   ```

```
     Node: node1

Total Data Reduction Efficiency Ratio:  4.50:1
Total Storage Efficiency Ratio:         5.49:1

cluster::*> aggr show-efficiency -details

Aggregate: aggr1
     Node: node1

Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1

Aggregate: aggr2
     Node: node1
Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1
```

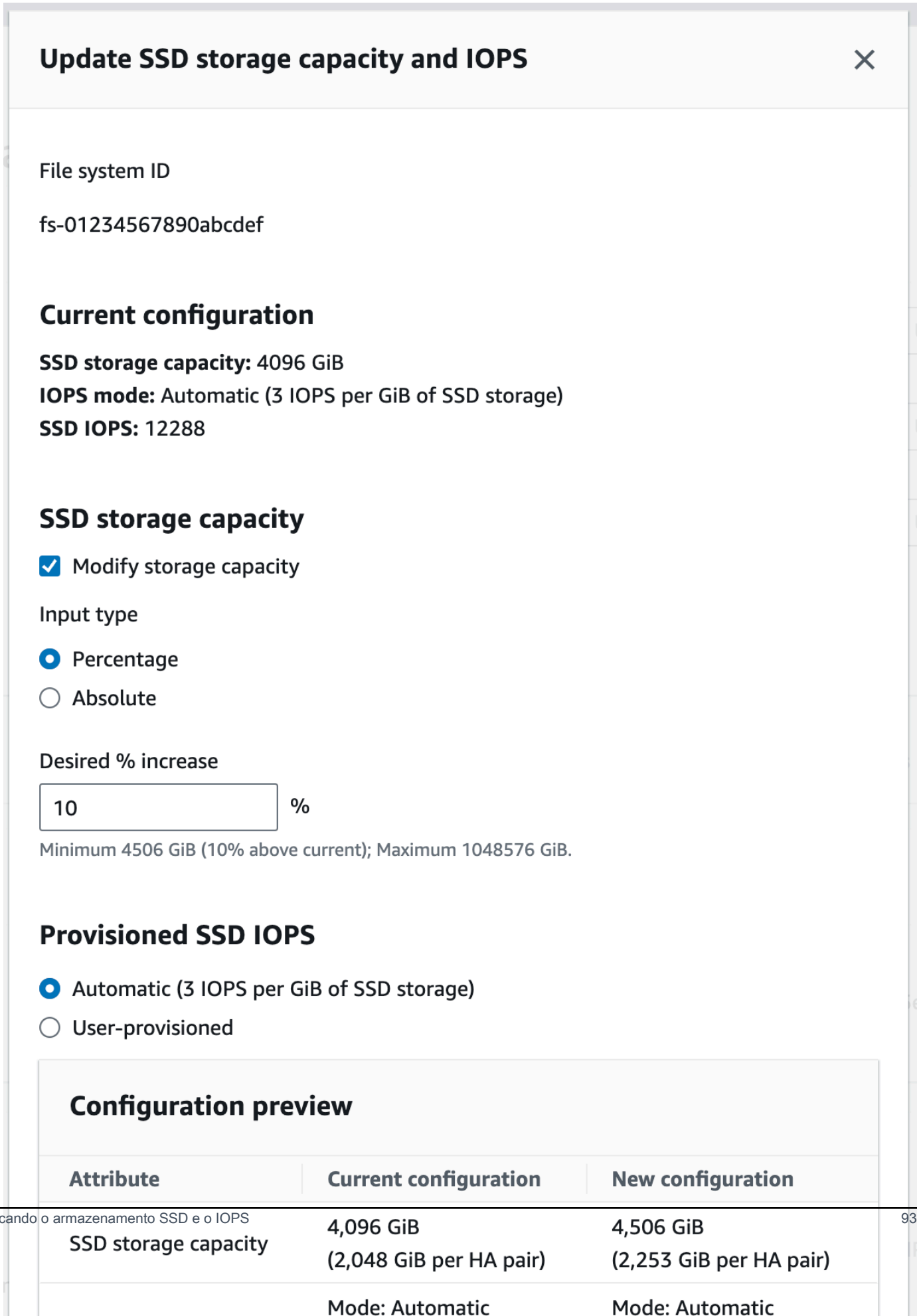
Modificando a capacidade de armazenamento SSD e o IOPS provisionado

Você pode aumentar o armazenamento baseado em SSD de um sistema de arquivos e aumentar ou diminuir a quantidade de IOPS de SSD provisionadas usando o console Amazon FSx, o e a API. AWS CLI

Para atualizar a capacidade de armazenamento SSD ou o IOPS provisionado para um sistema de arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Sistemas de arquivos. Na lista Sistemas de arquivos, selecione o sistema de arquivos do FSx para ONTAP para o qual você deseja atualizar a capacidade de armazenamento SSD e as IOPS de SSD.
3. Escolha Ações > Atualizar capacidade de armazenamento. Como alternativa, na seção Resumo, escolha Atualizar ao lado do valor da Capacidade de armazenamento SSD do sistema de arquivos.

   A caixa de diálogo Atualizar capacidade de armazenamento SSD e IOPS é exibida.



Update SSD storage capacity and IOPS

File system ID

fs-01234567890abcdef

Current configuration

SSD storage capacity: 4096 GiB
IOPS mode: Automatic (3 IOPS per GiB of SSD storage)
SSD IOPS: 12288

SSD storage capacity

Modify storage capacity

Input type

Percentage

Absolute

Desired % increase

10 %

Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.

Provisioned SSD IOPS

Automatic (3 IOPS per GiB of SSD storage)

User-provisioned

Configuration preview

Attribute	Current configuration	New configuration
SSD storage capacity	4,096 GiB (2,048 GiB per HA pair)	4,506 GiB (2,253 GiB per HA pair)
	Mode: Automatic	Mode: Automatic

4. Para aumentar a capacidade de armazenamento SSD, escolha Modificar capacidade de armazenamento.
5. Em Tipo de entrada, selecione uma das opções a seguir.
   - Para inserir a nova capacidade de armazenamento SSD como uma alteração percentual em relação ao valor atual, escolha Porcentagem.
   - Para inserir o novo valor em GiB, escolha Absoluto.
6. Dependendo do tipo de entrada, insira um valor em % de aumento desejado.
   - Em Porcentagem, insira o valor do aumento percentual. Esse valor deve ser pelo menos 10% maior que o valor atual.
   - Em Absoluto, insira o novo valor em GiB, até o valor máximo permitido de 196.608 GiB.
7. Em IOPS provisionadas de SSD, você tem as duas opções a seguir para modificar o número de IOPS provisionadas de SSD do sistema de arquivos.
   - Se você quiser que o Amazon FSx escale automaticamente suas IOPS de SSD para manter três IOPS provisionadas de SSD por GiB de capacidade de armazenamento SSD (até um máximo de 160.000), escolha Automático.
   - Se quiser especificar o número de IOPS de SSD, escolha Provisionado pelo usuário. Insira um número absoluto de IOPS que seja, pelo menos, três vezes a quantidade de GiB do nível de armazenamento SSD e menor ou igual a 160.000.

   > **Note**
   >
   > Para obter mais informações sobre o número máximo de IOPS de SSD que você pode provisionar para o sistema de arquivos do FSx para ONTAP, consulte Impacto da capacidade de throughput na performance.

8. Escolha Atualizar.

   > **Note**
   >
   > Na parte inferior do prompt, uma prévia da configuração é exibida para sua nova capacidade de armazenamento SSD e SSD IOPS. Para sistemas de arquivos escaláveis, o valor por par de HA também é mostrado.

Para atualizar a capacidade de armazenamento SSD e o IOPS provisionado para um sistema de arquivos (CLI)

Para atualizar a capacidade de armazenamento SSD e as IOPS provisionadas para um sistema de arquivos FSx for ONTAP, use o comando ou a AWS CLI ação de API equivalente. update-file-systemUpdateFileSystem Defina os seguintes parâmetros com seus valores:

- Defina `--file-system-id` como o ID do sistema de arquivos que está sendo atualizado.
- Para aumentar sua capacidade de armazenamento SSD, `--storage-capacity` defina o valor da capacidade de armazenamento de destino, que deve ser pelo menos 10% maior do que o valor atual.
- Para modificar as IOPS provisionadas de SSD, use a propriedade `--ontap-configuration DiskIopsConfiguration`. Essa propriedade tem dois parâmetros, `Iops` e `Mode`:
  - Se quiser especificar o número de IOPS provisionadas, use `Iops=`*`number_of_IOPS`* (até um máximo de 160.000) e `Mode=USER_PROVISIONED`. O valor de IOPS deve ser maior ou igual a três vezes a capacidade de armazenamento SSD solicitada. Se você não estiver aumentando a capacidade de armazenamento, o valor de IOPs deve ser maior ou igual a três vezes a capacidade atual de armazenamento SSD.
  - Se quiser que o Amazon FSx aumente automaticamente as IOPS de SSD, use `Mode=AUTOMATIC` e não use o parâmetro `Iops`. O Amazon FSx manterá automaticamente 3 SSD IOPS por GiB da capacidade de armazenamento SSD provisionada (até um máximo de 160.000).

> **Note**
>
> Para obter mais informações sobre o número máximo de IOPS de SSD que você pode provisionar para o sistema de arquivos do FSx para ONTAP, consulte Impacto da capacidade de throughput na performance.

O exemplo a seguir aumenta o armazenamento SSD do sistema de arquivos para 2.000 GiB e define a quantidade de IOPS SSD provisionadas pelo usuário como 7000.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 2000 \
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

Para monitorar o progresso da atualização, use o describe-file-systems AWS CLI comando. Procure a seção `AdministrativeActions` na saída.

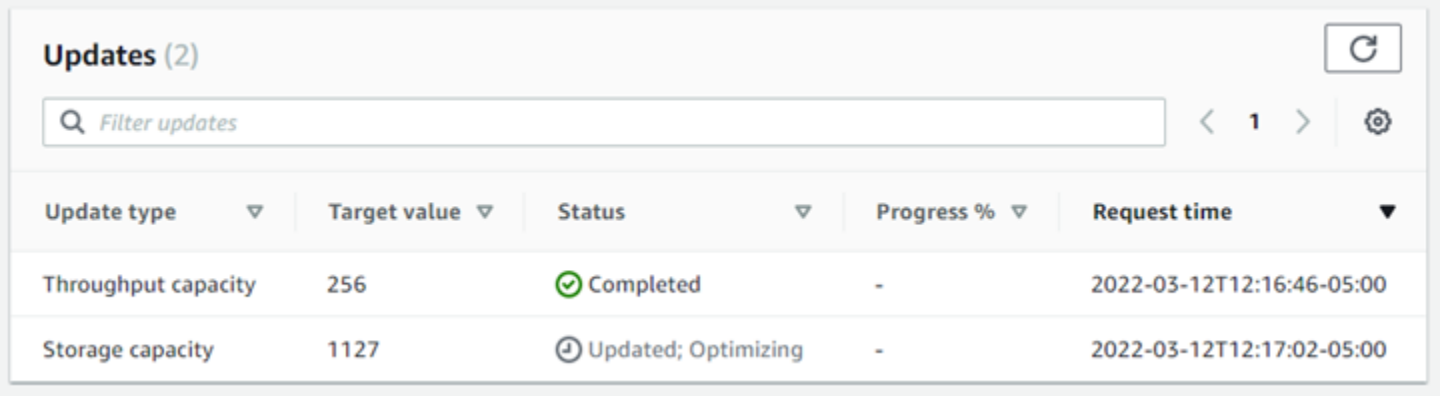
Para obter mais informações, consulte a AdministrativeActionreferência da API Amazon FSx for NetApp ONTAP.

Monitorar as atualizações da capacidade de armazenamento e das IOPS

Você pode monitorar o progresso da capacidade de armazenamento SSD e da atualização de IOPS usando o console, a CLI e a API do Amazon FSx.

Para monitorar o armazenamento e as atualizações de IOPS (console)

Na guia Atualizações na página Detalhes do sistema de arquivos do FSx para ONTAP, você visualiza as dez atualizações mais recentes para cada tipo de atualização.



Para atualizações da capacidade de armazenamento SSD e das IOPS, você pode ver as informações a seguir.

Tipo de atualização

Os tipos compatíveis são Capacidade de armazenamento, Modo e IOPS. Os valores de Modo e IOPS são listados para todas as solicitações de capacidade de armazenamento e escalabilidade de IOPS.

Target value (Valor de destino)

O valor especificado para atualizar a capacidade de armazenamento SSD ou as IOPS do sistema de arquivos.

Status

O status atual da atualização. Os valores possíveis são:

- Pendente: o Amazon FSx recebeu a solicitação de atualização, mas ainda 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 SSD do sistema de arquivos. Agora, o processo de otimização do armazenamento está reequilibrando seus dados em segundo plano.
- Concluída: a atualização foi concluída com êxito.
- Falha: a solicitação de atualização falhou. Escolha o ponto de interrogação (?) para ver os detalhes.

% 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.

Para monitorar o armazenamento e as atualizações de IOPS (CLI)

Você pode visualizar e monitorar as solicitações de aumento da capacidade de armazenamento SSD do sistema de arquivos usando o describe-file-systems AWS CLI comando e a operação 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 SSD de um sistema de arquivos, duas ações `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 ação administrativa pendente para aumentar a capacidade de armazenamento SSD para 2.000 GiB e as IOPS provisionadas de SSD para 7.000 GiB.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
```

```
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
             }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1586797629.095,
        "Status": "PENDING"
    }
]
```

O Amazon FSx processa primeiro a ação `FILE_SYSTEM_UPDATE`, adicionando os novos discos de armazenamento maiores 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`. Esse comportamento é mostrado a seguir, no trecho da resposta de um comando de CLI `describe-file-systems`.

A propriedade `ProgressPercent` exibe o progresso do processo de otimização do armazenamento. Após o processo de otimização do armazenamento ser concluído com êxito, o status da ação `FILE_SYSTEM_UPDATE` mudará para `COMPLETED`, e a ação `STORAGE_OPTIMIZATION` não aparecerá mais.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586799169.445,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        }
```

```
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "ProgressPercent": 41,
        "RequestTime": 1586799169.445,
        "Status": "IN_PROGRESS"
    }
]
```

Se a solicitação de atualização da capacidade de armazenamento ou das IOPS falhar, o status da ação `FILE_SYSTEM_UPDATE` mudará para `FAILED`, conforme mostrado no exemplo a seguir. a propriedade `FailureDetails` fornece informações sobre a falha.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586373915.697,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

Como aumentar a capacidade de armazenamento SSD de forma dinâmica

Use a solução a seguir para aumentar dinamicamente a capacidade de armazenamento SSD de um sistema de arquivos do FSx para ONTAP quando a quantidade de capacidade de armazenamento SSD usada exceder um limite especificado por você. Esse AWS CloudFormation modelo implanta automaticamente todos os componentes necessários para definir o limite de capacidade de armazenamento, o CloudWatch alarme da Amazon com base nesse limite e a AWS Lambda função que aumenta a capacidade de armazenamento do sistema de arquivos.

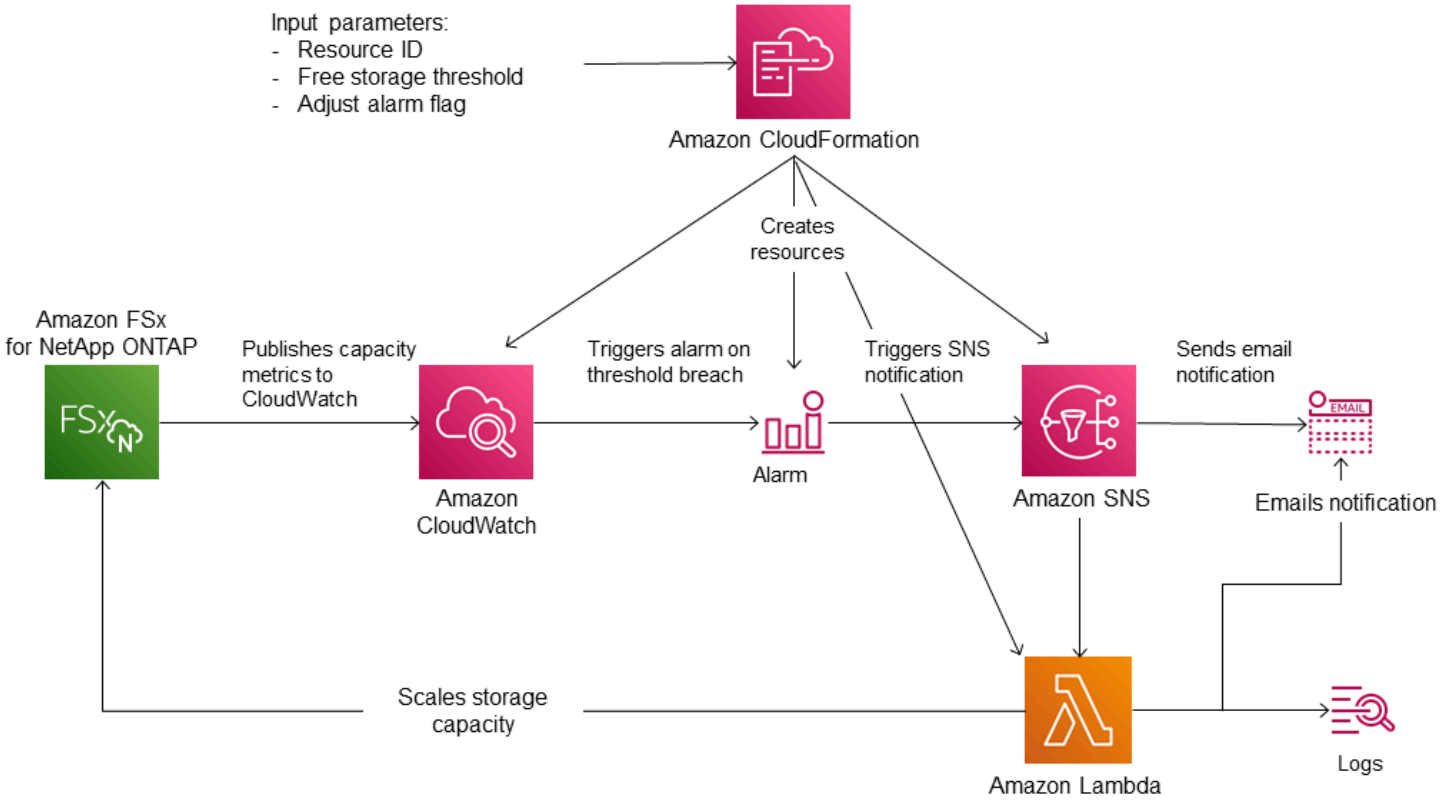
A solução implanta automaticamente todos os componentes necessários e usa os parâmetros a seguir.

- Seu ID do sistema de arquivos do FSx para ONTAP.
- O limite da capacidade de armazenamento SSD usada (valor numérico). Essa é a porcentagem na qual o CloudWatch alarme será acionado.
- A porcentagem pela qual aumentar a capacidade de armazenamento (%).
- O endereço de e-mail usado para receber notificações de escalabilidade.

Tópicos

Visão geral da arquitetura

A implantação dessa solução cria os recursos apresentados a seguir na Nuvem AWS.



O diagrama ilustra as seguintes etapas:

1. O AWS CloudFormation modelo implanta um CloudWatch alarme, uma AWS Lambda função, uma fila do Amazon Simple Notification Service (Amazon SNS) e todas as funções necessárias (IAM). AWS Identity and Access Management O perfil do IAM concede à função do Lambda permissão para invocar as operações de API do Amazon FSx.
2. CloudWatch aciona um alarme quando a capacidade de armazenamento usada pelo sistema de arquivos excede o limite especificado e envia uma mensagem para a fila do Amazon SNS. Um alarme é acionado somente quando a capacidade usada pelo sistema de arquivos excede continuamente o limite por um período de cinco minutos.
3. Em seguida, a solução aciona a função do Lambda que está inscrita nesse tópico do Amazon SNS.
4. A função do Lambda calcula a nova capacidade de armazenamento do sistema de arquivos com base no valor percentual de aumento especificado e define a nova capacidade de armazenamento do sistema de arquivos.
5. O estado original do CloudWatch alarme e os resultados das operações da função Lambda são enviados para a fila do Amazon SNS.

Para receber notificações sobre as ações que são executadas como resposta ao CloudWatch alarme, você deve confirmar a assinatura do tópico do Amazon SNS seguindo o link fornecido no e-mail de confirmação da assinatura.

AWS CloudFormation modelo

Essa solução é usada AWS CloudFormation para automatizar a implantação dos componentes usados para aumentar automaticamente a capacidade de armazenamento de um sistema de arquivos FSx for ONTAP. Para usar essa solução, baixe o SxOntapDynamicStorageScaling AWS CloudFormation modelo F.

O modelo usa os Parâmetros descritos a seguir. Revise os parâmetros do modelo e seus valores padrão, modificando-os de acordo com as necessidades do seu sistema de arquivos.

FileSystemId

Nenhum valor padrão. O ID do sistema de arquivos para o qual você deseja aumentar automaticamente a capacidade de armazenamento.

LowFreeDataStorageCapacityThreshold

Nenhum valor padrão. Especifica o limite da capacidade de armazenamento usado, no qual acionar um alarme e aumentar automaticamente a capacidade de armazenamento do sistema de arquivos, definido como porcentagem (%) da capacidade de armazenamento atual do sistema de arquivos. Considera-se que o sistema de arquivos tem baixa capacidade de armazenamento livre quando o armazenamento usado excede esse limite.

EmailAddress

Nenhum valor padrão. Especifica o endereço de e-mail a ser usado para a assinatura do SNS e recebe os alertas de limite da capacidade de armazenamento.

PercentIncrease

O padrão é 20%. Especifica a quantidade pela qual aumentar a capacidade de armazenamento, expressa como uma porcentagem da capacidade de armazenamento atual.

> **Note**
>
> O escalonamento do armazenamento é tentado uma vez toda vez que o CloudWatch alarme entra no `ALARM` estado. Se a utilização da capacidade de armazenamento SSD permanecer acima do limite após uma tentativa de operação de escalabilidade de armazenamento, não será feita uma nova tentativa dessa operação.

Máximo F B SxSizeinGi

O padrão é 196608. Especifica a capacidade máxima de armazenamento compatível com o armazenamento SSD.

Implantação automatizada com AWS CloudFormation

O procedimento a seguir configura e implanta uma AWS CloudFormation pilha para aumentar automaticamente a capacidade de armazenamento de um sistema de arquivos FSx for ONTAP. A implantação leva alguns minutos. Para obter mais informações sobre a criação de uma CloudFormation pilha, consulte Como criar uma pilha no AWS CloudFormation console no Guia do AWS CloudFormation usuário.

> **Note**
>
> A implementação dessa solução gera cobrança pelos serviços associados AWS . Para obter mais informações, consulte as páginas de detalhes de preços desses serviços.

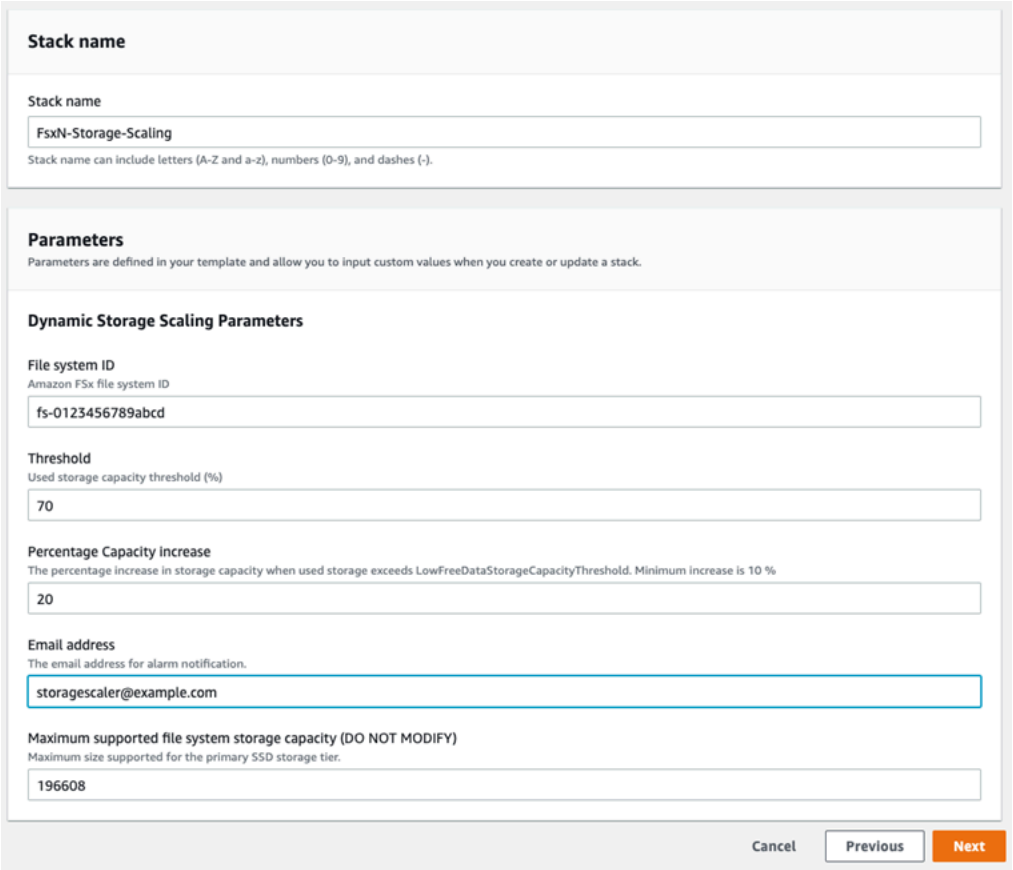
Antes de começar, você deve ter o ID do sistema de arquivos Amazon FSx que está sendo executado na Amazon Virtual Private Cloud (Amazon VPC) em seu. Conta da AWS Para obter mais informações sobre como criar recursos do Amazon FSx, consulte Introdução ao Amazon FSx for ONTAP NetApp .

Iniciar a pilha de soluções para o aumento automático da capacidade de armazenamento

1. Baixe o SxOntapDynamicStorageScaling AWS CloudFormation modelo F.

   > **Note**
   >
   > No momento, o Amazon FSx está disponível somente em regiões específicas AWS . Você deve iniciar essa solução em uma AWS região em que o Amazon FSx esteja disponível. Para obter mais informações, consulte Amazon FSx endpoints and quotas na Referência geral da AWS.

2. No AWS CloudFormation console, escolha Criar pilha > Com novos recursos.
3. Selecione O modelo está pronto. Na seção Especificar modelo, escolha Fazer upload de um arquivo de modelo e faça o upload do modelo baixado.
4. Em Especificar detalhes da pilha, insira os valores da solução para o aumento automático da capacidade de armazenamento.



5. Insira um Nome da pilha.
6. Em Parâmetros, revise os parâmetros do modelo e modifique-os para atender às necessidades do seu sistema de arquivos. Em seguida, escolha Próximo.

> **Note**
>
> Para receber notificações por e-mail quando esse CloudFormation modelo tentar escalar, confirme o e-mail de assinatura do SNS que você recebe após a implantação do modelo.

7. Insira as configurações de Opções que você deseja para a solução personalizada e escolha Próximo.
8. Em Analisar, revise e confirme as configurações da solução. Você deve selecionar a caixa de seleção confirmando que o modelo cria recursos do IAM.
9. Selecione Criar para implantar a stack.

Você pode ver o status da pilha no AWS CloudFormation console na coluna Status. Você verá um status de CREATE_COMPLETE em alguns minutos.

Atualizar a pilha

Depois que a pilha for criada, você poderá atualizá-la usando o mesmo modelo e fornecendo novos valores para os parâmetros. Para obter mais informações, consulte Atualizar pilhas diretamente no Guia do usuário do AWS CloudFormation .

Capacidade de armazenamento do volume

Os volumes do FSx para ONTAP são recursos virtuais usados para agrupar dados, determinar como são armazenados e o tipo de acesso a eles. Os volumes, assim como as pastas, não consomem a capacidade de armazenamento do sistema de arquivos sozinhos. Somente os dados armazenados em um volume consomem o armazenamento SSD e, dependendo da política de divisão em níveis do volume, o armazenamento do grupo de capacidade. Você define o tamanho de um volume ao criá-lo e pode alterá-lo posteriormente. Você pode monitorar e gerenciar a capacidade de armazenamento de seus volumes FSx for ONTAP usando a API AWS Management Console, AWS CLI e a CLI do ONTAP.

Tópicos

Divisão de dados em níveis no volume

Um sistema de arquivos Amazon FSx for NetApp ONTAP tem dois níveis de armazenamento: armazenamento primário e armazenamento em pool de capacidade. O armazenamento principal é um armazenamento SSD provisionado, escalável e de alta performance, criado especificamente para a parte ativa do seu conjunto de dados. O armazenamento do grupo de capacidade é um nível de armazenamento totalmente elástico cujo tamanho pode ser escalado para petabytes, sendo otimizado em termos de custo para dados acessados com pouca frequência.

Os dados em cada volume são automaticamente colocados em camadas no nível de armazenamento do pool de capacidade com base na política de classificação por níveis, no período de resfriamento e nas configurações de limite do volume. As seções a seguir descrevem as políticas de classificação por níveis de ONTAP volume e os limites usados para determinar quando os dados são hierarquizados no pool de capacidade.

Políticas de classificação por níveis de volume

Você determina como usar seu FSx para os níveis de armazenamento do sistema de arquivos ONTAP escolhendo a política de classificação por níveis para cada volume no sistema de arquivos. Você escolhe a política de classificação por níveis ao criar um volume e pode modificá-la a qualquer momento com o console Amazon FSx AWS CLI, a API ou NetApp usando ferramentas de gerenciamento. Você pode escolher uma das políticas a seguir que determinam quais dados, se houver algum, estão divididos em níveis no armazenamento do grupo de capacidade.

> **Note**
>
> A divisão em níveis pode mover seus dados de arquivos e dados de snapshots para o nível do grupo de capacidade. No entanto, os metadados de arquivos sempre permanecem no nível SSD. Para ter mais informações, consulte Como o armazenamento SSD é usado.

- Automática: essa política move todos os dados frios (dados do usuário e snapshots) para o nível do grupo de capacidade. A taxa de resfriamento dos dados é determinada pelo período de resfriamento da política, cujo padrão é 31 dias, podendo ser configurado para valores entre 2 e 183 dias. Quando os blocos de dados frios subjacentes são lidos aleatoriamente (como no acesso típico a arquivos), eles ficam quentes e são gravados no nível de armazenamento principal. Quando os blocos de dados frios são lidos sequencialmente (por exemplo, por meio de

uma verificação do antivírus), eles permanecem frios e no nível de armazenamento do grupo de capacidade. Essa é a política padrão ao criar um volume usando o console do Amazon FSx.

- Somente snapshot: essa política move somente os dados de snapshots para o nível de armazenamento do grupo de capacidade. A taxa na qual os snapshots são divididos em níveis no grupo de capacidade é determinada pelo período de resfriamento da política, cujo padrão é definido como dois dias e pode ser configurado para valores entre 2 e 183 dias. Quando os dados frios do snapshot são lidos, eles ficam quentes e são gravados no nível de armazenamento principal. Essa é a política padrão ao criar um volume usando a AWS CLI API Amazon FSx ou a CLI do NetApp ONTAP.
- Todos: essa política marca todos os dados do usuário e dados do snapshot como frios e os armazena no nível do grupo de capacidade. Quando os blocos de dados são lidos, eles permanecem frios e não são gravados no nível de armazenamento principal. Quando os dados são gravados em um volume com a política Todos de divisão em níveis, inicialmente, eles ainda são gravados no nível de armazenamento SSD e divididos em níveis no grupo de capacidade por meio de um processo em segundo plano. Observe que os metadados do arquivo sempre permanecem no nível SSD.
- Nenhum: essa política mantém todos os dados do volume no nível de armazenamento principal e impede que sejam movidos para o armazenamento do grupo de capacidade. Se você definir um volume para essa política depois de usar qualquer outra política, os dados existentes no volume que estavam no armazenamento do grupo de capacidade serão movidos para o armazenamento SSD por meio de um processo em segundo plano, desde que a utilização do SSD esteja abaixo de 90%. Esse processo em segundo plano pode ser acelerado pela leitura intencional dos dados ou pela modificação da política de recuperação na nuvem do volume. Para ter mais informações, consulte Políticas de recuperação na nuvem.

Como prática recomendada, ao migrar dados que planeja armazenar em longo prazo no armazenamento do grupo de capacidade, recomendamos usar a política de divisão Automática em níveis no volume. Com a divisão Automática em níveis, os dados são armazenados no nível de armazenamento SSD por, no mínimo, dois dias (com base no período de resfriamento do volume) antes de serem movidos para o nível do grupo de capacidade. Reter os dados no armazenamento SSD por, pelo menos, dois dias permite que o ONTAP realize economias neles com a compressão e a eliminação de duplicação pós-processamento, que são preservadas ao dividir os dados em níveis no grupo de capacidade. O ONTAP somente executa a compressão e a eliminação de duplicação pós-processamento em dados no armazenamento SSD. Portanto, selecionar essa política pode ajudar você a maximizar sua economia no armazenamento de longo prazo. Você também pode

maximizar as velocidades de transferência dos primeiros backups criados dos volumes, pois os dados sendo copiados estão no armazenamento SSD.

Para obter mais informações sobre como definir ou modificar a política de divisão em níveis de um volume, consulte Definir a política de divisão em níveis de um volume.

Período de resfriamento da divisão em níveis

O período de resfriamento da divisão em níveis de um volume define o tempo necessário para que os dados no nível SSD sejam marcados como frios. O período de resfriamento se aplica às políticas `Auto` e `Snapshot-only` de divisão em níveis. Você pode definir o período de resfriamento para um valor na faixa de 2 a 183 dias. Para obter mais informações sobre como definir o período de resfriamento, consulte Definir os dias mínimos de resfriamento.

Os dados são divididos em níveis de 24 a 48 horas após o período de resfriamento expirar. A divisão em níveis é um processo em segundo plano que consome recursos da rede e tem uma prioridade menor do que as solicitações voltadas ao cliente. A utilização das atividades de divisão em níveis é controlada quando há solicitações em andamento voltadas ao cliente.

Políticas de recuperação na nuvem

A política de recuperação na nuvem de um volume define as condições que especificam quando os dados lidos no nível do grupo de capacidade podem ser promovidos para o nível SSD. Quando a política de recuperação na nuvem é definida como algo diferente de `Default`, essa política substitui o comportamento de recuperação da política de divisão em níveis do volume. Um volume pode ter uma das políticas de recuperação na nuvem a seguir.

- Padrão: essa política recupera dados divididos em níveis com base na política de divisão em níveis subjacente do volume. Essa é a política padrão de recuperação na nuvem para todos os volumes.
- Nunca: essa política nunca recupera dados divididos em níveis, independentemente de as leituras serem sequenciais ou aleatórias. Isso é semelhante a definir a política de divisão em níveis do volume como Todos, exceto que você pode usá-la com outras políticas, a Automática ou a Somente Snapshot, para dividir os dados de acordo com o período mínimo de resfriamento, em vez de imediatamente.
- Em leitura: essa política recupera os dados divididos em níveis para todas as leituras de dados orientadas pelo cliente. Essa política não tem efeito ao usar a política Todos de divisão em níveis.
- Promover: essa política marca todos os dados de um volume que estão no grupo de capacidade para recuperação no nível SSD. Os dados serão marcados na próxima vez em que o verificador

diário de divisão em níveis em segundo plano for executado. Essa política é benéfica para aplicações com workloads cíclicas que são executadas com pouca frequência, mas exigem performance de nível SSD durante a execução. Essa política não tem efeito ao usar a política Todos de divisão em níveis.

Para obter informações sobre como definir a política de recuperação na nuvem de um volume, consulte Definir a política de recuperação na nuvem de um volume.

Limites de divisão em níveis

A utilização da capacidade de armazenamento SSD de um sistema de arquivos determina como ONTAP gerencia o comportamento de hierarquização de todos os seus volumes. Com base no uso da capacidade de armazenamento SSD de um sistema de arquivos, os seguintes limites definem o comportamento de divisão em níveis conforme descrito. Para obter informações sobre como monitorar a utilização da capacidade do nível de armazenamento SSD de um volume, consulte Monitorando a capacidade de armazenamento do volume.

> **Note**
>
> Recomendamos que você não exceda 80% da utilização da capacidade de armazenamento do seu nível de armazenamento SSD. Para sistemas de arquivos escaláveis, essa recomendação se aplica tanto à utilização média total em todos os agregados do seu sistema de arquivos quanto à utilização de cada agregado individual. Isso garante que a divisão em níveis funcione adequadamente e fornece sobrecarga para novos dados. Se nível de armazenamento SSD estiver consistentemente acima de 80% de utilização da capacidade de armazenamento, você poderá aumentar a capacidade do nível de armazenamento SSD. Para ter mais informações, consulte Atualizando o armazenamento SSD e o IOPS do sistema de arquivos.

O FSx para ONTAP usa os limites de capacidade de armazenamento a seguir para gerenciar a divisão em níveis nos volumes.

- <=50% de utilização do nível de armazenamento SSD: nesse limite, o nível de armazenamento SSD é considerado subutilizado, e somente os volumes que estão usando a política Todos de divisão em níveis têm os dados divididos no armazenamento do grupo de capacidade. Os volumes com as políticas Automática e Somente snapshot não dividem os dados em níveis nesse limite.

- > 50% de utilização do nível de armazenamento SSD: volumes com as políticas Automática e Somente snapshot de divisão em níveis dividem os dados com base na configuração de dias mínimos de resfriamento dos níveis. A configuração padrão é de 31 dias.
- >=90% de utilização do nível de armazenamento SSD: nesse limite, o Amazon FSx prioriza a preservação do espaço no nível de armazenamento SSD. Os dados frios do nível do grupo de capacidade não são mais movidos para o nível de armazenamento SSD quando lidos em volumes usando as políticas Automática e Somente snapshot.
- >=98% de utilização do nível de armazenamento SSD: toda a funcionalidade de divisão em níveis é interrompida quando o nível de armazenamento SSD atinge ou ultrapassa 98% de utilização. Você pode continuar lendo nos níveis de armazenamento, mas não é possível gravar neles.

Snapshots e capacidade de armazenamento de volumes

Um snapshot é uma imagem somente para leitura de um volume Amazon FSx for NetApp ONTAP em um determinado momento. Os snapshots oferecem proteção contra exclusão ou modificação acidental de arquivos nos volumes. Com os snapshots, seus usuários podem facilmente visualizar e restaurar arquivos individuais ou pastas de um snapshot anterior.

Os snapshots são armazenados com os dados do sistema de arquivos e consomem a capacidade de armazenamento do sistema de arquivos. No entanto, os snapshots consomem capacidade de armazenamento somente para as partes dos arquivos que foram alteradas após o último snapshot. Os snapshots não estão incluídos nos backups dos volumes do sistema de arquivos.

Os snapshots são habilitados por padrão nos volumes, usando a política de snapshots padrão. Os snapshots são armazenados no diretório `.snapshot` na raiz de um volume. Você pode gerenciar a capacidade de armazenamento de um volume para snapshots das maneiras a seguir.

- Políticas de snapshot: selecione uma política de snapshot incorporada ou uma política personalizada criada na CLI ou na API REST do ONTAP.
- Excluir os snapshots manualmente: recupere a capacidade de armazenamento excluindo os snapshots manualmente.
- Criar uma política de exclusão automática de snapshot: crie uma política que exclua mais snapshots do que a política de snapshot padrão.
- Desativar os snapshots automáticos: conserve a capacidade de armazenamento desativando os snapshots automáticos.

Para ter mais informações, consulte Trabalhar com snapshots.

Capacidade do arquivo de volumes

Os volumes do Amazon FSx for NetApp ONTAP têm ponteiros de arquivo que são usados para armazenar metadados de arquivos, como nome do arquivo, horário do último acesso, permissões, tamanho e para servir como ponteiros para blocos de dados. Esses ponteiros de arquivo são chamados de inodes. Cada volume tem uma capacidade finita para o número de inodes, que é chamada de capacidade do arquivo de volumes. Quando um volume fica com poucos arquivos disponíveis (inodes) ou os esgota, você não consegue gravar dados adicionais nesse volume.

O número de objetos do sistema de arquivos (arquivos, diretórios, cópias de snapshots) que um volume pode conter é determinado pela quantidade de inodes que ele tem. O número de inodes em um volume aumenta de acordo com a capacidade de armazenamento do volume (e o número de constituintes do volume para volumes). FlexGroup Por padrão, todos FlexVol os volumes (ou FlexGroup componentes) com capacidade de armazenamento de 648 GiB ou mais têm o mesmo número de inodes: 21.251.126. Se você criar um volume maior que 648 GiB e quiser que ele tenha mais de 21.251.126 inodes, deverá aumentar o número máximo de inodes (arquivos) manualmente. Para obter mais informações sobre como visualizar o número máximo de arquivos de um volume, consulteVisualizar a capacidade de arquivos de um volume.

O número padrão de inodes em um volume é de 1 inode para cada 32 KiB de capacidade de armazenamento de volume, até um tamanho de volume de 648 GiB. Para um volume de 1 GiB:

Volume_size_in_bytes × (1 arquivo ÷ inode_size_in_bytes) = maximum_number_of_files

1.073.741.824 bytes × (1 arquivo ÷ 32.768 bytes) = 32.768 arquivos

Você pode aumentar o número máximo de inodes que um volume pode conter, até um máximo de 1 inode para cada 4 KiB de capacidade de armazenamento. Para um volume de 1 GiB, isso aumenta o número máximo de inodes ou arquivos de 32.768 para 262.144:

1.073.741.824 bytes × (1 arquivo ÷ 4.096 bytes) = 262.144 arquivos

Um volume do FSx para ONTAP pode ter no máximo dois bilhões de inodes.

Para obter informações sobre como alterar o número máximo de arquivos que um volume pode armazenar, consulteComo aumentar o número máximo de arquivos em um volume.

Atualização da capacidade de armazenamento de um volume

Você pode gerenciar a capacidade de armazenamento de volume aumentando ou diminuindo manualmente o tamanho do volume usando a API AWS Management Console, AWS CLI e a CLI do ONTAP. Você também pode habilitar o dimensionamento automático do volume para que seu tamanho aumente ou diminua automaticamente quando atingir determinados limites de capacidade de armazenamento usada. Use a CLI do ONTAP para gerenciar o dimensionamento automático de volumes.

Para alterar a capacidade de armazenamento de um volume (console)

- Você pode aumentar ou diminuir a capacidade de armazenamento de um volume usando o console e a API do Amazon FSx. AWS CLI Para ter mais informações, consulte Atualizar um volume.

Você também pode usar a ONTAP CLI para modificar a capacidade de armazenamento de um volume usando o `volume modify`comando.

Para modificar o tamanho de um volume (ONTAP CLI)

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.
2. Use o comando volume modify ONTAP CLI para modificar a capacidade de armazenamento de um volume. Execute o comando a seguir, usando seus dados no lugar dos seguintes valores:

   - Substitua *`svm_name`* pelo nome da máquina virtual de armazenamento (SVM) na qual o volume foi criado.
   - *`vol_name`*Substitua pelo nome do volume que você deseja redimensionar.
   - Substitua *`vol_size`* pelo novo tamanho do volume no formato *`integer`*`[KB|MB|GB|TB|PB]`; por exemplo, `100GB` para aumentar o tamanho do volume para 100 gigabytes.

```
::> volume modify -vserver svm_name -volume vol_name -size vol_size
```

Habilitando o dimensionamento automático de volume

Dimensionamento automático do volume para que o volume cresça automaticamente até um tamanho especificado quando atingir um limite de espaço usado. Você pode fazer isso para tipos de FlexVol volume (o tipo de volume padrão para FSx for ONTAP) usando o comando ONTAP CLI. `volume autosize`

Habilitar o dimensionamento automático de volumes (CLI do ONTAP)

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Use o comando `volume autosize` conforme mostrado a seguir, substituindo também os valores.

   - Substitua *svm_name* pelo nome da SVM na qual o volume foi criado.
   - Substitua *vol_name* pelo nome do volume que deseja redimensionar.
   - Substitua *grow_threshold* por um valor percentual de espaço usado (como `90`) no qual o volume aumentará automaticamente de tamanho (até o valor *max_size*).
   - Substitua *max_size* pelo tamanho máximo até o qual o volume pode aumentar. Use o formato *integer*`[KB|MB|GB|TB|PB]`; por exemplo, `300TB`. O tamanho máximo é de 300 TB. O padrão é 120% do tamanho do volume.
   - Substitua *min_size* pelo tamanho mínimo para o qual o volume será reduzido. Use o mesmo formato de *max_size*.
   - Substitua *shrink_threshold* pela porcentagem de espaço usado na qual o volume diminuirá automaticamente de tamanho.

```
::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -
grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-
percent shrink_threshold -minimum-size min_size
```

Monitorando a capacidade de armazenamento do volume

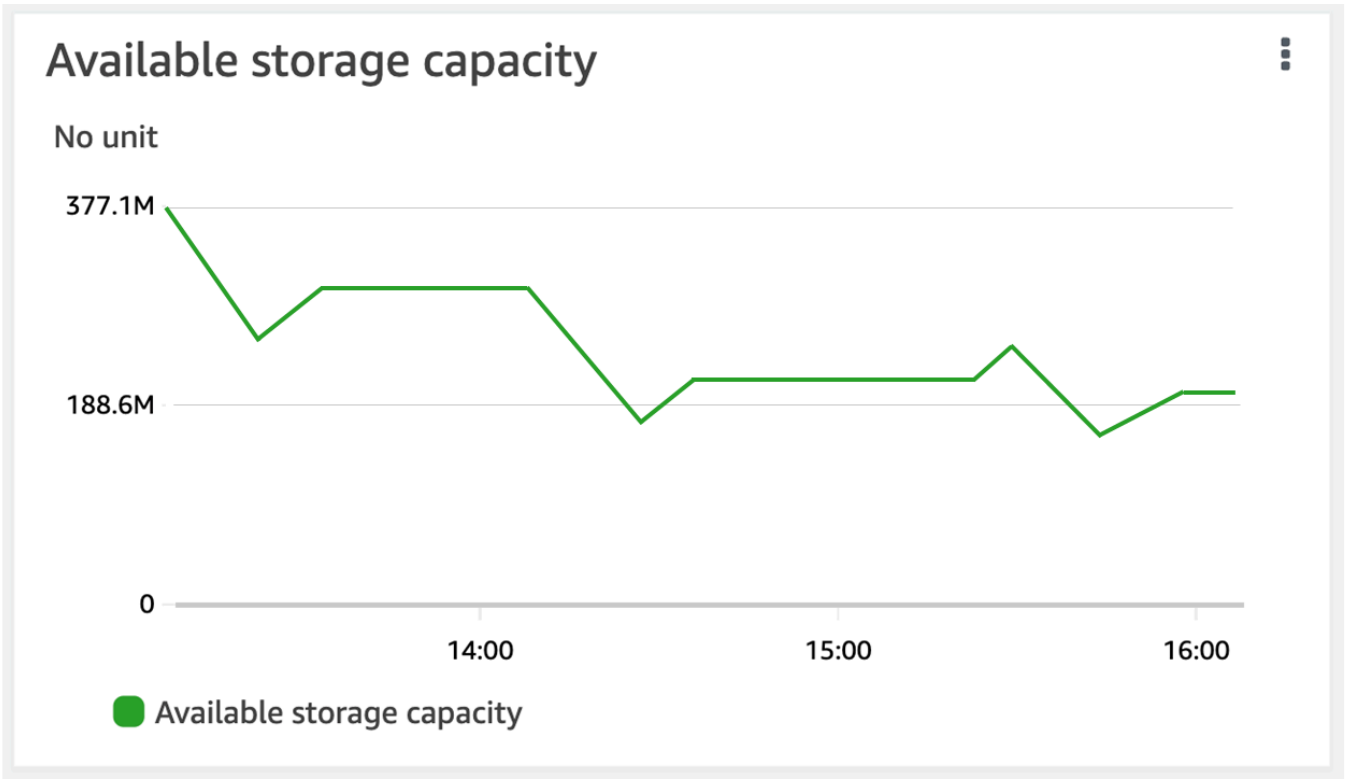
Você pode visualizar o armazenamento disponível de um volume e sua distribuição de armazenamento no AWS Management Console AWS CLI, e na CLI do NetApp ONTAP.

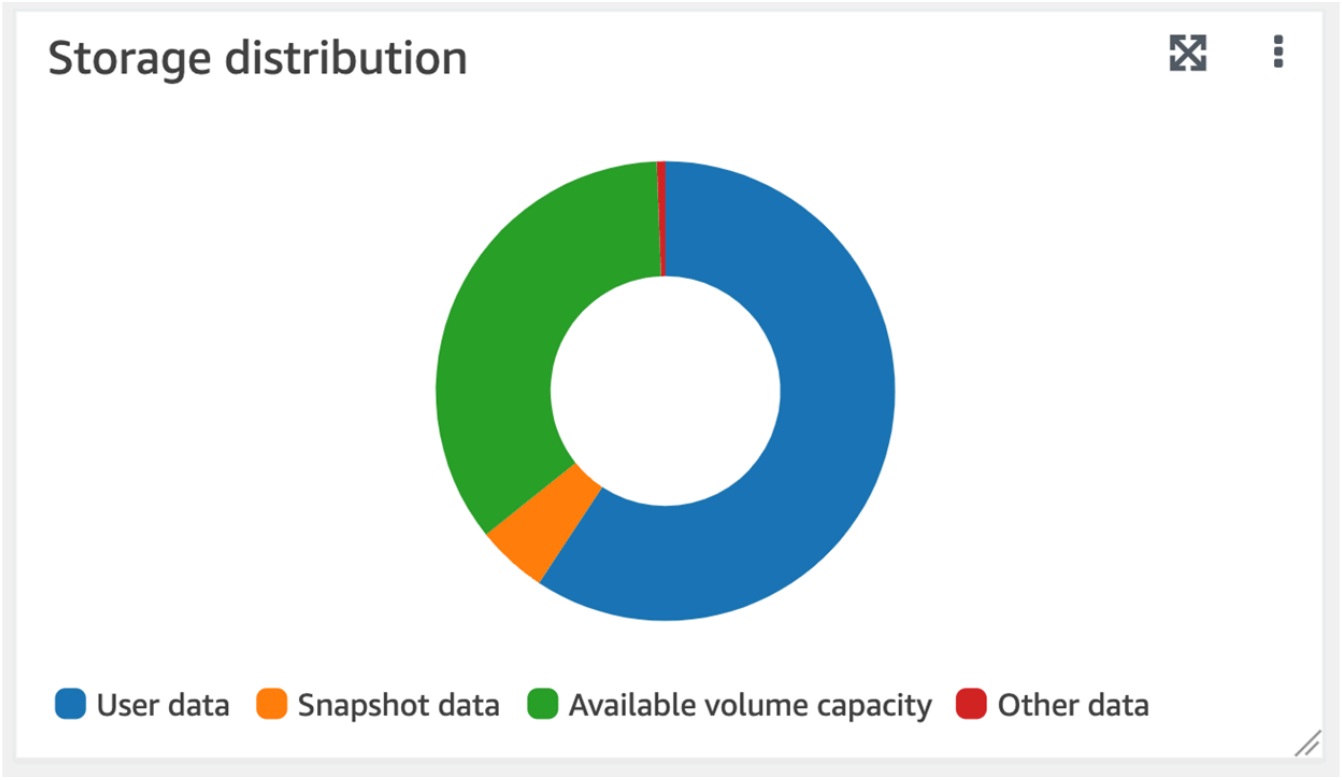
Para monitorar a capacidade de armazenamento de um volume (console)

O gráfico Armazenamento disponível exibe a quantidade de capacidade de armazenamento livre em um volume ao longo do tempo. O gráfico Distribuição do armazenamento mostra como a capacidade de armazenamento de um volume está atualmente distribuída em quatro categorias:

- Dados do usuário
- Dados de snapshot
- Capacidade de volume disponível
- Outros dados

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha Volumes na coluna de navegação à esquerda e selecione o volume do ONTAP para o qual deseja visualizar as informações sobre a capacidade de armazenamento. A página de detalhes do volume é exibida.
3. No segundo painel, escolha a guia Monitoramento. Os gráficos Armazenamento disponível e Distribuição do armazenamento são exibidos com vários outros gráficos.


Available storage capacity
No unit
377.1M
188.6M
0
14:00
15:00
16:00
Available storage capacity


Storage distribution
User data
Snapshot data
Available volume capacity
Other data

Para monitorar a capacidade de armazenamento (ONTAPCLI) de um volume

Você pode monitorar como a capacidade de armazenamento do seu volume está sendo consumida usando o comando `volume show-space` ONTAP CLI. Para obter mais informações, consulte `volume show-space`no Centro de NetApp ONTAP Documentação.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Visualize o uso da capacidade de armazenamento de um volume emitindo o comando a seguir, substituindo também os valores.

   - Substitua *`svm_name`* pelo nome da SVM na qual o volume foi criado.
   - Substitua *`vol_name`* pelo nome do volume para o qual você está definindo a política de divisão de dados em níveis.

   ```
   ::> volume show-space -vserver svm_name -volume vol_name
   ```

   Se o comando for bem-sucedido, você verá uma saída semelhante a esta:

   ```
   Vserver : svm_name
   Volume  : vol_name
   Feature                                     Used      Used%
   --------------------------------     ----------     ------
   User Data                                  140KB         0%
   Filesystem Metadata                      164.4MB         1%
   Inodes                                   10.28MB         0%
   Snapshot Reserve                         563.2MB         5%
   Deduplication                               12KB         0%
   Snapshot Spill                            9.31GB        85%
   Performance Metadata                       668KB         0%

   Total Used                               10.03GB        91%
   ```

```
Total Physical Used                    10.03GB        91%
```

A saída desse comando mostra a quantidade de espaço físico que diferentes tipos de dados ocupam nesse volume. Também mostra a porcentagem da capacidade total do volume que cada tipo de dado consome. Nesse exemplo, `Snapshot Spill` e `Snapshot Reserve` consomem um total de 90% da capacidade do volume.

`Snapshot Reserve` mostra a quantidade de espaço em disco reservada para armazenar cópias de snapshot. Se o armazenamento das cópias de snapshot exceder o espaço de reserva, ele será vazado para o sistema de arquivos e essa quantidade será mostrada em `Snapshot Spill`.

Para aumentar a quantidade de espaço disponível, você pode aumentar o tamanho do volume ou excluir snapshots que não está usando, conforme mostrado nos procedimentos a seguir.

Para tipos de FlexVol volume (o tipo de volume padrão para FSx para volumes ONTAP), você também pode ativar o dimensionamento automático de volume. Ao habilitar o dimensionamento automático, o tamanho do volume aumenta automaticamente quando atinge determinados limites. Você também pode desabilitar os snapshots automáticos. Esses dois recursos são explicados nas seções a seguir.

Definir a política de divisão em níveis de um volume

Você pode modificar a política de classificação por níveis de um volume usando a API AWS Management Console, AWS CLI e a CLI do ONTAP.

Modificar a política de camadas de dados de um volume (console)

Use o procedimento a seguir para modificar a política de divisão de dados em níveis de um volume usando o AWS Management Console.

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha Volumes no painel de navegação à esquerda e selecione o volume do ONTAP para o qual você deseja modificar a política de divisão de dados em níveis.
3. Escolha Atualizar volume no menu suspenso Ações. A janela Atualizar volume é exibida.
4. Em Política de divisão em níveis do grupo de capacidade, escolha a nova política para o volume. Para ter mais informações, consulte Políticas de classificação por níveis de volume.
5. Escolha Atualizar para aplicar a nova política ao volume.

Para definir a política de classificação por níveis (CLI) de um volume

- Modifique a política de classificação por níveis de um volume usando o comando da CLI update-volume (UpdateVolumeé a ação equivalente da API Amazon FSx). O exemplo de comando da CLI a seguir define a política de divisão de dados em níveis de um volume como SNAPSHOT_ONLY.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

Para uma solicitação bem-sucedida, o sistema responde com a descrição do volume.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 2,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

Modificar a política de camadas de um volume (CLI do ONTAP)

Use o comando `volume modify` da CLI do ONTAP para definir a política de divisão em níveis de um volume. Para obter mais informações, consulte o Centro `volume modify`de Documentação do NetApp ONTAP.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Entre no modo avançado da CLI do ONTAP usando o comando a seguir.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Use o comando a seguir para modificar a política de divisão de dados em níveis do volume, substituindo também os valores.

   - Substitua *`svm_name`* pelo nome da SVM na qual o volume foi criado.
   - Substitua *`vol_name`* pelo nome do volume para o qual você está definindo a política de divisão de dados em níveis.
   - Substitua *`tiering_policy`* pela política desejada. Os valores válidos são `snapshot-only`, `auto`, `all` ou none. Para ter mais informações, consulte Políticas de classificação por níveis de volume.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -tiering-
   policy tiering_policy
   ```

Definir os dias mínimos de resfriamento

Os dias mínimos de resfriamento de um volume definem o limite usado para determinar quais dados estão quentes e quais estão frios. Você pode definir os dias mínimos de resfriamento de um volume usando uma API AWS CLI e a CLI do ONTAP.

Para definir os dias mínimos de resfriamento (CLI) de um volume

- Modifique uma configuração de volume usando o comando da CLI update-volume (é a ação equivalente UpdateVolumeda API Amazon FSx). O exemplo a seguir de comando da CLI define o `CoolingPeriod` de um volume para 104 dias.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration
 TieringPolicy={CoolingPeriod=104}
```

O sistema responde com a descrição do volume para uma solicitação bem-sucedida.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 104,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
```

```
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

Definir os dias mínimos de resfriamento de um volume (CLI do ONTAP)

Use o comando `volume modify` da CLI do ONTAP para definir o número mínimo de dias de resfriamento para um volume existente. Para obter mais informações, consulte o Centro `volume modify`de Documentação do NetApp ONTAP.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Entre no modo avançado da CLI do ONTAP usando o comando a seguir.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Use o comando a seguir para alterar os dias mínimos de resfriamento da divisão em níveis do volume, substituindo também valores.

   - Substitua *`svm_name`* pelo nome da SVM na qual o volume foi criado.
   - Substitua *`vol_name`* pelo nome do volume para o qual você está definindo os dias de resfriamento.
   - Substitua *`cooling_days`* pelos dias desejados, um número inteiro entre 2 e 183.

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-
days cooling_days
```

O sistema responde da seguinte forma para uma solicitação bem-sucedida:

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Definir a política de recuperação na nuvem de um volume

Use o comando `volume modify` da CLI do ONTAP para definir a política de recuperação na nuvem de um volume existente. Para obter mais informações, consulte o Centro `volume modify`de Documentação do NetApp ONTAP.

Definir a política de recuperação na nuvem de um volume (CLI do ONTAP)

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Entre no modo avançado da CLI do ONTAP usando o comando a seguir.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Use o comando a seguir para definir a política de recuperação na nuvem do volume, substituindo também os valores.

   - Substitua *`svm_name`* pelo nome da SVM na qual o volume foi criado.

- Substitua *vol_name* pelo nome do volume para o qual você está definindo a política de recuperação na nuvem.
- Substitua *retrieval_policy* pelo valor desejado, `default`, `on-read`, `never` ou `promote`.

```
FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-
policy retrieval_policy
```

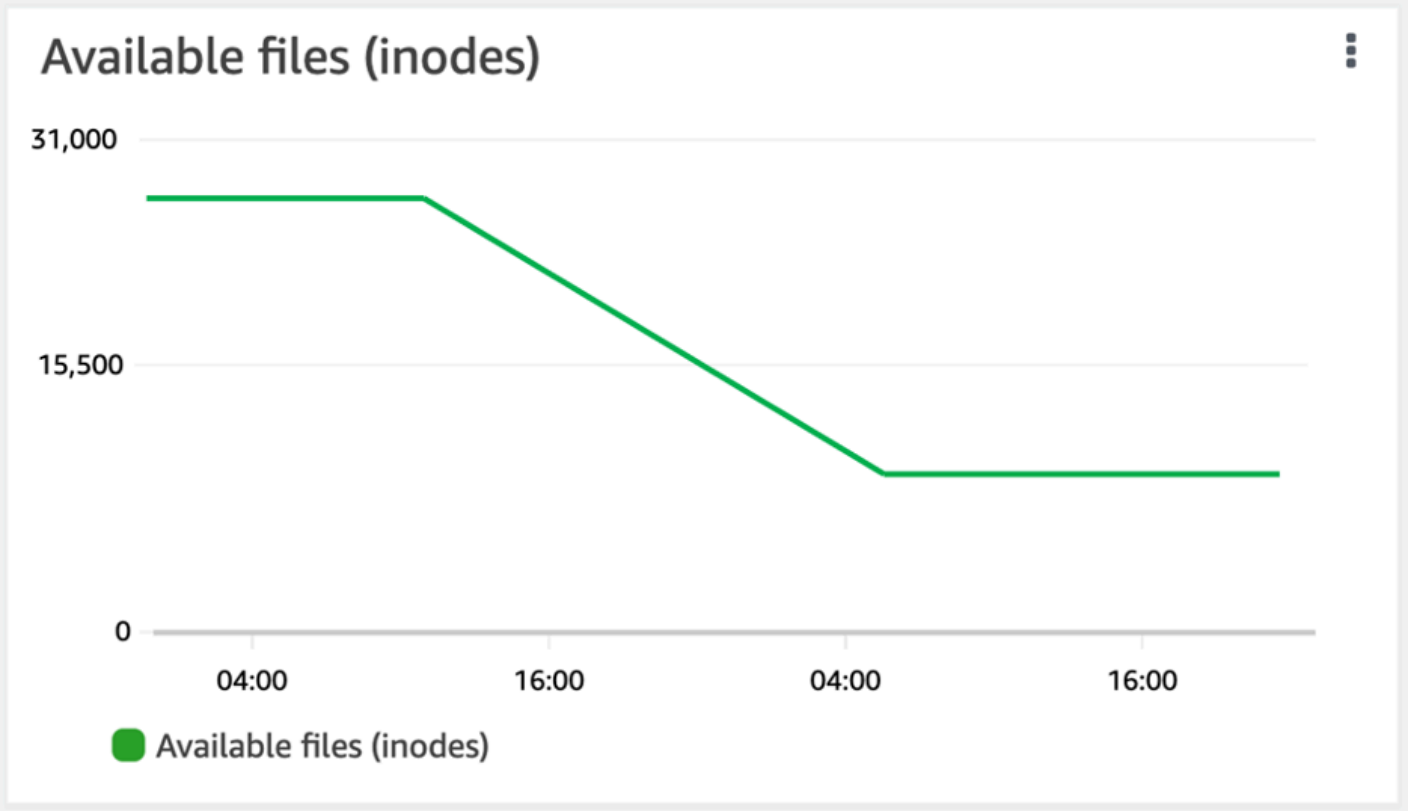
O sistema responde da seguinte forma para uma solicitação bem-sucedida:

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Visualizar a capacidade de arquivos de um volume

Você pode usar qualquer um dos métodos a seguir para visualizar o número máximo de arquivos permitidos e o número de arquivos já usados em um volume.

- As métricas de CloudWatch volume `FilesCapacity` `FilesUsed` e.
- No console do Amazon FSx, navegue até o gráfico Arquivos disponíveis (inodes) na guia Monitoramento do volume. A imagem a seguir mostra os Arquivos disponíveis (inodes) em um volume diminuindo com o tempo.



Como aumentar o número máximo de arquivos em um volume

Os volumes do FSx para ONTAP podem ficar sem capacidade de arquivos quando o número de inodes ou ponteiros de arquivo disponíveis estiver esgotado.

Para aumentar o número máximo de arquivos em um volume (ONTAPCLI)

Você usa o comando `volume modify` ONTAP CLI para aumentar o número máximo de arquivos em um volume. Para obter mais informações, consulte `volume modify`no Centro de NetApp ONTAP Documentação.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Faça um dos procedimentos a seguir, dependendo do seu caso de uso. Substitua *svm_name* e *vol_name* pelos seus valores.

   - Para configurar um volume para sempre ter o número máximo de arquivos (inodes) disponíveis, siga os passos a seguir.

     1. Entre no modo avançado na CLI do ONTAP usando o comando a seguir.

        ```
        ::> set adv
        ```

     2. Após executar esse comando, você verá essa saída. Insira y para continuar.

        ```
        Warning: These advanced commands are potentially dangerous; use them only
         when
        directed to do so by NetApp personnel.
        Do you want to continue? {y|n}: y
        ```

     3. Insira o seguinte comando para sempre usar o número máximo de arquivos no volume:

        ```
        ::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
        ```

   - Para especificar manualmente o número total de arquivos permitidos no volume, usando *max_number_files* `= (current_size_of_volume) × (1 file ÷ 4 KiB)`, com um valor máximo possível de dois bilhões, use o seguinte comando:

     ```
     ::> volume modify -vserver svm_name -volume vol_name -files max_number_files
     ```

Ativando o modo de gravação em nuvem de um volume

Use o comando `volume modify` ONTAP CLI para ativar ou desativar o modo de gravação em nuvem para um volume existente. Para obter mais informações, consulte o Centro `volume modify`de Documentação do NetApp ONTAP.

Os pré-requisitos para definir o modo de gravação na nuvem são:

- O volume deve ser um volume existente. Você só pode ativar o recurso em um volume existente.
- O volume deve ser um volume de leitura e gravação (RW).

- O volume deve ter a política de todos os níveis. Para obter mais informações sobre a modificação da política de classificação por níveis de um volume, consulte. Definir a política de divisão em níveis de um volume

O modo de gravação na nuvem é útil para casos como migrações, por exemplo, em que grandes quantidades de dados são transferidas para um sistema de arquivos usando o protocolo NFS.

Para definir o modo de gravação em nuvem de um volume (ONTAP CLI)

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Entre no modo avançado da CLI do ONTAP usando o comando a seguir.

   ```
   FSx::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Use o comando a seguir para definir o modo de gravação na nuvem do volume, substituindo os seguintes valores:

   - Substitua *svm_name* pelo nome da SVM na qual o volume foi criado.
   - *vol_name*Substitua pelo nome do volume para o qual você está configurando o modo de gravação na nuvem.
   - *vol_cw_mode*Substitua por qualquer um `true` para ativar o modo de gravação em nuvem no volume ou `false` para desativá-lo.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-
   enabled vol_cw_mode
   ```

   O sistema responde da seguinte forma para uma solicitação bem-sucedida:

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Como proteger seus dados

Além de replicar automaticamente os dados do sistema de arquivos para garantir alta durabilidade, o Amazon FSx oferece as seguintes opções para proteger ainda mais os dados armazenados nos sistemas de arquivos:

- Os backups nativos do Amazon FSx oferecem suporte às suas necessidades de retenção e conformidade de backup no Amazon FSx. Você também pode usar AWS Backup para gerenciar, automatizar e proteger centralmente seus backups Serviços da AWS na nuvem.
- Os snapshots permitem que seus usuários desfaçam alterações em arquivos de maneira fácil, além de comparar versões de arquivos restaurando-os para versões anteriores.
- A replicação do sistema de arquivos do Amazon FSx em um segundo sistema de arquivos para fornecer proteção e recuperação de dados. A replicação, quando habilitada, ocorre de forma automática e programada.
- O SnapLock protege seus arquivos fazendo a transição deles para o estado de gravação única e várias leituras (WORM), o que impede modificações ou exclusões durante um período de retenção especificado.

Tópicos

Trabalhar com backups

Com o FSx para ONTAP, você pode fazer backups diários automáticos e backups iniciados pelo usuário dos volumes do sistema de arquivos. Os backups do FSx for ONTAP são por volume, portanto, cada backup contém somente os dados em um volume específico. Os backups do Amazon FSx são altamente duráveis e incrementais.

Todos os backups do Amazon FSx (backups diários automáticos e backups iniciados pelo usuário) são incrementais. Isso significa que apenas os dados no volume que foi alterado após o backup mais recente são salvos. Isso minimiza o tempo necessário para criar o backup e o armazenamento

necessários para o backup, o que economiza nos custos de armazenamento ao não duplicar os dados. Ao excluir um backup, somente os dados exclusivos desse backup serão removidos. Cada backup do Amazon FSx contém todas as informações necessárias para criar um novo volume a partir do backup, restaurando efetivamente um point-in-time snapshot do volume do sistema de arquivos.

Criar backups regulares para seus volumes é uma prática recomendada que ajuda a apoiar suas necessidades de retenção de dados e conformidade. Trabalhar com backups do Amazon FSx é fácil, seja criando backups, restaurando com backups ou excluindo um backup.

O Amazon FSx suporta o backup de ONTAP FlexVol volumes (em todos os sistemas de arquivos) e FlexGroup volumes com um `OntapVolumeType` de `RW` (leitura/gravação).

> **Note**
>
> O Amazon FSx não oferece suporte ao backup de volumes de proteção de dados (DP), volumes de compartilhamento de carga (LS) ou volumes de destino. FlexCache

Há limites para o número de backups que você pode armazenar por sistema de arquivos e por volume. Para obter mais informações, consulte Cotas que podem ser aumentadas e Cotas de recursos para cada sistema de arquivos.

Tópicos

- Exclusão de um backup

Como funcionam os backups

Os backups do Amazon FSx usam snapshots — point-in-time imagens somente para leitura dos seus volumes — para manter a incrementalidade entre os backups. Sempre que um backup é feito, o Amazon FSx primeiro tira um snapshot do seu volume. O instantâneo de backup é armazenado em seu volume e consome espaço em seu nível de armazenamento SSD. Em seguida, o Amazon FSx compara esse snapshot com o snapshot de backup anterior (se houver) e copia somente os dados alterados ao backup.

Se não houver nenhum snapshot de backup anterior, todo o conteúdo do snapshot de backup mais recente será copiado ao backup. Depois que o último snapshot de backup for criado com sucesso, o Amazon FSx excluirá o snapshot de backup anterior. O snapshot usado para o backup mais recente permanece no volume até que o próximo backup seja feito, quando o processo se repete. Para otimizar os custos de armazenamento de backup, ONTAP preserva a economia de eficiência de armazenamento de um volume em seus backups.

O Amazon FSx não pode fazer backup de volumes que estão off-line.

Requisitos de armazenamento

Para fazer backups de seus volumes, tanto o volume quanto o sistema de arquivos devem ter capacidade de armazenamento SSD disponível suficiente para armazenar um instantâneo de backup. Ao tirar um instantâneo de backup, a capacidade de armazenamento adicional consumida pelo instantâneo não pode fazer com que o volume exceda 98% de utilização do armazenamento SSD. Se isso acontecer, o backup falhará. Você pode aumentar o armazenamento SSD de um volume ou sistema de arquivos a qualquer momento para garantir que seus backups não sejam interrompidos.

Como trabalhar com backups diários automáticos

Os backups diários automáticos dos volumes do seu sistema de arquivos são ativados por padrão quando você cria um sistema de arquivos. Você pode ativar ou desativar os backups diários automáticos de um sistema de arquivos a qualquer momento. Os backups diários automáticos ocorrem durante a janela de backup diário, que é definida automaticamente quando você cria um sistema de arquivos. Você pode modificar a janela de backup diário a qualquer momento. Recomendamos que você escolha uma hora do dia para o backup diário que esteja fora do horário

normal de operação dos aplicativos que usam seus volumes para melhorar o desempenho do backup. Para ter mais informações, consulte Desempenho de backup e restauração.

Você pode definir o período de retenção para backups diários automáticos entre 1 e 90 dias no console ao criar um sistema de arquivos ou a qualquer momento. O período padrão de retenção diária de backup automático é de 30 dias. O serviço exclui um backup diário automático quando o período de retenção expira. Usando a CLI ou a API, você pode definir o período de retenção entre 0 e 90 dias; defini-lo como 0 desativa os backups diários automáticos.

A janela de backup diário e o período de retenção de backup são configurações no nível do sistema de arquivos que se aplicam a todos os volumes do sistema de arquivos. Você pode usar o console Amazon FSx AWS CLI, o ou a API para alterar a janela de backup e o período de retenção de backup para seus sistemas de arquivos e para ativar ou desativar os backups diários automáticos. Para ter mais informações, consulte Atualização de um sistema de arquivos.

Você não pode criar um backup de volume se o volume estiver off-line. Para ter mais informações, consulte Backups e volumes off-line.

> **Note**
>
> Os backups diários automáticos têm um período máximo de retenção de 90 dias, mas os backups iniciados pelo usuário que você cria, que incluem backups criados usando AWS Backup, são mantidos para sempre, a menos que você ou o AWS Backup serviço os excluam.

Você pode excluir manualmente um backup diário automático usando o console, a CLI e a API. Ao excluir um volume, você também exclui os backups diários automáticos desse volume. O Amazon FSx oferece a opção de criar um backup final de um volume antes de excluí-lo. O backup final é mantido para sempre, a menos que você o exclua. Para obter mais informações, consulteExcluir backups.

Como trabalhar com backups iniciados pelo usuário

Com o Amazon FSx, você pode fazer backups manualmente dos volumes do seu sistema de arquivos a qualquer momento usando a AWS Management Console API AWS CLI, e. Seus backups iniciados pelo usuário são incrementais em relação a outros backups que podem ter sido criados para um volume e são retidos para sempre, a menos que você os exclua. Os backups iniciados pelo usuário são mantidos mesmo depois que você exclui o volume ou o sistema de arquivos no qual os

backups foram criados. Você pode excluir backups iniciados pelo usuário somente usando o console do Amazon FSx, a API ou a CLI. Eles nunca são excluídos automaticamente pelo Amazon FSx. Para ter mais informações, consulte Excluir backups.

Você não pode criar um backup de volume se o volume estiver off-line. Para ter mais informações, consulte Backups e volumes off-line.

Copiar tags para backups

Ao criar ou atualizar um volume usando a CLI ou a API, você pode habilitar `CopyTagsToBackups` a cópia automática de qualquer tag em seu volume para seus backups. No entanto, se você adicionar alguma tag ao criar um backup iniciado pelo usuário, incluindo nomear um backup ao usar o console, o serviço não copiará as tags do volume, mesmo se `CopyTagsToBackups` estiver ativado.

Desempenho de backup e restauração

Vários fatores podem influenciar o desempenho das operações de backup e restauração. As operações de backup e restauração são processos em segundo plano, o que significa que têm uma prioridade menor em relação às operações de E/S do cliente. As operações de E/S do cliente incluem leitura e gravação de dados NFS, CIFS e iSCSI. Todos os processos em segundo plano, incluindo operações de backup e restauração, utilizam somente a parte não utilizada da capacidade de taxa de transferência do sistema de arquivos e podem levar de alguns minutos a algumas horas para serem concluídos, dependendo do tamanho do backup e da quantidade de capacidade de transferência não utilizada do sistema de arquivos.

Outros fatores que afetam o desempenho do backup e da restauração incluem o nível de armazenamento no qual seus dados são armazenados e o perfil do conjunto de dados. Recomendamos que você crie os primeiros backups de seus volumes quando a maioria dos dados estiver no armazenamento SSD. Os conjuntos de dados que contêm principalmente arquivos pequenos geralmente têm um desempenho inferior em comparação com conjuntos de dados de tamanho semelhante que contêm principalmente arquivos grandes. Isso ocorre porque o processamento de um grande número de arquivos pequenos consome mais ciclos de CPU e sobrecarga de rede do que processar menos arquivos grandes.

Geralmente, você pode esperar as seguintes taxas de backup ao fazer backup de dados armazenados no nível de armazenamento SSD:

- 750 MBps em vários backups simultâneos contendo principalmente arquivos grandes.
- 100 MBps em vários backups simultâneos contendo principalmente arquivos pequenos.

Geralmente, você pode esperar as seguintes taxas de restauração:

- 250 MBps em várias restaurações simultâneas contendo principalmente arquivos grandes.
- 100 MBps em várias restaurações simultâneas contendo principalmente arquivos pequenos.

Usando AWS Backup com o Amazon FSx

AWS Backup é uma forma simples e econômica de proteger seus dados fazendo backup de seus volumes Amazon FSx for ONTAP. NetApp AWS Backup é um serviço de backup unificado projetado para simplificar a criação, restauração e exclusão de backups, ao mesmo tempo em que fornece relatórios e auditoria aprimorados. AWS Backup facilita o desenvolvimento de uma estratégia de backup centralizada para conformidade legal, normativa e profissional. AWS Backup também simplifica a proteção AWS de seus volumes de armazenamento, bancos de dados e sistemas de arquivos, fornecendo um local central onde você pode fazer o seguinte:

- Configure e audite os AWS recursos dos quais você deseja fazer backup.
- Automatizar a programação de backups.
- Definir políticas de retenção.
- Monitore todas as atividades recentes de backup, cópia e restauração.

AWS Backup usa a funcionalidade de backup integrada do Amazon FSx. Os backups criados usando o AWS Backup console têm o mesmo nível de consistência e desempenho do sistema de arquivos, são incrementais em relação a qualquer outro backup do Amazon FSx que você fizer do seu volume (iniciado pelo usuário ou automático) e oferecem as mesmas opções de restauração que os backups feitos pelo console do Amazon FSx. Se você usa AWS Backup para gerenciar esses backups, obtém funcionalidades adicionais, como a capacidade de criar backups agendados com a mesma frequência a cada hora. Você pode adicionar uma camada adicional de defesa para proteger os backups contra exclusões inadvertidas ou mal-intencionadas armazenando-os em um cofre. AWS Backup

Os backups criados por AWS Backup são considerados backups iniciados pelo usuário e contam para a cota de backup iniciada pelo usuário para o Amazon FSx. Para ter mais informações, consulte Cotas que podem ser aumentadas. Você pode visualizar e restaurar backups criados AWS Backup no console, na CLI e na API do Amazon FSx. No entanto, você não pode excluir backups criados AWS Backup no console, na CLI ou na API do Amazon FSx. Para obter mais informações, consulte Introdução AWS Backup no Guia do AWS Backup desenvolvedor.

AWS Backup não é possível fazer backup de volumes que estão off-line.

Restaurando backups em um novo volume

Você pode restaurar um backup de volume em um novo volume, restaurando efetivamente um point-in-time instantâneo de um volume usando o console, a CLI ou a API.

Ao restaurar um backup, todos os dados são gravados primeiro na camada de armazenamento SSD antes que o serviço comece a hierarquizar os dados no armazenamento do pool de capacidade de acordo com a política de classificação por níveis definida para o volume restaurado. Ao restaurar um backup em um volume com uma política de hierarquização de`All`, um processo periódico em segundo plano classifica os dados no pool de capacidade. Ao restaurar um backup em um volume com uma política de classificação em camadas de `Snapshot Only` ou`Auto`, os dados são colocados em camadas no pool de capacidade se a utilização do SSD no sistema de arquivos for maior que 50% e a taxa de resfriamento for determinada pelo período de resfriamento da política de classificação em camadas.

Quando você restaura um backup de FlexGroup volume em um sistema de arquivos que tem um número diferente de pares de alta disponibilidade (HA) do sistema de arquivos original, o Amazon FSx pode adicionar volumes constituintes adicionais para garantir que os constituintes sejam distribuídos uniformemente.

Para step-by-step obter instruções sobre como restaurar um backup em um novo volume, consulteRestaurando um backup em um novo volume.

> **Note**
>
> Um volume restaurado sempre tem o mesmo estilo de volume do volume original. Você não pode alterar o estilo do volume ao restaurar.

Excluir backups

Você pode excluir backups diários automáticos e backups iniciados pelo usuário de seus volumes. 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. Para obter instruções sobre como excluir backups, consulteExclusão de um backup.

Você não pode excluir backups criados por AWS Backup, que tenham tipo AWS Backup, no console, na CLI ou na API do Amazon FSx. Para obter informações sobre como excluir backups criados por AWS Backup, consulte Excluindo backups no Guia do AWS Backup desenvolvedor.

Você não pode excluir o backup de um volume se o volume estiver off-line. Para ter mais informações, consulte Backups e volumes off-line.

> **Important**
>
> Não exclua o instantâneo comum no volume porque ele é usado para manter a incrementalidade entre seus backups. A exclusão do instantâneo comum no volume fará com que o próximo backup seja do volume inteiro, em vez de apenas um backup incremental.

Backups e volumes off-line

Você não pode criar ou excluir backups de volume se esse volume estiver off-line. Use o comando `volume show`ONTAPCLI para determinar o estado e o status atuais de um volume.

Para colocar um volume off-line novamente on-line, use o comando `volume online`ONTAPCLI como no exemplo a seguir:

```
::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Criação de um backup iniciado pelo usuário

O procedimento a seguir descreve como usar o console Amazon FSx para criar um backup de um volume iniciado pelo usuário.

Você não pode criar um backup de volume se o volume estiver off-line. Para ter mais informações, consulte Backups e volumes off-line.

Para criar um backup de um volume iniciado pelo usuário (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 ONTAP arquivos do qual você deseja fazer backup de um volume.

3. Escolha a guia Volumes.
4. Escolha o volume do qual deseja fazer o backup.
5. Em Ações, escolha Criar backup.
6. 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 . + - = _ : /
7. Escolha Create backup.

Você acaba de criar um backup de um dos volumes do sistema de arquivos. Você pode encontrar uma tabela de todos os backups no console do Amazon FSx 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.

Ao criar um backup iniciado pelo usuário conforme descrito neste procedimento, ele terá o tipo `USER_INITIATED` e o status `CREATING` até que esteja totalmente disponível.

Restaurando um backup em um novo volume

Os procedimentos a seguir descrevem como restaurar um backup do FSx for ONTAP em um novo volume usando e. AWS Management Console AWS CLI

Para restaurar um backup de volume em um novo volume (Console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação, escolha Backups e, em seguida, escolha o backup de volume FSx for ONTAP que você deseja restaurar.
3. No menu Ações no canto superior direito, escolha Restaurar backup. A página Criar volume a partir do backup é exibida.
4. Escolha a máquina virtual FSx for ONTAP File System and Storage para a qual você deseja restaurar o backup nos menus suspensos.
5. Em Detalhes do volume, há várias seleções. Primeiro, insira o nome do volume. Você pode usar até 203 caracteres alfanuméricos ou sublinhado (_).
6. Em Tamanho do volume, insira qualquer número inteiro no intervalo de 20 a 314572800 para especificar o tamanho em mebibytes (MiB).
7. Para Tipo de volume, escolha Leitura-Gravação (RW) para criar um volume que seja legível e gravável ou Proteção de Dados (DP) para criar um volume que seja somente para leitura e

possa ser usado como destino de um relacionamento. NetApp SnapMirror SnapVault Para ter mais informações, consulte Tipos de volume.

8. Em Caminho da junção, insira um local no sistema de arquivos para montar o volume. O nome deve ter uma barra inicial, por exemplo `/vol3`.
9. Para eficiência de armazenamento, escolha Ativado para ativar os recursos de ONTAP eficiência de armazenamento (desduplicação, compactação e compactação). Para ter mais informações, consulte Eficiência de armazenamento do FSx para ONTAP.
10. Em Estilo de segurança do volume, escolha Unix (Linux), NTFS ou Misto. O estilo de segurança de um volume determina se é dada preferência às ACLs NTFS ou UNIX para acesso multiprotocolo. O modo MISTO não é necessário para acesso multiprotocolo e só é recomendado para usuários avançados.
11. Em Política de snapshots, escolha uma política de snapshots para o volume. Para obter mais informações sobre políticas de snapshots, consulte Políticas de snapshots.

    Se você escolher Política personalizada, especifique o nome da política no campo política personalizada. A política personalizada já deve existir na SVM ou no sistema de arquivos. Você pode criar uma política de snapshot personalizada com a ONTAP CLI ou a API REST. Para obter mais informações, consulte Criar uma política de snapshot na documentação do NetApp ONTAP produto.
12. Em Período de resfriamento da política de divisão em níveis, os valores válidos são de 2 a 183 dias. O período de resfriamento da política de camadas de um volume define o número de dias antes que os dados que não foram acessados sejam marcados como frios e movidos para o armazenamento do grupo de capacidade. Essa configuração afeta somente as políticas `Auto` e `Snapshot-only`.
13. Na seção Avançado, em SnapLockConfiguração, você pode deixar a configuração padrão Desativado ou escolher Ativado para configurar um SnapLock volume. Para obter mais informações sobre como configurar um SnapLock Compliance volume ou um SnapLock Enterprise volume, consulte Como criar um volume do SnapLock Compliance e. Como criar um volume do SnapLock Enterprise Para obter mais informações sobre o SnapLock, consulte Protegendo seus dados com SnapLock.
14. Escolha Confirmar para criar o volume.

Para restaurar um backup de volume em um novo volume (CLI)

Use o comando create-volume-from-backupCLI ou o comando de CreateVolumeFromBackupAPI equivalente para restaurar um backup de volume em um novo volume.

- ```
  $ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
        --name demo --ontap-configuration JunctionPath=/demo, SizeInMegabytes=100000,
   \
        StorageVirtualMachineId=svm-0f04a9c7c27e1908b, TieringPolicy={Name=ALL}
  ```

  A resposta do sistema para uma solicitação bem-sucedida:

  ```
  {
        "Volume": {
            "CreationTime": 1692721488.428,
            "FileSystemId": "fs-07ab735385276ed60",
            "Lifecycle": "CREATING",
            "Name": "demo",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
                "JunctionPath": "/demo",
                "SizeInMegabytes": 100000,
                "StorageEfficiencyEnabled": true,
                "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
                "StorageVirtualMachineRoot": false,
                "TieringPolicy": {
                    "Name": "ALL"
                },
                "OntapVolumeType": "DP",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
            },
            "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
  fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
            "VolumeId": "fsvol-0b6ec764c9c5f654a",
            "VolumeType": "ONTAP",

        }
    }
  ```

Exclusão de um backup

Você pode excluir backups diários automáticos e backups iniciados pelo usuário usando o console, a CLI e a API do Amazon FSx, conforme descrito nos procedimentos a seguir.
  ```

Para excluir backups criados usando AWS Backup, consulte Excluindo backups no Guia do AWS Backup desenvolvedor.

Para excluir um backup (console)

1. Abra o console do Amazon FSx 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 se abre, confirme se o ID do backup mostrado é 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 foram excluídos de forma permanente e irrecuperável.

Para excluir um backup (CLI)

- Use o comando da CLI delete-backup ou a ação de API DeleteBackup equivalente para excluir um FSx para backup de volume do ONTAP, conforme mostrado no exemplo a seguir.

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

A resposta do sistema inclui a ID do backup que está sendo excluído e o status do ciclo de vida, `DELETED` indicando que a solicitação foi bem-sucedida.

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

Trabalhar com snapshots

Um snapshot é uma imagem somente para leitura de um volume Amazon FSx for NetApp ONTAP em um determinado momento. Os snapshots oferecem proteção contra exclusão ou modificação acidental de arquivos nos volumes. Com os instantâneos, seus usuários podem facilmente visualizar

e restaurar arquivos ou pastas individuais de um instantâneo anterior para desfazer alterações, recuperar conteúdo excluído e comparar versões de arquivos.

Um instantâneo contém os dados que foram alterados desde o último instantâneo, que consome a capacidade de armazenamento SSD do sistema de arquivos. Os instantâneos não estão incluídos em nenhum backup de volume. Os instantâneos são habilitados por padrão em seus volumes usando a política de `default` instantâneos. Os snapshots são armazenados no diretório `.snapshot` na raiz de um volume. Você pode armazenar no máximo 1.023 instantâneos por volume a qualquer momento. Depois de atingir esse limite, você deve excluir um instantâneo existente antes que um novo instantâneo do seu volume possa ser criado.

Tópicos

Políticas de snapshots

A política de snapshots define como o sistema cria snapshots para um volume. A política especifica quando criar snapshots, quantas cópias devem ser retidas e como dar nomes a elas. Há três políticas de snapshots integradas do FSx para ONTAP:

- `default`
- `default-1weekly`
- `none`

Por padrão, cada volume está associado à política de snapshots `default` do sistema de arquivos. Recomendamos usar essa política para a maioria das workloads.

A política `default` cria snapshots automaticamente de acordo com a programação a seguir, com as cópias mais antigas de snapshots excluídas para liberar espaço para cópias mais recentes.

- No máximo seis snapshots por hora, feitos cinco minutos depois da hora.
- No máximo dois snapshots por dia, feitos de segunda a sábado, 10 minutos depois da meia-noite.
- No máximo dois snapshots por semana, feitos todos os domingos, 15 minutos depois da meia-noite.

> **Note**
>
> Os horários dos snapshots são baseados no fuso horário do sistema de arquivos, cujo padrão é o Tempo Universal Coordenado (UTC). Para obter informações sobre como alterar o fuso horário, consulte Exibição e configuração do fuso horário do sistema na documentação do NetApp Support.

A política `default-1weekly` funciona da mesma maneira que a política `default`, exceto por reter apenas um snapshot da agenda semanal.

A política `none` não cria nenhum snapshot. Essa política pode ser atribuída a volumes para evitar que snapshots automáticos sejam criados.

Você também pode criar uma política de snapshots personalizada usando a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política de snapshot na documentação do produto NetApp ONTAP. Você pode escolher uma política de snapshot ao criar ou atualizar um volume no console do Amazon FSx, no ou na AWS CLI API do Amazon FSx. Para obter mais informações, consulte Criação de volumes e Atualizar um volume.

Como restaurar arquivos e pastas individuais

Usando os snapshots no sistema de arquivos do Amazon FSx, seus usuários podem restaurar rapidamente versões anteriores de arquivos individuais ou pastas. Isso permite recuperar arquivos excluídos ou alterados armazenados no sistema de arquivos compartilhado. Isso é feito de forma autônoma, diretamente da área de trabalho, sem a ajuda do administrador. Essa abordagem de autoatendimento aumenta a produtividade e reduz a workload administrativa.

Clientes Linux e macOS podem visualizar snapshots no diretório `.snapshot` na raiz de um volume. Os clientes Windows podem visualizar snapshots na guia `Previous Versions` do Windows Explorer (ao clicar com o botão direito do mouse em um arquivo ou pasta).

Restaurar arquivos a partir de instantâneos

Restaurar um arquivo usando um snapshot (clientes Linux e macOS)

1. Se o arquivo original ainda existir e você não quiser substituí-lo pelo arquivo em um snapshot, use o cliente Linux ou macOS para renomear o arquivo original ou movê-lo para outro diretório.
2. No diretório `.snapshot`, localize o snapshot que contém a versão do arquivo que deseja restaurar.
3. Copie o arquivo do diretório `.snapshot` para o diretório no qual o arquivo existia originalmente.

Restaurar um arquivo usando um snapshot (clientes Windows)

Os usuários de clientes Windows podem restaurar arquivos para versões anteriores usando a interface familiar do Explorador de Arquivos do Windows.

1. Para restaurar um arquivo, os usuários escolhem o arquivo a ser restaurado e selecionam Restaurar versões anteriores no menu de contexto (clique com o botão direito do mouse).
2. Os usuários podem então visualizar e restaurar uma versão anterior na lista Versões anteriores.

Os dados em snapshots são somente leitura. Se quiser fazer modificações nos arquivos e pastas listados na guia Versões anteriores, é necessário salvar uma cópia dos arquivos e pastas que deseja modificar em um local gravável e fazer modificações nas cópias.

Exclusão de snapshots

Os instantâneos consomem capacidade de armazenamento somente para os dados em um volume que foi alterado desde o último instantâneo. Por esse motivo, se sua carga de trabalho grava dados rapidamente, os instantâneos de dados antigos podem ocupar uma quantidade significativa da capacidade de armazenamento de um volume.

Por exemplo, a saída do comando `volume show-space`ONTAPCLI mostra 140 KB de. `User Data` No entanto, o volume tinha 9,8 GB de `User Data` antes de os dados do usuário serem excluídos. Mesmo que você tenha excluído os arquivos do volume, um snapshot ainda pode fazer referência a

dados antigos do usuário. Por esse motivo, `Snapshot Reserve` e `Snapshot Spill` no exemplo anterior, ocupam um total de 9,8 GB de espaço, embora praticamente não haja dados do usuário no volume.

Para liberar espaço nos volumes, você pode excluir snapshots mais antigos que não são mais necessários. Você pode fazer isso criando uma política de exclusão automática de instantâneos ou excluindo manualmente os instantâneos. A exclusão de um snapshot exclui os dados alterados armazenados no snapshot.

Crie uma política de exclusão automática de instantâneos

Você pode criar uma política para excluir automaticamente os snapshots quando a quantidade de espaço disponível no volume estiver acabando. Use o comando ONTAPCLI do instantâneo de volume autodelete modify para estabelecer uma política de exclusão automática para um volume.

Ao usar esse comando, use seus dados para substituir os seguintes valores de espaço reservado:

- Substitua *`svm_name`* pelo nome da SVM na qual o volume foi criado.
- Substitua *`vol_name`* pelo nome do volume.

Para `-trigger`, atribua um dos valores a seguir.

- `volume`: use `volume` se quiser que o limite no qual os snapshots são excluídos corresponda a um limite de capacidade total do volume usado. Os limites de capacidade do volume usado que acionam a exclusão do snapshot são determinados pelo tamanho do volume, com o limite sendo escalonado de 85 a 98% da capacidade usada. Volumes menores têm um limite menor e volumes maiores têm um limite maior.
- `snap_reserve`: use `snap_reserve` se quiser que os snapshots sejam excluídos com base no que pode ser mantido na sua reserva de snapshots.

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true
 -trigger [volume|snap_reserve]
```

Para obter mais informações, consulte o comando volume snapshot autodelete modify no Centro de Documentação do NetApp ONTAP.

Excluir snapshots

Use o comando volume snapshot deleteONTAPCLI para excluir manualmente os instantâneos, substituindo os seguintes valores de espaço reservado pelos seus dados:

- Substitua *svm_name* pelo nome da SVM na qual o volume foi criado.
- Substitua *vol_name* pelo nome do volume.
- Substitua *snapshot_name* pelo nome do snapshot. Esse comando é compatível com caracteres curinga (*) para *snapshot_name*. Portanto, você pode excluir todos os snapshots de hora em hora, por exemplo, usando `hourly*`.

> **Important**
>
> Se os backups do Amazon FSx estiverem habilitados, o Amazon FSx retém um snapshot do backup mais recente do Amazon FSx de cada volume. Esses snapshots são usados para manter a incrementalidade entre os backups e não devem ser excluídos usando esse método.

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

Desabilitar snapshots automáticos

Os instantâneos automáticos são habilitados pela política de instantâneos padrão para volumes em seu sistema de arquivos FSx for ONTAP. Se você não precisar de instantâneos dos seus dados (por exemplo, se estiver usando dados de teste), poderá desabilitar os instantâneos definindo a política de instantâneos do volume para none usar a API AWS Management Console, a API AWS CLI e a ONTAP CLI, conforme descrito nos procedimentos a seguir.

Para desativar os instantâneos automáticos (AWS 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 ONTAP para o qual deseja atualizar um volume.
3. Escolha a guia Volumes.

4. Escolha o volume que deseja atualizar.
5. Em Ações, escolha Atualizar volume.

   A caixa de diálogo Atualizar volume é exibida com as configurações atuais do volume.
6. Em Política de snapshot, escolha Nenhuma.
7. Selecione Atualizar para atualizar o volume.

Para desativar os instantâneos automáticos (AWS CLI)

- Use o comando da AWS CLI update-volume (ou o comando de UpdateVolumeAPI equivalente) para definir o comonone, conforme mostrado no exemplo `SnapshotPolicy` a seguir.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=none, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Para desativar os instantâneos automáticos (ONTAPCLI)

Defina a política de instantâneos do volume para usar a política `none` padrão para desativar os instantâneos automáticos.

1. Use o comando `volume snapshot policy show`ONTAPCLI para mostrar a `none` política.

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                         Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ----------------------------------
none                               0 false   Policy for no automatic snapshots.
    Schedule              Count     Prefix                SnapMirror Label
    --------------------- -----     --------------------- -------------------
    -                         -     -                     -
```

2. Use o comando `volume modify`ONTAPCLi para definir a política de instantâneos do volume none para desativar os instantâneos automáticos. Substitua os seguintes valores de espaço reservado pelos seus dados:

   - *svm_name*— use o nome do seu SVM.
   - *vol_name*— use o nome do seu volume.

   Quando for solicitado que continue, insira **y**.

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none

Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
 Snapshot copies on this volume
         that do not match any of the prefixes of the new Snapshot policy will not
 be deleted. However, when
         the new Snapshot policy takes effect, depending on the new retention
 count, any existing Snapshot copies
         that continue to use the same prefixes might be deleted. See the 'volume
 modify' man page for more information.
Do you want to continue? {y|n}: y
Volume modify successful on volume vol_name of Vserver svm_name.
```

Reserva de instantâneos

A reserva de cópias instantâneas define uma porcentagem específica da capacidade de armazenamento de um volume para armazenar cópias instantâneas, com um valor padrão de 5%. A reserva de cópias do Snapshot deve ter espaço suficiente alocado para as cópias do Snapshot, incluindo backups de volume. Se as cópias do Snapshot excederem o espaço de reserva do Snapshot, você deverá excluir as cópias existentes do sistema de arquivos ativo para recuperar a capacidade de armazenamento para uso do sistema de arquivos. Você também pode modificar a porcentagem de espaço em disco alocada às cópias do Snapshot.

Sempre que os instantâneos consomem mais de 100% da reserva de instantâneos, eles começam a ocupar espaço de armazenamento SSD primário. Esse processo é chamado de derrame de instantâneos. Quando os instantâneos continuam ocupando o espaço ativo do sistema de arquivos, o sistema de arquivos corre o risco de ficar cheio. Se o sistema de arquivos ficar cheio devido ao vazamento de instantâneos, você poderá criar arquivos somente depois de excluir instantâneos suficientes.

Quando há espaço em disco suficiente para instantâneos na reserva de instantâneos, a exclusão de arquivos do nível SSD primário libera espaço em disco para novos arquivos, enquanto as cópias de instantâneos que fazem referência a esses arquivos consomem somente o espaço na reserva de cópias de instantâneos.

Como não há como evitar que os instantâneos consumam espaço em disco maior do que a quantidade reservada para eles (a reserva de instantâneos), é importante reservar espaço em disco suficiente para os instantâneos para que a camada principal do SSD sempre tenha espaço disponível para criar novos arquivos ou modificar os existentes.

Se um Snapshot for criado quando os discos estiverem cheios, a exclusão de arquivos da camada SSD primária não criará nenhum espaço livre, pois todos esses dados também são referenciados pelo Snapshot recém-criado. Você deve excluir o Snapshot para liberar espaço de armazenamento para criar ou atualizar qualquer arquivo.

Você pode modificar a quantidade de reserva de Snapshot em um volume usando a NetApp ONTAP CLI. Para ter mais informações, consulte Atualizando a reserva de instantâneos do volume.

Atualizando a reserva de instantâneos do volume

Você pode alterar a quantidade de reserva de Snapshot em um volume usando a NetApp ONTAP CLI ou a API, descrita no procedimento a seguir.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Use o comando `snap reserve` ONTAP CLI para alterar a porcentagem de espaço em disco usada para a reserva de cópias do Snapshot. *`vol_name`*Substitua pelo nome do volume e *`percent`* `with the percent of disk space you want to reserve for Snapshot copies.`

   ```
   ::> snap reserve vol_name percent
   ```

O exemplo a seguir altera a reserva de snapshot para vol1 para 25% da capacidade de armazenamento dos volumes.

```
::> snap reserve vol1 25
```

Replicação programada usando NetApp SnapMirror

Você pode usar NetApp SnapMirror para programar a replicação periódica do seu sistema de arquivos FSx for ONTAP de ou para um segundo sistema de arquivos. Esse recurso está disponível para implantações na região e entre regiões.

NetApp SnapMirror replica dados em alta velocidade, para que você obtenha alta disponibilidade de dados e rápida replicação de dados nos sistemas ONTAP, esteja você replicando entre dois sistemas de arquivos Amazon FSx no local ou no AWS local para. AWS A replicação pode ser programada na frequência de cinco minutos, embora os intervalos devam ser cuidadosamente escolhidos com base em RPOs (objetivos do ponto de recuperação), RTOs (objetivos do tempo de recuperação) e considerações sobre a performance.

Quando você replica dados para sistemas NetApp de armazenamento e atualiza continuamente os dados secundários, seus dados são mantidos atualizados e permanecem disponíveis sempre que você precisar. Não são necessários servidores de replicação externos. Para obter mais informações sobre como usar NetApp SnapMirror para replicar seus dados, consulte Saiba mais sobre o serviço de replicação na documentação do NetApp BlueXP.

Você pode criar um volume de destino de proteção de dados (DP) para NetApp SnapMirror usar o console Amazon FSx, AWS CLI o e a API Amazon FSx, além da CLI e da API REST do NetApp ONTAP. Para obter informações sobre a criação de um volume de destino usando o console Amazon FSx AWS CLI, consulte. Criação de volumes

Você pode usar o NetApp BlueXP ou o NetApp ONTAP CLI para programar a replicação para seu sistema de arquivos.

> **Note**
>
> Há dois tipos de replicação do SnapMirror: SnapMirror em nível de volume e SVM Disaster Recovery (SVMDR). Somente a replicação do SnapMirror em nível de volume tem suporte do FSx para ONTAP.

Usando o NetApp BlueXP para agendar a replicação

Você pode usar o NetApp BlueXP para configurar a replicação em SnapMirror seu sistema de arquivos FSx for ONTAP. Para obter mais informações, consulte Replicação de dados entre sistemas na documentação do NetApp BlueXP.

Usando a CLI do NetApp ONTAP para agendar a replicação

Você pode usar a CLI do NetApp ONTAP para configurar a replicação programada de volumes. Para obter informações, consulte Gerenciando a replicação de SnapMirror volumes no Centro de Documentação do NetApp ONTAP.

Protegendo seus dados com SnapLock

O SnapLock é um recurso que permite proteger seus arquivos fazendo a transição deles para o estado de gravação única e várias leituras (WORM), o que impede modificações ou exclusões dentro de um período de retenção especificado. Você pode usar o SnapLock para atender à conformidade regulatória, proteger dados essenciais aos negócios contra ataques de ransomware e fornecer uma camada adicional de proteção para os dados contra alteração ou exclusão.

O Amazon FSx for NetApp ONTAP suporta os modos de retenção Compliance e Enterprise com. SnapLock Para obter mais informações, consulte SnapLock Enterprise e SnapLock Compatibilidade.

Você pode criar volumes do SnapLock em sistemas de arquivos do FSx para ONTAP criados a partir de 13 de julho de 2023. Os sistemas de arquivos existentes receberão suporte do SnapLock durante uma próxima janela de manutenção semanal.

Tópicos

Como a SnapLock funciona

O SnapLock ajuda você a atender às finalidades regulatórias e de governança, impedindo que seus arquivos sejam excluídos, alterados ou renomeados. Ao criar um volume do SnapLock, você disponibiliza seus arquivos para o armazenamento de gravação única e várias leituras (WORM) e define períodos de retenção para os dados. Seus arquivos podem ser armazenados em um estado não apagável e não gravável por um período designado ou indefinidamente.

> **Important**
>
> Você deve especificar se um volume usará as configurações do SnapLock no momento da criação. Um volume que não pertença ao SnapLock não pode ser convertido em um volume do SnapLock após a criação.

Modos de retenção

O SnapLock tem dois modos de retenção: Compliance e Enterprise. O Amazon FSx for NetApp ONTAP oferece suporte a ambos. Eles têm casos de uso distintos e alguns dos recursos são diferentes, mas ambos protegem seus dados contra modificação ou exclusão usando o modelo WORM. A tabela a seguir explica algumas das semelhanças e diferenças entre esses modos de retenção.

Recurso do SnapLock	SnapLock Compatibilidade	SnapLock Enterprise
Descrição	Os arquivos que recebem a transição para o WORM em um volume Compliance não podem ser excluídos até que seus períodos de retenção expirem.	Os arquivos que recebem a transição para o WORM em um volume Enterprise podem ser excluídos por usuários autorizados antes que seus períodos de retenção expirem usando a exclusão privilegi ada.
Casos de uso	• Tratar de exigência s governamentais ou específicos do setor, como a Norma 17a-4(f) da SEC,	• Promover a integridade dos dados e a conformidade interna de uma organização.

Recurso do SnapLock	SnapLock Compatibilidade	SnapLock Enterprise
	a Norma 4511 da FINRA e a Regulamentação 1.31 da CFTC. • Proteger-se contra ataques de ransomware.	• Testar as configurações de retenção antes de usar o SnapLock Compliance.
Confirmação automática	Sim	Sim
Retenção baseada em eventos (EBR)*	Sim	Sim
Retenções jurídicas*	Sim	Não
Exclusão privilegiada	Não	Sim
Modo de acréscimo de volume	Sim	Sim
Volumes de log de auditoria do SnapLock	Sim	Sim

*Há suporte para as operações de EBR e retenção jurídica na CLI e na API REST do ONTAP.

Administrador da SnapLock

É necessário ter privilégios de administrador do SnapLock para realizar determinadas ações em volumes do SnapLock. Os privilégios de administrador do SnapLock são definidos no perfil de `vsadmin-snaplock` na CLI do ONTAP. É necessário ser administrador de cluster para criar uma conta de administrador na máquina virtual de armazenamento (SVM) com o perfil de administrador do SnapLock.

Você pode realizar as seguintes ações com o perfil de `vsadmin-snaplock` na CLI do ONTAP:

- Gerenciar sua própria conta de usuário, senha local e informações importantes
- Gerenciar volumes, exceto volumes móveis
- Gerenciar cotas, qtrees, cópias de snapshots e arquivos
- Executar ações do SnapLock, incluindo exclusão privilegiada e retenção jurídica

- Configurar os protocolos Network File System (NFS) e Server Message Block (SMB)
- Configurar os serviços do Sistema de Nomes de Domínio (DNS), do Lightweight Directory Access Protocol (LDAP) e do Network Information Service (NIS)
- Monitorar trabalhos

O procedimento a seguir detalha como criar um administrador do SnapLock na CLI do ONTAP. É necessário fazer login como administrador de cluster em uma conexão segura, como o protocolo Secure Shell (SSH), para realizar essa tarefa.

Para criar uma conta de administrador na SVM com o perfil de vsadmin-snaplock na CLI do ONTAP

- Execute o seguinte comando . Substitua *SVM_name* por suas *SnapLockAdmin*próprias informações.

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

Volumes de log de auditoria do SnapLock

Um volume de log de auditoria do SnapLock contém logs de auditoria do SnapLock, contendo timestamps de eventos, como quando um administrador do SnapLock foi criado, quando operações de exclusão privilegiada foram executadas ou quando uma retenção jurídica foi aplicada em arquivos. O volume do log de auditoria do SnapLock é um registro de eventos que não pode ser apagado.

Você deve criar um volume do log de auditoria do SnapLock na mesma SVM do volume do SnapLock para as seguintes ações:

- Ativar ou desativar a exclusão privilegiada em um volume do SnapLock Enterprise.
- Para aplicar a retenção jurídica em um arquivo em um volume do SnapLock Compliance.

> ⚠ Warning
>
> - O período mínimo de retenção para um volume do log de auditoria do SnapLock é de seis meses. Até que esse período de retenção expire, o volume do log de auditoria do

SnapLock, a SVM e o sistema de arquivos associados a ele não poderão ser excluídos, mesmo que o volume tenha sido criado no modo SnapLock Enterprise.

- Se um arquivo for excluído usando a exclusão privilegiada e seu período de retenção for maior que o período de retenção do volume, o volume do log de auditoria herdará o período de retenção do arquivo. Por exemplo, se um arquivo com um período de retenção de dez meses for excluído usando a exclusão privilegiada e o período de retenção do volume do log de auditoria for de seis meses, o período de retenção do volume do log de auditoria será estendido para dez meses.

Você pode ter somente um volume do log de auditoria do SnapLock ativo em uma SVM, mas ele pode ser compartilhado por vários volumes do SnapLock na SVM. Para montar um volume do log de auditoria do SnapLock com êxito, defina o caminho da junção como `/snaplock_audit_log`. Nenhum outro volume pode usar esse caminho da junção, incluindo volumes que não sejam do log de auditoria.

Você pode encontrar logs de auditoria do SnapLock no diretório `/snaplock_log` sob raiz do volume do log de auditoria. As operações de exclusão privilegiadas são registradas em log no subdiretório `privdel_log`. As operações de início e término da retenção jurídica são registradas em log em `/snaplock_log/legal_hold_logs/`. Todos os outros log são armazenados no subdiretório `system_log`.

Você pode criar um volume do log de auditoria do SnapLock com o console do Amazon FSx, a AWS CLI e a API do Amazon FSx, bem como a CLI e a API REST do ONTAP.

> **Note**
>
> Um volume de proteção de dados (DP) não pode ser usado como um volume do log de auditoria do SnapLock.

O procedimento a seguir explica como criar um volume do log de auditoria do SnapLock no console do Amazon FSx.

Criar um volume do log de auditoria do SnapLock no console do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para criar um volume em Criação de volumes.

3. Na seção Avançado, em SnapLock Configuração, escolha Ativado.

   Marque a caixa de seleção para confirmar o aviso sobre habilitar o SnapLock no volume.
4. Em Volume do log de auditoria, escolha Habilitado.

   Certifique-se de que o Caminho da junção esteja definido como `/snaplock_audit_log`.
5. Siga o restante do procedimento para criar um volume em Criação de volumes.
6. Escolha Confirmar para criar o volume.

Para ativar o volume do log de auditoria do SnapLock com a API do Amazon FSx, use `AuditLogVolume` em `CreateSnaplockConfiguration`.

Acessar os dados em um volume do SnapLock

Você pode usar protocolos de arquivos abertos, como NFS e SMB, para acessar seus dados em um volume do SnapLock. Não há impacto na performance ao gravar dados em um volume do SnapLock ou ler dados protegidos pelo WORM.

Você pode copiar arquivos em volumes do SnapLock com NFS e SMB, mas eles não reterão suas propriedades WORM no volume do SnapLock de destino. Você deve reconfirmar os arquivos copiados para o WORM a fim de evitar que sejam modificados ou excluídos. Para ter mais informações, consulte Confirmar arquivos para o estado WORM.

Você também pode replicar dados do SnapLock com o SnapMirror, mas os volumes de origem e destino devem ser volumes do SnapLock com o mesmo modo de retenção (por exemplo, ambos devem ser de Compliance ou Enterprise).

SnapLock Compatibilidade

O Amazon FSx for NetApp ONTAP oferece suporte SnapLock a volumes de conformidade.

Como usar o SnapLock Compliance

Esta seção descreve casos de uso e considerações para o modo de retenção Compliance.

Casos de uso para o SnapLock Compliance

Você pode escolher o modo de retenção Compliance para os casos de uso a seguir.

- Você pode usar o SnapLock Compliance para atender a exigências governamentais ou específicas do setor, como a Norma 17a-4(f) da SEC, a Norma 4511 da FINRA e a Regulamentação 1.31

da CFTC. SnapLock A conformidade com o Amazon FSx for NetApp ONTAP foi avaliada quanto a esses mandatos e regulamentações por. Cohasset Associates Para obter mais informações, consulte o Relatório de avaliação de conformidade do Amazon FSx for NetApp ONTAP.

- Você pode usar o SnapLock Compliance para complementar ou aprimorar uma estratégia abrangente de proteção de dados que combata ataques de ransomware.

Considerações sobre o SnapLock Compliance

Veja a seguir alguns itens importantes a serem considerados sobre o modo de retenção Compliance.

- Depois que é feita a transição de um arquivo para o estado de gravação única e várias leituras (WORM) em um volume do SnapLock Compliance, ele não pode ser excluído por qualquer usuário antes que seu período de retenção expire.
- Um volume do SnapLock Compliance só pode ser excluído quando os períodos de retenção de todos os arquivos WORM no volume expirarem e os arquivos WORM tiverem sido excluídos do volume.
- Não é possível renomear um volume do SnapLock Compliance após a criação.
- Você pode usar SnapMirror para replicar arquivos WORM, mas o volume de origem e o volume de destino devem ter o mesmo modo de retenção (por exemplo, ambos devem estar em conformidade).
- Um volume do SnapLock Compliance não pode ser convertido em um volume do SnapLock Enterprise e vice-versa.

Como criar um volume do SnapLock Compliance

Você pode criar um volume do SnapLock Compliance com o console, a AWS CLI e a API do Amazon FSx, bem como a CLI e a API REST do ONTAP.

Para criar um volume do SnapLock Compliance com a API do Amazon FSx, use `SnaplockType` em `CreateSnaplockConfiguration`.

O procedimento a seguir explica como criar um volume do SnapLock Compliance no console do Amazon FSx.

Criar um volume do SnapLock Compliance no console do Amazon FSx

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

2. Siga o procedimento para criar um volume em Criação de volumes.
3. Na seção Avançado, em SnapLock Configuração, escolha Ativado.

   Marque a caixa de seleção para confirmar o aviso sobre habilitar o SnapLock no volume.
4. Em Modo de retenção, escolha Compliance.
5. Em Volume do log de auditoria, escolha entre Habilitado e Desabilitado.

   Se escolher Habilitado, verifique se o Caminho da junção está definido como `/snaplock_audit_log`.

   Para ter mais informações, consulte Volumes de log de auditoria do SnapLock.
6. Em Período de retenção, insira valores para Retenção padrão, Retenção mínima e Retenção máxima. Em seguida, escolha uma Unidade correspondente para cada uma.

   Para ter mais informações, consulte Trabalhar com o período de retenção no SnapLock.
7. Em Confirmação automática, escolha entre Habilitado e Desabilitado.

   Se escolher Habilitado, em Período de confirmação automática, insira um valor e selecione uma Unidade de confirmação automática correspondente.

   Você pode especificar um valor entre cinco minutos e dez anos.

   Para ter mais informações, consulte Confirmação automática.
8. Em Modo de acréscimo de volume, escolha entre Habilitado e Desabilitado.

   Para ter mais informações, consulte Modo de acréscimo de volume.
9. Siga o restante do procedimento para criar um volume em Criação de volumes.
10. Escolha Confirmar para criar o volume.

SnapLock Enterprise

O Amazon FSx for NetApp ONTAP oferece suporte SnapLock a volumes corporativos.

Como usar o SnapLock Enterprise

Esta seção descreve casos de uso e considerações para o modo de retenção Enterprise.

Casos de uso para o SnapLock Enterprise

Você pode escolher o modo de retenção Enterprise para os casos de uso a seguir.

- Você pode usar o SnapLock Enterprise para autorizar somente usuários específicos a excluir arquivos.
- Você pode usar o SnapLock Enterprise para aprimorar a integridade dos dados e a conformidade interna da sua organização.
- Você pode usar o SnapLock Enterprise para testar as configurações de retenção antes de usar o SnapLock Compliance.

Considerações sobre o uso do SnapLock Enterprise

Veja a seguir alguns itens importantes a serem considerados sobre o modo de retenção Enterprise.

- Você pode usar o SnapMirror para replicar arquivos WORM, mas o volume de origem e o volume de destino devem ter o mesmo modo de retenção (por exemplo, ambos devem ser Enterprise).
- Um volume do SnapLock não pode ser convertido de Enterprise para Compliance ou de Compliance para Enterprise.
- O SnapLock Enterprise não oferece suporte à retenção jurídica.

Exclusão privilegiada

Uma das principais diferenças entre o SnapLock Enterprise e o SnapLock Compliance é que um administrador do SnapLock pode ativar a exclusão privilegiada em um volume do SnapLock Enterprise para permitir que um arquivo seja excluído antes que o período de retenção do arquivo expire. O administrador do SnapLock é o único usuário que pode excluir arquivos de um volume do SnapLock Enterprise que tenha políticas de retenção ativas aplicadas nele. Para ter mais informações, consulte Administrador da SnapLock.

Você pode ativar ou desativar a exclusão privilegiada com o console, a AWS CLI e a API do Amazon FSx, bem como a CLI e a API REST do ONTAP. Para ativar a exclusão privilegiada, primeiro você deve criar um volume de log de auditoria do SnapLock na mesma SVM do volume do SnapLock. Para ter mais informações, consulte Volumes de log de auditoria do SnapLock.

Para ativar a exclusão privilegiada com a API do Amazon FSx, use `PrivilegedDelete` em `CreateSnaplockConfiguration`.

O procedimento a seguir explica como ativar a exclusão privilegiada no console do Amazon FSx.

Ativar a exclusão privilegiada em um volume do SnapLock Enterprise no console do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para criar um volume em Criação de volumes.
3. Na seção Avançado, em SnapLock Configuração, escolha Ativado.

   Marque a caixa de seleção para confirmar o aviso sobre habilitar o SnapLock no volume.
4. Em Modo de retenção, escolha Enterprise.
5. Em Exclusão privilegiada, escolha Habilitado.
6. Siga o restante do procedimento para criar um volume em Criação de volumes.
7. Escolha Confirmar para criar o volume.

> **Note**
>
> Não é possível emitir um comando de exclusão privilegiada para excluir um arquivo de gravação única e várias leituras (WORM) que tenha um período de retenção expirado. Você pode executar uma operação de exclusão normal após o período de retenção expirar.

Você pode optar por desativar a exclusão privilegiada permanentemente, mas essa ação é irreversível. Se a exclusão privilegiada estiver permanentemente desativada, você não precisará ter um volume do log de auditoria do SnapLock associado ao volume do SnapLock Enterprise.

Para desativar permanentemente a exclusão privilegiada com a API do Amazon FSx, use `PrivilegedDelete` em `CreateSnaplockConfiguration`.

Desativar permanentemente a exclusão privilegiada em um volume do SnapLock Enterprise no console do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para criar um volume em Criação de volumes.
3. Na seção Avançado, em SnapLock Configuração, escolha Ativado.

   Marque a caixa de seleção para confirmar o aviso sobre habilitar o SnapLock no volume.

4. Em Modo de retenção, escolha Enterprise.
5. Em Exclusão privilegiada, escolha Desabilitado permanentemente.
6. Siga o restante do procedimento para criar um volume em Criação de volumes.
7. Escolha Confirmar para criar o volume.

Como criar um volume do SnapLock Enterprise

Você pode criar um volume do SnapLock Enterprise com o console do Amazon FSx, a AWS CLI e a API do Amazon FSx, bem como a CLI e a API REST do ONTAP.

Para criar um volume do SnapLock Enterprise com a API do Amazon FSx, use `SnaplockType` em `CreateSnaplockConfiguration`.

Criar um volume do SnapLock Enterprise no console do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para criar um volume em Criação de volumes.
3. Na seção Avançado, em SnapLock Configuração, escolha Ativado.

   Marque a caixa de seleção para confirmar o aviso sobre habilitar o SnapLock no volume.
4. Em Modo de retenção, escolha Enterprise.
5. Em Volume do log de auditoria, escolha entre Habilitado e Desabilitado.

   Se escolher Habilitado, verifique se o Caminho da junção está definido como `/snaplock_audit_log`.

   Para ter mais informações, consulte Volumes de log de auditoria do SnapLock.
6. Em Período de retenção, insira valores para Retenção padrão, Retenção mínima e Retenção máxima. Em seguida, escolha uma Unidade correspondente para cada uma.

   Para ter mais informações, consulte Trabalhar com o período de retenção no SnapLock.
7. Em Confirmação automática, escolha entre Habilitado e Desabilitado.

   Se escolher Habilitado, em Período de confirmação automática, insira um valor e selecione uma Unidade de confirmação automática correspondente.

   Você pode especificar um valor entre cinco minutos e dez anos.

Para ter mais informações, consulte Confirmação automática.

8. Em Exclusão privilegiada, escolha entre Habilitado, Desabilitado e Desabilitado permanentemente.

   Para ter mais informações, consulte Exclusão privilegiada.

9. Em Modo de acréscimo de volume, escolha entre Habilitado e Desabilitado.

   Para ter mais informações, consulte Modo de acréscimo de volume.

10. Siga o restante do procedimento para criar um volume em Criação de volumes.
11. Escolha Confirmar para criar o volume.

Ignorar o modo Enterprise

Se estiver usando o console do Amazon FSx ou a API do Amazon FSx, deverá ter a permissão `fsx:BypassSnapLockEnterpriseRetention` do IAM para excluir um volume do SnapLock Enterprise que contenha arquivos WORM com políticas de retenção ativas.

Para ter mais informações, consulte Excluir volumes do SnapLock.

Trabalhar com o período de retenção no SnapLock

Ao criar um volume do SnapLock, você pode definir um período de retenção padrão para o volume ou o período de retenção para os arquivos de gravação única e várias leituras (WORM) explicitamente. Durante o período de retenção, não é possível excluir nem modificar arquivos protegidos por WORM. O período de retenção é usado para calcular o tempo de retenção. Por exemplo, se fizer a transição de um arquivo para o WORM em 14 de julho de 2023 à meia-noite e definir o período de retenção como cinco anos, o tempo de retenção será até 14 de julho de 2028 à meia-noite.

Para obter mais informações sobre o WORM, consulte Confirmar arquivos para o estado WORM.

Políticas de período de retenção

O período de retenção é determinado pelos valores atribuídos aos seguintes parâmetros:

- Retenção padrão: o período de retenção padrão atribuído a um arquivo WORM se você não fornecer um período de retenção explícito para ele.
- Retenção mínima: o período de retenção mais curto que pode ser atribuído a um arquivo WORM.

- Retenção máxima: o período de retenção mais longo que pode ser atribuído a um arquivo WORM.

> **Note**
>
> Mesmo após o período de retenção expirar, não será possível modificar um arquivo WORM. Você só poderá excluí-lo ou definir um novo período de retenção para ativar a proteção WORM novamente.

Você pode especificar o período de retenção usando várias unidades de tempo diferentes. A tabela a seguir lista os intervalos específicos com suporte.

Tipo	Valor	Observações
Segundos	0 - 65.535	
Minutos	0 - 65.535	
Horas	0 - 24	
Dias	0 - 365	
Meses	0 -12	
Anos	0 - 100	
Infinito	-	Retém os arquivos para sempre. Disponível para Retenção padrão, Retenção máxima e Retenção mínima.
Não especificado*	-	Retém os arquivos até que você defina um período de retenção. Disponível somente para Retenção padrão.

* Ao fazer a transição de arquivos para o WORM com um período de retenção não especificado, eles recebem o período mínimo de retenção configurado para o volume do SnapLock. Ao fazer a transição dos arquivos protegidos por WORM para um tempo de retenção absoluto, o novo período de retenção deve ser maior do que o período mínimo definido anteriormente nos arquivos.

Período de retenção expirado

Após o período de retenção de um arquivo WORM expirar, você poderá excluir o arquivo ou definir um novo período de retenção para ativar a proteção WORM novamente. Os arquivos WORM não são excluídos automaticamente após o período de retenção expirar. Ainda assim, não é possível modificar o conteúdo de um arquivo WORM, mesmo após o período de retenção expirar.

Configurar o período de retenção de um volume do SnapLock

Você pode definir o período de retenção de um volume do SnapLock com o console do Amazon FSx, a AWS CLI e a API do Amazon FSx, bem como a CLI e a API REST do ONTAP.

Para definir o período de retenção com a API do Amazon FSx, use a configuração `SnaplockRetentionPeriod`.

O procedimento a seguir explica como definir o período de retenção no console do Amazon FSx.

Definir o período de retenção de um volume do SnapLock no console do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para criar um volume em Criação de volumes.
3. Na seção Avançado, em SnapLock Configuração, escolha Ativado.

   Marque a caixa de seleção para confirmar o aviso sobre habilitar o SnapLock no volume.
4. Em Período de retenção, insira valores para Retenção padrão, Retenção mínima e Retenção máxima. Em seguida, escolha uma Unidade correspondente para cada uma.
5. Siga o restante do procedimento para criar um volume em Criação de volumes.
6. Escolha Confirmar para criar o volume.

Confirmar arquivos para o estado WORM

Esta seção explica como fazer a transição dos seus arquivos para um estado de gravação única e várias leituras (WORM). Também será discutido o modo de acréscimo de volume, que é uma forma de gravar dados de forma incremental em arquivos protegidos por WORM.

Confirmação automática

Você pode usar a confirmação automática para fazer a transição de arquivos para o WORM se eles não tiverem sido modificados durante um período especificado por você. Você pode ativar a confirmação automática com o console do Amazon FSx, a AWS CLI e a API do Amazon FSx, bem como a CLI e a API REST do ONTAP.

Você pode especificar um período de confirmação automática entre cinco minutos e dez anos. A tabela a seguir lista os intervalos específicos com suporte.

Unidade	Valor
Minutos	5 - 65.535
Horas	1 - 65.535
Dias	1 - 3.650
Meses	1 - 120
Anos	1 a 10

Para ativar a confirmação automática com a API do Amazon FSx, use `AutocommitPeriod` em `CreateSnaplockConfiguration`.

O procedimento a seguir explica como ativar a confirmação automática no console do Amazon FSx.

Ativar a confirmação automática no console do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para criar um volume em Criação de volumes.
3. Na seção Avançado, em SnapLock Configuração, escolha Ativado.

   Marque a caixa de seleção para confirmar o aviso sobre habilitar o SnapLock no volume.

4. Em Confirmação automática, escolha Habilitado.
5. Em Período de confirmação automática, insira um valor e escolha uma Unidade de confirmação automática correspondente.

   Você pode especificar um valor entre cinco minutos e dez anos.
6. Siga o restante do procedimento para criar um volume em Criação de volumes.
7. Escolha Confirmar para criar o volume.

Modo de acréscimo de volume

Não é possível modificar dados existentes em um arquivo protegido por WORM. No entanto, o SnapLock permite que você mantenha a proteção dos dados existentes usando arquivos com acréscimo ao WORM. Por exemplo, você pode gerar arquivos de log ou preservar dados de streaming de áudio ou vídeo enquanto grava dados neles de forma incremental. Você pode ativar ou desativar o modo de acréscimo de volume com o console do Amazon FSx, a AWS CLI e a API do Amazon FSx, bem como a CLI e a API REST do ONTAP.

Requisitos para atualizar o modo de acréscimo de volume

- O volume do SnapLock deve estar desmontado.
- O volume do SnapLock deve estar vazio de cópias de snapshot e dados do usuário.

Para ativar o modo de acréscimo de volume com a API do Amazon FSx, use `VolumeAppendModeEnabled` em `CreateSnaplockConfiguration`.

O procedimento a seguir explica como ativar o modo de acréscimo de volume no console do Amazon FSx.

Ativar o modo de acréscimo de volume no console do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para criar um volume em Criação de volumes.
3. Na seção Avançado, em SnapLock Configuração, escolha Ativado.

   Marque a caixa de seleção para confirmar o aviso sobre habilitar o SnapLock no volume.
4. Em Modo de acréscimo de volume, escolha Habilitado.

5. Siga o restante do procedimento para criar um volume em Criação de volumes.
6. Escolha Confirmar para criar o volume.

Retenção baseada em eventos (EBR)

Você pode usar a retenção baseada em eventos (EBR) para criar políticas personalizadas com períodos de retenção associados. Por exemplo, você pode fazer a transição de todos os arquivos em um caminho especificado para o WORM e definir o período de retenção para um ano com os comandos `snaplock event-retention policy create` e `snaplock event-retention apply`. Ao usar a EBR, é necessário especificar um volume, um diretório ou um arquivo. O período de retenção selecionado ao criar a política de EBR é aplicado a todos os arquivos no caminho especificado.

A EBR é compatível com a CLI e a API REST do ONTAP.

> **Note**
>
> ONTAPnão suporta EBR com FlexGroup volumes.

Os procedimentos a seguir explicam como criar, aplicar, modificar e excluir uma política de EBR. É necessário ser administrador do SnapLock (ter um perfil de `vsadmin-snaplock`) para concluir essas tarefas na CLI do ONTAP. Para ter mais informações, consulte Administrador da SnapLock.

Criar uma política de EBR na CLI do ONTAP

Execute o seguinte comando . Substitua *`p1`* e *`"10 years"`* por suas próprias informações.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

Aplicar uma política de EBR na CLI do ONTAP

Execute o seguinte comando . Substitua *`p1`* e *`slc`* por suas próprias informações. Você pode adicionar um caminho após a barra (/) se quiser especificar um determinado caminho para a política de EBR. Caso contrário, esse comando aplicará a política de EBR a todos os arquivos no volume.

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

Modificar uma política de EBR na CLI do ONTAP

Execute o seguinte comando . Substitua *p1* e *"5 years"* por suas próprias informações.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

Excluir uma política de EBR na CLI do ONTAP

Execute o seguinte comando . Substitua *p1* por suas próprias informações.

```
vs1::> snaplock event-retention policy delete -name p1
```

Comandos relacionados no NetApp Documentation Center:

- snaplock event-retention abort
- snaplock event-retention show-vservers
- snaplock event-retention show
- snaplock event-retention policy show

Retenções jurídicas

É possível reter arquivos WORM por um período indefinido usando a retenção jurídica. Geralmente, a retenção jurídica é usada para fins de litígio. Um arquivo WORM sujeito a uma retenção jurídica não pode ser excluído até que a restrição legal seja suspensa.

A retenção jurídica é compatível com a CLI e a API REST do ONTAP.

> **Note**
>
> ONTAPnão suporta Legal Hold com FlexGroup volumes.

Os procedimentos a seguir explicam como iniciar e encerrar uma retenção jurídica. É necessário ser administrador do SnapLock (ter um perfil de `vsadmin-snaplock`) para concluir essas tarefas na CLI do ONTAP. Para ter mais informações, consulte Administrador da SnapLock.

Iniciar uma retenção jurídica em um arquivo em um volume do SnapLock Compliance com a CLI do ONTAP

Execute o seguinte comando . Substitua *litigation1*, *slc_vol1* e *file1* por suas próprias informações.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Iniciar uma retenção jurídica em todos os arquivos em um volume do SnapLock Compliance com a CLI do ONTAP

Execute o seguinte comando . Substitua *litigation1* e *slc_vol1* por suas próprias informações.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -path /
```

Encerrar uma retenção jurídica em um arquivo em um volume do SnapLock Compliance com a CLI do ONTAP

Execute o seguinte comando . Substitua *litigation1*, *slc_vol1* e *file1* por suas próprias informações.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Encerrar uma retenção jurídica em todos os arquivos em um volume do SnapLock Compliance com a CLI do ONTAP

Execute o seguinte comando . Substitua *litigation1* e *slc_vol1* por suas próprias informações.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -path /
```

> **Note**
>
> Recomendamos que monitore o `-operation-status` com o comando `snaplock legal-hold show` ao emitir uma retenção jurídica para garantir que ela não falhe.

Comandos relacionados no NetApp Documentation Center:

- snaplock legal-hold abort
- snaplock legal-hold dump-files

- snaplock legal-hold dump-litigations
- snaplock legal-hold show

Fazer o backup de volumes do SnapLock

Você pode fazer o backup de volumes do SnapLock para obter proteção adicional de dados. Ao restaurar um volume do SnapLock, as configurações originais do volume, como a retenção padrão, a retenção mínima e a retenção máxima, são preservadas. As configurações de gravação única e várias leituras (WORM) e de retenção jurídica também são preservadas.

> **Note**
>
> Você não pode fazer backup de um SnapLock FlexGroup volume.

Você pode restaurar o backup de um volume do SnapLock como um volume do SnapLock ou que não seja do SnapLock. No entanto, você não pode restaurar o backup de um volume que não seja do SnapLock como um volume do SnapLock.

Para obter mais informações sobre backups, consulte Trabalhar com backups.

Excluir volumes do SnapLock

Você pode excluir um volume do SnapLock Compliance se os períodos de retenção de todos os arquivos de gravação única e várias leituras (WORM) nele estiverem expirados.

> **Note**
>
> Ao encerrar uma Conta da AWS que contenha volumes do SnapLock Enterprise ou do Compliance, a AWS e o FSx para ONTAP suspendem sua conta por 90 dias com seus dados intactos. Se você não reabrir sua conta durante esses 90 dias, a AWS excluirá seus dados, incluindo aqueles em volumes do SnapLock, independentemente das suas configurações de retenção.

Você pode excluir um volume do SnapLock Enterprise a qualquer momento se tiver as permissões apropriadas. É necessário ser administrador do Amazon FSx. Além disso, se estiver usando o console do Amazon FSx ou a API do Amazon FSx, você deve ter a permissão

`fsx:BypassSnapLockEnterpriseRetention` do IAM para excluir um volume do SnapLock Enterprise que contenha dados WORM com uma política de retenção ativa.

> **Warning**
>
> O período mínimo de retenção para um volume do log de auditoria do SnapLock é de seis meses. Até que esse período de retenção expire, você não poderá excluir o volume do log de auditoria do SnapLock, a máquina virtual de armazenamento (SVM) ou o sistema de arquivos associado à SVM, mesmo que o volume tenha sido criado no modo SnapLock Enterprise. Para ter mais informações, consulte Volumes de log de auditoria do SnapLock.

Excluir um volume do SnapLock Enterprise no console do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, selecione Volumes.
3. Escolha o volume que deseja excluir.
4. Em Ações, escolha Excluir volume.
5. Para Bypass SnapLock Enterprise Retention, escolha Sim.
6. Na caixa de diálogo de confirmação, escolha uma das seguintes opções em Criar backup final:
   - Escolha Sim para fazer um backup final do volume. O nome do backup final é exibido.
   - Escolha Não se não quiser um backup final do volume. Você deverá aceitar que, após a exclusão do volume, os backups automáticos não estarão mais disponíveis.
7. Confirme a exclusão do volume inserindo **`delete`** no campo Confirmar exclusão.
8. Escolha Excluir volumes.

Trabalhar com o Microsoft Active Directory no FSx para ONTAP

O Amazon FSx trabalha com o Microsoft Active Directory para se integrar aos seus ambientes existentes. O Active Directory é o serviço de diretório da Microsoft usado para armazenar informações sobre objetos na rede e ajudar administradores e usuários a encontrar e usar essas informações. Esses objetos geralmente incluem recursos compartilhados, como servidores de arquivos e contas de usuários e computadores da rede.

Opcionalmente, você pode unir suas máquinas virtuais de armazenamento (SVMs) FSx for ONTAP ao seu domínio do Active Directory para fornecer autenticação de usuário e controle de acesso em nível de arquivo e pasta. Os clientes do bloco de mensagens do servidor (SMB) podem então usar suas identidades de usuário existentes no Active Directory para se autenticar e acessar os volumes SVM. Seus usuários podem utilizar suas identidades existentes para controlar o acesso a arquivos e pastas individuais. Além disso, você pode migrar arquivos e pastas existentes e as configurações de lista de controle de acesso (ACL) de segurança para o Amazon FSx sem nenhuma modificação.

Ao unir o Amazon FSx for NetApp ONTAP a um Active Directory, você associa as SVMs do sistema de arquivos ao Active Directory de forma independente. Isso significa que você pode ter um sistema de arquivos com algumas SVMs que estão unidas a um Active Directory e outras SVMs que não estão.

Depois que uma SVM é unida a um Active Directory, você pode atualizar as seguintes propriedades de configuração do Active Directory:

- Endereços IP do servidor DNS
- Nome de usuário e senha da conta de serviço autogerenciada do Active Directory

Tópicos

Pré-requisitos para unir uma SVM a um Microsoft AD autogerenciado

Antes de associar uma SVM do FSx para ONTAP a um domínio do Microsoft AD autogerenciado, verifique se o Active Directory e a rede atendem aos requisitos descritos nas seções a seguir.

Tópicos

Requisitos do Active Directory on-premises

Verifique se você já tem um Microsoft AD on-premises ou autogerenciado ao qual possa unir a SVM. Esse Active Directory deve ter a seguinte configuração:

- O nível funcional do domínio do controlador de domínio do Active Directory está no Windows Server 2000 ou superior.
- O Active Directory usa um nome de domínio que não está no formato SLD (Single Label Domain). O Amazon FSx não é compatível com domínios de SLD.
- Se você tiver sites do Active Directory definidos, certifique-se de que as sub-redes na VPC associadas ao seu sistema de arquivos FSx for ONTAP estejam definidas nos mesmos sites do Active Directory e que não existam conflitos entre as sub-redes da VPC e as sub-redes nos sites do Active Directory.

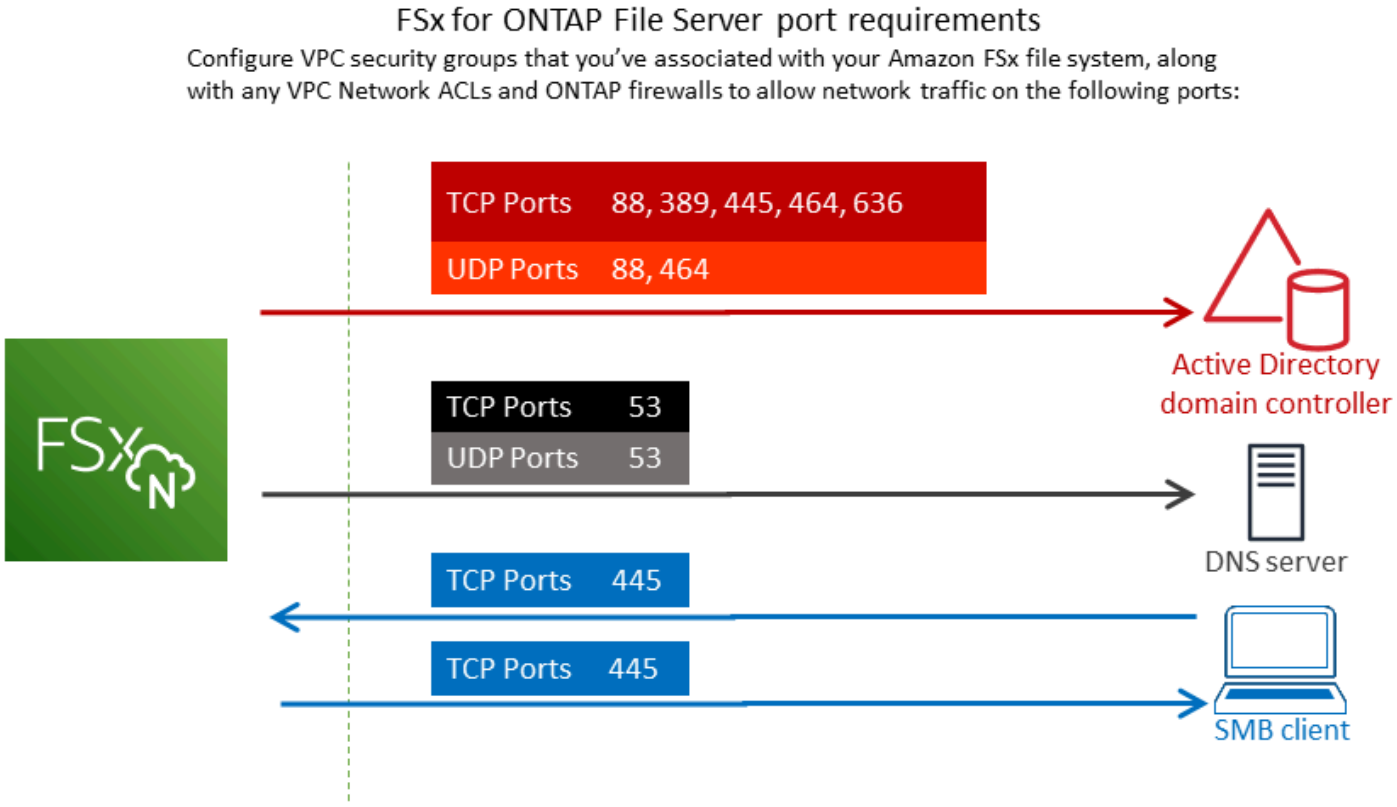
> **Note**
>
> Se você estiver usando AWS Directory Service, o FSx for ONTAP não suporta a junção de SVMs ao Simple Active Directory.

Requisitos de configuração de rede

Confira se você tem as configurações de rede a seguir e as informações associadas disponíveis para você.

> **Important**
>
> Para a junção de uma SVM com o Active Directory, você precisa garantir que as portas documentadas neste tópico permitam tráfego entre todos os controladores de domínio do Active Directory e os dois endereços IP iSCSI (as interfaces lógicas iscsi_1 e iscsi_2) na SVM.

- Os endereços IP do servidor DNS e do controlador de domínio do Active Directory.
- Conectividade entre a Amazon VPC em que você está criando o sistema de arquivos e o Active Directory autogerenciado usando AWS Direct Connect, AWS VPN ou AWS Transit Gateway.
- O grupo de segurança e as ACLs da rede VPC para as sub-redes em que você está criando o sistema de arquivos devem permitir tráfego nas portas e nas direções mostradas no diagrama a seguir.



A função de cada porta é descrita na tabela a seguir.

Protocolo	Portas	Função
TCP/UDP	53	Domain Name System (DNS)
TCP/UDP	88	Autenticação de Kerberos
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)
TCP	445	Compartilhamento de arquivos de SMB para serviços de diretório
TCP/UDP	464	Alterar/definir senha
TCP	636	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)

- Essas regras de tráfego também devem ser espelhadas nos firewalls que se aplicam a cada um dos controladores de domínio do Active Directory, servidores DNS, clientes FSx e administradores FSx.

> **Important**
>
> Embora os grupos de segurança da Amazon VPC exijam que as portas sejam abertas apenas na direção em que o tráfego de rede é iniciado, a maioria dos firewalls do Windows e das ACLs das redes VPC exige que as portas sejam abertas nas duas direções.

Requisitos de conta de serviço do Active Directory

Confira se você tem uma conta de serviço em seu Microsoft AD autogerenciado, com permissões delegadas para unir computadores ao domínio. Uma conta de serviço é uma conta de usuário em seu Active Directory autogerenciado à qual foram delegadas determinadas tarefas.

No mínimo, as seguintes permissões devem ser delegadas à conta de serviço na UO à qual você está unindo a SVM:

- Capacidade de redefinir senhas
- Capacidade de restringir contas de ler e gravar dados

- Capacidade de definir a `msDS-SupportedEncryptionTypes` propriedade em objetos de computador
- Capacidade validada para gravar no nome do host DNS
- Capacidade validada para gravar no nome da entidade principal de serviço
- Capacidade para criar e excluir objetos de computador
- Capacidade validada para ler e gravar restrições de conta

Elas representam o conjunto mínimo de permissões necessárias para associar objetos de computador ao Active Directory. Para obter mais informações, consulte o tópico da documentação do Windows Server Erro: o acesso é negado quando usuários não administradores que receberam controle delegado tentam unir computadores a um controlador de domínio.

Para saber mais sobre como criar uma conta de serviço com as permissões corretas, consulte Delegar permissões à conta de serviço do Amazon FSx.

> **Important**
>
> O Amazon FSx exige uma conta de serviço válida durante toda a vida útil do sistema de arquivos do Amazon FSx. O Amazon FSx deve ser capaz de gerenciar totalmente o sistema de arquivos e executar tarefas que exijam que ele desassocie e reuna recursos ao seu domínio do Active Directory. Essas tarefas incluem a substituição de um sistema de arquivos ou SVM com falha ou a correção do software NetApp ONTAP. Mantenha suas informações de configuração do Active Directory atualizadas com o Amazon FSx, incluindo as credenciais da conta de serviço. Para saber mais, consulte Manter a configuração do Active Directory atualizada com o Amazon FSx.

Se esta é a primeira vez que você usa AWS um FSx for ONTAP, certifique-se de concluir as etapas iniciais de configuração antes de iniciar sua integração com o Active Directory. Para ter mais informações, consulte Configurar o FSx para ONTAP.

> **Important**
>
> Não mova objetos de computador que o Amazon FSx cria na OU após a criação das SVMs, nem exclua o Active Directory enquanto a SVM estiver associada a ele. Isso fará com que as SVMs sejam configuradas incorretamente.

Práticas recomendadas para trabalhar com o Active Directory

Aqui estão algumas sugestões e diretrizes que você deve considerar ao unir as SVMs do Amazon FSx for NetApp ONTAP ao seu Microsoft Active Directory autogerenciado. Observe que elas são práticas recomendadas, mas não obrigatórias.

Delegar permissões à conta de serviço do Amazon FSx

Certifique-se de configurar a conta de serviço fornecida ao Amazon FSx com as permissões mínimas necessárias. Além disso, separe a unidade organizacional (UO) de outras preocupações do controlador de domínio.

Para associar as SVMs do Amazon FSx ao seu domínio, certifique-se de que a conta de serviço tenha as permissões delegadas. Os membros do grupo Administradores de domínio têm permissões suficientes para realizar essa tarefa. No entanto, como prática recomendada, use uma conta de serviço que tenha apenas as permissões mínimas necessárias para fazer isso. O procedimento a seguir demonstra como delegar somente as permissões necessárias para associar as SVMs do FSx para ONTAP ao domínio.

Execute este procedimento em uma máquina que esteja associada ao seu diretório e tenha instalado o snap-in do MMC Active Directory User and Computers.

Para criar uma conta de serviço para seu domínio do Microsoft Active Directory

1. Verifique se você está conectado como administrador de domínio do seu domínio do Microsoft Active Directory.
2. Abra o snap-in do MMC de Computadores e Uuários do Active Directory.
3. No painel de tarefas, expanda o nó do domínio.
4. Localize e abra o menu de contexto (clique com o botão direito do mouse) na UO que deseja modificar e selecione Delegar controle.
5. Na página Assistente de delegação de controle, escolha Próximo.
6. Escolha Adicionar para adicionar um usuário específico ou um grupo específico em Usuários e grupos selecionados e selecione Próximo.
7. Na página Tasks to Delegate (Tarefas para delegar), selecione Create a custom task to delegate (Criar uma tarefa personalizada para delegar) e, em seguida, selecione Next (Avançar).
8. Escolha Somente os objetos a seguir na pasta, e depois Objetos de computador.

9. Selecione Criar objetos selecionados nesta pasta e Excluir objetos selecionados nesta pasta. Em seguida, escolha Próximo.
10. Em Mostrar essas permissões, certifique-se de que Geral e Específico da propriedade estejam selecionados.
11. Em Permissões, escolha o seguinte:
    - Redefinir senha
    - Restrições de leitura e gravação da conta
    - Gravação validada no nome do host DNS
    - Gravação validada no nome da entidade principal do serviço
    - Escreva MSDs- SupportedEncryptionTypes
12. Escolha Next (Próximo) e, em seguida, escolha Finish (Concluir).
13. Feche o snap-in do MMC de Computadores e Usuários do Active Directory.

> **Important**
>
> Não mova objetos de computador que o Amazon FSx cria na UO após a criação das SVMs. Isso fará com que as SVMs sejam configuradas incorretamente.

Manter a configuração do Active Directory atualizada com o Amazon FSx

Para obter disponibilidade ininterrupta das SVMs do Amazon FSx, atualize a configuração do Active Directory (AD) autogerenciado de uma SVM ao alterar sua configuração do AD autogerenciado.

Por exemplo, suponha que o seu AD use uma política de redefinição de senha baseada em tempo. Nesse caso, assim que a senha for redefinida, certifique-se de atualizar a senha da conta de serviço com o Amazon FSx. Para isso, use o console do Amazon FSx, a API do Amazon FSx ou a AWS CLI. Da mesma forma, se os endereços IP do servidor DNS mudarem no seu domínio do Active Directory, assim que a alteração ocorrer, atualize os endereços IP do servidor DNS com o Amazon FSx.

Se houver um problema com a configuração atualizada do AD autogerenciado, o estado da SVM mudará para Configuração incorreta. Esse estado mostra uma mensagem de erro e uma ação recomendada ao lado da descrição da SVM no console, na API e na CLI. Se ocorrer um problema com a configuração do AD da SVM, certifique-se de seguir a ação corretiva recomendada para as

propriedades de configuração. Se o problema for resolvido, verifique se o estado da SVM muda para Criado.

Para obter mais informações, consulte Modificar uma configuração do Active Directory usando a CLI do ONTAP e Atualização de uma configuração existente do SVM Active Directory usando a AWS Management Console API, AWS CLI, e.

Como usar grupos de segurança para limitar o tráfego na VPC

Para limitar o tráfego de rede na nuvem privada virtual (VPC), você pode implementar o princípio do privilégio mínimo na VPC. Em outras palavras, você pode limitar as permissões ao mínimo necessário. Para isso, use as regras do grupo de segurança. Para saber mais, consulte Grupos de segurança da Amazon VPC.

Como criar regras de saída de grupo de segurança para a interface de rede do sistema de arquivos

Para maior segurança, considere configurar um grupo de segurança com regras de tráfego de saída. Essas regras devem permitir o tráfego de saída somente para os controladores de domínios do AD autogerenciado ou dentro da sub-rede ou do grupo de segurança. Aplique esse grupo de segurança à VPC associada à interface de rede elástica do sistema de arquivos do Amazon FSx. Para saber mais, consulte Controle de acesso ao sistema de arquivos com a Amazon VPC.

Junção de SVMs com um Microsoft Active Directory

Sua organização pode gerenciar identidades e dispositivos usando um Active Directory, seja no local ou na nuvem. Com o FSx for ONTAP, você pode unir suas SVMs diretamente ao seu domínio existente do Active Directory das seguintes formas:

- Unindo novas SVMs a um Active Directory na criação:
  - Usando a opção de criação padrão no console do Amazon FSx para criar um novo FSx para o sistema de arquivos ONTAP, você pode unir o SVM padrão a um Active Directory autogerenciado. Para ter mais informações, consulte Criar um sistema de arquivos (console).
  - Usando o console Amazon FSx ou a API Amazon FSx para criar uma nova SVM em um sistema de arquivos FSx for ONTAP existente. AWS CLI Para ter mais informações, consulte Como criar uma máquina virtual de armazenamento.
- Unindo SVMs existentes a um Active Directory:

- Usando a API AWS Management Console AWS CLI, e para unir uma SVM a um Active Directory e tentar unir novamente uma SVM a um Active Directory se a tentativa inicial de associação falhar. Você também pode atualizar algumas propriedades de configuração do Active Directory para SVMs que já estão associadas a um Active Directory. Para ter mais informações, consulte Gerenciando configurações do SVM Active Directory.
- Usando a CLI do NetApp ONTAP ou a API REST para unir, tentar unir e desassociar novamente as configurações do SVM Active Directory. Para ter mais informações, consulte Gerenciando a configuração do SVM Active Directory usando a CLI NetApp .

⚠ Important

- O Amazon FSx só fará registros de DNS para uma SVM se você usar o Microsoft DNS como serviço DNS padrão. Se você usar um DNS de terceiros, configure entradas de DNS manualmente para suas SVMs do Amazon FSx depois de criá-las.
- Se você usa AWS Managed Microsoft AD, você deve especificar um grupo como Administradores AWS Delegados FSx AWS , Administradores Delegados ou um grupo personalizado com permissões delegadas para a OU.

Quando você une um FSx for ONTAP SVM diretamente a um Active Directory autogerenciado, o SVM reside na mesma floresta do Active Directory (o contêiner lógico mais alto em uma configuração do Active Directory que contém domínios, usuários e computadores) e no mesmo domínio do Active Directory que seus usuários e recursos existentes, incluindo servidores de arquivos existentes.

Informações necessárias ao unir uma SVM a um Active Directory

Você precisa fornecer as seguintes informações sobre seu Active Directory ao associar uma SVM a um Active Directory, independentemente da operação de API escolhida:

- O nome NetBIOS do objeto de computador do Active Directory que será criado para a SVM. Esse é o nome do SVM no Active Directory, que deve ser exclusivo em seu Active Directory. Não use o nome NetBIOS do domínio inicial. O nome NetBIOS não pode ter mais de 15 caracteres.
- O nome de domínio totalmente qualificado (FQDN) do Active Directory. O FQDN não pode ter mais de 255 caracteres.

> **Note**
>
> O FQDN não pode estar no formato de domínio de rótulo único (SLD). O Amazon FSx não é compatível com domínios de SLD.

- Até três endereços IP dos servidores DNS ou dos hosts do domínio.

  Os endereços IP do servidor DNS e os endereços IP do controlador de domínio do Active Directory podem estar em qualquer intervalo de endereços IP, exceto:

  - endereços IP que entram em conflito com aqueles de propriedade da Amazon Web Services nessa Região da AWS. Para obter uma lista de endereços AWS IP por região, consulte os intervalos de endereços AWS IP.
  - Endereços IP no seguinte intervalo de blocos CIDR: 198.19.0.0/16
- Nome de usuário e senha de uma conta de serviço em seu domínio do Active Directory para o Amazon FSx usar ao unir a SVM ao domínio do Active Directory. Para obter mais informações sobre requisitos de conta de serviço, consulte Requisitos de conta de serviço do Active Directory.
- (Opcional) A Unidade Organizacional (UO) no domínio ao qual você une a SVM.

> **Note**
>
> Se você unir sua SVM a um AWS Directory Service Active Directory, deverá fornecer uma OU que esteja dentro da OU padrão AWS Directory Service criada para os objetos de diretório relacionados a. AWS Isso ocorre porque o AWS Directory Service não fornece acesso à `Computers` OU padrão do Active Directory. Por exemplo, se o seu domínio do Active Directory for`example.com`, você pode especificar a seguinte OU:`OU=Computers,OU=example,DC=example,DC=com`.

- (Opcional) O grupo de domínio ao qual você está delegando autoridade para executar ações administrativas em seu sistema de arquivos. Por exemplo, esse grupo de domínio pode gerenciar compartilhamentos de arquivos SMB do Windows, assumir a propriedade de arquivos e pastas e assim por diante. Se você não especificar esse grupo, o Amazon FSx delegará essa autoridade ao grupo de administradores de domínio em seu domínio do Active Directory por padrão.

Gerenciando configurações do SVM Active Directory

Esta seção descreve como usar a API AWS Management Console, AWS CLI, FSx e a CLI ONTAP para fazer o seguinte:

- Unindo uma SVM existente a um Active Directory
- Modificando uma configuração existente do SVM Active Directory
- Removendo SVMs de um Active Directory

Para remover uma SVM de um Active Directory, você deve usar a NetApp CLI do ONTAP.

Tópicos

Unindo uma SVM a um Active Directory usando a API AWS Management Console, AWS CLI e

Use o procedimento a seguir para unir uma SVM existente a um Active Directory. Nesse procedimento, o SVM ainda não está associado a um Active Directory.

Para unir uma SVM a um Active Directory () AWS Management Console

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha o SVM que você deseja associar a um Active Directory:

   - No painel de navegação à esquerda, escolha Sistemas de arquivos e, em seguida, escolha o sistema de arquivos do ONTAP com a SVM que você deseja atualizar.
   - Escolha a guia Máquinas virtuais de armazenamento.

     Ou

   - Para exibir uma lista de todas as SVMs disponíveis, no painel de navegação esquerdo, expanda ONTAP e escolha Máquinas virtuais de armazenamento. Uma lista de todas as SVMs em sua conta no Região da AWS é exibida.

Selecione o SVM que você deseja associar a um Active Directory na lista.

3. No canto superior direito do painel Resumo da SVM, escolha Ações > Ingressar/atualizar o Active Directory. A janela Integrar a SVM a um Active Directory é exibida.
4. Insira as seguintes informações para o Active Directory ao qual você está ingressando no SVM:

   - O nome NetBIOS do objeto de computador do Active Directory a ser criado para seu SVM. Esse é o nome do SVM no Active Directory, que deve ser exclusivo em seu Active Directory. Não use o nome NetBIOS do domínio inicial. O nome NetBIOS não pode ter mais de 15 caracteres.
   - O nome de domínio totalmente qualificado (FQDN) do Active Directory. O nome do domínio não pode ter mais de 255 caracteres.
   - Endereços IP do servidor DNS: os endereços IPv4 dos servidores DNS do seu domínio.
   - Nome de usuário da conta de serviço: o nome de usuário da conta de serviço no seu Active Directory existente. Não inclua um prefixo ou sufixo de domínio. Por exemplo, para `EXAMPLE\ADMIN`, use apenas `ADMIN`.
   - Senha da conta de serviço: a senha da conta de serviço.
   - Confirmar senha: a senha da conta de serviço.
   - (Opcional) Unidade organizacional (UO): o nome do caminho distinto da unidade organizacional à qual você deseja unir sua SVM.
   - Grupo de administradores delegado do sistema de arquivos: o nome do grupo no Active Directory que pode administrar o sistema de arquivos.

     Se você estiver usando AWS Managed Microsoft AD, você deve especificar um grupo como Administradores AWS Delegados FSx AWS , Administradores Delegados ou um grupo personalizado com permissões delegadas para a OU.

     Se você estiver ingressando em um Active Directory autogerenciado, use o nome do grupo em seu Active Directory. O grupo padrão é `Domain Admins`.
5. Escolha Ingressar no Active Directory para unir o SVM ao Active Directory usando a configuração que você forneceu.

Para unir uma SVM a um Active Directory (AWS CLI)

- Para unir um FSx for ONTAP SVM a um Active Directory, use o comando update-storage-virtual-machineCLI (ou a operação de UpdateStorageVirtualMachineAPI equivalente), conforme mostrado no exemplo a seguir.

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
\
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Depois de criar com êxito a máquina virtual de armazenamento, o Amazon FSx retorna a descrição no formato JSON, conforme mostrado no exemplo a seguir.

```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
```

```
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],

  }
}
```


Atualização de uma configuração existente do SVM Active Directory usando a AWS Management Console API, AWS CLI, e

Use o procedimento a seguir para atualizar a configuração do Active Directory de uma SVM que já está associada a um Active Directory.

Para atualizar uma configuração do SVM Active Directory () AWS Management Console

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha a SVM a ser atualizada da seguinte forma:

- No painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema de arquivos do ONTAP com a SVM que você deseja atualizar.
- Escolha a guia Máquinas virtuais de armazenamento.

  Ou

- Para exibir uma lista de todas as SVMs disponíveis, no painel de navegação esquerdo, expanda ONTAP e escolha Máquinas virtuais de armazenamento.

  Selecione a SVM que você deseja atualizar na lista.

3. No painel Resumo da SVM, escolha Ações > Ingressar/atualizar o Active Directory. A janela Atualizar a configuração do Active Directory da SVM é exibida.
4. Você pode atualizar as seguintes propriedades de configuração do Active Directory nessa janela.
   - Endereços IP do servidor DNS: os endereços IPv4 dos servidores DNS do seu domínio.
   - Nome de usuário da conta de serviço: o nome de usuário da conta de serviço em seu Active Directory existente. Não inclua um prefixo ou sufixo de domínio. Para `EXAMPLE\ADMIN`, use `ADMIN`.
   - Senha da conta de serviço — A senha da conta de serviço do Active Directory.
5. Depois de informar suas atualizações, escolha Atualizar o Active Directory para fazer as alterações.

Use o procedimento a seguir para atualizar a configuração do Active Directory de uma SVM que já está associada a um Active Directory.

Para atualizar uma configuração do SVM Active Directory () AWS CLI

- Para atualizar a configuração do Active Directory de uma SVM com a API AWS CLI ou, use o comando update-storage-virtual-machineCLI (ou a operação de API UpdateStorageVirtualMachineequivalente), conforme mostrado no exemplo a seguir.

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-abcdef0123456789a\
    --active-directory-configuration \
    SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
    Password="password", \
```

```
    DnsIps=["10.0.1.18"]}'
```

Gerenciando a configuração do SVM Active Directory usando a CLI NetApp

Você pode usar a CLI do NetApp ONTAP para unir e desassociar sua SVM a um Active Directory e para modificar uma configuração existente do SVM Active Directory.

Unindo uma SVM a um Active Directory usando a CLI do ONTAP

Você pode unir SVMs existentes a um Active Directory usando a CLI do ONTAP, conforme descrito no procedimento a seguir. Você pode fazer isso mesmo se sua SVM já estiver associada a um Active Directory.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.
2. Crie uma entrada de DNS do Active Directory fornecendo o nome DNS completo do diretório (`corp.example.com`) e pelo menos um endereço IP do servidor DNS.

   ```
   ::>vserver services name-service dns create -vserver svm_name -
   domains corp.example.com -name-servers dns_ip_1, dns_ip_2
   ```

   Para verificar a conexão com os servidores DNS, execute o comando a seguir. Substitua *`svm_name`* pelas próprias informações.

   ```
   FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name

                               Name Server
   Vserver       Name Server     Status       Status Details
   ------------- --------------- ------------ --------------------------
   svm_name      172.31.14.245   up           Response time (msec): 0
   svm_name      172.31.25.207   up           Response time (msec): 1
   2 entries were displayed.
   ```

3. Para unir a SVM ao Active Directory, execute o comando a seguir. Observe que você deverá especificar um `computer_name` que ainda não exista no Active Directory e fornecer o nome DNS do diretório para o `-domain`. Para `-OU`, insira as UOs nas quais você deseja que a SVM ingresse, bem como o nome DNS completo no formato DC.

```
::>vserver cifs create -vserver svm_name -cifs-server computer_name -
domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
```

Para verificar o status da sua conexão com o Active Directory, execute o seguinte comando:

```
::>vserver cifs check -vserver svm_name

              Vserver : svm_name
                    Cifs NetBIOS Name : svm_netBIOS_name
                          Cifs Status : Running
                                 Site : Default-First-Site-Name
Node Name       DC Server Name  DC Server IP    Status   Status Details
--------------- --------------  --------------- ------   --------------
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245   up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245   up       Response time (msec): 20
2 entries were displayed.
```

4. Se você não conseguir acessar compartilhamentos após essa junção, determine se a conta que você está usando para acessar o compartilhamento tem permissões. Por exemplo, se você estiver usando a `Admin` conta padrão (um administrador delegado) com um Active Directory AWS gerenciado, deverá executar o seguinte comando no ONTAP. O `netbios_domain` corresponde ao nome de domínio do Active Directory (para`corp.example.com`, o `netbios_domain` usado aqui é`example`).

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
 svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

Modificar uma configuração do Active Directory usando a CLI do ONTAP

Você pode usar a CLI do ONTAP para modificar uma configuração existente do Active Directory.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Execute o comando a seguir para derrubar temporariamente o servidor CIFS da SVM:

   ```
   FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
   ```

3. Se você precisar modificar as entradas de DNS do seu Active Directory, execute o seguinte comando:

   ```
   ::>vserver services name-service dns modify -vserver svm_name -
   domains corp.example.com -name-servers dns_ip_1,dns_ip_2
   ```

   Você pode validar o status da conexão com os servidores DNS do Active Directory usando o `vserver services name-service dns check -vserver svm_name` comando.

   ```
   ::>vserver services name-service dns check -vserver svm_name
                                Name Server
   Vserver       Name Server    Status       Status Details
   ------------- -------------- ------------ --------------------------
   svmciad       dns_ip_1       up           Response time (msec): 1
   svmciad       dns_ip_2       up           Response time (msec): 1
   2 entries were displayed.
   ```

4. Se você precisar modificar a própria configuração do Active Directory, poderá alterar os campos existentes usando o seguinte comando, substituindo:

   - *computer_name*, se você quiser modificar o nome NetBIOS (conta da máquina) da SVM.
   - *domain_name*, se você quiser modificar o nome do domínio. Isso deverá corresponder à entrada do domínio do DNS anotada na Etapa 3 desta seção (`corp.example.com`).
   - `organizational_unit`, se você quiser modificar UO (`OU=Computers,OU=example,DC=corp,DC=example,DC=com`).

Você precisará inserir novamente as credenciais do Active Directory que você usou para associar esse dispositivo ao Active Directory.

```
::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
domain domain_name -OU organizational_unit
```

Você pode verificar o status da conexão do Active Directory usando o `vserver cifs check -vserver svm_name` comando.

5. Ao terminar de modificar a configuração do Active Directory e do DNS, reinicie o servidor CIFS executando o seguinte comando:

```
::>vserver cifs modify -vserver svm_name -status-admin up
```

Desassocie um Active Directory do seu SVM usando a CLI do NetApp ONTAP

A CLI do NetApp ONTAP também pode ser usada para desassociar seu SVM de um Active Directory seguindo as etapas abaixo:

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Exclua o servidor CIFS que desassociou seu dispositivo do Active Directory executando o comando a seguir. Para que o ONTAP exclua a conta da máquina do seu SVM, forneça as credenciais que você usou originalmente para associar o SVM ao Active Directory.

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Se você precisar modificar as entradas de DNS do seu Active Directory, execute o seguinte comando:

```
FsxId0123456789a::vserver cifs delete -vserver svm_name
```

```
In order to delete an Active Directory machine account for the CIFS server, you
 must supply the name and password of a Windows account with
sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

Enter the user name: user_name

Enter the password:

Warning: There are one or more shares associated with this CIFS server
         Do you really want to delete this CIFS server and all its shares? {y|n}: y
```

4. Exclua os servidores DNS do seu Active Directory executando o seguinte comando:

```
::vserver services name-service dns delete -vserver svm_name
```

Se você receber um aviso como o seguinte, indicando que ele `dns` deve ser removido como um, `ns-switch` e você não planeja unir novamente esse dispositivo a um Active Directory, você pode remover as entradas. `ns-switch`

```
Warning: "DNS" is present as one of the sources in one or more ns-switch databases
 but no valid DNS configuration was found for Vserver
         "svm_name". Remove "DNS" from ns-switch using the "vserver services name-
service ns-switch" command. Configuring "DNS" as a source
         in the ns-switch setting when there is no valid configuration can cause
 protocol access issues.
```

5. (Opcional) Remova as entradas `ns-switch` do `dns` executando o comando a seguir. Verifique a ordem de fontes e, em seguida, remova a entrada `dns` do banco de dados `hosts` modificando as `sources` para que elas contenham apenas as outras fontes listadas. Neste exemplo, a única outra fonte é `files`.

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts

                    Vserver: svm_name
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

6. (Opcional) Remova a entrada dns modificando as `sources` para que o host do banco de dados inclua apenas `files`.

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

Amazon FSx para NetApp desempenho de ONTAP

Veja a seguir uma visão geral do desempenho do sistema de arquivos Amazon FSx for NetApp ONTAP, com uma discussão sobre as opções disponíveis de desempenho e taxa de transferência e dicas úteis de desempenho.

Tópicos

Como a performance é avaliada nos sistemas de arquivos do FSx para ONTAP

A performance do sistema de arquivos é avaliada por latência, throughput e operações de E/S por segundo (IOPS).

Latência

O Amazon FSx for NetApp ONTAP fornece latências de operação de arquivos abaixo de um milissegundo com armazenamento em unidade de estado sólido (SSD) e dezenas de milissegundos de latência para armazenamento em pool de capacidade. Além disso, o Amazon FSx tem duas camadas de armazenamento em cache de leitura em cada servidor de arquivos, nas unidades de NVMe (memória não volátil expressa) e em memória, para fornecer latências ainda mais baixas ao acessar seus dados lidos com mais frequência.

Throughput e IOPS

Cada sistema de arquivos Amazon FSx fornece até dezenas de GB/s de taxa de transferência e milhões de IOPS. A quantidade específica de taxa de transferência e IOPS que sua carga de trabalho pode gerar no sistema de arquivos depende da capacidade total de taxa de transferência

e da configuração da capacidade de armazenamento do sistema de arquivos, juntamente com a natureza da carga de trabalho, incluindo o tamanho do conjunto de trabalho ativo.

Suporte para SMB Multichannel e NFS nconnect

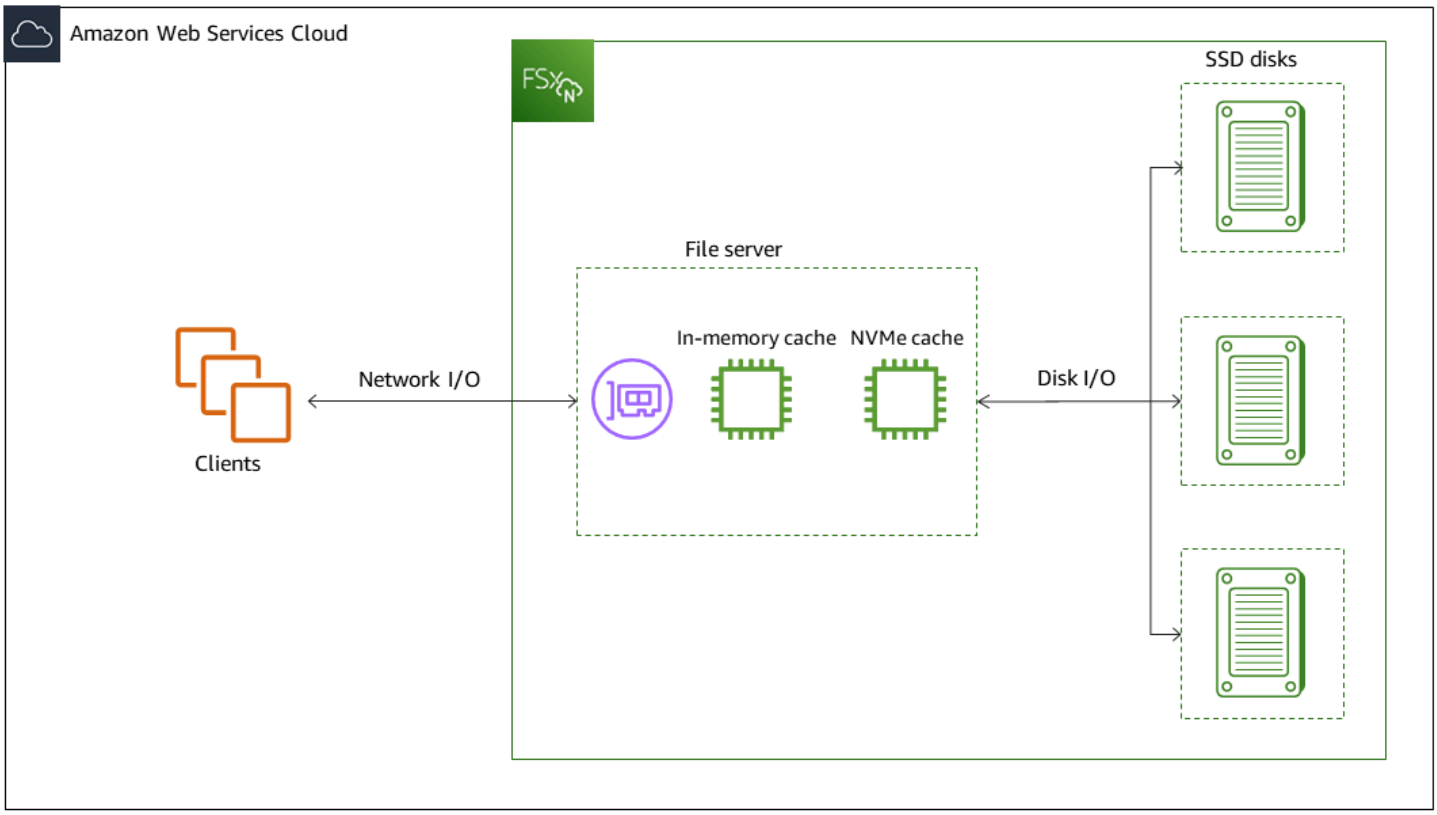
Com o Amazon FSx, você pode configurar o SMB Multichannel para fornecer várias conexões entre ONTAP e clientes em uma única sessão SMB. O SMB Multichannel usa várias conexões de rede entre o cliente e o servidor simultaneamente para agregar largura de banda da rede para a máxima utilização. Para obter informações sobre como usar a NetApp ONTAP CLI para configurar o SMB Multicanal, consulte Configurando o Multicanal SMB para desempenho e redundância.

Os clientes NFS podem usar a opção de montagem `nconnect` para ter várias conexões TCP (até 16) associadas a uma única montagem NFS. Esse cliente NFS multiplexa as operações de arquivo em várias conexões TCP de forma round-robin e, assim, obtém maior throughput da largura de banda da rede disponível. NFSv3 e NFSv4.1+ são compatíveis com o `nconnect`. A largura de banda da rede da instância do Amazon EC2 descreve o limite de largura de banda full duplex de 5 Gbps por fluxo de rede. Você pode superar esse limite usando vários fluxos de rede com `nconnect` ou SMB Multichannel. Consulte a documentação do seu cliente NFS para confirmar se há suporte para `nconnect` na versão do cliente. Para obter mais informações sobre NetApp ONTAP suporte para`nconnect`, consulte ONTAPsuporte para NFSv4.1.

Detalhes da performance

Para entender detalhadamente o modelo de desempenho do Amazon FSx for NetApp ONTAP, você pode examinar os componentes arquitetônicos de um sistema de arquivos Amazon FSx. Suas instâncias de computação cliente, estejam elas no local AWS ou no local, acessam seu sistema de arquivos por meio de uma ou várias interfaces de rede elástica (ENI). Essas interfaces de rede residem na Amazon VPC associada ao seu sistema de arquivos. Por trás de cada sistema de arquivos ENI está um servidor de NetApp ONTAP arquivos que está servindo dados pela rede para os clientes que acessam o sistema de arquivos. O Amazon FSx fornece um cache na memória rápido e um cache em NVMe em cada servidor de arquivos para melhorar a performance dos dados acessados com mais frequência. Os discos SSD que hospedam os dados do sistema de arquivos estão anexados a cada servidor de arquivos.

Esses componentes são ilustrados no diagrama a seguir.



Correspondendo a esses componentes arquitetônicos — interface de rede, cache na memória, cache NVMe e volumes de armazenamento — estão as principais características de desempenho de um sistema de arquivos Amazon FSx for NetApp ONTAP que determinam a taxa de transferência geral e o desempenho de IOPS.

- Performance de E/S de rede: throughput e IOPS de solicitações entre os clientes e o servidor de arquivos (em agregação)
- Tamanho do cache na memória e em NVMe no servidor de arquivos: tamanho do conjunto de trabalho ativo que pode ser acomodado para o armazenamento em cache
- Performance de E/S de disco: throughput e IOPS de solicitações entre o servidor de arquivos e os discos de armazenamento

Há dois fatores que determinam essas características de desempenho para seu sistema de arquivos: a quantidade total de SSD IOPS e a capacidade de taxa de transferência que você configura para ele. As duas primeiras características de performance (a performance de E/S de rede e o tamanho do cache na memória e em NVMe) são determinadas exclusivamente pela capacidade de throughput, enquanto a terceira (a performance de E/S de disco) é determinada por uma combinação de capacidade de throughput e IOPS de SSD.

As workloads baseadas em arquivos geralmente apresentam picos, caracterizados por períodos curtos e intensos de alta E/S com bastante tempo ocioso entre as intermitências. Para apoiar workloads com picos, além das velocidades básicas que um sistema de arquivos pode sustentar 24 horas por dia, sete dias por semana, o Amazon FSx oferece a capacidade de atingir velocidades mais altas em certos períodos, tanto para operações de E/S de rede quanto de E/S de disco. O Amazon FSx usa um mecanismo de crédito de E/S de rede para alocar throughput e IOPS com base na utilização média: os sistemas de arquivos acumulam créditos quando o throughput e o uso de IOPS estão abaixo dos limites básicos e podem usar esses créditos ao realizar operações de E/S.

As operações de gravação usam duas vezes mais largura de banda da rede do que as operações de leitura. Uma operação de gravação precisa ser replicada no servidor de arquivos secundário, portanto, uma única operação de gravação resulta no dobro da taxa de transferência da rede.

Impacto do tipo de implantação na performance

Você pode criar dois tipos de sistemas de arquivos com o FSx for ONTAP. Os sistemas de arquivos com um único par de servidores de arquivos de alta disponibilidade (HA) são chamados de sistemas de arquivos escaláveis. Os sistemas de arquivos com vários pares de HA são chamados de sistemas de arquivos escaláveis. Para ter mais informações, consulte Pares de alta disponibilidade (HA).

Os sistemas de arquivos multi-AZ e single-AZ do FSx para ONTAP fornecem latências consistentes de operação de arquivos abaixo de um milissegundo com armazenamento SSD e dezenas de milissegundos de latência com armazenamento em grupo de capacidade. Além disso, os sistemas de arquivos que atendem aos seguintes requisitos fornecem um cache de leitura de NVMe para reduzir as latências de leitura e aumentar a IOPS para dados lidos com frequência:

- Sistemas de arquivos multi-AZ
- Sistemas de arquivos escaláveis Single-AZ criados após 28 de novembro de 2022 com pelo menos 2 GBps de capacidade de taxa de transferência

As tabelas a seguir mostram a quantidade de capacidade de throughput que os sistemas de arquivos podem atingir, dependendo de fatores como o número de pares de alta disponibilidade (HA) e a Regiões da AWS disponibilidade.

Scale-up

Essas especificações de desempenho se aplicam a sistemas de arquivos escaláveis.

Taxa de transferência máxima do armazenamento SSD por par de HA para sistemas de arquivos escaláveis

	Regiões Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda)		Todos os outros Regiões da AWS em que o FSx for ONTAP está disponível	
	Throughput de leitura (MBps)	Throughput de gravação (MBps)	Throughput de leitura (MBps)	Throughput de gravação (MBps)
Single-AZ	4.096*	1.000	2.048	750
Multi-AZ	4.096*	1,800	2.048	1.300

> **Note**
>
> * Para provisionar 4 GBps de capacidade de taxa de transferência, seu sistema de arquivos deve ser configurado com um mínimo de 5.120 GiB de capacidade de armazenamento SSD e 160.000 SSD IOPS.

Scale-out

Essas especificações de desempenho se aplicam a sistemas de arquivos escaláveis.

Taxa de transferência máxima do armazenamento SSD por par de HA para sistemas de arquivos escaláveis

	Throughput de leitura (MBps)	Throughput de gravação (MBps)
Escalabilidade horizontal Single-AZ	6.144*	1.100*

> **Note**
>
> * Por par de HA (até 12). Para ter mais informações, consulte Pares de alta disponibilidade (HA).

Impacto da capacidade de armazenamento na performance

O throughput máximo de disco e os níveis de IOPS que o sistema de arquivos pode alcançar são os mais baixos entre:

- o nível de desempenho do disco fornecido pelos seus servidores de arquivos, com base na capacidade de taxa de transferência que você seleciona para seu sistema de arquivos
- o nível de performance do disco fornecido pelo número de IOPS de SSD provisionado para o sistema de arquivos

Por padrão, o armazenamento SSD do seu sistema de arquivos fornece até os seguintes níveis de taxa de transferência de disco e IOPS:

- Taxa de transferência de disco (MBps por TiB de armazenamento): 768
- IOPS de disco (IOPS por TiB de armazenamento): 3.072

Impacto da capacidade de throughput na performance

Cada sistema de arquivos do Amazon FSx tem uma capacidade de throughput configurada quando o sistema de arquivos é criado. A capacidade de taxa de transferência do seu sistema de arquivos determina o nível de desempenho de E/S da rede ou a velocidade com que cada um dos servidores de arquivos que hospedam seu sistema de arquivos pode fornecer dados de arquivos pela rede aos clientes que os acessam. Níveis mais altos de capacidade de taxa de transferência vêm com mais memória e armazenamento de memória expressa não volátil (NVMe) para armazenar dados em cache em cada servidor de arquivos e níveis mais altos de desempenho de E/S de disco suportados por cada servidor de arquivos.

Opcionalmente, você pode provisionar um nível mais alto de IOPS de SSD ao criar o sistema de arquivos. O nível máximo de IOPS de SSD que o sistema de arquivos pode alcançar também é

determinado pela capacidade de throughput do sistema de arquivos, mesmo ao provisionar IOPS de SSD adicionais.

As tabelas a seguir mostram o conjunto completo de especificações de capacidade de throughput, com os níveis de linha de base e de intermitência e a quantidade de memória para armazenamento em cache no servidor de arquivos nas Regiões da AWS correspondentes.

Single-AZ (scale-up)

Essas especificações de desempenho se aplicam aos sistemas de arquivos escaláveis Single-AZ criados após 28 de novembro de 2022 no especificado. Regiões da AWS

Especificações de desempenho para sistemas de arquivos nos seguintes Regiões da AWS: Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon) e Europa (Irlanda)

FSx capacidade de transferência (MBps)	Capacidade de throughput da rede (MBps)		IOPS de rede	Armazenamento em cache na memória (GB)	Armazenamento em cache de leitura em NVMe (GB)	Throughput de disco (MBps)		IOPS de unidade SSD *	
	Linha de base	Intermitência				Linha de base	Intermitência	Linha de base	Intermitência
128	188	1.500	Linha de base de dezenas de milhares	16	–	128	1.250	6.000	40.000
256	375	1.500		32	–	256	1.250	12.000	40.000
512	750	1.500		64	–	512	1.250	20.000	40.000
1,024	1.500	–		128	–	1,024	1.250	40.000	–

FSxcapacidade de transferência (MBps)	Capacidade de throughput da rede (MBps)		IOPS de rede	Armazenamento em cache na memória (GB)	Armazenamento em cache de leitura em NVMe (GB)	Throughput de disco (MBps)		IOPS de unidade SSD *	
2.048	3.125	–	de centenas	256	1.900	2.048	–	80.000	–
4.096	6.250	–	de milhares	512	5.400	4.096	–	160.000	–

> **Note**
>
> * As IOPS de SSD são usadas somente ao acessar dados que não estão armazenados em cache no cache na memória ou no cache em NVMe do servidor de arquivos.

Essas especificações de desempenho se aplicam aos sistemas de arquivos escaláveis Single-AZ em todos os outros em que o Regiões da AWS FSx for ONTAP está disponível.

Especificações de desempenho para sistemas de arquivos em [todos os outros em Regiões da AWS que o FSx for ONTAP](#) está disponível

Capacidade de throughput do FSx (MBps)	Capacidade de throughput da rede (MBps)		IOPS de rede	Armazenamento em cache na memória (GB)	Throughput de disco (MBps)		IOPS de unidade SSD *	
	Linha de base	Intermitência			Linha de base	Intermitência	Linha de base	Intermitência

Capacidade de throughput do FSx (MBps)	Capacidade de throughput da rede (MBps)		IOPS de rede	Armazenamento em cache na memória (GB)	Throughput de disco (MBps)		IOPS de unidade SSD *	
128	150	1.250	Linha de base de dezenas de milhares	16	128	600	6.000	18.750
256	300	1.250		32	256	600	12.000	18.750
512	625	1.250	Linha de base de centenas de milhares	64	512	600	18.750	–
1,024	1.500	–		128	1,024	–	40.000	–
2.048	3.125	–		256	2.048	–	80.000	–

> **Note**
>
> * As IOPS de SSD são usadas somente ao acessar dados que não estão armazenados em cache no cache na memória ou no cache em NVMe do servidor de arquivos.

Single-AZ (scale-out)

Essas especificações de desempenho se aplicam a sistemas de arquivos escaláveis.

Especificações de desempenho para sistemas de arquivos escaláveis

Capacidade de throughput do FSx (MBps)	Capacidade de throughput da rede (MBps)		IOPS de rede	Armazenamento em cache na memória (GB)	Throughput de disco (MBps)		IOPS de unidade SSD *	
	Linha de base	Intermitência			Linha de base	Intermitência	Linha de base	Intermitência
3.072**	6.250	–	Linha de base de centenas de milhares	128	3.072	–	100.000	–
6.14**	12.500	–		256	6,144	–	200.000	–

> **Note**
>
> * As IOPS de SSD são usadas somente ao acessar dados que não estão armazenados em cache no cache na memória ou no cache em NVMe do servidor de arquivos.
> ** Por par de HA (até 12). Para ter mais informações, consulte Pares de alta disponibilidade (HA).

Multi-AZ (scale-up)

Essas especificações de desempenho se aplicam aos sistemas de arquivos escaláveis Multi-AZ criados após 28 de novembro de 2022 no especificado. Regiões da AWS

Especificações de desempenho para sistemas de arquivos nos seguintes Regiões da AWS: Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon) e Europa (Irlanda)

Capacidade de throughput do FSx (MBps)	Capacidade de throughput da rede (MBps)		IOPS de rede	Armazenamento em cache na memória (GB)	Cache NVMe (GB)	Throughput de disco (MBps)		IOPS de unidade SSD *	
	Linha de base	Intermitência				Linha de base	Intermitência	Linha de base	Intermitência
128	188	1.500	Linha de base de dezenas de milhares	16	238	128	1.250	6.000	40.000
256	375	1.500		32	475	256	1.250	12.000	40.000
512	750	1.500		64	950	512	1.250	20.000	40.000
1,024	1.500	–		128	1.900	1,024	1.250	40.000	–
2.048	3.125	–		256	3.800	2.048	–	80.000	–
4.096	6.250	–		512	7.600	4.096	–	160.000	–

> **Note**
>
> * As IOPS de SSD são usadas somente ao acessar dados que não estão armazenados em cache no cache na memória ou no cache em NVMe do servidor de arquivos.

Essas especificações de desempenho se aplicam aos sistemas de arquivos escaláveis Multi-AZ em todos os outros em que o Regiões da AWS FSx for ONTAP está disponível.

Especificações de desempenho para sistemas de arquivos em [todos os outros em Regiões da AWS que o FSx for ONTAP](#) está disponível

Capacidade de throughput do FSx (MBps)	Capacidade de throughput da rede (MBps)		IOPS de rede	Armazenamento em cache na memória (GB)	Cache NVMe (GB)	Throughput de disco (MBps)		IOPS de unidade SSD *	
	Linha de base	Intermitência				Linha de base	Intermitência	Linha de base	Intermitência
128	150	1.250	Linha de base de dezenas de milhares	16	150	128	600	6.000	18.750
256	300	1.250		32	300	256	600	12.000	18.750
512	625	1.250		64	600	512	600	18.750	–
1,024	1.500	–		128	1.200	1,024	–	40.000	–
2.048	3.125	–	de centenas de milhares	256	2.400	2.048	–	80.000	–

> **Note**
>
> * As IOPS de SSD são usadas somente ao acessar dados que não estão armazenados em cache no cache na memória ou no cache em NVMe do servidor de arquivos.

Exemplo: capacidade de armazenamento e capacidade de throughput

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

Um sistema de arquivos escalável configurado com 2 TiB de capacidade de armazenamento SSD e 512 MBps de capacidade de taxa de transferência tem os seguintes níveis de taxa de transferência:

- Throughput de rede: linha de base de 625 MBps e intermitência de 1.250 MBps (consulte a tabela de capacidade de throughput)
- Throughput de disco: linha de base de 512 MBps e intermitência de 600 MBps.

Portanto, sua workload que acessa o sistema de arquivos será capaz de gerar até 625 MBps de linha de base e 1.250 MBps de throughput de intermitência para operações de arquivo executadas em dados acessados ativamente e armazenados em cache no cache na memória e no cache em NVMe do servidor de arquivos.

Administração do FSx para ONTAP

Usando a CLI e a API do AWS Management Console AWS CLI, e do ONTAP, você pode realizar as seguintes ações administrativas para recursos do FSx for ONTAP:

- Criação, listagem, atualização e exclusão de sistemas de arquivos, máquinas virtuais de armazenamento (SVMs), volumes, backups e tags.
- Gerenciamento de acesso, contas e senhas administrativas, requisitos de senha, protocolos SMB e iSCSI, acessibilidade de rede para os destinos de montagem dos sistemas de arquivos existentes

Tópicos

Como gerenciar sistemas de arquivos do FSx para ONTAP

Um sistema de arquivos é o principal recurso do Amazon FSx, análogo a um cluster on-premises do ONTAP. Você especifica a capacidade do armazenamento SSD e a capacidade de throughput

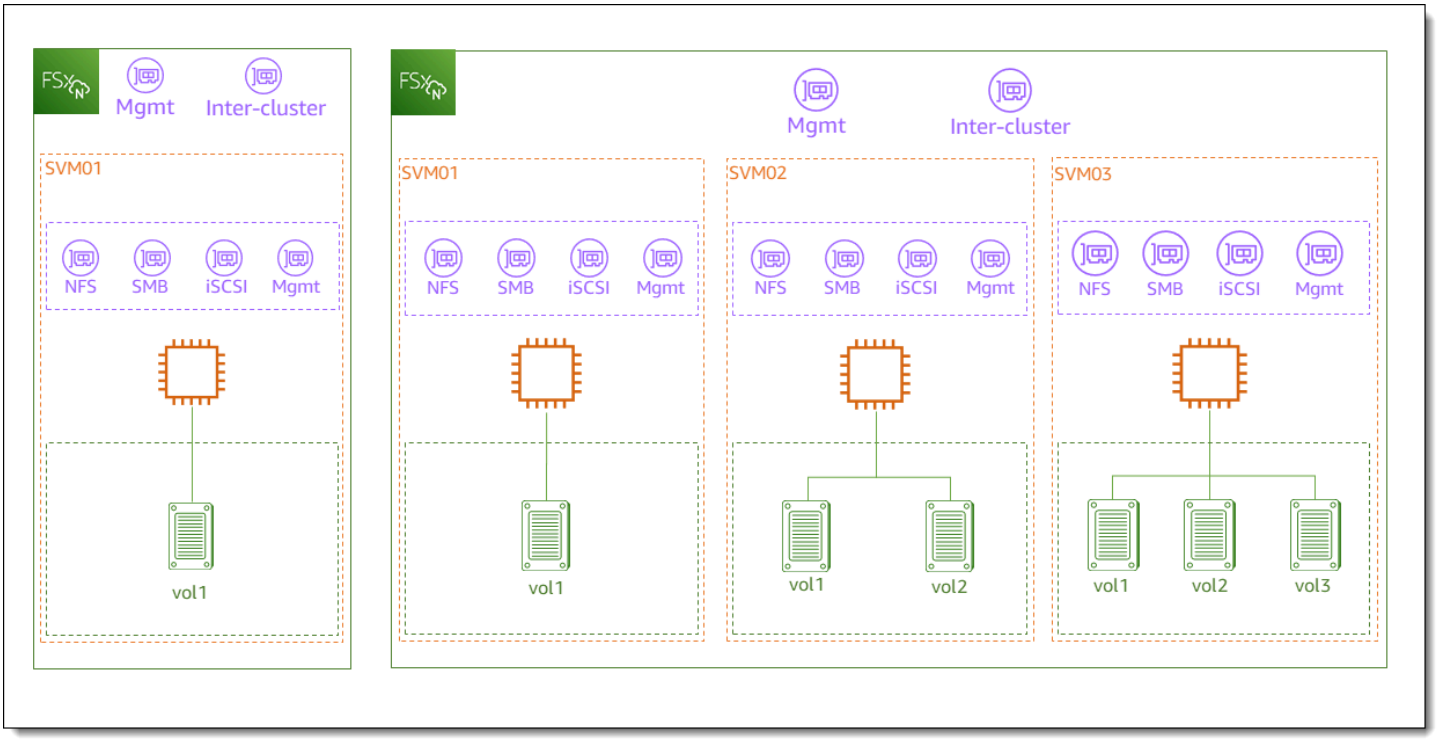
do seu sistema de arquivos e escolhe uma nuvem privada virtual (VPC) na qual criar o sistema de arquivos. Cada sistema de arquivos tem um endpoint de gerenciamento que você pode usar para gerenciar recursos e dados com a CLI ou a API REST do ONTAP.

Recursos do sistema de arquivos

Um sistema de arquivos Amazon FSx for NetApp ONTAP é composto pelos seguintes recursos principais:

- O hardware físico do próprio sistema de arquivos, que inclui os servidores de arquivos e a mídia de armazenamento.
- Um ou mais pares de servidores de arquivos de alta disponibilidade (HA), que hospedam suas máquinas virtuais de armazenamento (SVMs). Os sistemas de arquivos escaláveis têm um par de HA, e os sistemas de arquivos de escalabilidade horizontal têm dois ou mais pares de HA. Cada par de HA tem um pool de armazenamento chamado agregado. A coleção de agregados em todos os pares de HA compõe seu nível de armazenamento SSD.
- Uma ou mais máquinas virtuais de armazenamento (SVMs) que hospedam os volumes do sistema de arquivos e têm suas próprias credenciais e gerenciamento de acesso.
- Um ou mais volumes que organizam virtualmente seus dados e são montados por seus clientes.

A imagem a seguir ilustra a arquitetura de um FSx de expansão ascendente para sistema de arquivos ONTAP com um par de HA e a relação entre seus recursos principais. O sistema de arquivos do FSx para ONTAP à esquerda é o mais simples, com ums SVM e um volume. O sistema de arquivos à direita tem várias SVMs, com algumas delas tendo diversos volumes. Cada sistema de arquivos e SVMs tem vários endpoints de gerenciamento, e os SVMs também têm endpoints de acesso a dados.



Ao criar um sistema de arquivos do FSx para oONTAP, você define as seguintes propriedades:

- Tipo de implantação: o tipo de implantação do seu sistema de arquivos (várias AZs ou uma única AZ). Os sistemas de arquivos Single-AZ replicam seus dados e oferecem failover automático em uma única zona de disponibilidade, além de oferecer sistemas de arquivos escaláveis. Os sistemas de arquivos com várias AZs oferecem maior resiliência ao também replicar seus dados e oferecer suporte ao failover em várias zonas de disponibilidade dentro da mesma Região da AWS.
- Capacidade de armazenamento — Essa é a quantidade de armazenamento SSD, de até 192 tebibytes (TiB) para sistemas de arquivos escaláveis e 1 pebibyte (PiB) para sistemas de arquivos escaláveis.
- SSD IOPS — Por padrão, cada gigabyte de armazenamento SSD inclui três SSD IOPS (até o máximo suportado pela configuração do sistema de arquivos). Você tem a opção de provisionar IOPS de SSD adicionais conforme necessário.
- Capacidade de throughput: a velocidade sustentada na qual o servidor de arquivos pode fornecer dados.
- Rede: a VPC e as sub-redes para os endpoints de gerenciamento e de acesso a dados que o sistema de arquivos cria. Para um sistema de arquivos com várias AZs, você também define um intervalo de endereços IP e tabelas de rotas.

- Criptografia — A chave AWS Key Management Service (AWS KMS) usada para criptografar os dados do sistema de arquivos em repouso.
- Acesso administrativo: você pode especificar a senha do usuário `fsxadmin`. Você pode usar esse usuário para administrar o sistema de arquivos usando a NetApp CLI e a API REST do ONTAP.

Você pode gerenciar FSx para sistemas de arquivos ONTAP usando a NetApp CLI do ONTAP ou a API REST. Você também pode configurar SnapMirror ou SnapVault relacionar um sistema de arquivos Amazon FSx e outra implantação do ONTAP (incluindo outro sistema de arquivos Amazon FSx). Cada sistema de arquivos FSx for ONTAP tem os seguintes endpoints do sistema de arquivos que fornecem acesso aos aplicativos: NetApp

- Gerenciamento — Use esse endpoint para acessar a NetApp CLI do ONTAP via Secure Shell (SSH) ou para usar a API REST do NetApp ONTAP com seu sistema de arquivos.
- Intercluster — Use esse endpoint ao configurar o uso da replicação NetApp SnapMirror ou do armazenamento em cache. NetApp FlexCache

Para obter mais informações, consulte Gerenciando recursos do FSx for ONTAP usando aplicativos NetApp e Replicação programada usando NetApp SnapMirror.

Pares de alta disponibilidade (HA)

Cada sistema de arquivos FSx for ONTAP é alimentado por um ou vários pares de servidores de arquivos de alta disponibilidade (HA) em uma configuração de espera ativa. Nessa configuração, há um servidor de arquivos preferencial que fornece tráfego ativamente e um servidor de arquivos secundário que assume o controle se o servidor ativo não estiver disponível. Os sistemas de arquivos escaláveis FSx for ONTAP são alimentados por um par de HA, que oferece até 4 GBps de capacidade de taxa de transferência e 160.000 IOPs SSD. Os sistemas de arquivos escaláveis FSx for ONTAP são alimentados por até 12 pares de HA, que podem fornecer até 72 GBps de capacidade de taxa de transferência e 2.400.000 IOPS de SSD (6 GBps de capacidade de taxa de transferência e 200.000 SSD IOPS por par de HA).

Quando você cria seu sistema de arquivos a partir do console do Amazon FSx, o Amazon FSx recomenda o número de pares de HA que você deve usar com base no armazenamento SSD desejado. Você também pode escolher manualmente o número de pares de HA com base em sua carga de trabalho e requisitos de desempenho. Recomendamos que você use um único par de HA se os requisitos do seu sistema de arquivos forem atendidos por até 4 GBps de capacidade de

taxa de transferência e 160.000 IOPs de SSD, e vários pares de HA se suas cargas de trabalho precisarem de níveis mais altos de escalabilidade de desempenho.

Cada par de HA tem um agregado, que é um conjunto lógico de discos físicos.

> **Note**
>
> Você não pode adicionar pares de HA aos sistemas de arquivos existentes. Em vez disso, você pode migrar dados entre sistemas de arquivos (com diferentes pares de HA) usando SnapMirror ou restaurando seus dados de um backup para um novo sistema de arquivos. AWS DataSync

Como criar sistemas de arquivos do FSx para ONTAP

Esta seção descreve como criar um FSx para o sistema de arquivos ONTAP usando o console do Amazon FSx ou a API AWS CLI do Amazon FSx. Você pode criar um sistema de arquivos em uma nuvem privada virtual (VPC) de sua propriedade ou em uma VPC que outra pessoa Conta da AWS compartilhou com você. Há considerações ao criar um sistema de arquivos Multi-AZ em uma VPC da qual você é participante. Essas considerações são explicadas neste tópico.

Por padrão, quando você cria um novo sistema de arquivos a partir do console Amazon FSx, o Amazon FSx cria automaticamente um sistema de arquivos com uma única máquina virtual de armazenamento (SVM) e um volume, permitindo acesso rápido aos dados de instâncias Linux por meio do protocolo Network File System (NFS). Ao criar o sistema de arquivos, você pode unir a SVM a um Active Directory para permitir o acesso de clientes Windows e macOS por meio do protocolo Server Message Block (SMB). Depois que seu sistema de arquivos for criado, você poderá criar SVMs e volumes adicionais conforme necessário.

Criar um sistema de arquivos (console)

Esse procedimento usa a opção Criação padrão para criar um sistema de arquivos do FSx para ONTAP com uma configuração que você personaliza de acordo com suas necessidades. Para obter informações sobre como usar a opção de criação rápida para criar rapidamente um sistema de arquivos com um conjunto padrão de parâmetros de configuração, consulte Etapa 1: Criar um sistema de arquivos Amazon FSx for NetApp ONTAP.

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel, escolha Criar sistema de arquivos.

3. Na página Selecionar tipo de sistema de arquivos, em Opções do sistema de arquivos, escolha Amazon FSx for NetApp ONTAP e, em seguida, escolha Avançar.
4. Na seção Método de criação, escolha Criação padrão.
5. Na seção Detalhes do sistema de arquivos, forneça as seguintes informações:

   - Em Nome do sistema de arquivos (opcional), insira um nome para seu sistema de arquivos. É mais fácil encontrar e gerenciar seus sistemas de arquivos quando você define um nome para eles. É possível usar até 256 letras do Unicode, espaço em branco e números, além dos caracteres especiais + - = . _ : /
   - Em Tipo de implantação, escolha Multi-AZ ou Single-AZ.
     - Os sistemas de arquivos Multi-AZ replicam dados e oferecem suporte ao failover em várias zonas de disponibilidade dentro da mesma Região da AWS.
     - Os sistemas de arquivos single-AZ replicam os dados e oferecem failover automático em uma única zona de disponibilidade.

     > **Note**
     >
     > Escolha Single-AZ se quiser a opção de criar um sistema de arquivos com dois ou mais pares de alta disponibilidade (HA) (até 12). Para ter mais informações, consulte Pares de alta disponibilidade (HA).

     Para ter mais informações, consulte Disponibilidade e durabilidade.
   - Em Capacidade de armazenamento SSD, informe a capacidade de armazenamento do sistema de arquivos, em gibibytes (GiB). Insira qualquer número inteiro no intervalo de 1.024 a 1.048.576 GiB (até 1 pebibyte [PiB]).

     Você pode aumentar a capacidade de armazenamento, conforme necessário, a qualquer momento após a criação do sistema de arquivos. Para ter mais informações, consulte Como gerenciar a capacidade de armazenamento.
   - Em IOPS de SSD provisionadas, você tem duas opções para provisionar o número de IOPS para seu sistema de arquivos:
     - Escolha Automático (o padrão) se quiser que o Amazon FSx provisione automaticamente três IOPS por GiB de armazenamento SSD.
     - Escolha Provisionado pelo usuário se quiser especificar o número de IOPS. Você pode provisionar no máximo 200.000 SSD IOPS por sistema de arquivos.

> **Note**
>
> Você pode aumentar suas IOPS de SSD provisionadas depois de criar o sistema de arquivos. Lembre-se de que o nível máximo de IOPS de SSD que o sistema de arquivos pode alcançar também é determinado pela capacidade de throughput do sistema de arquivos, mesmo ao provisionar IOPS de SSD adicionais. Para obter mais informações, consulte Impacto da capacidade de throughput na performance e Como gerenciar a capacidade de armazenamento.

- Para a capacidade de taxa de transferência, você tem duas opções para determinar sua capacidade de taxa de transferência em megabytes por segundo (MBps):
  - Escolha Capacidade de taxa de transferência recomendada se quiser que o Amazon FSx escolha automaticamente a capacidade de taxa de transferência com base na quantidade de capacidade de armazenamento que você escolheu.
  - Escolha Especificar capacidade de taxa de transferência se quiser especificar a quantidade de capacidade de taxa de transferência. Se você escolher essa opção, uma lista suspensa de capacidade de taxa de transferência será exibida e preenchida com base no tipo de implantação que você escolheu. Você também pode escolher o número de pares de HA (até 12). Para ter mais informações, consulte Pares de alta disponibilidade (HA).

  Capacidade de throughput: é a velocidade sustentada na qual o servidor de arquivos que hospeda o sistema de arquivos pode fornecer dados. Para ter mais informações, consulte Amazon FSx para NetApp desempenho de ONTAP.

6. Na seção Rede, forneça as seguintes informações:

   - Em Nuvem privada virtual (VPC), escolha a VPC que você deseja associar ao sistema de arquivos.
   - Para grupos de segurança da VPC, você pode escolher um grupo de segurança para associar à interface de rede do seu sistema de arquivos. Se você não especificar um, o Amazon FSx associará o grupo de segurança padrão da VPC ao seu sistema de arquivos.
   - Especifique uma sub-rede para seu servidor de arquivos. Se você estiver criando um sistema de arquivos com várias AZs, escolha também uma Sub-rede em espera para o servidor de arquivos em espera.
   - (Somente Multi-AZ) Para Tabelas de rotas da VPC, especifique as tabelas de rotas da VPC para criar endpoints do sistema de arquivos. Selecione todas as tabelas de rotas da VPC

associadas às sub-redes nas quais seus clientes estão localizados. Por padrão, o Amazon FSx seleciona a tabela de rotas padrão da VPC. Para ter mais informações, consulte Acesso a dados de fora da VPC de implantação.

> **Note**
>
> O Amazon FSx gerencia essas tabelas de rotas para sistemas de arquivos Multi-AZ usando autenticação baseada em tags. Essas tabelas de rotas estão marcadas com`Key: AmazonFSx; Value: ManagedByAmazonFSx`. Ao criar FSx para sistemas de arquivos ONTAP Multi-AZ usando, AWS CloudFormation recomendamos que você adicione a tag manualmente. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

- (Somente Multi-AZ) Intervalo de endereços IP do endpoint especifica o intervalo de endereços IP no qual são criados os endpoints para acessar o sistema de arquivos.

  Você tem três opções para o intervalo de endereços IP do endpoint:

  - Intervalo de endereços IP não alocados da sua VPC: o Amazon FSx escolhe os últimos 64 endereços IP do intervalo CIDR primário da VPC para usar como intervalo de endereços IP do endpoint para o sistema de arquivos. Esse intervalo será compartilhado entre vários sistemas de arquivos se você escolher essa opção várias vezes.

    > **Note**
    >
    > Essa opção ficará desabilitada se algum dos últimos 64 endereços IP no intervalo CIDR primário de uma VPC estiver sendo usado por uma sub-rede. Nesse caso, você ainda pode escolher um intervalo de endereços na VPC (ou seja, um intervalo que não esteja no final do intervalo CIDR primário ou um intervalo que esteja em um CIDR secundário da VPC) escolhendo a opção Inserir um intervalo de endereços IP.

  - Em Sub-rede preferencial, especifique uma sub-rede para seu servidor de arquivos. Se você estiver criando um sistema de arquivos com várias AZs, escolha também uma Sub-rede em espera para o servidor de arquivos em espera.
  - (Somente Multi-AZ) Para Tabelas de rotas da VPC, especifique as tabelas de rotas da VPC para criar endpoints do sistema de arquivos. Selecione todas as tabelas de rotas da VPC associadas às sub-redes nas quais seus clientes estão localizados. Por padrão, o Amazon FSx seleciona a tabela de rotas padrão da VPC.

- (Somente Multi-AZ) Intervalo de endereços IP do endpoint especifica o intervalo de endereços IP no qual são criados os endpoints para acessar o sistema de arquivos.

  Você tem três opções para o intervalo de endereços IP do endpoint:

  - Intervalo de endereços IP não alocados da sua VPC: o Amazon FSx escolhe os últimos 64 endereços IP do intervalo CIDR primário da VPC para usar como intervalo de endereços IP do endpoint para o sistema de arquivos. Esse intervalo será compartilhado entre vários sistemas de arquivos se você escolher essa opção várias vezes.

    > **Note**
    >
    > Essa opção ficará desabilitada se algum dos últimos 64 endereços IP no intervalo CIDR primário de uma VPC estiver sendo usado por uma sub-rede. Nesse caso, você ainda pode escolher um intervalo de endereços na VPC (ou seja, um intervalo que não esteja no final do intervalo CIDR primário ou um intervalo que esteja em um CIDR secundário da VPC) escolhendo a opção Inserir um intervalo de endereços IP.

  - Intervalo de endereços IP flutuante fora da VPC: o Amazon FSx escolhe um intervalo de endereços 198.19.x.0/24 que ainda não é usado por nenhum outro sistema de arquivos com a mesma VPC e as mesmas tabelas de rotas.
  - Inserir um intervalo de endereços IP: você pode fornecer um intervalo CIDR de sua escolha. O intervalo de endereços IP que você escolher poderá estar dentro ou fora do intervalo de endereços IP da VPC, desde que não se sobreponha a nenhuma sub-rede.

    > **Note**
    >
    > Não escolha um intervalo que esteja dentro dos seguintes intervalos CIDR, uma vez que eles são incompatíveis com o FSx para ONTAP:
    >
    > - 0.0.0.0/8
    > - 127.0.0.0/8
    > - 198.19.0.0/20
    > - 224.0.0.0/4
    > - 240.0.0.0/4
    > - 255.255.255/32

7. Na seção Segurança e criptografia, em Chave de criptografia, escolha a chave de criptografia AWS Key Management Service (AWS KMS) que protege os dados em repouso do sistema de arquivos.
8. Em Senha administrativa do sistema de arquivos, insira uma senha segura para o usuário `fsxadmin`. Confirme a senha.

   É possível utilizar o usuário `fsxadmin` para administrar o sistema de arquivos usando a CLI e a API REST do ONTAP. Para obter mais informações sobre o usuário `fsxadmin`, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.
9. Na seção Configuração de máquina virtual de armazenamento padrão, forneça as seguintes informações:

   - No campo Nome da máquina virtual de armazenamento, forneça um nome para a máquina virtual de armazenamento. Você pode usar, no máximo, 47 caracteres alfanuméricos, além do caractere especial de sublinhado (_).
   - Para Senha administrativa da SVM, você pode escolher Especificar uma senha e fornecer uma senha para o usuário `vsadmin` da SVM. Você pode usar o usuário `vsadmin` para administrar a SVM utilizando a CLI ou a API REST do ONTAP. Para obter mais informações sobre o usuário `vsadmin`, consulte Gerenciando SVMs com a CLI ONTAP.

     Se você escolher Não especificar uma senha (o padrão), ainda poderá utilizar o usuário `fsxadmin` do sistema de arquivos para gerenciar o sistema usando a CLI ou a API REST do ONTAP, mas não poderá utilizar o usuário `vsadmin` da SVM para fazer o mesmo.
   - Na seção Active Directory, você pode unir um Active Directory à SVM. Para ter mais informações, consulte Trabalhar com o Microsoft Active Directory no FSx para ONTAP.

     Se você não quiser unir a SVM a um Active Directory, escolha Não ingressar em um Active Directory.

     Se você quiser unir a SVM a um domínio autogerenciado do Active Directory, escolha Ingressar em um Active Directory e forneça os seguintes detalhes do Active Directory:
     - O nome NetBIOS do objeto de computador do Active Directory que será criado para a SVM. O nome NetBIOS não pode ter mais de 15 caracteres.
     - O nome totalmente qualificado do domínio do Active Directory. O nome do domínio não pode ter mais de 255 caracteres.
     - Endereços IP do servidor DNS: os endereços IPv4 dos servidores do Sistema de Nomes de Domínio (DNS) do seu domínio.

- Nome de usuário da conta de serviço: o nome de usuário da conta de serviço no seu Active Directory existente. Não inclua um prefixo ou sufixo de domínio.
- Senha da conta de serviço: a senha da conta de serviço.
- Confirmar senha: a senha da conta de serviço.
- (Opcional) Unidade organizacional (UO): o nome do caminho distinto da unidade organizacional à qual você deseja unir seu sistema de arquivos.
- Grupo de administradores delegado do sistema de arquivos: o nome do grupo no Active Directory que pode administrar o sistema de arquivos.

  Se você estiver usando AWS Managed Microsoft AD, precisará especificar um grupo, como Administradores FSx AWS Delegados AWS , Administradores Delegados ou um grupo personalizado com permissões delegadas à OU.

  Se você estiver ingressando em um AD autogerenciado, use o nome do grupo em seu AD. O grupo padrão é `Domain Admins`.

10. Na seção Configuração de volume padrão, forneça as seguintes informações para o volume padrão criado com seu sistema de arquivos:

    - No campo Nome do volume, forneça um nome para o volume. Você pode usar até 203 caracteres alfanuméricos ou sublinhados (_).
    - (Somente sistemas de arquivos de expansão) Para estilo de volume, escolha ou. FlexVolFlexGroup FlexVolvolumes são volumes de uso geral que podem ter até 300 TiB de tamanho. FlexGroupos volumes são destinados a cargas de trabalho de alto desempenho e podem ter até 20 PiB de tamanho.
    - Em Tamanho do volume, insira qualquer número inteiro na faixa de 800 gibibytes (GiB) a 2.000 pebibytes (PiB).
    - Para Tipo de volume, escolha Leitura-Gravação (RW) para criar um volume que seja legível e gravável ou Proteção de Dados (DP) para criar um volume que seja somente para leitura e possa ser usado como destino de um relacionamento. NetApp SnapMirror SnapVault Para ter mais informações, consulte Tipos de volume.
    - Em Caminho da junção, insira um local no sistema de arquivos para montar o volume. O nome deve ter uma barra inicial, por exemplo `/vol3`.
    - Para Eficiência de armazenamento, escolha Habilitado para habilitar os recursos de eficiência de armazenamento do ONTAP (eliminação da duplicação, compressão e compactação). Para ter mais informações, consulte Eficiência de armazenamento do FSx para ONTAP.

- Para o estilo de segurança de volume, escolha entre Unix (Linux), NTFS e Mixed para o volume. Para ter mais informações, consulte Estilo de segurança do volume.
- Em Política de snapshots, escolha uma política de snapshots para o volume. Para obter mais informações sobre políticas de snapshots, consulte Políticas de snapshots.

  Se você escolher Política personalizada, especifique o nome da política no campo política personalizada. A política personalizada já deve existir na SVM ou no sistema de arquivos. Você pode criar uma política de snapshots personalizada com a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política de snapshot na documentação do produto NetApp ONTAP.

11. Na seção Camadas padrão de armazenamento de volume, para Política de camadas do grupo de capacidade, escolha a política de camadas do grupo de armazenamento, que pode ser Automático (o padrão), Somente snapshot, Todos ou Nenhum. Para obter mais informações sobre políticas de camadas do grupo de capacidade, consulte Políticas de classificação por níveis de volume.

    Em Período de resfriamento da política de camadas, se você tiver definido camadas de armazenamento como `Auto` e `Snapshot-only`, os valores válidos das políticas serão de 2 a 183 dias. O período de resfriamento da política de camadas de um volume define o número de dias antes que os dados que não foram acessados sejam marcados como frios e movidos para o armazenamento do grupo de capacidade.

12. Em Backup e manutenção: opcional, você pode definir as seguintes opções:

    - Em Backup automático diário, escolha Habilitado para backups diários automáticos. Essa opção é habilitada por padrão.
    - Em Janela de backup automático diário, defina a hora do dia no Tempo Universal Coordenado (UTC) em que você deseja que a janela de backup automático diário seja iniciada. A janela é de 30 minutos a partir desse horário especificado. Essa janela não pode se sobrepor à janela de backup de manutenção semanal.
    - Para Período de retenção de backup automático, defina um período de 1 a 90 dias em que você deseja manter os backups automáticos.
    - Para Janela de manutenção semanal, você pode definir a hora da semana em que deseja iniciar a janela de manutenção. O dia 1 é segunda-feira, o dia 2 é terça-feira, e assim por diante. A janela é de 30 minutos a partir desse horário especificado. Essa janela não pode se sobrepor à janela de backup automático diário.

13. Em Tags: opcional, você pode inserir uma chave e um valor para adicionar tags ao sistema de arquivos. Uma tag é um par de chave/valor que diferencia maiúsculas de minúsculas e ajuda você a gerenciar, filtrar e pesquisar o sistema de arquivos.

    Selecione Next (Próximo).

14. Verifique a configuração do sistema de arquivos mostrada na página Criar sistema de arquivos. Para sua referência, anote quais configurações do sistema de arquivos você pode modificar após a criação do sistema de arquivos.
15. Escolha Create file system (Criar sistema de arquivos).

Criar um sistema de arquivos (CLI)

- Para criar um FSx para o sistema de arquivos ONTAP, use o comando da CLI create-file-system (ou a operação equivalente da API do sistema), conforme mostrado no exemplo a CreateFileseguir.

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \

    --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
    --ontap-configuration DeploymentType=MULTI_AZ_1,
        ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

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

```
{
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
```

```
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
                "Mode": "AUTOMATIC",
                "Iops": 3072
      },
      "PreferredSubnetId": "subnet-abcdef1234567890b",
      "RouteTableIds": [
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
      ],
      "ThroughputCapacity": 512,
      "WeeklyMaintenanceStartTime": "4:10:00"
    }
  }
}
```

> **Note**
>
> Diferentemente do processo de criação de um sistema de arquivos no console, o comando da `create-file-system` CLI e a operação da `CreateFileSystem` API não criam um SVM ou volume padrão. Para criar uma SVM, consulte Como criar uma máquina virtual de armazenamento; para criar um volume, consulte Criação de volumes.

Criação de FSx para sistemas de arquivos ONTAP em sub-redes compartilhadas

O compartilhamento de VPC permite que vários Contas da AWS criem recursos em nuvens privadas virtuais (VPCs) compartilhadas e gerenciadas centralmente. Nesse modelo, a conta proprietária da VPC (proprietário) compartilha uma ou mais sub-redes com outras contas (participantes) que pertencem à mesma organização da. AWS Organizations

As contas dos participantes podem criar FSx para sistemas de arquivos ONTAP Single-AZ e Multi-AZ em uma sub-rede VPC que a conta do proprietário compartilhou com elas. Para que uma conta de participante crie um sistema de arquivos Multi-AZ, a conta do proprietário também precisa conceder permissão ao Amazon FSx para modificar tabelas de rotas nas sub-redes compartilhadas em nome da conta do participante. Para ter mais informações, consulte Gerenciando o suporte compartilhado de VPC para sistemas de arquivos Multi-AZ.

> **Note**
>
> É responsabilidade da conta do participante coordenar-se com o proprietário da VPC para evitar a criação de quaisquer sub-redes de VPC subsequentes que se sobreponham ao CIDR in-VPC dos sistemas de arquivos do participante. Se as sub-redes se sobrepuserem, o tráfego para o sistema de arquivos poderá ser interrompido.

Requisitos e considerações de sub-redes

Ao criar sistemas de arquivos FSx for ONTAP em sub-redes compartilhadas, observe o seguinte:

- O proprietário da sub-rede VPC deve compartilhar uma sub-rede com uma conta participante antes que essa conta possa criar um sistema de arquivos FSx for ONTAP nela.
- Você não pode iniciar recursos usando o grupo de segurança padrão da VPC, pois ele pertence ao proprietário. Além disso, as contas dos participantes não podem lançar recursos usando grupos de segurança pertencentes a outros participantes ou ao proprietário.
- Em uma sub-rede compartilhada, o participante e o proprietário controlam separadamente os grupos de segurança na respectiva conta. A conta do proprietário pode ver os grupos de segurança criados pelos participantes, mas não pode realizar nenhuma ação neles. Se a conta do proprietário quiser remover ou modificar esses grupos de segurança, o participante que criou o grupo de segurança deve realizar a ação.

- As contas dos participantes podem visualizar, criar, modificar e excluir sistemas de arquivos Single-AZ e seus recursos associados em sub-redes que a conta do proprietário compartilhou com elas.
- As contas dos participantes podem criar, visualizar, modificar e excluir sistemas de arquivos Multi-AZ e seus recursos associados em sub-redes que a conta do proprietário compartilhou com elas. Além disso, a conta do proprietário também deve conceder ao serviço Amazon FSx permissões para modificar tabelas de rotas nas sub-redes compartilhadas em nome da conta do participante. Para mais informações, consulte Gerenciando o suporte compartilhado de VPC para sistemas de arquivos Multi-AZ.
- O proprietário da VPC compartilhada não pode visualizar, modificar ou excluir recursos que um participante cria na sub-rede compartilhada. Isso é além dos recursos da VPC aos quais cada conta tem acesso diferente. Para obter mais informações, consulte Responsabilidades e permissões para proprietários e participantes no Guia do usuário da Amazon VPC.

Para obter informações, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

Ao compartilhar uma sub-rede VPC

Ao compartilhar suas sub-redes com contas de participantes que criarão sistemas de arquivos FSx for ONTAP nas sub-redes compartilhadas, você precisará fazer o seguinte:

- O proprietário da VPC precisa usar AWS Resource Access Manager para compartilhar com segurança VPCs e sub-redes com outras pessoas. Contas da AWS Para obter mais informações, consulte Compartilhando seus AWS recursos no Guia AWS Resource Access Manager do usuário.
- O proprietário da VPC precisa compartilhar uma ou mais VPCs com uma conta de participante. Para obter mais informações, consulte Compartilhe sua VPC com outras contas no Guia do usuário da Amazon Virtual Private Cloud.
- Para que as contas dos participantes criem FSx para sistemas de arquivos ONTAP Multi-AZ, o proprietário da VPC também deve conceder ao serviço Amazon FSx permissões para criar e modificar tabelas de rotas nas sub-redes compartilhadas em nome das contas dos participantes. Isso ocorre porque os sistemas de arquivos FSx for ONTAP Multi-AZ usam endereços IP flutuantes para que os clientes conectados possam fazer a transição perfeita entre os servidores de arquivos preferenciais e os de espera durante um evento de failover. Quando ocorre um evento de failover, o Amazon FSx atualiza todas as rotas em todas as tabelas de rotas associadas ao sistema de arquivos para apontar para o servidor de arquivos atualmente ativo.

Gerenciando o suporte compartilhado de VPC para sistemas de arquivos Multi-AZ

As contas do proprietário podem gerenciar se as contas dos participantes podem ou não criar FSx Multi-AZ para sistemas de arquivos ONTAP em sub-redes VPC que o proprietário compartilhou com os participantes usando a API,, e AWS CLI, conforme descrito nas seções AWS Management Console a seguir.

Para gerenciar o compartilhamento de VPC para sistemas de arquivos Multi-AZ (console)

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

1. No painel de navegação, selecione Configurações.
2. Localize as configurações de VPC compartilhada Multi-AZ na página Configurações.
   - Para habilitar o compartilhamento de VPC para sistemas de arquivos Multi-AZ nas sub-redes VPC que você compartilha, escolha Habilitar atualizações da tabela de rotas das contas dos participantes.
   - Para desativar o compartilhamento de VPC para sistemas de arquivos Multi-AZ em todas as VPCs que você possui, escolha Desativar atualizações da tabela de rotas das contas dos participantes. A tela de confirmação é exibida.

   > **Important**
   >
   > É altamente recomendável que os sistemas de arquivos Multi-AZ criados pelos participantes na VPC compartilhada sejam excluídos antes de você desativar esse recurso. Depois que o recurso for desativado, esses sistemas de arquivos entrarão em um `MISCONFIGURED` estado e correrão o risco de ficarem indisponíveis.

3. Entre **`confirm`** e escolha Confirmar para desativar o recurso.

Para gerenciar o compartilhamento de VPC para sistemas de arquivos Multi-AZ ()AWS CLI

1. Para visualizar a configuração atual do compartilhamento de VPC Multi-AZ, use o comando da CLI describe-shared-vpc-configuration ou o comando de API equivalente, mostrado a seguir: DescribeSharedVpcConfiguration

   ```
   $ aws fsx describe-shared-vpc-configuration
   ```

O serviço responde a uma solicitação bem-sucedida da seguinte forma:

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

2. Para gerenciar a configuração da VPC compartilhada Multi-AZ, use o comando da CLI update-shared-vpc-configuration ou o comando equivalente da API. UpdateSharedVpcConfiguration O exemplo a seguir permite o compartilhamento de VPC para sistemas de arquivos Multi-AZ.

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
```

O serviço responde a uma solicitação bem-sucedida da seguinte forma:

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
}
```

3. Para desativar o recurso, `EnableFsxRouteTableUpdatesFromParticipantAccounts` defina como`false`, conforme mostrado no exemplo a seguir.

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts false
```

O serviço responde a uma solicitação bem-sucedida da seguinte forma:

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

Atualização de um sistema de arquivos

Este tópico explica quais propriedades de um sistema de arquivos existente você pode atualizar e fornece procedimentos para fazer isso usando o console e a CLI.

Você pode atualizar as seguintes propriedades do sistema de arquivos FSx for ONTAP usando o console do Amazon FSx, o e a API AWS CLI do Amazon FSx:

- Backups automáticos diários. Ativa ou desativa os backups automáticos diários, modifica a janela de backup e o período de retenção do backup. Para obter mais informações sobre backups, consulte Como trabalhar com backups diários automáticos.
- Janela de manutenção semanal. Define o dia da semana e a hora em que o Amazon FSx executa a manutenção e as atualizações do sistema de arquivos. Para obter mais informações sobre janela de manutenção, consulte Otimizar a performance com janelas de manutenção do Amazon FSx.
- Senha administrativa do sistema de arquivos. Altera a senha do usuário `fsxadmin` do sistema de arquivos. É possível utilizar o usuário `fsxadmin` para administrar o sistema de arquivos usando a CLI e a API REST do ONTAP. Para obter mais informações sobre o usuário `fsxadmin`, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.
- Tabelas de rotas da Amazon VPC. Com sistemas de arquivos do FSx para ONTAP com diversas AZs, os endpoints que você usa para acessar dados via NFS ou SMB e os endpoints de gerenciamento para acessar a CLI, a API e o BlueXP do ONTAP usam endereços IP flutuantes nas tabelas de rotas da Amazon VPC que você associa ao seu sistema de arquivos. Você pode associar novas tabelas de rotas que você cria aos seus sistemas de arquivos com várias AZs existentes, permitindo que você configure quais clientes podem acessar seus dados mesmo à medida que sua rede evolui. Você também pode desassociar (remover) as tabelas de rotas existentes do seu sistema de arquivos.

> **Note**
>
> O Amazon FSx gerencia tabelas de rotas de VPC para sistemas de arquivos Multi-AZ usando autenticação baseada em tags. Essas tabelas de rotas estão marcadas com`Key: AmazonFSx; Value: ManagedByAmazonFSx`. Ao criar ou atualizar o FSx para sistemas de arquivos ONTAP Multi-AZ usando, AWS CloudFormation recomendamos que você adicione a tag manualmente. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Atualizar um sistema de arquivos (console)

Os procedimentos a seguir fornecem instruções sobre como fazer atualizações em um sistema de arquivos FSx for ONTAP existente usando o. AWS Management Console

Atualizar backups automáticos diários

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

2. Para exibir a página de detalhes do sistema de arquivos, no painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema de arquivos do FSx para ONTAP que você deseja atualizar.
3. Escolha a guia Backups no segundo painel da página.
4. Selecione Atualizar.
5. Modifique as configurações de backup automático diário desse sistema de arquivos.
6. Escolha Salvar para salvar as alterações.

Atualizar a janela de manutenção semanal

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Para exibir a página de detalhes do sistema de arquivos, no painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema de arquivos do FSx para ONTAP que você deseja atualizar.
3. Escolha a guia Administração no segundo painel da página.
4. No painel Manutenção, escolha Atualizar.
5. Modifique quando a janela de manutenção semanal ocorre para esse sistema de arquivos.
6. Escolha Salvar para salvar as alterações.

Alterar a senha administrativa do sistema de arquivos

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Para exibir a página de detalhes do sistema de arquivos, no painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema de arquivos do FSx para ONTAP que você deseja atualizar.
3. Escolha a guia Administração.
4. No painel Administração do ONTAP, escolha Atualizar em Senha do administrador ONTAP.
5. Na caixa de diálogo Atualizar credenciais de administrador ONTAP, digite uma nova senha no campo Senha administrativa do ONTAP.
6. Use o campo Confirmar senha para confirmar a senha.
7. Escolha Atualizar credenciais para salvar sua alteração.

> **Note**
>
> Se você receber um erro informando que a nova senha não atende aos requisitos de senha, você pode usar o comando `security login role config show`ONTAPCLI para visualizar as configurações dos requisitos de senha no sistema de arquivos. Para obter mais informações, incluindo instruções sobre como alterar a configuração da senha, consulteFalha na atualização `fsxadmin` da senha da conta.

Para atualizar as tabelas de rotas da VPC em sistemas de arquivos Multi-AZ

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Para exibir a página de detalhes do sistema de arquivos, no painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema de arquivos do FSx para ONTAP que você deseja atualizar.
3. Em Ações, escolha Gerenciar tabelas de rotas. Essa opção só está disponível para sistemas de arquivos com várias AZs.
4. Na caixa de diálogo Gerenciar tabelas de rotas, faça o seguinte:
   - Para associar uma nova tabela de rotas de VPC, selecione uma tabela de rotas na lista suspensa Associar novas tabelas de rotas e escolha Associar.
   - Para desassociar uma tabela de rotas de VPC existente, selecione uma tabela de rotas no painel Tabelas de rotas atuais e escolha Desassociar.
5. Escolha Fechar.

Atualizar um sistema de arquivos (CLI)

O procedimento a seguir ilustra como fazer atualizações em um sistema de arquivos FSx for ONTAP existente usando o. AWS CLI

1. Para atualizar a configuração de um FSx para o sistema de arquivos ONTAP, use o comando da CLI update-file-system (ou a operação equivalente da API do UpdateFilesistema), conforme mostrado no exemplo a seguir.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
```

```
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
      FsxAdminPassword=new-fsx-admin-password
```

2. Para desativar os backups diários automáticos, defina a `AutomaticBackupRetentionDays` propriedade como 0.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

Excluir um sistema de arquivos

Você pode excluir um sistema de arquivos FSx for ONTAP usando o console do Amazon FSx, o e a API e os SDKs AWS CLI do Amazon FSx.

Para excluir um sistema de arquivos:

- Como usar o console: siga o procedimento descrito em Etapa 3: Limpar os recursos.
- Como usar a CLI ou a API: exclua primeiro todos os volumes e as SVMs do sistema de arquivos. Em seguida, use o comando da CLI delete-file-system ou a operação da API do sistema. DeleteFile

Visualizando detalhes do sistema de arquivos

Você pode visualizar informações detalhadas de configuração do seu sistema de arquivos FSx for ONTAP usando o console Amazon FSx, o AWS CLI, a API e os SDKs compatíveis. AWS

Para ver informações detalhadas do sistema de arquivos:

- Como usar o console: escolha um sistema de arquivos para visualizar a página de detalhes dos Sistemas de arquivos. O painel Resumo mostra o ID do sistema de arquivos, o status do ciclo de vida, o tipo de implantação, a capacidade de armazenamento SSD, a capacidade de throughput, as IOPS provisionadas, as zonas de disponibilidade e o horário de criação.

  As guias a seguir fornecem informações detalhadas de configuração e edição de propriedades que podem ser modificadas:

- Rede e segurança
- Monitoramento e desempenho — Exibe CloudWatch alarmes que você criou e métricas e avisos para as seguintes categorias:
  - Resumo — resumo de alto nível das métricas de atividade do sistema de arquivos
  - Capacidade de armazenamento do sistema de arquivos
  - Desempenho do servidor de arquivos e do disco

  Para ter mais informações, consulte Monitoramento com a Amazon CloudWatch.
- Administração — Exibe as seguintes informações de administração do sistema de arquivos:
  - Os DNS nomes e IP endereços do gerenciamento do sistema de arquivos e dos endpoints entre clusters.
  - O nome ONTAP de usuário do administrador.
  - A opção de atualizar a senha ONTAP do administrador.
- Lista dos SVMs do sistema de arquivos
- Lista dos volumes do sistema de arquivos
- Configurações de backup — altere a configuração de backup diário automático do sistema de arquivos.
- Atualizações — mostra o status das atualizações iniciadas pelo usuário feitas na configuração do sistema de arquivos.
- Tags — visualize, edite, adicione, remova pares de tags Chave:Valor.
- Usando a CLI ou a API — Use o comando describe-file-systems da CLI ou a operação da API Systems. DescribeFile

Status do sistema de arquivos do FSx para ONTAP

Você pode visualizar o status de um sistema de arquivos Amazon FSx usando o console do Amazon FSx, o AWS CLI comando describe-file-systems ou os sistemas operacionais da API. DescribeFile

Status do sistema de arquivos	Descrição
DISPONÍVEL	O sistema de arquivos foi criado com êxito e está disponível para uso.

Status do sistema de arquivos	Descrição
CRIANDO	O Amazon FSx está criando um novo sistema de arquivos.
EXCLUINDO	O Amazon FSx está excluindo um sistema de arquivos existente.
CONFIGURAÇÃO INCORRETA	O sistema de arquivos está em um estado de configuração incorreta, mas recuperável.
COM FALHA	1. O sistema de arquivos falhou e o Amazon FSx não consegue recuperá-lo. 2. Ao criar um sistema de arquivos, o Amazon FSx não conseguiu criá-lo.

Como gerenciar máquinas virtuais de armazenamento do FSx para ONTAP

No FSx para ONTAP, os volumes são hospedados em servidores de arquivos virtuais chamados de máquinas virtuais de armazenamento (SVMs). Uma SVM é um servidor de arquivos isolado com suas próprias credenciais administrativas e endpoints para administrar e acessar dados. Ao acessar dados no FSx para ONTAP, seus clientes e estações de trabalho montam um volume, um compartilhamento SMB ou um LUN de iSCSI hospedado por uma SVM usando o endpoint (endereço IP) da SVM.

O Amazon FSx cria automaticamente uma SVM padrão no seu sistema de arquivos quando você cria um sistema de arquivos usando o AWS Management Console. Você pode criar SVMs adicionais em seu sistema de arquivos a qualquer momento usando o console ou a API e AWS CLI os SDKs do Amazon FSx. Não é possível criar SVMs usando a CLI ou a API REST do ONTAP.

Você pode associar as SVMs a um Microsoft Active Directory para autenticação e autorização de acesso a arquivos. Para ter mais informações, consulte Trabalhar com o Microsoft Active Directory no FSx para ONTAP.

Número máximo de SVMs por sistema de arquivos

A tabela a seguir lista o número máximo de SVMs que você pode criar para um sistema de arquivos. O número máximo de SVMs depende da quantidade de capacidade de throughput provisionada em megabytes por segundo (MBps).

Tipo de implantação	Quantidade de capacidade de throughput (MBps)	Número máximo de SVMs por sistema de arquivos
Single-AZ (expansão ascendente) e Multi-AZ (expansão ascendente)	128	6
	256	6
	512	14
	1,024	14
	2.048	24
	4.096	24
Single-AZ (expansão horizontal)	Any	5

Tópicos

- Como criar uma máquina virtual de armazenamento
- Atualizar uma máquina virtual de armazenamento
- Excluir uma máquina virtual de armazenamento (SVM)
- Visualizar detalhes de configuração da máquina virtual de armazenamento

Como criar uma máquina virtual de armazenamento

Você pode criar um FSx para ONTAP SVM usando a API AWS Management Console, e. AWS CLI

O número máximo de SVMs que você pode criar para um sistema de arquivos depende do tipo de implantação do sistema de arquivos e da quantidade de capacidade de transferência provisionada. Para ter mais informações, consulte Número máximo de SVMs por sistema de arquivos.

Propriedades da SVM

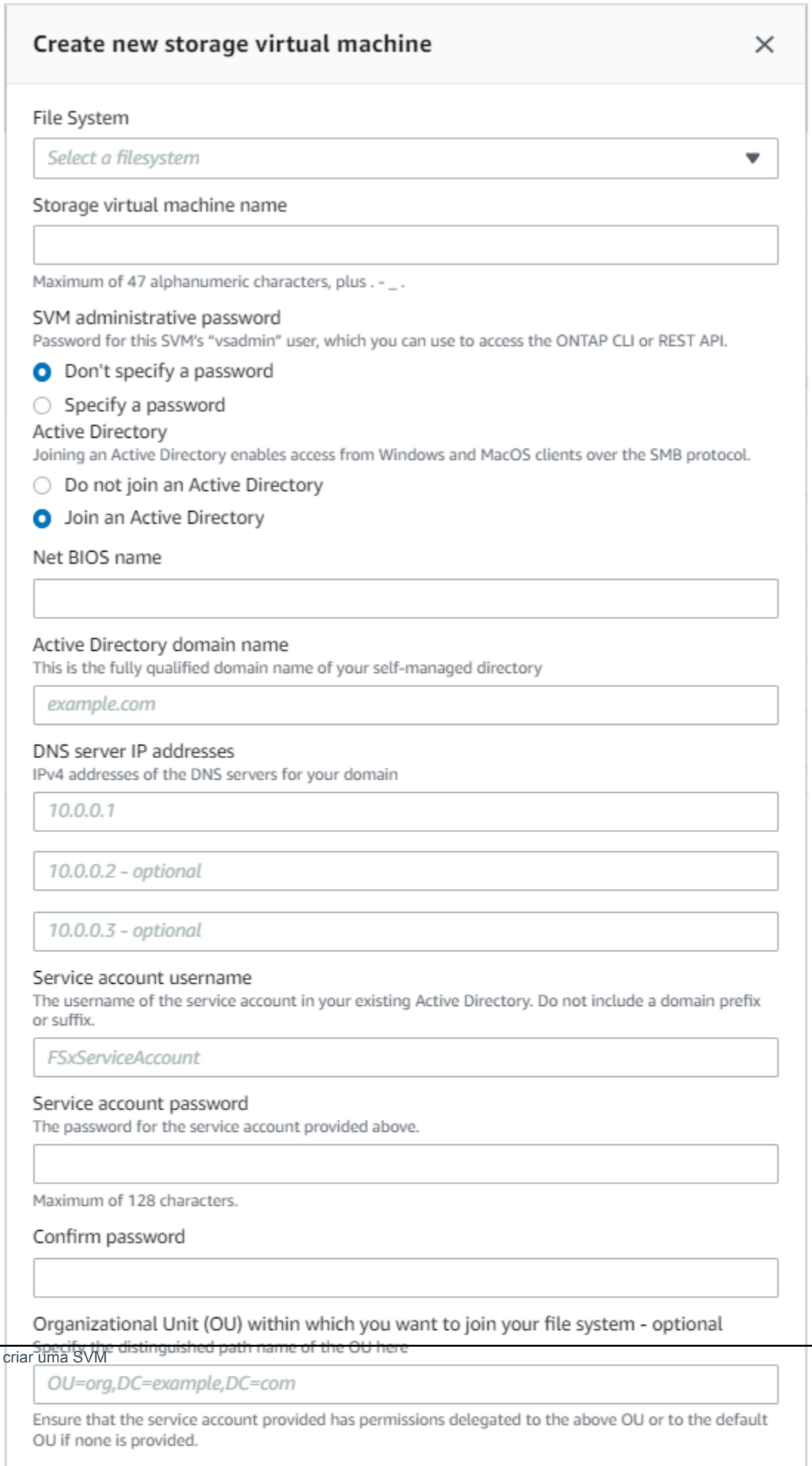
Ao criar uma SVM, defina as propriedades a seguir.

- O sistema de arquivos do FSx para ONTAP ao qual ela pertence.
- A configuração do Microsoft Active Directory (AD). Opcionalmente, você pode associar a SVM a um AD autogerenciado para fins de autenticação e controle de acesso de clientes Windows e macOS. Para ter mais informações, consulte Trabalhar com o Microsoft Active Directory no FSx para ONTAP.
- O estilo de segurança do volume raiz: defina o estilo de segurança do volume raiz (Unix, NTFS ou Misto) para se alinhar ao tipo de clientes que está usando para acessar os dados na SVM. Para ter mais informações, consulte Estilo de segurança do volume.
- A senha administrativa da SVM. Opcionalmente, você pode definir a senha para o usuário `vsadmin` da SVM. Para ter mais informações, consulte Gerenciando SVMs com a CLI ONTAP.

Criar uma máquina virtual de armazenamento (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Máquinas virtuais de armazenamento.
3. Escolha Criar máquina virtual de armazenamento.

   A caixa de diálogo Criar máquina virtual de armazenamento é exibida.


Create new storage virtual machine
File System
Select a filesystem
Storage virtual machine name
Maximum of 47 alphanumeric characters, plus . - _ .
SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.
Don't specify a password
Specify a password
Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.
Do not join an Active Directory
Join an Active Directory
Net BIOS name
Active Directory domain name
This is the fully qualified domain name of your self-managed directory
example.com
DNS server IP addresses
IPv4 addresses of the DNS servers for your domain
10.0.0.1
10.0.0.2 - optional
10.0.0.3 - optional
Service account username
The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
FSxServiceAccount
Service account password
The password for the service account provided above.
Maximum of 128 characters.
Confirm password
Organizational Unit (OU) within which you want to join your file system - optional
Specify the distinguished path name of the OU here
OU=org,DC=example,DC=com
Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

4. Em Sistema de arquivos, escolha o sistema de arquivos no qual criar a máquina virtual de armazenamento.
5. No campo Nome da máquina virtual de armazenamento, forneça um nome para a máquina virtual de armazenamento. Você pode usar, no máximo, 47 caracteres alfanuméricos, além do caractere especial de sublinhado (_).
6. Em Senha administrativa da SVM, você pode, opcionalmente, escolher Especificar uma senha e fornecer uma senha para o usuário `vsadmin` dessa SVM. Você pode usar o usuário `vsadmin` para administrar a SVM utilizando a CLI ou a API REST do ONTAP. Para obter mais informações sobre o usuário `vsadmin`, consulte Gerenciando SVMs com a CLI ONTAP.

   Se você escolher Não especificar uma senha (o padrão), ainda poderá utilizar o usuário `fsxadmin` do sistema de arquivos para gerenciar o sistema usando a CLI ou a API REST do ONTAP, mas não poderá utilizar o usuário `vsadmin` da SVM para fazer o mesmo.
7. Em Active Directory, você tem as opções a seguir.

   - Se não estiver associando o sistema de arquivos a um Active Directory (AD), escolha Não associar um Active Directory.
   - Se estiver associando a SVM ao domínio de um AD autogerenciado, escolha Associar um Active Directory e forneça os detalhes a seguir para o AD. Para ter mais informações, consulte Pré-requisitos para unir uma SVM a um Microsoft AD autogerenciado.
     - O nome NetBIOS do objeto de computador do Active Directory que será criado para a SVM. O nome NetBIOS não pode ter mais de 15 caracteres. Esse é o nome dessa SVM no Active Directory.
     - O nome de domínio totalmente qualificado (FQDN) do Active Directory. O FQDN não pode exceder 255 caracteres.
     - Endereços IP do servidor DNS: os endereços IPv4 dos servidores DNS do seu domínio.
     - Nome de usuário da conta de serviço: o nome de usuário da conta de serviço em seu Active Directory existente. Não inclua um prefixo ou sufixo de domínio. Para `EXAMPLE\ADMIN`, use `ADMIN`.
     - Senha da conta de serviço: a senha da conta de serviço.
     - Confirmar senha: a senha da conta de serviço.
     - (Opcional) Unidade organizacional (UO): o nome do caminho distinto da unidade organizacional à qual você deseja unir seu sistema de arquivos.
     - Grupo de administradores delegado do sistema de arquivos: o nome do grupo em seu AD que pode administrar seu sistema de arquivos.

Se você estiver usando AWS Managed Microsoft AD, você deve especificar um grupo como Administradores AWS Delegados FSx AWS , Administradores Delegados ou um grupo personalizado com permissões delegadas para a OU.

Se você estiver ingressando em um AD autogerenciado, use o nome do grupo em seu AD. O grupo padrão é `Domain Admins`.

8. Em Estilo de segurança do volume raiz da SVM, escolha o estilo de segurança da SVM, dependendo do tipo de clientes que acessam seus dados. Escolha Unix (Linux) se clientes Linux são seu principal meio de acesso aos dados; escolha NTFS se clientes Windows são seu principal meio de acesso aos dados. Para ter mais informações, consulte Estilo de segurança do volume.
9. Escolha Confirmar para criar a máquina virtual de armazenamento.

Você pode monitorar o progresso da atualização na página de detalhes Sistemas de arquivos, na coluna Status do painel Máquinas virtuais de armazenamento. A máquina virtual de armazenamento estará pronta para uso quando o status for Criado.

Criar uma máquina virtual de armazenamento (CLI)

- Para criar um FSx para a máquina virtual de armazenamento (SVM) ONTAP, use o comando create-storage-virtual-machineCLI (ou a operação de CreateStorageVirtualMachineAPI equivalente), conforme mostrado no exemplo a seguir.

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name svm1 \
    --svm-admin-password password \
    --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Depois de criar com êxito a máquina virtual de armazenamento, o Amazon FSx retorna a descrição no formato JSON, conforme mostrado no exemplo a seguir.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
```

```
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Atualizar uma máquina virtual de armazenamento

Você pode atualizar as seguintes propriedades de configuração da máquina virtual de armazenamento (SVM) usando o console AWS CLI do Amazon FSx e a API do Amazon FSx:

- Senha da conta administrativa da SVM.
- Configuração do Active Directory (AD) da SVM: você pode associar uma SVM a um AD ou modificar a configuração do AD de uma SVM já associada a um AD. Para ter mais informações, consulte Gerenciando configurações do SVM Active Directory.

Atualizar as credenciais da conta de administrador da SVM (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha a SVM a ser atualizada da seguinte forma:
   - No painel de navegação à esquerda, escolha Sistemas de arquivos e selecione o sistema de arquivos do ONTAP para o qual deseja atualizar uma SVM.
   - Escolha a guia Máquinas virtuais de armazenamento.

     Ou

   - Para exibir uma lista de todas as SVMs disponíveis Conta da AWS na sua atual Região da AWS, expanda ONTAP e escolha Armazenamento de máquinas virtuais.
3. Escolha a máquina virtual de armazenamento que deseja atualizar.
4. Escolha Ações > Atualizar senha do administrador. A janela Atualizar credenciais administrativas da SVM é exibida.
5. Insira a nova senha do usuário `vsadmin` e confirme-a.
6. Escolha Atualizar credenciais para salvar a nova senha.

Atualizar as credenciais da conta de administrador da SVM (CLI)

- Para atualizar a configuração de um FSx para ONTAP SVM, use o comando update-storage-virtual-machineCLI (ou a operação de UpdateStorageVirtualMachineAPI equivalente), conforme mostrado no exemplo a seguir.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

Depois de criar com êxito a máquina virtual de armazenamento, o Amazon FSx retorna a descrição no formato JSON, conforme mostrado no exemplo a seguir.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
```

```
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
    "StorageVirtualMachineId": "svm-abcdef01234567890",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Excluir uma máquina virtual de armazenamento (SVM)

Você só pode excluir um FSx para ONTAP SVM usando o console Amazon FSx, o e a API. AWS CLI Antes de excluir uma SVM, você deve primeiro excluir todos os volumes não raiz anexados à SVM.

> **Important**
>
> Você não pode excluir uma SVM usando a NetApp CLI ou a API do ONTAP.

> **Note**
>
> Antes de excluir uma máquina virtual de armazenamento, verifique se nenhuma aplicação está acessando os dados na SVM e se você excluiu todos os volumes não raiz anexados à SVM.

Excluir uma máquina virtual de armazenamento (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha a SVM que deseja excluir como mostrado a seguir.

   - No painel de navegação à esquerda, escolha Sistemas de arquivos e o sistema de arquivos do ONTAP do qual você deseja excluir uma SVM.
   - Escolha a guia Máquinas virtuais de armazenamento.

   Ou

   - Para exibir uma lista de todas as SVMs disponíveis, expanda ONTAP e escolha Máquinas virtuais de armazenamento.

   Na lista, selecione a SVM que deseja excluir.
3. Na guia Volumes, visualize a lista de volumes anexados à SVM. Se houver volumes não raiz anexados à SVM, é necessário excluí-los antes de excluir a SVM. Consulte Excluir um volume para obter mais informações.
4. Escolha Excluir máquina virtual de armazenamento no menu Ações.
5. Na caixa de diálogo de confirmação da exclusão, escolha Excluir máquina virtual de armazenamento.

Excluir uma máquina virtual de armazenamento (CLI)

- Para excluir uma máquina virtual de armazenamento FSx for ONTAP, use o comando delete-storage-virtual-machineCLI (ou a operação de DeleteStorageVirtualMachineAPI equivalente), conforme mostrado no exemplo a seguir.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

Visualizar detalhes de configuração da máquina virtual de armazenamento

Você pode ver as máquinas virtuais de armazenamento FSx for ONTAP que estão atualmente em seu sistema de arquivos usando o console Amazon FSx, o e AWS CLI a API Amazon FSx.

Para visualizar uma máquina virtual de armazenamento no sistema de arquivos:

- Como usar o console: escolha um sistema de arquivos para visualizar a página de detalhes Sistemas de arquivos. Para listar todas as máquinas virtuais de armazenamento no sistema de arquivos, escolha a guia Máquinas virtuais de armazenamento e selecione a máquina virtual de armazenamento que deseja visualizar.
- Usando a CLI ou a API — Use o comando da describe-storage-virtual-machinesCLI ou a operação da API. DescribeStorageVirtualMachines

  A resposta do sistema é uma lista com descrições completas de todas as SVMs da sua conta na Região da AWS.

Como gerenciar volumes do FSx para ONTAP

Cada máquina virtual de armazenamento (SVM) em um sistema de arquivos do FSx para ONTAP pode ter um ou mais volumes. Um volume é um contêiner de dados isolado para arquivos, diretórios ou unidades lógicas de armazenamento (LUNs) de iSCSI. Os volumes têm provisionamento reduzido, ou seja, consomem capacidade de armazenamento somente para os dados armazenados neles.

É possível acessar um volume de clientes Linux, Windows ou macOS por meio dos protocolos Network File System (NFS), Server Message Block (SMB) ou Internet Small Computer Systems Interface (iSCSI), criando um LUN de iSCSI (armazenamento em blocos compartilhado). O FSx para ONTAP também oferece suporte ao acesso multiprotocolo (acesso simultâneo a NFS e SMB) ao mesmo volume.

Você pode criar volumes usando o AWS Management Console, AWS CLI, a API Amazon FSx ou NetApp o BlueXP. Você também pode usar o endpoint administrativo do sistema de arquivos ou do SVM para criar, atualizar e excluir volumes usando a CLI ou a API NetApp REST do ONTAP.

> **Note**
>
> Você pode criar 500 volumes por par de HA, até 1.000 volumes em todos os pares de HA. FlexGroupos volumes constituintes contam para esse limite. Por padrão, há oito volumes constituintes por agregado, por. FlexGroup

Ao criar um volume, defina as propriedades a seguir.

- Estilo de volume — O estilo de volume pode ser FlexVol ouFlexGroup.
- Nome do volume — O nome do volume.
- Tipo do volume: o tipo do volume pode ser leitura e gravação (RW) ou proteção de dados (DP). Os volumes DP são somente para leitura e usados como destino em um NetApp SnapMirror relacionamento. SnapVault
- Tamanho do volume: essa é a quantidade máxima de dados que o volume pode armazenar, independentemente do nível de armazenamento.
- Caminho da junção: esse é o local no namespace da SVM no qual o volume é montado.
- Eficiência de armazenamento — Os recursos de eficiência de armazenamento, incluindo compactação, compactação e desduplicação de dados, proporcionam uma economia de armazenamento típica de 65% para cargas de trabalho de compartilhamento de arquivos de uso geral.
- Estilo de segurança do volume (Unix, NTFS ou Misto) — Determina quais tipos de permissões são usadas para acesso aos dados no volume ao autorizar usuários.
- Classificação por níveis de dados — a política de classificação por níveis define quais dados são armazenados no nível econômico do pool de capacidade.
- Período de resfriamento da política de classificação por níveis — define quando os dados são marcados como frios e movidos para o armazenamento do pool de capacidade.
- Política de snapshots: as políticas de snapshots definem como o sistema cria snapshots para um volume. Você pode escolher entre três políticas predefinidas ou usar uma política personalizada que você criou usando a CLI do ONTAP ou a API REST.
- Copiar tags para backups — O Amazon FSx copiará automaticamente todas as tags de seus volumes para backups usando essa opção. Você pode definir essa opção usando a API AWS CLI ou Amazon FSx.

Tópicos

Estilos de volume

O FSx for ONTAP oferece dois estilos de volumes que você pode usar para finalidades diferentes. Você pode criar um FlexVol ou vários FlexGroup volumes usando o console do Amazon FSx AWS CLI, o e a API do Amazon FSx.

- FlexVolos volumes oferecem a experiência mais simples para sistemas de arquivos com um par de alta disponibilidade (HA) e são o estilo de volume padrão para sistemas de arquivos escaláveis. O tamanho mínimo de um FlexVol volume é 20 mebibytes (MiB) e o tamanho máximo é 314.572.800 MiB.
- FlexGroupos volumes são compostos por vários FlexVol volumes constituintes, o que lhes permite oferecer maior desempenho e escalabilidade de armazenamento do que os FlexVol volumes para sistemas de arquivos com vários pares de HA. FlexGroupvolumes são o estilo de volume padrão para sistemas de arquivos escaláveis. O tamanho mínimo de um FlexGroup volume é de 100 gibibytes (GiB) por componente e o tamanho máximo é de 20 pebibytes (PiB).

Você pode converter um volume com o FlexVol estilo no FlexGroup estilo com a ONTAP CLI, que cria um FlexGroup com um único constituinte. No entanto, recomendamos que você use AWS DataSync para mover dados entre um FlexVol volume e um novo FlexGroup volume para garantir que os dados sejam distribuídos uniformemente entre os FlexGroup's constituintes. Para ter mais informações, consulte FlexGroupconstituintes.

> **Note**
>
> Se você quiser usar a ONTAP CLI para converter um FlexVol volume em um FlexGroup volume, certifique-se de excluir todos os backups do FlexVol volume antes de convertê-lo. ONTAPnão reequilibra automaticamente os dados como parte da conversão, portanto, os dados podem estar desequilibrados entre os FlexGroup constituintes.

FlexGroupconstituintes

Um FlexGroup volume é composto de constituintes, que são FlexVol volumes. Por padrão, o FSx for ONTAP atribui oito constituintes a um FlexGroup volume por par de HA.

Quando você cria seu FlexGroup volume, o tamanho dele é dividido igualmente entre seus constituintes. Por exemplo, se você criar um FlexGroup volume de 800 gigabytes (GB) com oito

componentes, cada componente terá 100 GB de tamanho. Um FlexGroup volume pode ter entre 100 GB e 20 PiB, mas o tamanho total depende do tamanho dos componentes. Cada componente tem um tamanho mínimo de 100 GB e um tamanho máximo de 300 TiB. Por exemplo, um FlexGroup volume com oito componentes tem um tamanho mínimo de 800 GB e um tamanho máximo de 20 PiB.

O ONTAP distribui dados no nível do arquivo entre os constituintes. Você pode armazenar até dois bilhões de arquivos em cada componente do seu FlexGroup volume.

Quando você atualiza o tamanho do seu FlexGroup volume, o novo tamanho é distribuído uniformemente entre os componentes existentes.

Você também pode adicionar mais componentes ao seu FlexGroup volume usando a ONTAP CLI ou a API REST. No entanto, recomendamos que você faça isso somente se precisar de capacidade de armazenamento adicional e todos os seus componentes já estiverem no tamanho máximo (300 TiB por componente). Adicionar componentes pode levar a um desequilíbrio de dados e E/S entre os componentes. Até que os constituintes estejam balanceados, é possível que a taxa de transferência de gravação seja 5 a 10% menor do que um volume balanceadoFlexGroup. Quando novos dados são gravados no FlexGroup volume, o ONTAP prioriza distribuí-los entre os novos constituintes até que os constituintes estejam equilibrados. Se você adicionar novos constituintes, recomendamos escolher um número par e não exceder oito por agregado.

> **Note**
>
> Se você adicionar novos componentes, seus instantâneos existentes se tornarão instantâneos parciais; portanto, eles não poderão ser usados para restaurar totalmente seu FlexGroup volume a um estado anterior. Os instantâneos anteriores não oferecem uma point-in-time imagem completa do seu FlexGroup volume porque os novos componentes ainda não existiam. No entanto, os instantâneos parciais podem ser usados para restaurar arquivos e diretórios individuais, criar um novo volume ou replicá-lo. SnapMirror

Tipos de volume

O FSx for ONTAP oferece dois tipos de volumes que você pode criar usando o console do Amazon FSx, o e a API AWS CLI do Amazon FSx.

- Os volumes de leitura e gravação (RW) são usados na maioria dos casos. Como o nome indica, eles podem ser lidos e gravados.

- Os volumes de proteção de dados (DP) são volumes somente para leitura que você usa como destino de um NetApp SnapMirror relacionamento ou. SnapVault Você deve usar os volumes DP quando quiser migrar ou proteger os dados de um único volume.

FlexVole FlexGroup os volumes podem ser RW ou DP.

> **Note**
>
> Você não pode atualizar o tipo de um volume após a criação do volume.

Estilo de segurança do volume

O FSx for ONTAP suporta 3 estilos diferentes de segurança de volume: Unix, NTFS e misto. Cada estilo de segurança tem um efeito diferente na forma como as permissões são tratadas para os dados. Você deve compreender os diferentes efeitos para garantir a seleção do estilo de segurança apropriado para seus propósitos.

É importante entender que os estilos de segurança não determinam quais tipos de clientes podem ou não acessar os dados. Os estilos de segurança determinam apenas o tipo de permissões que o FSx for ONTAP usa para controlar o acesso aos dados e qual tipo de cliente pode modificar essas permissões.

Os dois fatores que você usa para determinar o estilo de segurança de um volume são o tipo de administrador que gerencia o sistema de arquivos e o tipo de usuários ou serviços que acessam os dados no volume.

Ao criar um volume no console, na CLI e na API do Amazon FSx, o estilo de segurança é automaticamente definido como o estilo de segurança do volume raiz. Você pode modificar o estilo de segurança de um volume usando a API AWS CLI ou. É possível modificar essa configuração após a criação do volume. Consulte Atualizar um volume Para mais informações.

Ao configurar o estilo de segurança em um volume, considere as necessidades do seu ambiente para garantir que você selecione o melhor estilo de segurança para evitar problemas com o gerenciamento de permissões. Tenha em mente que o estilo de segurança não determina quais tipos de clientes podem acessar os dados. O estilo de segurança determina as permissões usadas para permitir o acesso aos dados e os tipos de clientes que podem modificar essas permissões. Veja a seguir algumas considerações que podem ajudar você a decidir qual estilo de segurança escolher para um volume.

- Unix (Linux): escolha esse estilo de segurança se o sistema de arquivos for gerenciado por um administrador do Unix, se a maioria dos usuários for de clientes NFS e se uma aplicação acessando os dados usar um usuário do Unix como conta de serviço. Somente clientes Linux podem modificar permissões com o estilo de segurança Unix, e os tipos de permissões usados em arquivos e diretórios são mode-bits ou ACLs NFS v4.x.
- NTFS: escolha esse estilo de segurança se o sistema de arquivos for gerenciado por um administrador do Windows, se a maioria dos usuários for de clientes SMB e se uma aplicação acessando os dados usar um usuário do Windows como conta de serviço. Se for necessário qualquer acesso do Windows a um volume, recomendamos usar o estilo de segurança NTFS. Somente clientes Windows podem modificar permissões com o estilo de segurança NTFS, e os tipos de permissões usados em arquivos e diretórios são ACLs NTFS.
- Misto: essa configuração é avançada. Para obter mais informações, consulte o tópico Quais são os estilos de segurança e seus efeitos no Centro de NetApp Documentação.

Criação de volumes

Você pode criar um FSx para ONTAP FlexVol ou FlexGroup volume usando o console Amazon FSx, o e a API Amazon FSx, além AWS CLI da interface de linha de NetApp comando (CLI) e da API REST do ONTAP.

Para criar um FlexVol volume (console)

> **Note**
>
> O estilo de segurança do volume é automaticamente definido como o estilo de segurança do volume raiz.

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, selecione Volumes.
3. Escolha Create volume (Criar volume).
4. Em Tipo de sistema de arquivos, escolha Amazon FSx for NetApp ONTAP.
5. Na seção Detalhes do sistema de arquivos, forneça as seguintes informações:
   - Em Sistema de arquivos, escolha o sistema de arquivos no qual criar o volume.

- Em Máquina virtual de armazenamento, escolha a máquina virtual de armazenamento (SVM) na qual criar o volume.

6. Na seção Estilo de volume, escolha FlexVol.
7. Na seção Detalhes do volume, forneça as seguintes informações:

   - No campo Nome do volume, forneça um nome para o volume. Você pode usar até 203 caracteres alfanuméricos ou sublinhados (_).
   - Em Tamanho do volume, insira qualquer número inteiro no intervalo de 20 a 314572800 para especificar o tamanho em mebibytes (MiB).
   - Para Tipo de volume, escolha Leitura-Gravação (RW) para criar um volume que seja legível e gravável ou Proteção de Dados (DP) para criar um volume que seja somente para leitura e possa ser usado como destino de um relacionamento. NetApp SnapMirror SnapVault Para ter mais informações, consulte Tipos de volume.
   - Em Caminho da junção, insira um local no sistema de arquivos para montar o volume. O nome deve ter uma barra inicial, por exemplo `/vol3`.
   - Para Eficiência de armazenamento, escolha Habilitado para habilitar os recursos de eficiência de armazenamento do ONTAP (eliminação da duplicação, compressão e compactação). Para ter mais informações, consulte Eficiência de armazenamento do FSx para ONTAP.
   - Para o estilo de segurança de volume, escolha entre Unix (Linux), NTFS e Mixed para o volume. Para ter mais informações, consulte Estilo de segurança do volume.
   - Em Política de snapshots, escolha uma política de snapshots para o volume. Para obter mais informações sobre políticas de snapshots, consulte Políticas de snapshots.

     Se você escolher Política personalizada, especifique o nome da política no campo política personalizada. A política personalizada já deve existir na SVM ou no sistema de arquivos. Você pode criar uma política de snapshots personalizada com a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política de snapshot na documentação do produto NetApp ONTAP.

8. Na seção Classificação por níveis de armazenamento, forneça as seguintes informações:

   - Para a política de classificação por níveis do pool de capacidade, escolha a política de classificação por níveis do pool de armazenamento para o volume, que pode ser Automática (o padrão), Somente Snapshot, Tudo ou Nenhuma. Para ter mais informações, consulte Políticas de classificação por níveis de volume.

- Se você escolher Automático ou Somente Snapshot, poderá definir o período de resfriamento da política de hierarquização para definir o número de dias antes que os dados que não foram acessados sejam marcados como frios e movidos para o armazenamento do pool de capacidade. Você pode fornecer um valor entre 2 e 183 dias. A configuração padrão é de 31 dias.

9. Na seção Avançado, em SnapLockConfiguração, escolha entre Ativado e Desativado. Para obter mais informações sobre como configurar um volume de SnapLock conformidade ou um volume SnapLock corporativo, consulte Como criar um volume do SnapLock Compliance e. Como criar um volume do SnapLock Enterprise Para obter mais informações sobre o SnapLock, consulte Protegendo seus dados com SnapLock.
10. Escolha Confirmar para criar o volume.

Você pode monitorar o progresso da atualização na página de detalhes Sistemas de arquivos, na coluna Status do painel Volumes. O volume estará pronto para uso quando o status for Criado.

Para criar um FlexGroup volume (console)

> **Note**
>
> Você só pode criar FlexGroup volumes para sistemas de arquivos escaláveis usando o console Amazon FSx. Para criar FlexVol volumes para seus sistemas de arquivos escaláveis, use a API AWS CLI Amazon FSx ou as ferramentas de gerenciamento. NetApp

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, selecione Volumes.
3. Escolha Create volume (Criar volume).
4. Em Tipo de sistema de arquivos, escolha Amazon FSx for NetApp ONTAP.
5. Na seção Detalhes do sistema de arquivos, forneça as seguintes informações:
   - Em Sistema de arquivos, escolha o sistema de arquivos no qual criar o volume.
   - Em Máquina virtual de armazenamento, escolha a máquina virtual de armazenamento (SVM) na qual criar o volume.
6. Na seção Estilo de volume, escolha FlexGroup.
7. Na seção Detalhes do volume, forneça as seguintes informações:

- No campo Nome do volume, forneça um nome para o volume. Você pode usar até 203 caracteres alfanuméricos ou sublinhados (_).
- Em Tamanho do volume, insira qualquer número inteiro na faixa de 800 gibibytes (GiB) a 2.000 pebibytes (PiB).
- Para Tipo de volume, escolha Leitura-Gravação (RW) para criar um volume que seja legível e gravável ou Proteção de Dados (DP) para criar um volume que seja somente para leitura e possa ser usado como destino de um relacionamento. NetApp SnapMirror SnapVault Para ter mais informações, consulte Tipos de volume.
- Em Caminho da junção, insira um local no sistema de arquivos para montar o volume. O nome deve ter uma barra inicial, por exemplo `/vol3`.
- Para Eficiência de armazenamento, escolha Habilitado para habilitar os recursos de eficiência de armazenamento do ONTAP (eliminação da duplicação, compressão e compactação). Para ter mais informações, consulte Eficiência de armazenamento do FSx para ONTAP.
- Para o estilo de segurança de volume, escolha entre Unix (Linux), NTFS e Mixed para o volume. Para ter mais informações, consulte Estilo de segurança do volume.

  > **Note**
  >
  > O estilo de segurança do volume é automaticamente definido como o estilo de segurança do volume raiz.

- Em Política de snapshots, escolha uma política de snapshots para o volume. Para obter mais informações sobre políticas de snapshots, consulte Políticas de snapshots.

  Se você escolher Política personalizada, especifique o nome da política no campo política personalizada. A política personalizada já deve existir na SVM ou no sistema de arquivos. Você pode criar uma política de snapshots personalizada com a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política de snapshot na documentação do produto NetApp ONTAP.

8. Na seção Classificação por níveis de armazenamento, forneça as seguintes informações:

   - Para a política de classificação por níveis do pool de capacidade, escolha a política de classificação por níveis do pool de armazenamento para o volume, que pode ser Automática (o padrão), Somente Snapshot, Tudo ou Nenhuma. Para ter mais informações, consulte Políticas de classificação por níveis de volume.

- Se você escolher Automático ou Somente Snapshot, poderá definir o período de resfriamento da política de hierarquização para definir o número de dias antes que os dados que não foram acessados sejam marcados como frios e movidos para o armazenamento do pool de capacidade. Você pode fornecer um valor entre 2 e 183 dias. A configuração padrão é de 31 dias.

9. Na seção Avançado, em SnapLockConfiguração, escolha entre Ativado e Desativado. Para obter mais informações sobre como configurar um volume de SnapLock conformidade ou um volume SnapLock corporativo, consulte Como criar um volume do SnapLock Compliance e. Como criar um volume do SnapLock Enterprise Para obter mais informações sobre o SnapLock, consulte Protegendo seus dados com SnapLock.
10. Escolha Confirmar para criar o volume.

Você pode monitorar o progresso da atualização na página de detalhes Sistemas de arquivos, na coluna Status do painel Volumes. O volume estará pronto para uso quando o status for Criado.

Para criar um volume (CLI)

- Para criar um volume FSx para ONTAP, use o comando da CLI create-volume (ou a operação de CreateVolumeAPI equivalente), conforme mostrado no exemplo a seguir.

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
          SizeInMegabytes=1024,SnapshotPolicy=default, \
          StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
          StorageEfficiencyEnabled=true
```

Depois de criar o volume com êxito, o Amazon FSx retorna a descrição no formato JSON, conforme mostrado no exemplo a seguir.

```
{
    "Volume": {
        "CreationTime": "2022-08-12T13:03:37.625000-04:00",
        "FileSystemId": "fs-abcdef0123456789c",
        "Lifecycle": "CREATING",
        "Name": "vol1",
```

```
        "OntapConfiguration": {
            "CopyTagsToBackups": true,
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "NTFS",
            "SizeInMegabytes": 1024,
            "SnapshotPolicy": "default",
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abcdef0123456789a",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "NONE"
            },
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
        "VolumeId": "fsvol-abcdef0123456789b",
        "VolumeType": "ONTAP"


    }
}
```

Você também pode criar um novo volume restaurando um backup de um volume em um novo volume. Para ter mais informações, consulte Restaurando backups em um novo volume.

Atualizar um volume

Você pode atualizar a configuração de um volume FSx for ONTAP usando o console Amazon FSx, o e a API Amazon FSx, além AWS CLI da interface de linha de NetApp comando (CLI) e da API REST do ONTAP. Você pode modificar as seguintes propriedades de um volume existente do FSx para ONTAP:

- Nome do volume
- Caminho da junção
- Tamanho do volume
- Eficiência de armazenamento
- Política de divisão em níveis do grupo de capacidade
- Estilo de segurança do volume

- Política de snapshots
- Período de resfriamento da política de divisão em níveis
- Copie tags para backups (usando AWS CLI a API Amazon FSx)

Para ter mais informações, consulte Como gerenciar volumes do FSx para ONTAP.

Para atualizar a configuração de um volume (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 ONTAP para o qual deseja atualizar um volume.
3. Escolha a guia Volumes.
4. Escolha o volume que deseja atualizar.
5. Em Ações, escolha Atualizar volume.

   A caixa de diálogo Atualizar volume é exibida com as configurações atuais do volume.
6. Em Caminho da junção, insira um local existente no sistema de arquivos para montar o volume. O nome deve ter uma barra inicial, como `/vol5`.
7. Para Tamanho do volume, você pode aumentar ou diminuir o tamanho do volume dentro do intervalo especificado no console do Amazon FSx. Para FlexVol volumes, o tamanho máximo é 300 TiB. Para FlexGroup volumes, o tamanho máximo é 300 TiB multiplicado pelo número total de volumes constituintes que você FlexGroup tem, até um máximo de 20 PiB.
8. Em Eficiência do armazenamento, escolha Habilitado para habilitar os recursos de eficiência do armazenamento do ONTAP (eliminação de duplicação, compressão e compactação), ou escolha Desabilitado para desabilitá-los.
9. Em Política de divisão em níveis do grupo de capacidade, escolha uma nova política de divisão em níveis do grupo de armazenamento para o volume, que pode ser Automática (o padrão), Somente snapshot, Todos ou Nenhuma. Para obter mais informações sobre políticas de camadas do grupo de capacidade, consulte Políticas de classificação por níveis de volume.
10. Em Estilo de segurança do volume, escolha Unix (Linux), NTFS ou Misto. O estilo de segurança de um volume determina se é dada preferência às ACLs NTFS ou UNIX para acesso multiprotocolo. O modo MISTO não é necessário para acesso multiprotocolo e só é recomendado para usuários avançados.
11. Em Política de snapshots, escolha uma política de snapshots para o volume. Para obter mais informações sobre políticas de snapshots, consulte Políticas de snapshots.

Se você escolher Política personalizada, especifique o nome da política no campo política personalizada. A política personalizada já deve existir na SVM ou no sistema de arquivos. Você pode criar uma política de snapshots personalizada com a CLI ou a API REST do ONTAP. Para obter mais informações, consulte Criar uma política de snapshot na documentação do produto NetApp ONTAP.

12. Em Período de resfriamento da política de divisão em níveis, os valores válidos são de 2 a 183 dias. O período de resfriamento da política de camadas de um volume define o número de dias antes que os dados que não foram acessados sejam marcados como frios e movidos para o armazenamento do grupo de capacidade. Essa configuração afeta somente as políticas `Auto` e `Snapshot-only`.
13. Selecione Atualizar para atualizar o volume.

Atualizar a configuração de um volume (CLI)

- Para atualizar a configuração de um volume FSx for ONTAP, use o comando da CLI update-volume (ou a operação de UpdateVolumeAPI equivalente), conforme mostrado no exemplo a seguir.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Excluir um volume

Você pode excluir um volume FSx for ONTAP usando o console Amazon FSx, o e a API Amazon FSx, além AWS CLI da interface de linha de NetApp comando (CLI) e da API REST do ONTAP.

> **Important**
>
> Você só pode excluir volumes usando o console do Amazon FSx, a API ou a CLI se o volume tiver os backups do Amazon FSx habilitados.

> **Important**
>
> Ao excluir um volume usando o console do Amazon FSx, você tem a opção de fazer um backup final do volume. Você pode criar volumes usando backups. Recomendamos que você faça um backup final como prática recomendada. Se achar que não precisa dele após um determinado período, poderá excluir esse e outros backups de volume criados manualmente. Ao excluir um volume usando o comando de CLI `delete-volume`, o Amazon FSx faz um backup final por padrão.

Antes de excluir um volume, certifique-se de que nenhuma aplicação esteja acessando os dados do volume que deseja excluir.

Excluir um volume (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Sistemas de arquivos e o sistema de arquivos do ONTAP do qual deseja excluir um volume.
3. Escolha a guia Volumes.
4. Escolha o volume que deseja excluir.
5. Em Ações, escolha Excluir volume.
6. Na caixa de diálogo de confirmação, em Criar backup final, há duas opções:
   - Escolha Sim para fazer um backup final do volume. O nome do backup final é exibido.
   - Escolha Não se não quiser um backup final do volume. Você deverá aceitar que, após a exclusão do volume, os backups automáticos não estarão mais disponíveis.
7. Confirme a exclusão do volume inserindo excluir no campo Confirmar exclusão.
8. Escolha Excluir volumes.

Excluir um volume (CLI)

- Para excluir um volume FSx for ONTAP, use o comando da CLI delete-volume (ou a operação de DeleteVolumeAPI equivalente), conforme mostrado no exemplo a seguir.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Visualizar um volume

Você pode ver os volumes FSx for ONTAP que estão atualmente em seu sistema de arquivos usando o console do Amazon FSx, o e a API e os SDKs AWS CLI do Amazon FSx.

Visualizar os volumes no sistema de arquivos:

- Como usar o console: escolha um sistema de arquivos para visualizar a página de detalhes dos Sistemas de arquivos. Escolha a guia Volumes para listar todos os volumes no sistema de arquivos e selecione o que deseja visualizar.
- Usando a CLI ou a API — Use o comando describe-volumes da CLI ou a operação da API. DescribeVolumes

Como criar um LUN de iSCSI

Esse processo descreve como criar um iSCSI LUN em um sistema de arquivos escalável Amazon FSx for NetApp ONTAP usando o comando ONTAP CLI. NetApp lun create Para obter mais informações, consulte o Centro lun createde Documentação do NetApp ONTAP.

> **Note**
>
> O protocolo iSCSI não é compatível com sistemas de arquivos escaláveis.

Esse processo pressupõe que você já tenha um volume criado em seu sistema de arquivos. Para ter mais informações, consulte Criação de volumes.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.
2. Crie um LUN usando o comando lun create NetApp CLI, substituindo os seguintes valores:

- ***svm_name***: o nome da máquina virtual de armazenamento (SVM) que fornece o destino iSCSI. O host usa esse valor para acessar o LUN.
- ***vol_name***: o nome do volume que hospeda o LUN.
- ***lun_name***: o nome que você quer atribuir ao LUN.
- ***size***: o tamanho, em bytes, do LUN. O tamanho máximo do LUN que você pode criar é 128 TB.

  > **Note**
  >
  > Recomendamos que você use um volume pelo menos 5% maior do que o tamanho do LUN. Essa margem deixa espaço para snapshots de volume.

- ***ostype***: o sistema operacional do host, `windows_2008` ou `linux`. Use `windows_2008` para todas as versões do Windows, garantindo assim que o LUN tenha um deslocamento de bloco adequado para o sistema operacional e otimize a performance.

> **Note**
>
> Recomendamos ativar a alocação de espaço no LUN. Com a alocação de espaço habilitada, o ONTAP pode informar o host quando o LUN está sem capacidade e reivindicar espaço à medida que você exclui dados do LUN.

Para obter mais informações, consulte a `lun create`documentação do NetApp ONTAP CLI.

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
ostype ostype -space-allocation enabled
```

```
Created a LUN of size 10g (10737418240)
```

3. Confirme se o LUN foi criado, está on-line e foi mapeado.

```
> lun show
```

O sistema responde com a seguinte saída:

```
Vserver   Path                            State   Mapped   Type         Size
--------- ------------------------------- ------- -------- ------------ --------
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

Próximas etapas

Agora que você criou um LUN de iSCSI, a próxima etapa no processo de usá-lo como armazenamento em blocos é mapear o LUN para um `igroup`. Para obter mais informações, consulte Montar LUNs de iSCSI em um cliente Linux ou Montar LUNs de iSCSI em um cliente Windows.

Como gerenciar compartilhamentos de SMB

Para gerenciar compartilhamentos de arquivos SMB em seu sistema de arquivos do Amazon FSx, você pode usar a GUI de pastas compartilhadas do Microsoft Windows. A GUI de pastas compartilhadas fornece um local central para gerenciar todas as pastas compartilhadas de sua máquina virtual de armazenamento (SVM). Os procedimentos a seguir detalham como criar, atualizar e remover compartilhamentos de arquivos.

> **Note**
>
> Você também pode gerenciar compartilhamentos de arquivos SMB usando o NetApp System Manager. Para ter mais informações, consulte Usando o NetApp System Manager com BlueXP.

Para conectar pastas compartilhadas ao sistema de arquivos do Amazon FSx

1. Inicie a instância do Amazon EC2 e conecte-a ao Microsoft Active Directory ao qual o sistema de arquivos do Amazon FSx está associado. Para fazer isso, escolha um dos seguintes procedimentos no Guia de administração do AWS Directory Service :

   - Associe continuamente uma instância do EC2 do Windows
   - Associar manualmente uma instância do Windows

2. Conecte-se a uma instância como usuário membro do grupo de administradores do sistema de arquivos. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
3. Abra o menu Iniciar e execute fsmgmt.msc usando Executar como administrador. Essa ação abre a ferramenta de pastas compartilhadas da GUI.
4. Em Ação, escolha Conectar a outro computador.
5. Em Outro computador, insira o nome DNS da sua máquina virtual de armazenamento (SVM), por exemplo, **`netbios_name.corp.example.com`**.

   Para encontrar o nome DNS da sua SVM no console do Amazon FSx, escolha Máquinas virtuais de armazenamento, escolha sua SVM e, em seguida, role para baixo até Endpoints até encontrar a opção Nome DNS do SMB. Você também pode obter o nome DNS na resposta da operação da DescribeStorageVirtualMachinesAPI.
6. Escolha OK. Uma entrada para seu sistema de arquivos do Amazon FSx então é exibida na lista da ferramenta Pastas compartilhadas.

Agora que as pastas compartilhadas estão conectadas ao seu sistema de arquivos do Amazon FSx, você pode gerenciar os compartilhamentos de arquivos do Windows no sistema de arquivos com as seguintes ações:

> **Note**
>
> Recomendamos que você localize seus compartilhamentos SMB em um volume diferente do volume raiz.

- Criar um novo compartilhamento de arquivos: na ferramenta Pastas compartilhadas, escolha Compartilhamentos no painel esquerdo para ver os compartilhamentos ativos do sistema de arquivos do Amazon FSx. Os volumes são mostrados montados no caminho escolhido durante a criação do volume. Escolha Novo compartilhamento e conclua o assistente de criação de uma pasta compartilhada.

  Você precisa criar a pasta local antes de criar o novo compartilhamento de arquivos. Você pode fazer isso da seguinte maneira:

  - Usando a ferramenta Pastas compartilhadas: escolha Procurar ao especificar um caminho de pasta local, escolha Criar nova pasta para criar a pasta local.

- Como usar a linha de comando:

```
New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
$volume_path\MyNewFolder
```

- Modificar um compartilhamento de arquivos: na ferramenta Pastas compartilhadas, abra o menu de contexto (clique com o botão direito do mouse) do compartilhamento de arquivos a ser modificado no painel direito e selecione Propriedades. Modifique as propriedades e escolha OK.
- Remover um compartilhamento de arquivos: na ferramenta Pastas compartilhadas, abra o menu de contexto (clique com o botão direito do mouse) do compartilhamento de arquivos a ser removido no painel direito e escolha Interromper o compartilhamento.

> **Note**
>
> A remoção de compartilhamentos de arquivos pela GUI só será possível se você estiver conectado ao fsmgmt.msc usando o nome DNS do sistema de arquivos do Amazon FSx. Se você se conectou usando o endereço IP ou o nome do alias DNS do sistema de arquivos, a opção Interromper o compartilhamento não funcionará e o compartilhamento de arquivos não será removido.

Auditoria de acesso a arquivos

O Amazon FSx para NetApp ONTAP oferece suporte à auditoria de acessos do usuário final a arquivos e diretórios em uma máquina virtual de armazenamento (SVM).

Tópicos

- Visão geral da auditoria de acesso a arquivos
- Visão geral das tarefas para configurar a auditoria de acesso a arquivos

Visão geral da auditoria de acesso a arquivos

A auditoria de acesso a arquivos permite que você registre os acessos do usuário final a arquivos e diretórios individuais com base nas políticas de auditoria que você define. A auditoria de acesso a arquivos ajuda a melhorar a segurança do sistema e reduzir o risco de acesso não autorizado aos dados do sistema. A auditoria de acesso a arquivos ajuda as organizações a permanecerem

em conformidade com os requisitos de proteção de dados, identificarem ameaças potenciais com antecedência e reduzirem o risco de uma violação de dados.

Em todos os acessos a arquivos e diretórios, o Amazon FSx oferece suporte ao registro em log das tentativas com êxito (como um usuário com permissões suficientes acessando com êxito um arquivo), tentativas malsucedidas ou ambas. Você também pode desativar a auditoria de acesso a arquivos a qualquer momento.

Por padrão, os logs de eventos de auditoria são armazenados no formato de arquivo EVTX, o que permite visualizá-los usando o Microsoft Event Viewer.

Eventos de acesso SMB que podem ser auditados

A tabela a seguir lista os eventos de acesso a arquivos e pastas SMB que podem ser auditados.

ID do evento (EVT/ EVTX)	Evento	Descrição	Categoria
560/4656	Abrir objeto/Criar objeto	ACESSO AO OBJETO: objeto (arquivo ou diretório) aberto	Acesso a arquivos
563/4659	Abrir objeto com a intenção de exclusão	ACESSO AO OBJETO: um identific ador para um objeto (arquivo ou diretório) foi solicitado com a intenção de exclusão	Acesso a arquivos
564/4660	Excluir objeto	ACESSO AO OBJETO: excluir objeto (arquivo ou diretório) O ONTAP gera esse evento quando um cliente Windows tenta excluir o objeto (arquivo ou diretório)	Acesso a arquivos

ID do evento (EVT/ EVTX)	Evento	Descrição	Categoria
567/4663	Ler objeto/Gravar objeto/Obter atributos do objeto/Definir atributos do objeto	ACESSO AO OBJETO: tentativa de acesso ao objeto (leitura, gravação, obtenção do atributo, definição do atributo). **Note** Para esse evento, o ONTAP audita somente a primeira operação de leitura e gravação SMB (êxito ou falha) em um objeto. Isso impede que o ONTAP crie entradas de logs excessivas quando um único cliente abre um objeto e executa várias operações sucessivas de leitura ou gravação	Acesso a arquivos

ID do evento (EVT/EVTX)	Evento	Descrição	Categoria
		no mesmo objeto.	
N/A/4664	Links físicos	ACESSO AO OBJETO: Foi feita uma tentativa de criar um link físico	Acesso a arquivos
ID 9999 do evento N/A/N/A do ONTAP	Renomear objeto	ACESSO AO OBJETO: objeto renomeado. Este é um evento do ONTAP. No momento, o Windows não oferece suporte como evento único.	Acesso a arquivos
ID 9998 do evento N/A/N/A do ONTAP	Desvincular objeto	ACESSO AO OBJETO: objeto desvinculado. Este é um evento do ONTAP. No momento, o Windows não oferece suporte como evento único.	Acesso a arquivos

Eventos de acesso ao NFS que podem ser auditados

Os eventos de acesso a arquivos e pastas NFS a seguir que podem ser auditados.

- READ
- OPEN
- CLOSE

- READDIR
- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

Visão geral das tarefas para configurar a auditoria de acesso a arquivos

A configuração do FSx para ONTAP para auditoria de acesso a arquivos envolve as seguintes tarefas de alto nível:

1. Familiarize-se com os requisitos e considerações sobre auditoria de acesso a arquivos.
2. Crie uma configuração de auditoria em uma SVM específica.
3. Ative a auditoria nessa SVM.
4. Configure políticas de auditoria em seus arquivos e diretórios.
5. Visualize os logs de eventos de auditoria após a emissão do FSx para ONTAP.

Os detalhes da tarefa são fornecidos nos procedimentos a seguir.

Repita as tarefas para qualquer outra SVM em seu sistema de arquivos para a qual você deseja habilitar a auditoria de acesso a arquivos.

Requisitos de auditoria

Antes de configurar e habilitar a auditoria em uma SVM, você deve estar ciente dos requisitos e considerações a seguir.

- A auditoria NFS oferece suporte a entradas de controle de acesso (ACEs) de auditoria designadas como tipo u, que geram uma entrada de log de auditoria quando há uma tentativa de acesso

ao objeto. Para auditoria NFS, não há mapeamento entre bits de modo e ACEs de auditoria. Ao converter ACLs em bits de modo, as ACEs de auditoria são ignoradas. Ao converter bits de modo em ACLs, as ACEs de auditoria não são geradas.

- A auditoria depende da disponibilidade de espaço nos volumes de preparação. (Um volume de preparação é um volume dedicado criado pelo ONTAP para armazenar arquivos de preparação, que são arquivos binários intermediários em nós individuais, nos quais os registros de auditoria são armazenados antes da conversão em um formato de arquivo EVTX ou XML.) Você deve garantir que haja espaço suficiente para os volumes de preparação nas agregações que contêm volumes auditados.
- A auditoria depende de ter espaço disponível no volume que contém o diretório no qual os logs de eventos de auditoria convertidos são armazenados. Certifique-se de que haja espaço suficiente nos volumes usados para armazenar logs de eventos. Você pode especificar o número de logs de auditoria a serem retidos no diretório de auditoria usando o parâmetro `-rotate-limit` ao criar uma configuração de auditoria, o que pode ajudar a garantir que haja espaço disponível suficiente para os logs de auditoria no volume.

Como criar configurações de auditoria nas SVMs

Antes de começar a auditar eventos de arquivos e diretórios, crie uma configuração de auditoria na máquina virtual de armazenamento (SVM). Depois de criar a configuração de auditoria, você deve habilitá-la na SVM.

Antes de usar o comando `vserver audit create` para criar a configuração de auditoria, certifique-se de ter criado um diretório para ser usado como destino dos logs e de que o diretório não tenha links simbólicos. Você especifica o diretório de destino com o parâmetro `-destination`.

Você pode criar uma configuração de auditoria que alterne os logs de auditoria com base no tamanho do log ou em uma programação, da seguinte maneira:

- Para alternar os logs de auditoria com base no tamanho do registro, use este comando:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

  O exemplo a seguir cria uma configuração de auditoria para a SVM chamada `svm1` que audita operações de arquivo e eventos de logon e logoff do CIFS (SMB) (o padrão) usando rotação

baseada em tamanho. O formato de log é EVTX (o padrão), os logs são armazenados no diretório `/audit_log` e você terá um único arquivo de log por vez (até 200 MB de tamanho).

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- Para alternar os logs de auditoria com base em uma programação, use este comando:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]
       [-rotate-limit integer] [-rotate-schedule-month chron_month]
       [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-
day chron_dayofmonth]
       [-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

O parâmetro `-rotate-schedule-minute` será obrigatório se você estiver configurando a rotação de logs de auditoria com base no tempo.

O exemplo a seguir cria uma configuração de auditoria para a SVM chamada `svm2` usando rotação baseada em tempo. O formato do log é EVTX (o padrão) e os logs de auditoria são alternados mensalmente, às 12h30, todos os dias da semana.

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB  -
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -
rotate-schedule-minute 30
```

Você pode usar o parâmetro `-format` para especificar se os logs de auditoria são criados no formato EVTX convertido (o padrão) ou no formato de arquivo XML. O formato EVTX permite que você visualize os arquivos de log com o Microsoft Event Viewer.

Por padrão, as categorias de eventos a serem auditados são eventos de acesso a arquivos (SMB e NFS), eventos de logon e logoff do CIFS (SMB) e eventos de alteração da política de autorização. Você pode ter maior controle sobre quais eventos registrar pelo parâmetro `-events`, que tem o seguinte formato:

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-
account|authorization-policy-change|security-group}
```

Por exemplo, o uso de `-events file-share` permite a auditoria dos eventos de compartilhamento de arquivos.

Para obter mais informações sobre o comando `vserver audit create`, consulte Criar uma configuração de auditoria.

Ativação da auditoria em uma SVM

Depois de concluir a definição da configuração de auditoria, você deve habilitá-la na SVM. Para fazer isso, use o seguinte comando:

```
vserver audit enable -vserver svm_name
```

Por exemplo, use o comando a seguir para habilitar a auditoria na SVM chamada `svm1`.

```
vserver audit enable -vserver svm1
```

Você pode desabilitar a auditoria de acesso a qualquer momento. Por exemplo, use o comando a seguir para desativar a auditoria na SVM chamada `svm4`.

```
vserver audit disable -vserver svm4
```

Quando você desabilita a auditoria, a configuração de auditoria não é excluída na SVM, o que significa que você pode reabilitar a auditoria nessa SVM a qualquer momento.

Como configurar as políticas de auditoria de arquivos e pastas

Você precisa configurar as políticas de auditoria nos arquivos e pastas em que deseja auditar tentativas de acesso do usuário. Você pode configurar políticas de auditoria para monitorar as tentativas de acesso com êxito e falha.

É possível configurar as políticas de auditoria SMB e NFS. As políticas de auditoria SMB e NFS têm requisitos de configuração e recursos de auditoria diferentes com base no estilo de segurança do volume.

Políticas de auditoria em arquivos e diretórios no estilo de segurança NTFS

Você pode configurar políticas de auditoria NTFS usando a guia Segurança do Windows ou a CLI do ONTAP.

Para configurar políticas de auditoria NTFS (guia Segurança do Windows)

Configure políticas de auditoria NTFS adicionando entradas às SACLs do NTFS associadas a um descritor de segurança NTFS. O descritor de segurança é então aplicado aos arquivos e diretórios

NTFS. Essas tarefas são gerenciadas automaticamente pela GUI do Windows. O descritor de segurança pode conter listas de controle de acesso (DACLs) discricionárias para aplicar permissões de acesso a arquivos e pastas, SACLs para auditoria de arquivos e pastas ou SACLs e DACLs.

1. No menu Ferramentas do Windows Explorer, selecione Mapear unidade de rede.
2. Preencha a caixa Mapear unidade de rede:

   a. Escolha uma letra de Unidade.

   b. Na caixa Pasta, digite o nome do servidor SMB (CIFS) que contém o compartilhamento, contendo os dados que você deseja auditar e o nome do compartilhamento.

   c. Escolha Finish.

   A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.
3. Selecione o arquivo ou diretório cujo acesso de auditoria você deseja habilitar.
4. Clique com o botão direito do mouse no arquivo ou diretório e escolha Propriedades.
5. Escolha a guia Segurança.
6. Clique em Avançado.
7. Escolha a guia Auditoria.
8. Execute as ações desejadas:

Se você deseja...	Faça o seguinte
Configurar a auditoria para um novo usuário ou grupo	1. Escolha Add (Adicionar). 2. Na caixa Digite o nome do objeto a ser selecionado, digite o nome do usuário ou grupo que você deseja adicionar. 3. Escolha OK.
Remover a auditoria de um usuário ou grupo	1. Na caixa Digite o nome do objeto a ser selecionado, selecione o usuário ou grupo que você deseja remover. 2. Escolha Remove. 3. Escolha OK. 4. Ignore o restante deste procedimento.

Se você deseja...	Faça o seguinte
Alterar a auditoria de um usuário ou grupo	1. Na caixa Digite o nome do objeto a ser selecionado, escolha o usuário ou grupo que você deseja alterar. 2. Escolha Editar. 3. Escolha OK.

Se você estiver configurando a auditoria em um usuário ou grupo ou alterando a auditoria em um usuário ou grupo existente, a caixa Entrada de auditoria para ***objeto*** será aberta.

9. Na caixa Aplicar a, selecione como você deseja aplicar essa entrada de auditoria.

   Se você estiver configurando a auditoria em um único arquivo, a caixa Aplicar a não estará ativa, pois o padrão é Somente este objeto.

10. Na caixa Acesso, selecione o que você deseja auditar e se deseja auditar eventos com êxito, eventos de falha ou ambos.

    - Para auditar eventos com êxito, escolha a caixa Sucesso.
    - Para auditar eventos de falha, escolha a caixa Falha.

    Escolha as ações que você precisa monitorar para atender aos seus requisitos de segurança. Para obter mais informações sobre esses eventos auditáveis, consulte a documentação do Windows. Você pode auditar os seguintes eventos:

    - Controle total
    - Percorrer pasta/executar arquivo
    - Listar pasta//ler dados
    - Ler atributos
    - Ler atributos estendidos
    - Criar arquivos/gravar dados
    - Criar pastas/anexar dados
    - Gravar atributos
    - Gravar atributos estendidos
    - Excluir subpastas e arquivos

- Excluir
- Permissões de leitura
- Alterar permissões.
- Assumir a propriedade

11. Se você não quiser que a configuração de auditoria se propague para arquivos e pastas subsequentes do contêiner original, escolha a caixa Aplicar estas entradas de auditoria somente a objetos e/ou contêineres dentro deste contêiner.
12. Escolha Apply (Aplicar).
13. Ao terminar de adicionar, remover ou editar entradas de auditoria, escolha OK.

    A caixa Entrada de auditoria para ***objeto*** é fechada.
14. Na caixa Auditoria, escolha as configurações de herança para essa pasta. Escolha somente o nível mínimo que forneça os eventos de auditoria que atendam aos seus requisitos de segurança.

    Você pode escolher uma das seguintes opções:

    - Escolha a caixa Incluir entradas de auditoria herdáveis na entrada principal deste objeto.
    - Escolha a caixa Substituir todas as entradas de auditoria herdáveis existentes em todos os descendentes por entradas de auditoria herdáveis deste objeto.
    - Escolha as duas caixas.
    - Escolha nenhuma das caixas.

    Se você estiver definindo SACLs em um único arquivo, a caixa Substituir todas as entradas de auditoria herdáveis existentes em todos os descendentes por entradas de auditoria herdáveis deste objeto não estará presente na caixa Auditoria.
15. Escolha OK.

Configurar políticas de auditoria do NTFS (CLI do ONTAP)

Usando a CLI do ONTAP, você pode configurar políticas de auditoria do NTFS sem precisar se conectar aos dados usando um compartilhamento SMB em um cliente Windows.

- Você pode configurar políticas de auditoria do NTFS usando a família de comandos vserver security file-directory.

Por exemplo, o comando a seguir aplica uma política de segurança chamada `p1` à SVM chamada `vs0`.

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

Políticas de auditoria em arquivos e diretórios no estilo de segurança do UNIX

Configure a auditoria de arquivos e diretórios no estilo de segurança do UNIX adicionando ACEs de auditoria (expressões de controle de acesso) às ACLs (listas de controle de acesso) do NFS v4.x. Isso permite monitorar determinados eventos de acesso a arquivos e diretórios NFS para fins de segurança.

> **Note**
>
> No NFS v4.x, as ACEs discricionárias e as do sistema são armazenadas na mesma ACL. Portanto, tenha cuidado ao adicionar ACEs de auditoria a uma ACL existente para evitar sobrescrever e perder uma ACL existente. A ordem na qual você adiciona as ACEs de auditoria a uma ACL existente não importa.

Configurar políticas de auditoria do UNIX

1. Recupere a ACL existente para o arquivo ou diretório usando o comando `nfs4_getfacl` ou um equivalente.
2. Anexe as ACEs de auditoria desejadas.
3. Aplique a ACL atualizada ao arquivo ou diretório usando o comando `nfs4_setfacl` ou um equivalente.

   Este exemplo usa a opção `-a` para dar a um usuário (chamado `testuser`) permissões de leitura para o arquivo chamado `file1`.

   ```
   nfs4_setfacl -a "A::testuser@example.com:R" file1
   ```

Visualização de logs de evento de auditoria

Você pode visualizar os logs de evento de auditoria salvos nos formatos de arquivo `EVTX` ou `XML`.

- Formato de arquivo EVTX: você pode abrir os logs de evento de auditoria EVTX convertidos como arquivos salvos usando o Microsoft Event Viewer.

  Há duas opções que você pode usar ao visualizar logs de eventos usando o visualizador de eventos:

  - Visualização geral: as informações comuns a todos os eventos são exibidas no registro do evento. Os dados específicos do evento para o registro do evento não são exibidos. Você pode usar a visualização detalhada para exibir dados específicos do evento.
  - Visualização detalhada: uma visualização amigável e uma visualização em XML estão disponíveis. As visualizações amigável e em XML exibem as informações que são comuns a todos os eventos e os dados específicos do evento para o registro de eventos.
- Formato de arquivo XML: você pode visualizar e processar logs de evento de auditoria XML em aplicações de terceiros que aceitam o formato de arquivo XML. As ferramentas de visualização em XML podem ser usadas para visualizar os logs de auditoria, desde que você tenha o esquema XML e informações sobre as definições dos campos XML.

Escala da capacidade de armazenamento SSD e IOPS provisionadas

Quando precisar de armazenamento adicional para a parte ativa do seu conjunto de dados, você pode aumentar a capacidade de armazenamento da unidade de estado sólido (SSD) do seu sistema de arquivos Amazon FSx NetApp for ONTAP. Para fazer isso, use o console e a API do Amazon FSx ou a AWS Command Line Interface (AWS CLI).

Você também pode alterar as IOPS de SSD provisionadas para seu sistema de arquivos, seja quando aumentar a capacidade de armazenamento SSD principal ou como ação independente. Para obter mais informações sobre como escalar a capacidade de armazenamento SSD principal de um sistema de arquivos e a quantidade de IOPS provisionadas, consulte Atualizando o armazenamento SSD e o IOPS do sistema de arquivos.

Como gerenciar a capacidade de throughput

O FSx para ONTAP configura a capacidade de throughput quando você cria o sistema de arquivos. Você pode modificar a capacidade de taxa de transferência do seu sistema de arquivos de expansão a qualquer momento, mas não pode modificar a capacidade de taxa de transferência do seu sistema de arquivos expansível. Lembre-se de que seu sistema de arquivos requer uma configuração

específica para atingir a quantidade máxima de capacidade de throughput. Por exemplo, para provisionar 4 GBps de capacidade de taxa de transferência para um sistema de arquivos escalável, seu sistema de arquivos requer uma configuração com um mínimo de 5.120 GiB de capacidade de armazenamento SSD e 160.000 SSD IOPS. Para obter mais informações, consulte Impacto da capacidade de throughput na performance.

A capacidade de throughput é um fator que determina a velocidade com que o servidor de arquivos que hospeda o sistema de arquivos pode fornecer os dados de arquivos. Níveis mais altos de capacidade de throughput vêm com níveis mais altos de rede, operações de E/S de leitura de disco por segundo (IOPS) e capacidade de armazenamento de dados em cache no servidor de arquivos. Para obter mais informações, consulte Performance.

Ao modificar a capacidade de throughput do sistema de arquivos, o Amazon FSx desativa o servidor de arquivos que está alimentando seu sistema de arquivos. Os sistemas de arquivos single-AZ e multi-AZ passam por um failover e um failback automáticos durante esse processo, que normalmente leva alguns minutos para ser concluído. Os processos de failover e failback são transparentes para os clientes NFS (Network File Sharing), SMB (Server Message Block) e iSCSI (Internet Small Computer Systems Interface), permitindo que suas workloads continuem em execução sem interrupção ou intervenção manual. Você receberá uma cobrança pela nova quantidade de capacidade de throughput quando ela estiver disponível para o seu sistema de arquivos.

> **Note**
>
> Para garantir a integridade dos dados durante a atividade de manutenção, o FSx para ONTAP fecha todos os bloqueios oportunistas e conclui todas as operações de gravação pendentes nos volumes de armazenamento subjacentes que estão hospedando seu sistema de arquivos antes do início da manutenção. Durante uma janela de manutenção programada do sistema de arquivos, as modificações do sistema (como as modificações na capacidade de throughput) podem atrasar. A manutenção do sistema pode fazer com que essas alterações fiquem na fila até que sejam processadas. Para obter mais informações, consulte the section called “Janelas de manutenção”.

Tópicos

- Quando modificar a capacidade de throughput
- Como as solicitações simultâneas de throughput e escalabilidade de armazenamento são tratadas
- Como modificar a capacidade de throughput

- Como monitorar as alterações na capacidade de throughput

Quando modificar a capacidade de throughput

O Amazon FSx se integra à Amazon CloudWatch, o que ajuda você a monitorar os níveis contínuos de uso da taxa de transferência do seu sistema de arquivos. A performance do throughput e das IOPS que você pode direcionar por meio do sistema de arquivos dependem das características específicas da workload, além da capacidade de throughput do sistema de arquivos. Como regra, você deve provisionar capacidade de throughput suficiente para suportar o throughput de leitura da sua workload mais o dobro do throughput de gravação da workload. Você pode usar CloudWatch métricas para determinar quais dessas dimensões devem ser alteradas para melhorar o desempenho. Para obter mais informações, consulte the section called “Como usar o FSx para métricas ONTAP CloudWatch”.

> **Note**
>
> Você não pode modificar a capacidade de taxa de transferência para sistemas de arquivos escaláveis.

Como as solicitações simultâneas de throughput e escalabilidade de armazenamento são tratadas

Você pode solicitar uma atualização da capacidade de throughput pouco antes do início do fluxo de trabalho de atualização da capacidade de armazenamento SSD e das IOPS provisionadas ou enquanto ele estiver em andamento. A sequência de como o Amazon FSx trata as duas solicitações é a seguinte:

- Se você enviar uma atualização de SSD e IOPS e uma atualização de capacidade de throughput ao mesmo tempo, ambas as solicitações serão aceitas. A atualização de SSD e IOPS tem prioridade em relação à atualização da capacidade de throughput.
- Se você enviar uma atualização da capacidade de throughput enquanto uma atualização de SSD e IOPS estiver em andamento, a solicitação de atualização da capacidade de throughput será aceita e colocada na fila para ocorrer após a atualização de SSD e IOPS. A atualização da capacidade de throughput começa após a atualização de SSD e IOPS (novos valores estão disponíveis) e durante a etapa de otimização. Normalmente, isso demora menos de dez minutos.

- Se você enviar uma atualização de SSD e IOPS enquanto uma atualização da capacidade de throughput estiver em andamento, a solicitação de atualização do armazenamento SSD e IOPS será aceita e colocada na fila para ser iniciada após a conclusão da atualização da capacidade de throughput (nova capacidade de throughput está disponível). Normalmente, isso demora 20 minutos.

Para obter mais informações sobre atualizações de armazenamento SSD e de IOPS provisionadas, consulte Como gerenciar a capacidade de armazenamento.

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 ONTAP para o qual você deseja aumentar a capacidade de throughput.
3. Em Ações, escolha Atualizar capacidade de throughput. Como alternativa, no painel Resumo, escolha Atualizar ao lado da Capacidade de throughput do sistema de arquivos.
4. Escolha o novo valor para Capacidade de throughput na lista.

   > **Note**
   >
   > Você pode alterar a capacidade de throughput de qualquer sistema de arquivos do FSx para ONTAP. No entanto, somente sistemas de arquivos criados a partir de 9 de dezembro de 2021 são compatíveis com uma capacidade de throughput de 128 MB/s ou 256 MB/s.

5. Escolha Atualizar para iniciar a atualização da capacidade de throughput.
6. Você pode monitorar o progresso da atualização na página de detalhes dos Sistemas de arquivos, na guia Atualizações.

   Você pode monitorar o progresso da atualização usando o console do Amazon FSx, a AWS CLI e a API. Para obter mais informações, consulte Como monitorar as alterações na capacidade de throughput.

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 AWS CLI comando update-file-system. Defina os seguintes parâmetros:

- `--file-system-id` para o ID do sistema de arquivos que você está atualizando.
- `ThroughputCapacity` para o valor desejado para o qual atualizar o sistema de arquivos.

Você pode monitorar o progresso da atualização usando o console do Amazon FSx, a AWS CLI e a API. Para obter mais informações, consulte Como monitorar as alterações na capacidade de throughput.

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.

Como monitorar as alterações na capacidade de throughput no console

Na guia Atualizações, na janela Detalhes do sistema de arquivos, você pode 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

Os tipos compatíveis são Capacidade de throughput, Capacidade de armazenamento e Otimização de armazenamento.

Target value (Valor de destino)

O valor desejado para o qual alterar a capacidade de throughput do sistema de arquivos.

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.
- 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.

Como monitorar as alterações com a AWS CLI e a API

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 uma capacidade de throughput de 128 MB/s e uma capacidade de throughput de destino de 256 MB/s.

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

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 `ThroughputCapacity`. Isso é mostrado no trecho de resposta a seguir de um comando describe-file-systems da CLI.

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Se a modificação da capacidade de throughput apresentar falhas, o status será alterado para `FAILED` e a propriedade `FailureDetails` fornecerá informações sobre a falha.

Otimizar a performance com janelas de manutenção do Amazon FSx

Como um serviço totalmente gerenciado, o FSx para ONTAP realiza regularmente manutenções e atualizações no sistema de arquivos. Essa manutenção não afeta a maioria das workloads. Em workloads que são sensíveis à performance, em raras ocasiões, você poderá notar um breve impacto (menos de 60 segundos) na performance quando a manutenção estiver ocorrendo; o Amazon FSx permite usar a janela de manutenção para controlar a ocorrência de qualquer atividade potencial de manutenção.

A aplicação de patches ocorre com pouca frequência, normalmente uma vez a cada várias semanas. Para sistemas de arquivos em expansão, a aplicação de patches normalmente requer apenas 30 minutos a partir do início da janela de manutenção. Para sistemas de arquivos escaláveis, a aplicação de patches requer até 90 minutos a partir do início da janela de manutenção. Durante esses poucos minutos, seus sistemas de arquivos fazem o failover e o failback automaticamente.

Você escolhe a janela de manutenção durante a criação do sistema de arquivos. Se você não tiver preferência de horário, será atribuído um horário de início de 30 minutos.

O FSx para ONTAP permite ajustar sua janela de manutenção conforme necessário para acomodar sua workload e seus requisitos operacionais. Você pode mover sua janela de manutenção com a frequência necessária, desde que uma janela de manutenção ocorra pelo menos uma vez a cada 14 dias. Se um patch for lançado e uma janela de manutenção não ocorrer dentro de 14 dias, o FSx for ONTAP prosseguirá com a manutenção no sistema de arquivos para garantir sua segurança e confiabilidade.

> **Note**
>
> Para garantir a integridade dos dados durante a atividade de manutenção, o FSx para ONTAP fecha todos os bloqueios oportunistas e conclui todas as operações de gravação pendentes nos volumes de armazenamento subjacentes que estão hospedando seu sistema de arquivos antes do início da manutenção.

Você pode usar o Amazon FSx Management Console AWS CLI, a AWS API ou um dos AWS SDKs para alterar a janela de manutenção dos seus sistemas de arquivos.

Alterar a janela de manutenção semanal (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha Sistemas de arquivos na coluna de navegação à esquerda.
3. Escolha o sistema de arquivos do qual deseja alterar a janela de manutenção semanal. A página de detalhes Resumo do sistema de arquivos é exibida.
4. Escolha Administração para exibir o painel Configurações de administração do sistema de arquivos.
5. Escolha Atualizar para exibir a janela Alterar janela de manutenção.
6. Insira o novo dia e horário que você deseja para o início da janela de manutenção semanal.
7. Escolha Salvar para salvar as alterações. O novo horário de início da manutenção é exibido no painel Configurações de administração do sistema de arquivos.

Para alterar a janela de manutenção semanal usando o comando update-file-systemCLI, consulte. Atualizar um sistema de arquivos (CLI)

Marcar os recursos do Amazon FSx

Para ajudar você a gerenciar seus sistemas de arquivos e outros recursos do Amazon FSx, é possível atribuir seus próprios metadados a cada recurso na forma de tags. Com as tags, é possível categorizar seus recursos da AWS de diferentes formas, por exemplo, por finalidade, proprietário ou ambiente. Essa categorização é útil quando você tem muitos recursos do mesmo tipo. É possível identificar rapidamente um recurso específico com base nas tags atribuídas a ele. Este tópico descreve as etiquetas e mostra como criá-las.

Tópicos

Conceitos básicos de tags

Uma tag é um rótulo atribuído a um recurso da AWS. Cada tag consiste em duas partes que você define:

- Uma chave de tag (por exemplo `CostCenter`, `Environment` ou `Project`). Chaves de tag fazem distinção entre maiúsculas e minúsculas.
- Umvalor de tag (por exemplo, `111122223333` ou `Production`). Como chaves de tag, os valores das tags diferenciam maiúsculas de minúsculas. Os valores das tags são opcionais.

Você pode usar as tags para categorizar os recursos da AWS de diferentes formas, como por finalidade, proprietário ou ambiente. Por exemplo, é possível definir um conjunto de tags para os sistemas de arquivos do Amazon FSx da sua conta que ajuda a rastrear o proprietário e o nível da 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. Para obter mais informações sobre como implementar uma estratégia eficaz de marcação de recursos com tags, consulte Tagging AWS resources na Referência geral da AWS.

Alguns comportamentos de marcação com tags a serem considerados:

- 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 recursos.
- É possível editar chaves de tags e valores, e é possível remover as tags de um recurso a qualquer momento.
- Você pode definir o valor de uma tag para uma string vazia, mas esse valor não pode ser definido como `null`.
- 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 você estiver usando a API do Amazon FSx, a AWS Command Line Interface (AWS CLI) ou um AWS SDK, faça o seguinte:
  - Você pode usar a ação de API `TagResource` para aplicar tags a recursos existentes.
  - Para algumas ações de criação de recursos, será possível especificar tags para um recurso quando ele for criado. 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.

    Se as tags não puderem ser aplicadas durante a criação dos recursos, o Amazon FSx reverterá o processo de criação de recursos. Esse comportamento ajuda a garantir que os recursos sejam criados com tags ou, então, não sejam criados, e que nenhum recurso seja deixado sem tags em nenhum momento.

    > **Note**
    >
    > Determinadas permissões do AWS Identity and Access Management (IAM) são necessárias para que os usuários marquem recursos com tags na criação. Para obter mais informações, consulte Conceder permissão para marcar recursos durante a criação.

Marcar recursos da

É possível usar tags nos recursos do Amazon FSx que existem na 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. No entanto, embora o console organize os recursos de acordo com a chave Nome, ela não tem nenhum significado semântico para o serviço do Amazon FSx.

É possível aplicar permissões no nível do recurso com base em tags nas suas políticas do IAM para as ações de API do Amazon FSx que são compatíveis com a marcação durante a criação, a fim de implementar controle granular sobre os usuários e grupos que podem marcar recursos na criação. Ao usar essas permissões nas suas políticas, você obtém os seguintes benefícios:

- Seus recursos ficam devidamente protegidos desde a criação.
- Como as tags são aplicadas instantaneamente aos seus recursos, 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.

Você pode aplicar permissões no nível de recurso às ações `TagResource` e `UntagResource` da API do Amazon FSx nas suas políticas do IAM, de forma a controlar quais chaves e valores de tags são definidos nos recursos existentes.

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 como usar tags para restringir o acesso a recursos do Amazon FSx nas políticas do IAM, consulte Como usar tags para controlar o acesso aos seus recursos do Amazon FSx.

Para obter informações sobre a aplicação de tags nos seus recursos para fins de faturamento, consulte Usar tags de alocação de custos no Guia do usuário do AWS Billing.

Copiar tags para backups

Ao criar ou atualizar um volume na API do Amazon FSx ou na AWS CLI, você pode habilitar `CopyTagsToBackups` para copiar automaticamente qualquer tag dos seus volumes para backups.

> **Note**
>
> Se você especificar tags ao criar um backup iniciado pelo usuário (incluindo a tag de nome ao criar um backup usando o console do Amazon FSx), as tags não serão copiadas do volume, mesmo que tenha habilitado `CopyTagsToBackups`.

Para obter mais informações sobre backups, consulte Trabalhar com backups. Para obter mais informações sobre como habilitar `CopyTagsToBackups`, consulte Para criar um volume (CLI) e Atualizar a configuração de um volume (CLI) no Guia do usuário do Amazon FSx para NetApp ONTAP ou CreateVolume e UpdateVolume na referência de APIs do Amazon FSx para NetApp ONTAP..

Restrições de tags

As restrições básicas a seguir se aplicam às tags.

- O número máximo de tags por recurso é 50.
- O comprimento máximo da chave da é de 128 caracteres Unicode em UTF-8.
- O comprimento máximo do valor da é de 256 caracteres Unicode em UTF-8.
- Os caracteres permitidos são letras, números e espaços representáveis em UTF-8, além dos seguintes caracteres: `+ - =` (hífen) `. _` (sublinhado) `: / @`.
- Em todos os recursos, cada chave de tag deve ser exclusiva e pode ter apenas um valor.
- 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 se ela tiver 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 marcados

com uma chave de tag denominada `DeleteMe`, use a ação `DeleteFileSystem` com o identificador de recursos do sistema de arquivos, como `fs-1234567890abcdef0`.

Quando você marca recursos públicos ou compartilhados, as tags atribuídas ficam 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 marcação de tags

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 como usar tags para restringir o acesso a recursos do Amazon FSx nas políticas do IAM, consulte Como usar tags para controlar o acesso aos seus recursos do Amazon FSx.

Gerenciando recursos do FSx for ONTAP usando aplicativos NetApp

Além da AWS API e dos SDKs AWS Management Console AWS CLI, você também pode usar essas ferramentas e aplicativos NetApp de gerenciamento para gerenciar seus recursos do FSx for ONTAP:

Tópicos

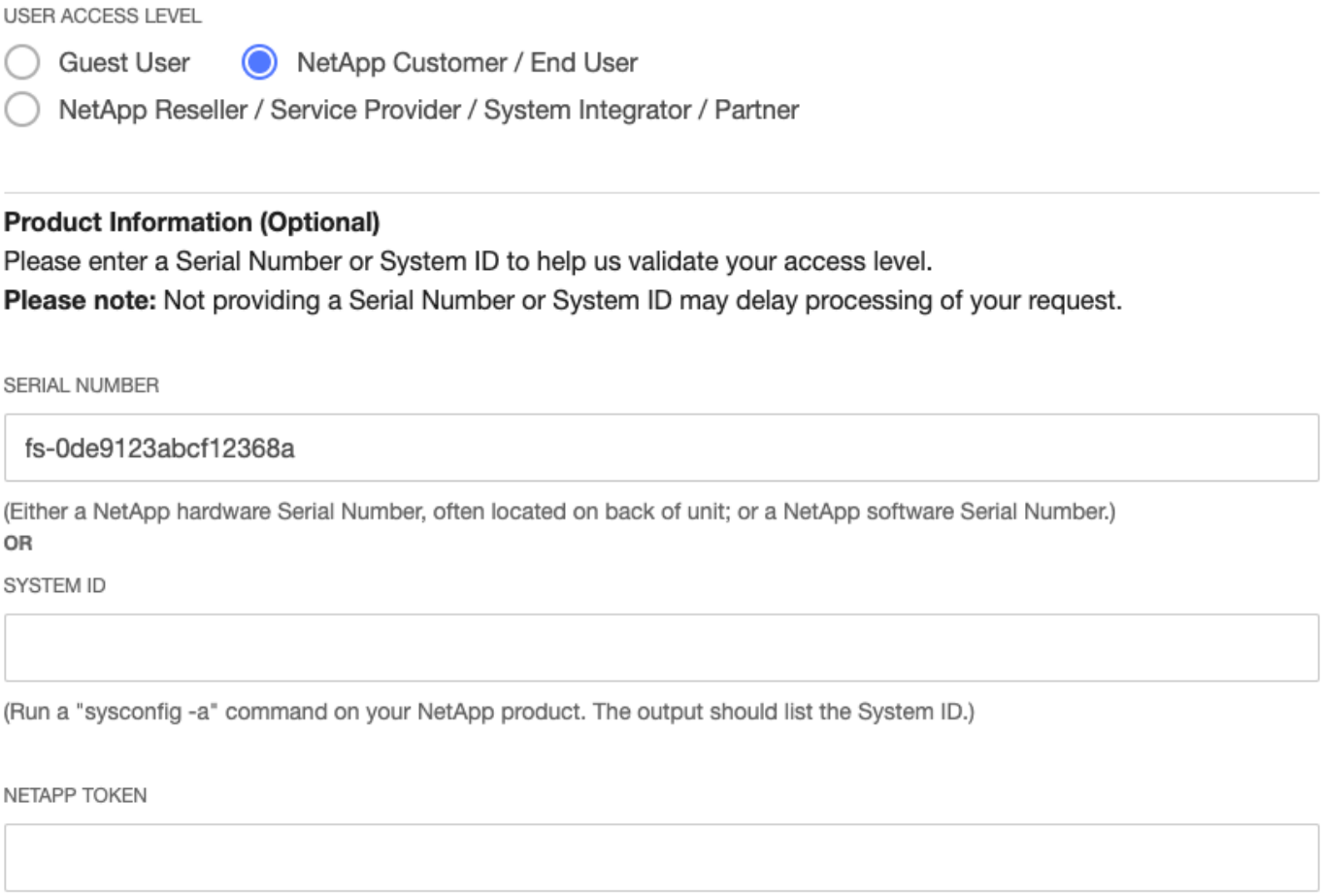
- Inscrevendo-se em uma NetApp conta
- Usar o NetApp BlueXP
- Usar a CLI do NetApp ONTAP
- Como usar a API REST do ONTAP

> **Important**
>
> O Amazon FSx sincroniza periodicamente com o Amazon FSx para garantir ONTAP a consistência. Se você criar ou modificar volumes usando NetApp aplicativos, pode levar alguns minutos para que essas alterações sejam refletidas na API AWS Management Console, AWS CLI, e nos SDKs.

Inscrevendo-se em uma NetApp conta

Para baixar alguns NetApp softwares, como, BlueXPSnapCenter, e o conector do ONTAP Antivirus, você precisa ter uma NetApp conta. Para se inscrever em uma NetApp conta, execute as seguintes etapas:

1. Acesse a página de Registro de NetApp Usuário e cadastre-se para uma nova conta de NetApp usuário.
2. Preencha os formulários com suas informações. Certifique-se de selecionar o nível de acesso do NetAppcliente/usuário final. No campo SERIAL NUMBER, copie e cole o ID do sistema de arquivos do FSx para ONTAP. Veja o exemplo a seguir:



O que esperar após o cadastro

Clientes com NetApp produtos existentes terão sua conta NSS nivelada até o nível de acesso ao nível de cliente em um dia útil. Os novos clientes NetApp serão integrados usando práticas

comerciais padrão, além de terem suas contas do NSS niveladas até o nível de acesso ao nível do cliente. Fornecer a ID do sistema de arquivos ajuda a acelerar esse processo. Você pode verificar o status da sua conta NSS fazendo login em mysupport.netapp.com e navegando até a página Welcome. O nível de acesso da sua conta deve ser Customer Access.

Usar o NetApp BlueXP

NetApp O BlueXP é um plano de controle unificado que simplifica as experiências de gerenciamento de serviços de armazenamento e dados em ambientes locais e na nuvem. O BlueXP fornece uma interface de usuário centralizada para gerenciar, monitorar e automatizar as implantações do ONTAP no local e no local. AWS Para obter mais informações, consulte a documentação do NetApp BlueXP e a documentação do NetApp BlueXP for Amazon FSx for ONTAP. NetApp

> **Note**
>
> NetApp BlueXPnão é compatível com sistemas de arquivos escaláveis.

Usando o NetApp System Manager com BlueXP

Você pode gerenciar seus sistemas de arquivos Amazon FSx for NetApp ONTAP usando o System Manager diretamente do. BlueXP BlueXPpermite que você use a mesma interface do System Manager que você está acostumado a usar, para que você possa gerenciar sua infraestrutura híbrida de várias nuvens a partir de um único plano de controle. Você também tem acesso às outras funcionalidades do BlueXP. Para obter mais informações, consulte o tópico Integração do System Manager com o BlueXP na documentação do NetApp ONTAP.

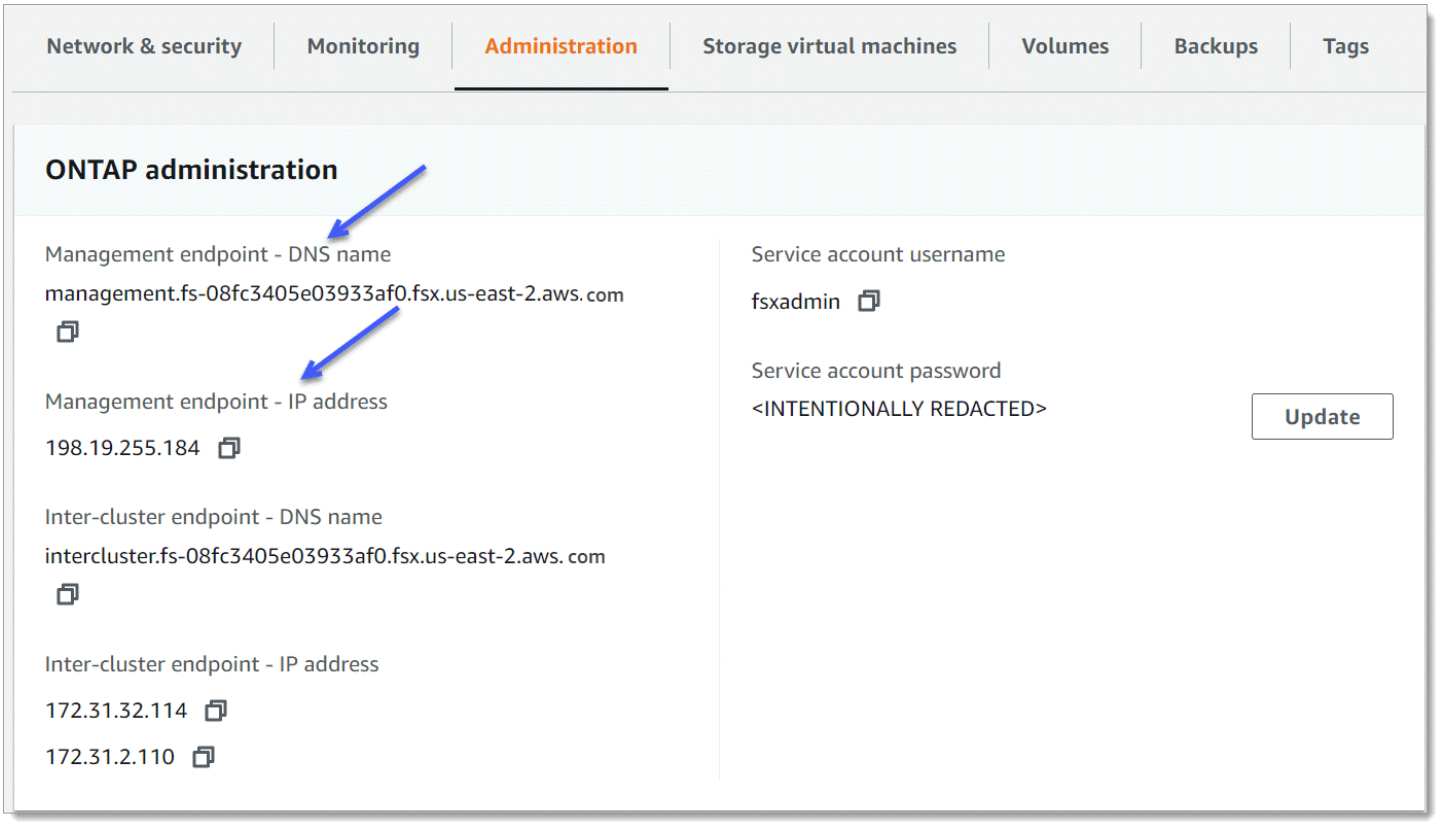
> **Note**
>
> NetApp O System Manager não é compatível com sistemas de arquivos escaláveis.

Usar a CLI do NetApp ONTAP

Você pode gerenciar seus recursos do Amazon FSx for NetApp ONTAP usando a CLI. NetApp ONTAP Você pode gerenciar recursos no nível do sistema de arquivos (análogo ao cluster NetApp ONTAP) e no nível do SVM.

Gerenciando sistemas de arquivos com a ONTAP CLI

Você pode executar comandos ONTAP CLI em seu sistema de arquivos FSx for ONTAP, da mesma forma que executá-los em um cluster. NetApp ONTAP Você acessa a ONTAP CLI em seu sistema de arquivos estabelecendo uma conexão shell segura (SSH) com o endpoint de gerenciamento do sistema de arquivos, fazendo login com o nome de usuário e a `fsxadmin` senha. Você tem a opção de definir a senha ao criar o sistema de arquivos usando o fluxo de criação personalizado ou usando AWS CLI o. Se você criou o sistema de arquivos usando a opção Criação rápida, a `fsxadmin` senha não foi definida, então você precisará definir uma para fazer login na CLI do ONTAP. Para ter mais informações, consulte Atualização de um sistema de arquivos. Você pode encontrar o nome DNS e o endereço IP do endpoint de gerenciamento do seu sistema de arquivos no console do Amazon FSx, na guia Administração da página de detalhes do sistema de arquivos FSx for ONTAP, mostrada no gráfico a seguir.



Para se conectar ao endpoint de gerenciamento do sistema de arquivos com SSH, use o `fsxadmin` usuário e a senha. Você pode acessar por SSH o endereço IP ou o nome DNS do endpoint de gerenciamento do sistema de arquivos a partir de um cliente que esteja na mesma VPC do sistema de arquivos, como nos exemplos a seguir.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

O comando de SSH com valores de exemplo:

```
ssh fsxadmin@198.51.100.0
```

O comando SSH usando o nome DNS do endpoint de gerenciamento:

```
ssh fsxadmin@file-system-management-endpoint-dns-name
```

O comando de SSH usando um nome de DNS de exemplo:

```
$ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Escopo dos comandos ONTAP CLI disponíveis para **`fsxadmin`**

A visão administrativa `fsxadmin` do sistema de arquivos está no nível do sistema de arquivos, que inclui todas as SVMs e volumes do sistema de arquivos. A `fsxadmin` função executa a função do administrador do ONTAP cluster. Como os sistemas de arquivos Amazon FSx for NetApp ONTAP são totalmente gerenciados, a `fsxadmin` função pode executar um subconjunto dos comandos da CLI disponíveis. ONTAP

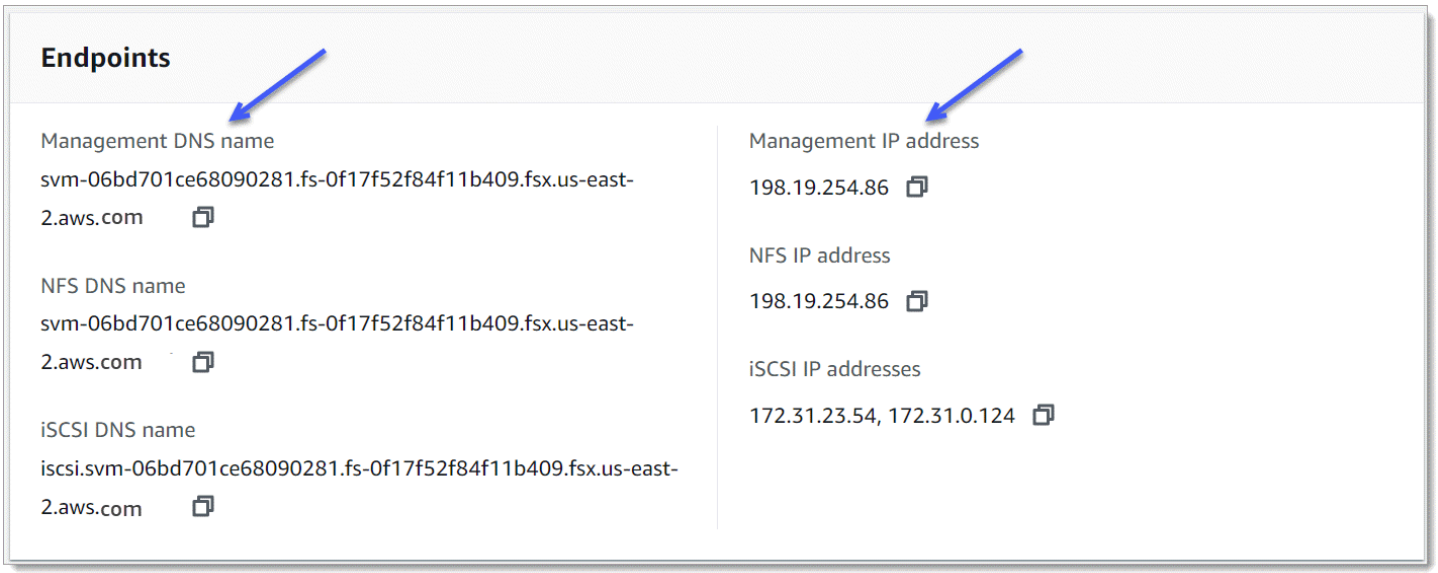
Para ver uma lista dos comandos que `fsxadmin` podem ser executados, use o seguinte comando da `security login role show`ONTAPCLI:

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
           Role          Command/                                  Access
Vserver    Name          Directory                        Query Level
---------- ------------- --------- ---------------------------------- --------
FsxId0abcdef123456789
           fsxadmin      application                                 all
                         cluster application-record                  all
                         cluster date show                           readonly
                         cluster ha modify                           readonly
                         cluster ha show                             readonly
                         cluster identity modify                     readonly
```

```
                        cluster identity show                              readonly
                        cluster log-forwarding           -port !55555 all
                        cluster modify                                     readonly
                        cluster peer                                       all
                        cluster show                                       readonly
                        cluster statistics show                            readonly
                        cluster time-service ntp server create             readonly
                        cluster time-service ntp server delete             readonly
                        cluster time-service ntp server modify             readonly
                        cluster time-service ntp server show               readonly
                        debug network tcpdump       -ipspace !Cluster      all
                        debug san lun                                      all
                        df         -vserver !FsxId* -vserver !Cluster      readonly
                        echo                                               all
                        event catalog show                                 readonly
                        event config                                       all
.
.
.
363 entries were displayed.
```

Gerenciando SVMs com a CLI ONTAP

Você pode acessar a ONTAP CLI em sua SVM estabelecendo uma conexão de shell segura (SSH) com o endpoint de gerenciamento da SVM usando o nome de usuário e a senha`fsxadmin`. `vsadmin` Você pode encontrar o nome DNS e o endereço IP do endpoint de gerenciamento do SVM no console do Amazon FSx, no painel Endpoints da página de detalhes das máquinas virtuais de armazenamento, mostrada no gráfico a seguir.



Para se conectar ao endpoint de gerenciamento do SVM com SSH, você pode usar o nome de usuário e a `fsxadmin` senha `vsadmin` ou. Se você não definiu uma senha para o `vsadmin` usuário quando o SVM foi criado, você pode definir a `vsadmin` senha a qualquer momento. Para ter mais informações, consulte Atualizar uma máquina virtual de armazenamento. Você pode efetuar SSH na SVM por meio de um cliente que esteja na mesma VPC do sistema de arquivos, usando o endereço IP ou o nome DNS do endpoint de gerenciamento.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

O comando com exemplo de valores:

```
ssh vsadmin@198.51.100.10
```

O comando SSH usando o nome DNS do endpoint de gerenciamento:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

O comando de SSH usando um nome de DNS de exemplo:

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

O Amazon FSx for NetApp ONTAP oferece suporte aos comandos da CLINetApp ONTAP.

Para obter uma referência completa dos comandos da NetApp ONTAP CLI, consulte Comandos ONTAP: Referência da página de manual.

Como usar a API REST do ONTAP

Ao acessar seu sistema de arquivos FSx for ONTAP usando a API ONTAP REST usando `fsxadmin` as credenciais, faça o seguinte:

- Desabilite a validação TLS.

  Ou

- Confie nas autoridades de AWS certificação (CAs) — O pacote de certificados para as CAs em cada região pode ser encontrado nos seguintes URLs:
  - https://fsx-aws-certificates.s3.amazonaws.com/bundle - *`aws-region .pem`* para o público Regiões da AWS
  - https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle - *`aws-region .pem`* para regiões AWS GovCloud
  - https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle - *`aws-region .pem`* para regiões da China AWS

Para obter uma referência completa dos comandos da API NetApp ONTAP REST, consulte a Referência on-line da API NetApp ONTAP REST.

Segurança no Amazon FSx for ONTAP NetApp

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 isso como a segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon FSx for NetApp ONTAP, consulte AWS Services in Scope by Compliance Program Scope by Compliance Program.
- 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. 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 AWS serviços que ajudam a monitorar e proteger seus recursos do Amazon FSx.

Tópicos

- Funções e usuários no Amazon FSx for ONTAP NetApp

Proteção de dados no Amazon FSx for ONTAP NetApp

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no Amazon FSx for NetApp ONTAP. 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 AWS postagem do blog Shared Responsibility Model and GDPR no AWS Blog de segurança da.

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 email dos seus clientes, em marcações ou campos de formato livre, como um campo Name (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, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia de dados no FSx para ONTAP

O Amazon FSx for NetApp ONTAP suporta criptografia de dados em repouso e criptografia de dados em trânsito. A criptografia de dados em repouso é habilitada automaticamente ao criar um sistema de arquivos do Amazon FSx. O Amazon FSx for NetApp ONTAP oferece suporte à criptografia baseada em Kerberos em trânsito pelos protocolos NFS e SMB se você estiver acessando dados em uma máquina virtual de armazenamento (SVM) associada a um Active Directory ou a um domínio usando o Lightweight Directory Access Protocol (LDAP).

Quando usar a criptografia

Se sua organização estiver sujeita a políticas corporativas ou regulatórias que exigem criptografia de dados e metadados em repouso, seus dados serão automaticamente criptografados em repouso. É recomendável também que você habilite a criptografia de dados em trânsito montando seu sistema de arquivos com o uso da criptografia de dados em trânsito.

Para obter mais informações sobre criptografia de dados com o Amazon FSx for NetApp ONTAP, consulte e. Criptografia de dados em repouso Criptografia de dados em trânsito

Criptografia de dados em repouso

Todos os sistemas de arquivos Amazon FSx for NetApp ONTAP são criptografados em repouso com chaves gerenciadas usando AWS Key Management Service ().AWS KMS Os dados são criptografados automaticamente antes de serem gravados no sistema de arquivos e automaticamente decriptografados à medida que são lidos. Esses processos são tratados de maneira transparente pelo Amazon FSx. Portanto, não é necessário modificar as aplicações.

O Amazon FSx usa um algoritmo de criptografia AES-256 padrão do setor para criptografar dados e metadados em repouso do Amazon FSx. Para obter mais informações, consulte Cryptography Basics no Guia do desenvolvedor do AWS Key Management Service .

> **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).

Como o Amazon FSx usa AWS KMS

O Amazon FSx se integra ao gerenciamento de chaves AWS KMS . O Amazon FSx usa chaves do KMS para criptografar o sistema de arquivos. Você escolhe a chave KMS usada para criptografar e decriptografar sistemas de arquivos (dados e metadados). 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 KMS gerenciada pela AWS: essa é a chave KMS padrão e de uso gratuito.
- chave KMS gerenciada pelo cliente: essa é a chave KMS mais flexível em termos de uso, pois é possível configurar suas políticas de chaves e concessões para vários usuários ou serviços. Para obter mais informações sobre a criação de chaves KMS, consulte Criação de chaves no Guia do AWS Key Management Service desenvolvedor.

> **Important**
>
> O Amazon FSx aceita somente chaves do KMS com criptografia simétrica. Não é possível usar chaves do KMS assimétricas com o Amazon FSx.

Se você usa uma chave KMS gerenciada pelo cliente como sua chave KMS de criptografia e decriptografia de dados de arquivos, pode habilitar a rotação de chaves. Ao habilitar a rotação de chaves, o AWS KMS gira sua chave automaticamente uma vez por ano. Além disso, com uma chave KMS gerenciada pelo cliente, você pode escolher quando desabilitar, reabilitar, excluir ou revogar o acesso à sua KMS a qualquer momento. Para obter mais informações, consulte Rotação de AWS KMS keys e Como ativar e desativar chaves no Guia do desenvolvedor do AWS Key Management Service .

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 AWS KMS relacionadas suportadas pelo 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 os dados no lado do servidor com um novo AWS KMS key, 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: GenerateData KeyWithout Texto simples — (Obrigatório) Retorna uma chave de criptografia de dados criptografada sob uma chave KMS. Essa permissão está incluída na política de chaves padrão em kms: GenerateData Key*.
- 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 Usar concessões 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 de chaves 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

Este tópico explica as diferentes opções disponíveis para criptografar seus dados de arquivo enquanto eles estão em trânsito entre um sistema de arquivos FSx for ONTAP e clientes conectados. Ele também fornece orientação para ajudá-lo a escolher qual método de criptografia é mais adequado para seu fluxo de trabalho.

Todos os dados que fluem Regiões da AWS pela rede AWS global são criptografados automaticamente na camada física antes de saírem das instalações AWS protegidas. Todo o tráfego

entre as zonas de disponibilidade é criptografado. Camadas adicionais de criptografia, inclusive as listadas nesta seção, fornecem mais proteções. Para obter mais informações sobre como AWS fornece proteção para o fluxo de dados Regiões da AWS, zonas disponíveis e instâncias, consulte Criptografia em trânsito no Guia do usuário do Amazon Elastic Compute Cloud para instâncias Linux.

O Amazon FSx for NetApp ONTAP oferece suporte aos seguintes métodos para criptografar dados em trânsito entre sistemas de arquivos FSx for ONTAP e clientes conectados:

- Criptografia automática baseada em Nitro em todos os protocolos e clientes com suporte em execução nos tipos de instância do Amazon EC2 para Linux e Windows.
- Criptografia baseada em Kerberos com os protocolos NFS e SMB.
- Criptografia baseada em IPsec com os protocolos NFS, iSCSI e SMB.

Todos os métodos suportados para criptografar dados em trânsito usam algoritmos criptográficos AES-256 padrão do setor que fornecem criptografia de força corporativa.

Tópicos

Como escolher um método para criptografar dados em trânsito

Esta seção fornece informações que podem ajudar você a decidir qual dos métodos de criptografia em trânsito com suporte é melhor para seu fluxo de trabalho. Consulte esta seção novamente ao explorar as opções com suporte descritas detalhadamente nas seções a seguir.

Há vários fatores a serem considerados ao escolher como você vai criptografar os dados em trânsito entre o sistema de arquivos do FSx para ONTAP e os clientes conectados. Esses fatores incluem:

- O em Região da AWS que seu sistema de arquivos FSx for ONTAP está sendo executado.

- O tipo de instância no qual o cliente está sendo executado.
- A localização do cliente que está acessando o sistema de arquivos.
- Requisitos de performance da rede.
- O protocolo de dados que você deseja criptografar.
- Se você estiver usando o Microsoft Active Directory.

Região da AWS

A configuração em Região da AWS que seu sistema de arquivos está sendo executado determina se você pode ou não usar a criptografia baseada no Amazon Nitro. A criptografia baseada em Nitro está disponível nas seguintes Regiões da AWS:

- Leste dos EUA (Norte da Virgínia)
- Leste dos EUA (Ohio)
- Oeste dos EUA (Oregon)
- Europa (Irlanda)

Além disso, a criptografia baseada em Nitro está disponível para sistemas de arquivos escaláveis na Ásia-Pacífico (Sydney). Região da AWS

Tipo de instância do cliente

Você poderá usar a criptografia baseada no Amazon Nitro se o cliente que está acessando o sistema de arquivos estiver sendo executado em qualquer um dos tipos de instância Mac, Linux ou Windows com suporte do Amazon EC2 e o fluxo de trabalho atender a todos os outros requisitos de uso da criptografia baseada em Nitro. Não há requisitos de tipo de instância de cliente para uso da criptografia Kerberos ou IPsec.

Client location (Localização do cliente)

A localização do cliente que acessa dados em relação à localização do sistema de arquivos afeta quais métodos de criptografia em trânsito estão disponíveis para uso. Você poderá usar qualquer um dos métodos de criptografia com suporte se o cliente e o sistema de arquivos estiverem localizados na mesma VPC. Isso também valerá se o cliente e o sistema de arquivos estiverem localizados em VPCs emparelhadas, desde que o tráfego não passe por um dispositivo ou serviço de rede virtual, como um gateway de trânsito. A criptografia baseada em Nitro não será uma opção disponível se o cliente não estiver na mesma VPC ou na VPC emparelhada, ou se o tráfego passar por um dispositivo ou serviço de rede virtual.

Performance de rede

O uso da criptografia baseada no Amazon Nitro não tem impacto na performance da rede. Isso ocorre porque as instâncias com suporte do Amazon EC2 utilizam os recursos de descarregamento do hardware Nitro System subjacente para criptografar automaticamente o tráfego em trânsito entre instâncias.

O uso da criptografia Kerberos ou IPsec tem impacto na performance da rede. Isso ocorre porque esses dois métodos de criptografia são baseados em software, o que exige que o cliente e o servidor usem recursos de computação para criptografar e decriptografar o tráfego em trânsito.

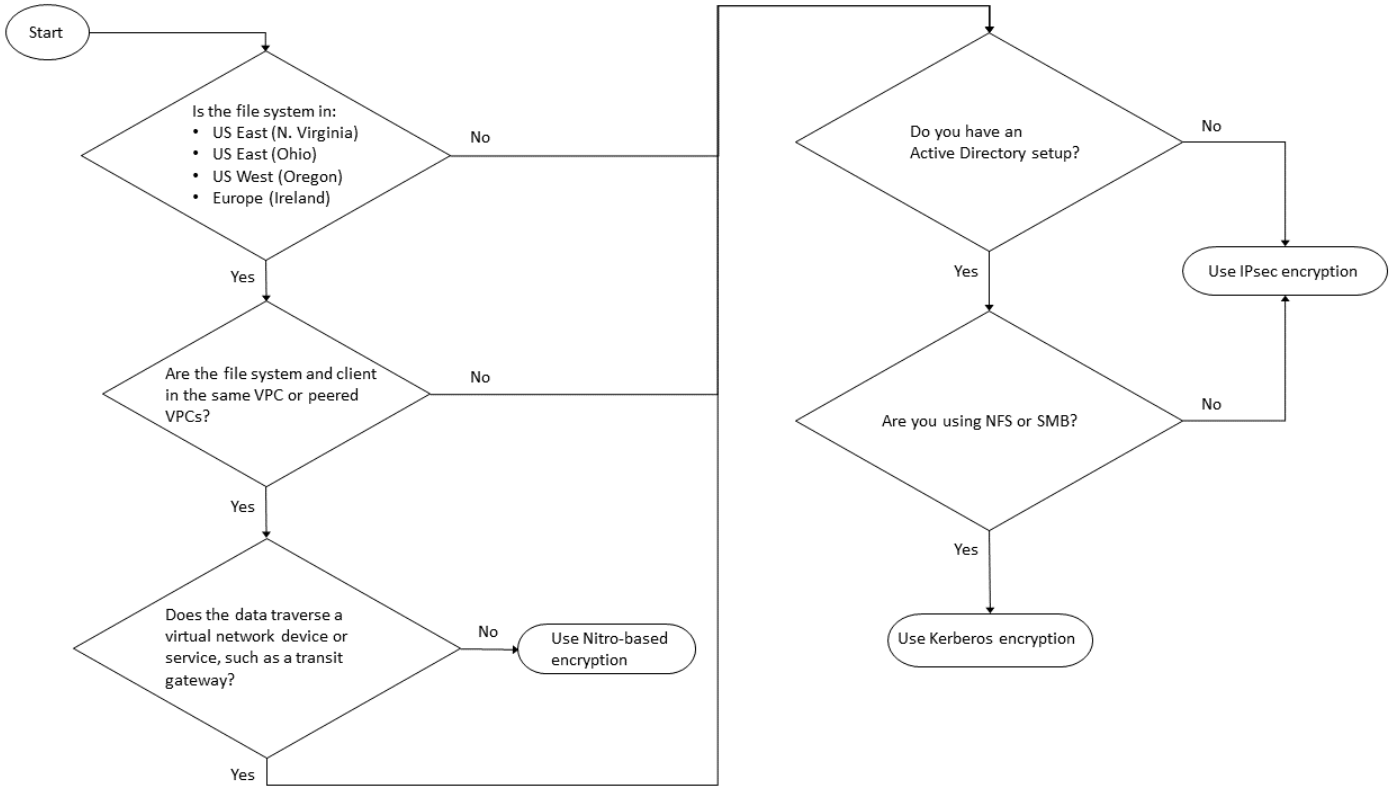
Protocolo de dados

Você pode usar a criptografia baseada no Amazon Nitro e a criptografia IPsec com todos os protocolos com suporte, como NFS, SMB e iSCSI. Você pode usar a criptografia Kerberos com os protocolos NFS e SMB (com um Active Directory).

Active Directory

Se você estiver usando o Microsoft Active Directory, poderá usar a criptografia Kerberos nos protocolos NFS e SMB.

Use o diagrama a seguir como ajuda para decidir qual método de criptografia em trânsito usar.



A criptografia IPsec é a única opção disponível quando todas as condições a seguir se aplicam ao fluxo de trabalho:

- Você está usando o protocolo NFS, SMB ou iSCSI.
- Seu fluxo de trabalho não dá suporte ao uso da criptografia baseada no Amazon Nitro.
- Você não está usando um domínio do Microsoft Active Directory.

Criptografando dados em trânsito com o AWS Nitro System

Com a criptografia baseada em Nitro, os dados em trânsito são criptografados automaticamente quando os clientes que acessam seus sistemas de arquivos estão sendo executados em tipos de instância do Linux ou Windows do Amazon EC2 com suporte.

O uso da criptografia baseada no Amazon Nitro não tem impacto na performance da rede. Isso ocorre porque as instâncias com suporte do Amazon EC2 utilizam os recursos de descarregamento do hardware Nitro System subjacente para criptografar automaticamente o tráfego em trânsito entre instâncias.

A criptografia baseada em Nitro é habilitada automaticamente quando os tipos de instância de cliente com suporte estão localizados na mesma Região da AWS e na mesma VPC ou em uma VPC emparelhada com a VPC do sistema de arquivos. Além disso, se o cliente estiver em uma VPC emparelhada, os dados não poderão passar por um dispositivo ou serviço de rede virtual (como um gateway de trânsito) para que a criptografia baseada em Nitro seja habilitada automaticamente. Para obter mais informações sobre criptografia baseada em Nitro, consulte a seção Criptografia em trânsito do Guia do usuário do Amazon EC2 para os tipos de instância do Linux ou Windows.

A criptografia em trânsito baseada em Nitro está disponível para sistemas de arquivos criados após 28 de novembro de 2022 da seguinte forma: Regiões da AWS

- Leste dos EUA (Norte da Virgínia)
- Leste dos EUA (Ohio)
- Oeste dos EUA (Oregon)
- Europa (Irlanda)

Além disso, a criptografia baseada em Nitro está disponível para sistemas de arquivos escaláveis na Ásia-Pacífico (Sydney). Região da AWS

Para obter mais informações sobre Regiões da AWS onde o FSx for ONTAP está disponível, consulte os preços do Amazon FSx for ONTAP. NetApp

Para obter mais informações sobre as especificações de performance dos sistemas de arquivos do FSx para ONTAP, consulte Impacto da capacidade de throughput na performance.

Criptografia de dados em trânsito com criptografia baseada em Kerberos

Se você estiver usando o Microsoft Active Directory, poderá usar a criptografia baseada em Kerberos nos protocolos NFS e SMB para criptografar dados em trânsito para volumes secundários de SVMs que estão associados a um Microsoft Active Directory.

Criptografia de dados em trânsito pelo NFS usando Kerberos

Há suporte para a criptografia de dados em trânsito usando Kerberos com os protocolos NFSv3 e NFSv4. Para habilitar a criptografia em trânsito usando o Kerberos com o protocolo NFS, consulte Uso do Kerberos com NFS para segurança forte no Centro de documentação do NetApp ONTAP

Criptografia de dados em trânsito pelo SMB usando Kerberos

Há suporte para criptografia de dados em trânsito pelo protocolo SMB nos compartilhamentos de arquivos mapeados em uma instância de computação compatível com o protocolo SMB 3.0 ou mais recente. Isso inclui todas as Microsoft Windows versões do Microsoft Windows Server 2012 e posterior e do Microsoft Windows 8 e posterior. Quando habilitado, o FSx para ONTAP criptografa automaticamente os dados em trânsito usando a criptografia SMB à medida que você acessa seu sistema de arquivos sem a necessidade de modificar suas aplicações.

O FSx para ONTAP SMB oferece suporte à criptografia de 128 e 256 bits, que é determinada pela solicitação de sessão do cliente. Para obter descrições dos diferentes níveis de criptografia, consulte a seção Definir o nível mínimo de segurança de autenticação do servidor SMB em Gerenciar SMB com a CLI no Centro de documentação do NetApp ONTAP.

> **Note**
>
> O cliente determina o algoritmo de criptografia. As autenticações NTLM e Kerberos funcionam com criptografia de 128 e 256 bits. O servidor SMB do FSx para ONTAP aceita todas as solicitações padrão do cliente Windows, e os controles granulares são gerenciados pelas configurações de política de grupo ou registro da Microsoft.

Você usa a CLI do ONTAP para gerenciar as configurações de criptografia em trânsito em SVMs e volumes do FSx para ONTAP. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na SVM na qual você está definindo as configurações de criptografia em trânsito, conforme descrito em Gerenciando SVMs com a CLI ONTAP.

Para obter instruções sobre como habilitar a criptografia SMB em um SVM ou volume, consulte. Ativação da criptografia SMB de dados em trânsito

Criptografia de dados em trânsito com criptografia IPsec

O FSx para ONTAP oferece suporte ao uso do protocolo IPsec no modo de transporte para garantir que os dados estejam continuamente seguros e criptografados enquanto estão em trânsito. O IPsec oferece end-to-end criptografia de dados em trânsito entre clientes e FSx para sistemas de arquivos ONTAP para todo o tráfego IP suportado — protocolos NFS, iSCSI e SMB. Com a criptografia IPsec, você estabelece um túnel IPsec entre uma SVM do FSx para ONTAP configurada com IPsec habilitado e um cliente IPsec em execução no cliente conectado que acessa os dados.

Recomendamos que você use IPsec para criptografar dados em trânsito pelos protocolos NFS, SMB e iSCSI ao acessar seus dados de clientes que não oferecem suporte à criptografia baseada em Nitro e se o cliente e as SVMs não estiverem associados a um Active Directory, o que é obrigatório para a criptografia baseada em Kerberos. A criptografia IPsec é a única opção disponível para criptografar dados em trânsito no tráfego iSCSI quando o cliente iSCSI não oferece suporte à criptografia baseada em Nitro.

Para autenticação IPsec, você pode usar chaves pré-compartilhadas (PSKs) ou certificados. Se você estiver usando uma PSK, o cliente IPsec que você usa deve oferecer suporte ao Internet Key Exchange versão 2 (IKEv2) com uma PSK. As etapas de alto nível para configurar a criptografia IPsec no FSx for ONTAP e no cliente são as seguintes:

1. Habilitar e configurar o IPsec no sistema de arquivos.
2. Instalar e configurar o IPsec no cliente
3. Configurar o IPsec para acesso a vários clientes

Para obter mais informações sobre como configurar o IPsec usando PSK, consulte Configurar a segurança IP (IPsec) por criptografia com fio no NetApp ONTAP centro de documentação.

Para obter mais informações sobre como configurar o IPsec usando certificados, consulteComo configurar o IPsec usando autenticação de certificado.

Ativação da criptografia SMB de dados em trânsito

Por padrão, quando você cria uma SVM, a criptografia SMB é desativada. Você pode habilitar a criptografia SMB necessária em compartilhamentos individuais ou em uma SVM, o que a ativa para todos os compartilhamentos nessa SVM.

> **Note**
>
> Quando a criptografia SMB necessária está habilitada em uma SVM ou em um compartilhamento, os clientes SMB que não oferecem suporte à criptografia não podem se conectar à SVM ou ao compartilhamento.

Para exigir criptografia SMB no tráfego SMB de entrada em uma SVM

Use o procedimento a seguir para exigir criptografia SMB em uma SVM usando a CLI do NetApp ONTAP.

1. Para se conectar ao endpoint de gerenciamento da SVM com SSH, use o nome de usuário `vsadmin` e a senha vsadmin definidos ao criar a SVM. Se você não tiver definido uma senha vsadmin, utilize o nome de usuário `fsxadmin` e a senha fsxadmin. Você pode efetuar SSH na SVM por meio de um cliente que esteja na mesma VPC do sistema de arquivos, usando o endereço IP ou o nome DNS do endpoint de gerenciamento.

   ```
   ssh vsadmin@svm-management-endpoint-ip-address
   ```

   O comando com exemplo de valores:

   ```
   ssh vsadmin@198.51.100.10
   ```

   O comando SSH usando o nome DNS do endpoint de gerenciamento:

   ```
   ssh vsadmin@svm-management-endpoint-dns-name
   ```

   O comando de SSH usando um nome de DNS de exemplo:

   ```
   ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-
   east-2.aws.com
   ```

   ```
   Password: vsadmin-password

   This is your first recorded login.
   FsxIdabcdef01234567892::>
   ```

2. Use o comando `vserver cifs security modify`NetApp ONTAPCLI para exigir criptografia SMB para tráfego SMB de entrada para o SVM.

   ```
   vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
   ```

3. Para deixar de exigir a criptografia SMB no tráfego SMB de entrada, use o comando a seguir.

   ```
   vserver cifs security modify -vserver vserver_name -is-smb-encryption-required
    false
   ```

4. Para ver a `is-smb-encryption-required` configuração atual em um SVM, use o comando `vserver cifs security show`NetApp ONTAPCLI:

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

Para obter mais informações sobre como gerenciar a criptografia SMB em uma SVM, consulte Configuração da criptografia SMB necessária em servidores SMB para transferências de dados por SMB no Centro de documentação do NetApp ONTAP,

Habilitar a criptografia SMB em um volume

Use o procedimento a seguir para exigir criptografia SMB em um compartilhamento usando a CLI do NetApp ONTAP.

1. Estabeleça uma conexão Secure Shell (SSH) com o endpoint de gerenciamento da SVM, conforme descrito em Gerenciando SVMs com a CLI ONTAP.
2. Use o comando da CLI do NetApp ONTAP a seguir para criar um novo compartilhamento SMB e exigir criptografia SMB ao acessar esse compartilhamento.

   ```
   vserver cifs share create -vserver vserver_name -share-name share_name -
   path share_path -share-properties encrypt-data
   ```

   Para obter mais informações, consulte vserver cifs share create nas páginas de manual de comandos da CLI do NetApp ONTAP.
3. Para exigir a criptografia SMB em um compartilhamento SMB existente, use o comando a seguir.

   ```
   vserver cifs share properties add -vserver vserver_name -share-name share_name -
   share-properties encrypt-data
   ```

   Para obter mais informações, consulte vserver cifs share create nas páginas de manual de comandos da CLI do NetApp ONTAP.
4. Para desativar a criptografia SMB em um compartilhamento SMB existente, use o comando a seguir.

```
vserver cifs share properties remove -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

Para obter mais informações, consulte `vserver cifs share properties remove` nas páginas de manual de comandos da CLI do NetApp ONTAP.

5. Para ver a configuração atual `is-smb-encryption-required` em um compartilhamento SMB, use o seguinte comando da CLI do NetApp ONTAP:

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -
fields share-properties
```

Se uma das propriedades retornadas pelo comando for `encrypt-data`, essa propriedade especificará que a criptografia SMB deve ser usada ao acessar esse compartilhamento.

Para obter mais informações, consulte `vserver cifs share properties show` nas páginas de manual de comandos da CLI do NetApp ONTAP.

Como configurar o IPsec usando a autenticação PSK

Se você estiver usando PSK para autenticação, as etapas de configuração da criptografia IPsec no FSx para ONTAP e no cliente serão as seguintes:

1. Habilitar e configurar o IPsec no sistema de arquivos.
2. Instalar e configurar o IPsec no cliente
3. Configurar o IPsec para acesso a vários clientes

Para obter detalhes sobre como configurar o IPsec usando PSK, consulte Configurar a segurança IP (IPsec) por criptografia com fio no centro de documentação do NetApp ONTAP.

Como configurar o IPsec usando autenticação de certificado

Os tópicos a seguir fornecem instruções para configurar a criptografia IPsec usando autenticação de certificado em um sistema de arquivos FSx for ONTAP e em um cliente executando o Libreswan IPsec. Essa solução usa AWS Certificate Manager e AWS Private Certificate Authority para criar uma autoridade de certificação privada e para gerar os certificados.

As etapas de alto nível para configurar a criptografia IPsec usando autenticação de certificado no FSx para sistemas de arquivos ONTAP e clientes conectados são as seguintes:

1. Tenha uma autoridade de certificação para emitir certificados.
2. Gere e exporte certificados CA para o sistema de arquivos e o cliente.
3. Instale o certificado e configure o IPsec na instância do cliente.
4. Instale o certificado e configure o IPsec em seu sistema de arquivos.
5. Defina o banco de dados de políticas de segurança (SPD).
6. Configure o IPsec para acesso a vários clientes.

Como criar e instalar certificados CA

Para autenticação de certificado, você precisa gerar e instalar certificados de uma autoridade de certificação em seu sistema de arquivos do FSx para ONTAP e nos clientes que acessarão os dados do sistema de arquivos. O exemplo a seguir é usado AWS Private Certificate Authority para configurar uma autoridade de certificação privada e gerar os certificados para instalação no sistema de arquivos e no cliente. Usando AWS Private Certificate Authority, você pode criar uma hierarquia totalmente AWS hospedada de autoridades de certificação (CAs) raiz e subordinadas para uso interno de sua organização. Esse processo tem cinco etapas:

1. Crie uma autoridade de certificação (CA) privada usando AWS Private CA
2. Emitir e instalar o certificado raiz na CA privada
3. Solicite um certificado privado AWS Certificate Manager para seu sistema de arquivos e clientes
4. Exportar o certificado para o sistema de arquivos e os clientes

Para obter mais informações, consulte Administração de CA privada no Guia AWS Private Certificate Authority do usuário.

Criar a CA privada raiz

1. Ao criar uma CA, especifique a configuração da CA em um arquivo fornecido por você. O comando a seguir usa o editor de texto Nano para criar o arquivo `ca_config.txt`, que especifica as seguintes informações:

   - O nome do algoritmo
   - O algoritmo de assinatura que a CA usa para assinar

- Informações do assunto X.500

```
$ > nano ca_config.txt
```

O editor de texto é exibido.

2. Edite o arquivo com as especificações da sua CA.

```
{
   "KeyAlgorithm":"RSA_2048",
   "SigningAlgorithm":"SHA256WITHRSA",
   "Subject":{
      "Country":"US",
      "Organization":"Example Corp",
      "OrganizationalUnit":"Sales",
      "State":"WA",
      "Locality":"Seattle",
      "CommonName":"*.ec2.internal"
   }
}
```

3. Salve e feche o arquivo, saindo do editor de texto. Para obter mais informações, consulte Procedimento para criar uma CA no Guia AWS Private Certificate Authority do Usuário.
4. Use o comando da CLI create-certificate-authority da AWS Private CA para criar uma CA privada.

```
~/home > aws acm-pca create-certificate-authority \
     --certificate-authority-configuration file://ca_config.txt \
     --certificate-authority-type "ROOT" \
     --idempotency-token 01234567 --region aws-region
```

Se obtiver êxito, esse comando produz o nome de recurso da Amazon (ARN) da CA.

```
{
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Para criar e instalar um certificado para a CA raiz privada (AWS CLI)

1. Gere uma solicitação de assinatura de certificado (CSR) usando o comando `get-certificate-authority-csr` AWS CLI.

```
$ aws acm-pca get-certificate-authority-csr \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --output text \
     --endpoint https://acm-pca.aws-region.amazonaws.com \
     --region eu-west-1 > ca.csr
```

   O arquivo resultante `ca.csr`, um arquivo PEM codificado no formato base64, tem a seguinte aparência.

```
-----BEGIN CERTIFICATE-----
 MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
 VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
 BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
 MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
 VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
 b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
 YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
 rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
 Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
 FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
 NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
 -----END CERTIFICATE-----
```

   Para obter mais informações, consulte Instalando um certificado CA raiz no Guia AWS Private Certificate Authority do usuário.

2. Use o `issue-certificate` AWS CLI comando para emitir e instalar o certificado raiz em sua CA privada.

```
$ aws acm-pca issue-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --csr file://ca.csr \
```

```
    --signing-algorithm SHA256WITHRSA \
    --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
    --validity Value=3650,Type=DAYS --region aws-region
```

3. Faça o download do certificado raiz usando o `get-certificate` AWS CLI comando.

```
$ aws acm-pca get-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
    --output text --region aws-region > rootCA.pem
```

4. Instale o certificado raiz em sua CA privada usando o `import-certificate-authority-certificate` AWS CLI comando.

```
$ aws acm-pca import-certificate-authority-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate file://rootCA.pem --region aws-region
```

Gerar e exportar o certificado do sistema de arquivos e do cliente

1. Use o `request-certificate` AWS CLI comando para solicitar um AWS Certificate Manager certificado para usar em seu sistema de arquivos e clientes.

```
$ aws acm request-certificate \
    --domain-name *.ec2.internal \
    --idempotency-token 12345 \
    --region aws-region \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

   Se a solicitação for bem-sucedida, o ARN do certificado emitido será retornado.

2. Por segurança, você deve atribuir uma frase-senha para a chave privada ao exportá-la. Crie uma frase-senha e armazene-a em um arquivo chamado `passphrase.txt`

3. Use o `export-certificate` AWS CLI comando para exportar o certificado privado emitido anteriormente. O arquivo exportado contém o certificado, a cadeia de certificados e a chave RSA

privada criptografada de 2048 bits associada à chave pública incorporada ao certificado. Por segurança, você deve atribuir uma frase-senha para a chave privada ao exportá-la. O exemplo a seguinte é de uma instância do LInux EC2.

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
     --passphrase $(cat passphrase.txt | base64)) --region aws-region >
 exported_cert.json
```

4. Use os comandos `jq` a seguir para extrair a chave privada e o certificado da resposta JSON.

```
$ cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

5. Use os comandos `openssl` a seguir para decriptografar a chave privada da resposta JSON. Depois de inserir o comando, você será solicitado a digitar a frase-senha.

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

Instalação e configuração do Libreswan IPsec em um cliente Amazon Linux 2

As seções a seguir fornecem instruções para instalar e configurar o Libreswan IPsec em uma instância do Amazon EC2 que executa o Amazon Linux 2.

Instalar e configurar o Libreswan

1. Conecte-se à sua instância do EC2 usando SSH. Para obter instruções específicas sobre como fazer isso, consulte Conectar-se à instância do Linux usando um cliente SSH no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux..
2. Execute o comando a seguir para instalar o `libreswan`:

```
$ sudo yum install libreswan
```

3. (Opcional) Ao verificar o IPsec em uma etapa posterior, essas propriedades poderão ser sinalizadas sem essas configurações. Sugerimos testar sua instalação primeiro sem essas

configurações. Se sua conexão tiver problemas, retorne a esta etapa e faça as alterações a seguir.

Após a conclusão da instalação, use seu editor de texto preferencial para adicionar as entradas a seguir ao arquivo `/etc/sysctl.conf`.

```
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
```

Salve as alterações e saia do editor de texto.

4. Aplique as alterações:

```
$ sudo sysctl -p
```

5. Verifique a configuração do IPsec.

```
$ sudo ipsec verify
```

Verifique se a versão do `Libreswan` que você instalou está em execução.

6. Inicialize o banco de dados IPsec NSS.

```
$ sudo ipsec checknss
```

Instalar o certificado no cliente

1. Copie o certificado que você gerou para o cliente no diretório de trabalho da instância do EC2. Você
2. Exporte o certificado gerado anteriormente em um formato compatível com o `libreswan`.

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \
    -certfile rootCA.pem -out certkey.p12 -name fsx
```

3. Importe a chave reformatada, fornecendo a frase-senha quando solicitado.

```
$ sudo ipsec import certkey.p12
```

4. Crie um arquivo de configuração IPsec usando o editor de texto preferencial.

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

Adicione as seguintes entradas ao arquivo de configuração:

```
conn fsxn
    authby=rsasig
    left=172.31.77.6
    right=198.19.254.13
    auto=start
    type=transport
    ikev2=insist
    keyexchange=ike
    ike=aes256-sha2_384;dh20
    esp=aes_gcm_c256
    leftcert=fsx
    leftrsasigkey=%cert
    leftid=%fromcert
    rightid=%fromcert
    rightrsasigkey=%cert
```

Você iniciará o IPsec no cliente depois de configurar o IPsec em seu sistema de arquivos.

Como configurar o IPsec em seu sistema de arquivos

Esta seção fornece instruções sobre como instalar o certificado no sistema de arquivos do FSx para ONTAP e configurar o IPsec.

Instalar o certificado no sistema de arquivos

1. Copie os arquivos do certificado raiz (`rootCA.pem`)), do certificado do cliente (`cert.pem`) e da chave decriptografada (`decrypted.key`) para o sistema de arquivos. Você precisará saber a senha do certificado.
2. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.
3. Use cat em um cliente (não no sistema de arquivos) para listar o conteúdo dos arquivos `rootCA.pem`, `cert.pem` e `decrypted.key` para que você possa copiar a saída de cada arquivo e colá-la quando solicitado nas etapas a seguir.

   ```
   $ > cat cert.pem
   ```

   Copie o conteúdo do certificado.
4. Instale todos os certificados da CA usados durante a autenticação mútua, incluindo CAs do lado do ONTAP e do lado do cliente, no gerenciamento de certificados do ONTAP, a menos que ele já esteja instalado (como é o caso de uma CA raiz autoassinada do ONTAP).

   Use o comando `security certificate install` NetApp CLI da seguinte forma para instalar o certificado do cliente:

   ```
   FSxID123:: > security certificate install -vserver dr -type client -cert-name
    ipsec-client-cert
   ```

   ```
   Please enter Certificate: Press <Enter> when done
   ```

   Cole o conteúdo do arquivo `cert.pem` que você copiou anteriormente e pressione Enter.

   ```
   Please enter Private Key: Press <Enter> when done
   ```

Cole o conteúdo do arquivo `decrypted.key` e pressione Enter.

```
Do you want to continue entering root and/or intermediate certificates {y|n}:
```

Insira n para concluir a inserção do certificado do cliente.

5. Crie e instale um certificado para uso da SVM. A CA emissora desse certificado já deve estar instalada no ONTAP e adicionada ao IPsec.

   Use o seguinte comando para instalar o certificado raiz:

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
 ipsec-ca-cert
```

```
Please enter Certificate: Press <Enter> when done
```

   Cole o conteúdo do arquivo `rootCA.pem` e pressione Enter.

6. Para garantir que a CA instalada esteja dentro do caminho de busca de CAs do IPsec durante a autenticação, adicione as CAs de gerenciamento de certificados do ONTAP ao módulo IPsec usando o comando “security ipsec ca-certificate add”.

   Digite o seguinte comando para adicionar o certificado raiz:

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. Digite o comando a seguir para criar a política IPsec obrigatória no banco de dados de políticas de segurança (SPD).

```
security ipsec policy create -vserver dr -name policy-name -local-ip-
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
 ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
 "CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. Use o comando a seguir para mostrar a política de IPsec para que o sistema de arquivos confirme.

```
FSxID123:: > security ipsec policy show -vserver dr -instance

                                    Vserver: dr
```

```
                                Policy Name: promise
                             Local IP Subnets: 198.19.254.13/32
                            Remote IP Subnets: 172.31.0.0/16
                                  Local Ports: 0-0
                                 Remote Ports: 0-0
                                    Protocols: any
                                       Action: ESP_TRA
                                Cipher Suite: SUITEB_GCM256
          IKE Security Association Lifetime: 86400
        IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
                            Is Policy Enabled: true
                               Local Identity: CN=*.ec2.internal
                              Remote Identity: CN=*.ec2.internal
                        Authentication Method: PKI
             Certificate for Local Identity: ipsec-client-cert
```

Iniciar o IPsec no cliente

Agora que o IPsec está configurado no sistema de arquivos do FSx para ONTAP e no cliente, você pode iniciá-lo no cliente.

1. Conecte-se ao sistema do cliente usando SSH.
2. Inicie o IPsec.

```
$ sudo ipsec start
```

3. Verifique o status do IPsec.

```
$ sudo ipsec status
```

4. Monte um volume no sistema de arquivos.

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. Verifique a configuração do IPsec mostrando a conexão criptografada no seu sistema de arquivos do FSx para ONTAP.

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
```

```
Vserver     Name    Address         Address         Initator-SPI     State
----------- ------ -------------- -------------- ---------------- -----------
dr          policy-name
                    198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                    198.19.254.38   172.31.65.193   4fd3f22c993e60c5 ESTABLISHED
2 entries were displayed.
```

Configuração do IPsec para vários clientes

Quando um número pequeno de clientes precisa utilizar o IPsec, o uso de uma única entrada SPD para cada cliente é suficiente. No entanto, quando centenas ou até milhares de clientes precisarem utilizar IPsec, recomendamos que você use a configuração de vários clientes IPsec.

O FSx para ONTAP fornece suporte a conexão de vários clientes em várias redes com um único endereço IP da SVM, com o IPsec habilitado. Você pode fazer isso usando a configuração `subnet` ou `Allow all clients`, que são explicadas nos seguintes procedimentos:

Configurar o IPsec para vários clientes usando uma configuração de sub-rede

Para permitir que todos os clientes de uma sub-rede específica (192.168.134.0/24, por exemplo) se conectem a um único endereço IP da SVM usando uma única entrada de política SPD, especifique `remote-ip-subnets` no formulário da sub-rede. Além disso, especifique o campo `remote-identity` com a identidade correta no lado do cliente.

> **Important**
>
> Ao usar a autenticação de certificado, cada cliente pode usar seu próprio certificado exclusivo ou um certificado compartilhado para autenticação. O IPsec do FSx para ONTAP verifica a validade do certificado com base nas CAs instaladas em seu armazenamento confiável local. O FSx para ONTAP também oferece suporte à verificação da lista de revogação de certificados (CRL).

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Use o comando `security ipsec policy create` da CLI do NetApp ONTAP conforme a seguir, substituindo os valores de *amostra* por seus valores específicos.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -remote-identity client_side_identity
```

Configurar o IPsec para vários clientes usando uma configuração que permite todos os clientes

Para permitir que qualquer cliente, independentemente do endereço IP de origem deles, se conecte ao endereço IP habilitado para IPsec da SVM, use o curinga `0.0.0.0/0` ao especificar o campo `remote-ip-subnets`.

Além disso, especifique o campo `remote-identity` com a identidade correta no lado do cliente. No caso da autenticação de certificado, você pode digitar `ANYTHING`.

Além disso, quando o curinga 0.0.0.0/0 é usado, você deve configurar um número de porta local ou remota específico para uso. Por exemplo, porta NFS 2049.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *management_endpoint_ip* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Use o comando `security ipsec policy create` da CLI do NetApp ONTAP conforme a seguir, substituindo os valores de *amostra* por seus valores específicos.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
```

```
-local-ports 2049 -protocols tcp -auth-method PSK \
-cert-name my_nfs_server_cert -local-identity ontap_side_identity \
-local-ports 2049 -remote-identity client_side_identity
```

Gerenciamento de identidade e acesso para Amazon FSx for ONTAP NetApp

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. 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 você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz 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 ajudar você a solicitar as permissões corretas ao

seu administrador. Se você não puder acessar um recurso no Amazon FSx, consulte Solução de problemas do Amazon FSx para identidade e acesso ao NetApp ONTAP.

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 for NetApp ONTAP 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 Amazon FSx for ONTAP NetApp .

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no AWS IAM Identity Center Guia do Usuário. Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode 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 usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o . AWS IAM Identity Center Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no AWS IAM Identity Center Manual do Usuário do.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de 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 uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne 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 usar 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 nome de grupo 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 um aplicativo, mas uma função pode ser assumida por qualquer pessoa que precisar dela. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando Criar um Usuário do IAM (Ao Invés de uma Função) no Guia do Usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Usando Funções do IAM no Guia do Usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode 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 Criando um Perfil para um Provedor de Identidades Terceirizado no Guia do Usuário do IAM. Se você usa o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no AWS IAM Identity Center Manual do Usuário.
- Permissões de usuários temporárias do IAM: um usuário ou perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.

- Acesso entre contas: você pode usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) acesse recursos na sua conta de uma conta diferente. As funções são a forma primária de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para aprender a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte Como as Funções do IAM Diferem das Políticas Baseadas em Recurso no Guia do Usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões de chamada da entidade principal, uma função de serviço ou uma função vinculada ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. 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.
  - Função de Serviço: uma função de serviço é uma função 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 Criando um Perfil para Delegar Permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de

instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para aprender se deseja usar perfis do IAM, consulte Quando Criar uma Função do IAM (em Vez de um Usuário) no Guia do Usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um 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 é armazenada 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 políticas AWS JSON para especificar quem tem acesso ao 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 permissão 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 às funções e os usuários podem assumir as funções.

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 função da AWS Management Console AWS CLI, da ou da AWS API.

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 do IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em quais 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 também podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são incorporadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como selecionar entre uma política gerenciada ou uma política em linha, consulte Selecionar entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas do bucket do Amazon S3. Em serviços que suportem 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. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em atributos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissão para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Saiba mais sobre ACLs em Configurações da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais 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 recurso 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 e dos seus limites de permissões. As políticas baseadas em atributo que especificam o usuário ou o perfil 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 Entidades 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 (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. 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 nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no AWS Organizations Manual do Usuário do.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para uma função 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 atributo. 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 AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o Amazon FSx for NetApp ONTAP 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.

Recursos do IAM que você pode usar com o Amazon FSx for ONTAP NetApp

Atributo do IAM	Suporte do Amazon FSx
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das 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 ter uma visão de alto nível de como o Amazon FSx e AWS outros serviços funcionam com a maioria dos recursos do IAM, AWS consulte os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade do Amazon FSx

Suporta com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em quais condições. Saiba como criar uma política baseada em identidade consultando Criando Políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim 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 função à qual ela está anexada. 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 Amazon FSx for ONTAP NetApp .

Políticas baseadas em recursos no Amazon FSx

Oferece suporte a políticas baseadas em recursos	Não

Ações de políticas para o Amazon FSx

Oferece suporte a ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao 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 você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que 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 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 Amazon FSx for ONTAP NetApp .

Recursos de políticas do Amazon FSx

Oferece suporte a atributos de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` de política 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 atributo específico, conhecido como permissões em nível de atributo.

Para ações não compatíveis com permissões no nível de recurso, como operações de listagem, use um 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 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 ver exemplos de políticas baseadas em identidade do Amazon FSx, consulte Exemplos de políticas baseadas em identidade para Amazon FSx for ONTAP NetApp .

Chaves de condição de política para o Amazon FSx

Suporta chaves de condição de política específicas de serviço	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite especificar condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. Você pode criar expressões condicionais que usem operadores de condição, como “igual a” ou “menor que”, para corresponder a condição da política 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, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo 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.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de condição do Amazon FSx, consulte Chaves de condição do Amazon FSx 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 ver exemplos de políticas baseadas em identidade do Amazon FSx, consulte Exemplos de políticas baseadas em identidade para Amazon FSx for ONTAP NetApp .

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. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. 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 recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre a tag no elemento de condição de uma política usando as chaves de condição `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para todo 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 recurso baseado em tags desse recurso, 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 “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (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 funções, consulte Alternar para uma Função (Console) no Guia do Usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para 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 uma função do IAM para realizar ações em AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. 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

Perfis vinculados ao serviço para Amazon FSx

Oferece suporte a perfis vinculados ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculadas ao serviço do Amazon FSx, consulte Como usar perfis vinculados a serviço no Amazon FSx.

Exemplos de políticas baseadas em identidade para Amazon FSx for ONTAP NetApp

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Amazon FSx. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissões de usuários para executar ações nos recursos que eles 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 para cada tipo de recurso, consulte Ações, recursos e chaves de condição do Amazon FSx na Referência de autorização do serviço.

Tópicos

- Melhores práticas de política
- Como usar o console do Amazon FSx
- Permitir que usuários visualizem suas próprias permissões

Melhores práticas de política

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 seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas Gerenciadas pela AWS ou AWS Políticas Gerenciadas para Funções 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 atributos 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.
- Utilize 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, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Condição de Elementos de Política JSON do IAM no Guia do Usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM para garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam o idioma de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e ações recomendadas para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de Política do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS 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 Configurando 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 for NetApp ONTAP, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Amazon FSx em seu. 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.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a 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 funções ainda possam usar o console do Amazon FSx, anexe também a política `AmazonFSxConsoleReadOnlyAccess` AWS gerenciada 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 usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita 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 programaticamente usando a API AWS CLI ou AWS .

```
{
    "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": "*"
        }
    ]
}
```

Solução de problemas do Amazon FSx para identidade e acesso ao NetApp ONTAP

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 de 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 recurso *`my-example-widget`* usando a ação `fsx:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. 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 uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada 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 precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas de fora da minha Conta da AWS acessem meus recursos do Amazon FSx

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização possam usar para acessar seus recursos. Você pode 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 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 for NetApp ONTAP funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Saiba como conceder acesso por meio da federação de identidades consultando Concedendo 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 recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos 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 recursos da API do Amazon FSx, você pode especificar tags quando cria o recurso. É possível usar essas tags de recurso para implementar o controle de acesso por atributo (ABAC). Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

Para permitir que os usuários marquem recursos na criação, eles devem ter permissão para usar a ação que cria o recurso, como `fsx:CreateFileSystem`, `fsx:CreateStorageVirtualMachine` ou `fsx:CreateVolume`. 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 máquinas virtuais de armazenamento (SVMs) e apliquem tags a eles durante a criação em um determinado Conta da AWS local.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:CreateStorageVirtualMachine",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*",
         "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
  ]
}
```

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, 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 AWS recursos, consulte Como controlar o 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: criar um sistema de arquivos somente quando uma tag específica for usada

Essa política permite que o usuário só crie um sistema de arquivos quando o marcar 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 — Crie backups somente dos volumes Amazon FSx for NetApp ONTAP com uma tag específica

Essa política permite que os usuários só criem backups de volumes do FSx para ONTAP marcados com o par de chave/valor `key=Department`, `value=Finance`. O backup é criado com a tag `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "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: criar um volume com uma tag específica usando backups com uma tag específica

Essa política só permite que os usuários criem volumes marcados com `Department=Finance` usando backups marcados com `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
```

```
            ],
            "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`.

```
{
    "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:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
```

```
        }
    ]
}
```

Example Exemplo de política: excluir um volume com tags específicas

Essa política só permite que o usuário exclua volumes marcados com `Department=Finance`. Se um backup final for criado, ele deverá ser marcado com `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "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 suportados por funções vinculadas a serviços, consulte Serviços da AWS Suportados pelo IAM e procure os serviços que apresentarem Sim na coluna Função Vinculada a Serviço.. 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 a função vinculada ao serviço chamada AWSServiceRoleForAmazonFSx— Que executa determinadas ações em sua conta, como criar interfaces de rede elásticas para seus sistemas de arquivos em sua VPC e publicar métricas de volume e sistema de arquivos em. CloudWatch

Para atualizações desta política, consulte Amazon F SxService RolePolicy

Detalhes da permissão

Detalhes da permissão

As permissões de AWSServiceRoleForAmazonFSx função são definidas pela política SxService RolePolicy AWS gerenciada da AmazonF. O AWSServiceRoleForAmazonFSx tem as seguintes permissões:

> **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 ONTAP.

- `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 Amazon 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 uma função vinculada a serviço. Para obter mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Como criar um perfil vinculado ao serviço para o Amazon FSx

Não é necessário criar manualmente uma função vinculada a serviço. Quando você cria um sistema de arquivos na CLI do IAM ou na API do IAM, o Amazon FSx cria a função vinculada ao serviço para você. AWS Management Console

> **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 a função vinculada ao AWSServiceRoleForAmazonFSx serviço. 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 do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a 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 a função vinculada a serviço usando o IAM

Use o console do IAM, a CLI do IAM ou a API do IAM para excluir a função vinculada ao AWSServiceRoleForAmazonFSx serviço. Para 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 mais informações, consulte Regiões e endpoints da AWS.

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 elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da 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) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Amazon F SxService RolePolicy

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 SxDelete ServiceLinked RoleAccess

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 no `iam` para permitir que o Amazon FSx visualize e exclua o status de exclusão dos perfis vinculados ao serviço FSx para acesso ao Amazon S3.

Para ver as permissões dessa política, consulte a AmazonF SxDelete ServiceLinked RoleAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: Amazon Access SxFull

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 o AmazonF SxFull Access no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonF SxConsole FullAccess

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 SxConsole FullAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: Amazon Access SxConsole ReadOnly

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 o AmazonF SxConsole ReadOnly Access no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonF SxRead OnlyAccess

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 SxRead OnlyAccess 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 de documentos do Amazon FSx for ONTAP NetApp do Amazon FSx.

Alteração	Descrição	Data
AmazonF SxService RolePolicy — 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.	9 de janeiro de 2024
AmazonF SxRead OnlyAccess — 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	9 de janeiro de 2024

Alteração	Descrição	Data
	que podem ser usados com uma VPC.	
Amazon SxConsole ReadOnly Access — 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.	9 de janeiro de 2024
Amazon SxFull Access — 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.	9 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.	9 de janeiro de 2024

Alteração	Descrição	Data
Amazon SxFull Access — 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
Amazon SxFull Access — 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

Alteração	Descrição	Data
Amazon SxFull Access — 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
Amazon SxFull Access — 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 SxService RolePolicy — 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

Alteração	Descrição	Data
Amazon SxFull Access — 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
Amazon SxConsole ReadOnly Access — 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 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 SxRead OnlyAccess — 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

Alteração	Descrição	Data
AmazonF SxDelete ServiceLinked RoleAccess — 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 SxService RolePolicy — 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
Amazon SxFull Access — 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

Alteração	Descrição	Data
AmazonF SxService RolePolicy — 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
AmazonF SxService RolePolicy — 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

Alteração	Descrição	Data
Amazon SxFull Access — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os diretores descrevam e criem grupos de CloudWatch logs, streams de logs e gravem eventos em streams de log. Isso é necessário para que os diretores possam visualiza r 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
Amazon SxFull Access — 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

Alteração	Descrição	Data
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
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

Alteração	Descrição	Data
Amazon SxConsole ReadOnly Access — 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 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 SxConsole ReadOnly Access — 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

Alteração	Descrição	Data
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

Controle de acesso ao sistema de arquivos com a Amazon VPC

Você acessa seus sistemas de arquivos e SVMs do Amazon FSx for NetApp ONTAP usando o nome DNS ou o endereço IP de um de seus endpoints, dependendo do tipo de acesso. O nome DNS é mapeado para o endereço IP privado da interface de rede elástica do sistema de arquivos ou da SVM na sua VPC. Somente recursos dentro da VPC associada, ou recursos conectados à VPC AWS Direct Connect ou VPN associada, podem acessar os dados em seu sistema de arquivos por meio dos protocolos NFS, SMB ou iSCSI. Para obter mais informações, consulte O que é a Amazon VPC? no Guia do usuário da Amazon VPC.

> **Warning**
>
> Você não deve modificar nem excluir as interfaces de rede elástica associadas ao seu 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.

Grupos de segurança da Amazon VPC

Um grupo de segurança age como firewall virtual para os sistemas de arquivos do FSx para ONTAP a fim de controlar o tráfego de entrada e saída. As regras de entrada controlam o tráfego de entrada para o sistema de arquivos e as regras de saída controlam o tráfego de saída do sistema de arquivos. Ao criar um sistema de arquivos, você especifica a VPC na qual ele é criado e o grupo de segurança padrão dessa VPC é aplicado. É possível adicionar regras a cada grupo de segurança que permitam o tráfego de entrada ou de saída nos sistemas de arquivos ou nas SVMs associadas. É possível modificar as regras de um grupo de segurança a qualquer momento. As regras novas e modificadas são aplicadas automaticamente a todos os recursos associados ao grupo de segurança. Quando o Amazon FSx decide se deve permitir que o tráfego atinja um recurso, ele avalia todas as regras de todos os grupos de segurança associados ao recurso.

Para usar um grupo de segurança para controlar o acesso ao sistema de arquivos do Amazon FSx, adicione regras de entrada e saída. As regras de entrada controlam o tráfego de entrada e as regras de saída controlam o tráfego de saída do sistema de arquivos. 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 em uma pasta na sua instância de computação com suporte.

Para obter mais informações sobre regras de grupos de segurança, consulte Regras de grupos de segurança no Guia do usuário do Amazon EC2.

Criar um grupo de segurança de VPC

Criar um grupo de segurança para o 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 Amazon VPC associada ao seu sistema de arquivos para criar o grupo de segurança dentro dessa VPC.
6. Para regras de saída, permita todo o tráfego em todas as portas.
7. Adicione a regras a seguir às portas de entrada do grupo de segurança. Para o campo de origem, você deve escolher Personalizado e inserir os grupos de segurança ou os intervalos de endereços IP associados às instâncias que precisam acessar seu sistema de arquivos do FSx para ONTAP, incluindo:

   - Clientes Linux, Windows e macOS que acessam dados em seu sistema de arquivos via NFS, SMB ou iSCSI.
   - Qualquer sistema de arquivos/clusters ONTAP que você conectará ao seu sistema de arquivos (por exemplo, para usar SnapMirror, SnapVault ou). FlexCache
   - Qualquer cliente que você usará para acessar a API REST, CLI ou ZAPIs do ONTAP (por exemplo, uma instância Harvest/Grafana, Connector ou BlueXP). NetApp NetApp

Protocolo	Portas	Função
Todos os ICMP	Todos	Como executar ping na instância

Protocolo	Portas	Função
SSH	22	Acesso SSH ao endereço IP da LIF de gerenciamento de cluster ou de uma LIF de gerenciamento de nós
TCP	111	Chamada de procedimento remoto para NFS
TCP	135	Chamada de procedimento remoto para CIFS
TCP	139	Sessão de serviço do NetBIOS para CIFS
TCP	161-162	Protocolo simples de gerenciamento de redes (SNMP)
TCP	443	Acesso da API REST do ONTAP ao endereço IP da LIF de gerenciamento de cluster ou de uma LIF de gerenciamento de SVM
TCP	445	Microsoft SMB/CIFS sobre TCP com enquadramento do NetBIOS
TCP	635	Montagem NFS
TCP	749	Kerberos
TCP	2049	Daemon do servidor NFS
TCP	3260	Acesso iSCSI por meio da LIF de dados do iSCSI
TCP	4045	Daemon de bloqueio NFS
TCP	4046	Monitor de status de rede para NFS
TCP	10000	Protocolo de gerenciamento de dados de rede (NDMP) e comunicação NetApp SnapMirror entre clusters
TCP	1104	Gerenciamento da comunicação NetApp SnapMirror entre clusters
TCP	11105	SnapMirror transferência de dados usando LIFs entre clusters

Protocolo	Portas	Função
UDP	111	Chamada de procedimento remoto para NFS
UDP	135	Chamada de procedimento remoto para CIFS
UDP	137	Resolução de nomes do NetBIOS para CIFS
UDP	139	Sessão de serviço do NetBIOS para CIFS
UDP	161-162	Protocolo simples de gerenciamento de redes (SNMP)
UDP	635	Montagem NFS
UDP	2049	Daemon do servidor NFS
UDP	4045	Daemon de bloqueio NFS
UDP	4046	Monitor de status de rede para NFS
UDP	4049	Protocolo de cota NFS

8. Adicione o grupo de segurança à interface de rede elástica do sistema de arquivos.

Proibir acesso a um sistema de arquivos

Para impedir temporariamente o acesso de todos os clientes à rede ao sistema de arquivos, você pode remover todos os grupos de segurança associados às interfaces de rede elástica do sistema de arquivos e substituí-los por um grupo que não tenha regras de entrada/saída.

Validação de conformidade do Amazon FSx for ONTAP NetApp

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte Referência dos Serviços Qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção 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)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno 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 com suporte e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.

- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Amazon FSx para NetApp ONTAP e endpoints de interface VPC ()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 VPC da Interface são alimentados por AWS PrivateLinkuma tecnologia que permite acessar de forma privada as APIs do Amazon FSx sem um gateway de internet, dispositivo NAT, conexão VPN ou conexão. 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 sua VPC e o Amazon FSx não sai da rede. 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 FSx para o sistema de arquivos ONTAP chamando a CreateFileSystem API de dentro da 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 diferentes Regiões da AWS.

O tráfego entre VPCs emparelhadas permanece na AWS rede e não atravessa a 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 VPC endpoint para a API Amazon FSx usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para obter mais informações, consulte Creating an interface VPC endpoint no Guia do usuário da Amazon VPC.

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.

Exceto Regiões da AWS na China, se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para o Amazon FSx com o VPC endpoint usando seu nome DNS padrão para o, por exemplo. Região da AWS`fsx.us-east-1.amazonaws.com` Para a China (Pequim) e a China (Ningxia) Regiões da AWS, você pode fazer solicitações de API com o VPC endpoint `fsx-api.cn-north-1.amazonaws.com.cn` usando `fsx-api.cn-northwest-1.amazonaws.com.cn` e, 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 o acesso à API Amazon FSx, você pode anexar uma política AWS Identity and Access Management (IAM) ao seu VPC endpoint. 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 mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Resiliência no Amazon NetApp FSx for ONTAP

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o Amazon FSx oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Backup e restauração

O Amazon FSx cria e salva backups automatizados dos volumes em seu sistema de arquivos Amazon FSx for NetApp ONTAP. O Amazon FSx cria backups automatizados de seus volumes durante a janela de backup do seu sistema de arquivos Amazon FSx for NetApp ONTAP. O Amazon FSx salva os backups automatizados dos volumes de acordo com o período de retenção de backup especificado. Também é possível fazer backup dos volumes manualmente, criando um backup iniciado pelo usuário. Você restaura um backup de volume a qualquer momento criando um novo volume com o backup especificado como origem.

Para ter mais informações, consulte Trabalhar com backups.

Snapshots

O Amazon FSx cria cópias instantâneas do Amazon FSx para volumes ONTAP. NetApp Esses snapshots oferecem proteção contra exclusão ou modificação acidental de arquivos em seus volumes pelos usuários finais. Para ter mais informações, consulte Trabalhar com snapshots.

Zonas de disponibilidade

Os sistemas de arquivos Amazon FSx for NetApp ONTAP foram projetados para fornecer disponibilidade contínua aos dados, mesmo no caso de uma falha no servidor. Cada sistema de arquivos é alimentado por dois servidores de arquivos em pelo menos uma zona de disponibilidade, cada um com seu próprio armazenamento. O Amazon FSx replica automaticamente seus dados para protegê-los contra falhas de componentes, monitora continuamente as falhas de hardware e substitui automaticamente os componentes da infraestrutura em caso de falha. Os sistemas de arquivos são alternados automaticamente conforme necessário (normalmente em 60 segundos), e os clientes também são alternados automaticamente com o sistema de arquivos.

Sistemas de arquivos multi-AZ

Os sistemas de arquivos Amazon FSx for NetApp ONTAP são altamente disponíveis e duráveis em todas as zonas de AWS disponibilidade e são projetados para fornecer disponibilidade contínua aos dados, mesmo no caso de uma zona de disponibilidade não estar disponível.

Para ter mais informações, consulte Disponibilidade e durabilidade.

Sistemas de arquivos com uma única AZ

Os sistemas de arquivos Amazon FSx for NetApp ONTAP são altamente disponíveis e duráveis em uma única zona de AWS disponibilidade e foram projetados para fornecer disponibilidade contínua dentro dessa zona de disponibilidade no caso de falha de um servidor de arquivos ou disco individual.

Para ter mais informações, consulte Disponibilidade e durabilidade.

Segurança da infraestrutura no Amazon FSx for ONTAP NetApp

Como um serviço gerenciado, o Amazon FSx for NetApp ONTAP é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Amazon FSx pela rede. Os clientes devem ser compatíveis com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com Perfect Forward Secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, suporta 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. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Use NetApp ONTAP Vscan com FSx para ONTAP

Você pode usar o recurso Vscan do NetApp ONTAP para executar software antivírus de terceiros compatível. Para obter mais informações, consulte os seguintes recursos para cada uma das soluções com suporte:

- McAfee — Guia de soluções antivírus para dados em cluster ONTAP: McAfee
- SentinelOne — Soluções de parceiros Vscan e SentinelOne Singularity Cloud Data Security
- Symantec — soluções parceiras da Vscan e Symantec Protection Engine
- Trend Micro: Guia de soluções antivírus para dados clusterizados ONTAP: Trend Micro

Funções e usuários no Amazon FSx for ONTAP NetApp

NetApp ONTAPinclui um recurso robusto e extensível de controle de acesso baseado em funções (RBAC). ONTAPas funções definem os recursos e privilégios do usuário ao usar a ONTAP CLI e a API REST. Cada função define um nível diferente de recursos e privilégios administrativos. Você atribui funções aos usuários com a finalidade de controlar seu acesso aos recursos do FSx for ONTAP ao usar a API ONTAP REST e a CLI. Há ONTAP funções disponíveis separadamente para FSx para usuários do sistema de arquivos ONTAP e usuários de máquinas virtuais de armazenamento (SVM).

Quando você cria um FSx para o sistema de arquivos ONTAP, um ONTAP usuário padrão é criado no nível do sistema de arquivos e no nível do SVM. Você pode criar usuários adicionais do sistema de arquivos e do SVM, além de criar funções adicionais do SVM para atender às necessidades da sua organização. Este capítulo explica ONTAP usuários e funções e fornece procedimentos detalhados para criar usuários adicionais e funções de SVM.

Funções e usuários do administrador do sistema de arquivos

O usuário padrão do sistema de ONTAP arquivos é`fsxadmin`, que tem a `fsxadmin` função atribuída a ele. Há duas funções predefinidas que você pode atribuir aos usuários do sistema de arquivos, listadas a seguir:

- **`fsxadmin`**—Os administradores com essa função têm direitos irrestritos no sistema. ONTAP Eles podem configurar todos os recursos do sistema de arquivos e do SVM disponíveis no FSx para sistemas de arquivos ONTAP.
- **`fsxadmin-readonly`**—Os administradores com essa função podem ver tudo no nível do sistema de arquivos, mas não podem fazer nenhuma alteração.

  Essa função é adequada para uso com aplicativos de monitoramento, por exemplo, NetApp Harvest porque ela tem acesso somente para leitura a todos os recursos disponíveis e suas propriedades, mas não pode fazer nenhuma alteração neles.

Você pode criar usuários adicionais do sistema de arquivos e atribuir a eles a `fsxadmin-readonly` função `fsxadmin` ou. Você não pode criar novas funções nem modificar as funções existentes. Para ter mais informações, consulte Criação de novos ONTAP usuários para administração do sistema de arquivos e do SVM.

A tabela a seguir descreve o nível de acesso que as funções de administrador do sistema de arquivos têm aos comandos e diretórios de comandos da ONTAP CLI e da API REST.

Nome do perfil	Nível de acesso	Para os seguintes comandos ou diretórios de comandos
`fsxadmin`	tudo	Todos os diretórios de comando disponíveis no FSx for ONTAP
`fsxadmin-readonly`	tudo	`security login password` Somente para gerenciar sua própria conta de usuário, senha local e informações importantes.

Nome do perfil	Nível de acesso	Para os seguintes comandos ou diretórios de comandos
	nenhuma	`security`
	somente leitura	Todos os outros diretórios de comando disponíveis no FSx for ONTAP

Funções e usuários do administrador do SVM

Cada SVM tem um domínio de autenticação separado e pode ser gerenciado de forma independente por seus próprios administradores. Para cada SVM em seu sistema de arquivos, o usuário padrão é vsadmin, que tem a `vsadmin` função atribuída por padrão. Além da `vsadmin` função, há outras funções predefinidas do SVM que fornecem permissões com escopo reduzido que você pode atribuir aos usuários do SVM. Você também pode criar funções personalizadas que forneçam o nível de controle de acesso que atenda às necessidades da sua organização.

As funções predefinidas para administradores de SVM e seus recursos são as seguintes:

Nome do perfil	Capacidades
`vsadmin`	• Gerenciar sua conta de usuário, senha local e informações importantes • Gerenciar volumes, exceto movimentações de volume • Gerenciar cotas, qtrees, cópias de snapshots e arquivos • Gerenciar LUNs • Execute SnapLock operações, exceto para exclusão privilegiada • Configurar protocolos: NFS, SMB e iSCSI • Configurar serviços: DNS, LDAP e NIS • Monitorar trabalhos

Nome do perfil	Capacidades
	• Monitorar as conexões de rede e a interface de rede • Monitorar a integridade da SVM
`vsadmin-volume`	• Gerenciar sua conta de usuário, senha local e informações importantes • Gerenciar volumes, incluindo movimentos de volume • Gerenciar cotas, qtrees, cópias de snapshots e arquivos • Gerenciar LUNs • Configurar protocolos: NFS, SMB e iSCSI • Configurar serviços: DNS, LDAP e NIS • Monitorar a interface de rede. • Monitorar a integridade da SVM
`vsadmin-protocol`	• Gerenciar sua conta de usuário, senha local e informações importantes • Gerenciar LUNs • Configurar protocolos: NFS, SMB e iSCSI • Configurar serviços: DNS, LDAP e NIS • Monitorar a interface de rede. • Monitorar a integridade da SVM
`vsadmin-backup`	• Gerenciar sua conta de usuário, senha local e informações importantes • Gerenciar operações NDMP • Tornar um volume restaurado em leitura/gravação • Gerencie SnapMirror relacionamentos e cópias de instantâneos • Visualizar volumes e informações de rede

Nome do perfil	Capacidades
`vsadmin-snaplock`	• Gerenciar sua conta de usuário, senha local e informações importantes • Gerenciar volumes, exceto movimentações de volume • Gerenciar cotas, qtrees, cópias de snapshots e arquivos • Execute SnapLock operações, incluindo exclusão privilegiada • Configurar protocolos: NFS e SMB • Configurar serviços: DNS, LDAP e NIS • Monitorar trabalhos • Monitorar as conexões de rede e a interface de rede
`vsadmin-readonly`	• Gerenciar sua conta de usuário, senha local e informações importantes • Monitorar a integridade da SVM • Monitorar a interface de rede. • Visualizar volumes e LUNs • Visualizar serviços e protocolos

Para obter mais informações sobre como criar uma nova função SVM, consulteCriação de uma nova função SVM.

Usando o Active Directory para autenticar ONTAP usuários

Você pode autenticar o acesso dos usuários do domínio Windows Active Directory a um FSx para sistema de arquivos ONTAP e SVM. Você deve executar as seguintes tarefas para que as contas do Active Directory possam acessar seu sistema de arquivos:

- Você precisa configurar o acesso do controlador de domínio do Active Directory ao SVM.

O SVM que você usa para configurar como gateway ou túnel para acesso ao controlador de domínio do Active Directory deve ter o CIFS habilitado, estar associado a um Active Directory ou ambos. Se você não estiver habilitando o CIFS e somente unindo o SVM do túnel a um Active Directory, certifique-se de que o SVM esteja associado ao seu Active Directory. Para ter mais informações, consulte Junção de SVMs com um Microsoft Active Directory.

- Você precisa habilitar uma conta de usuário de domínio do Active Directory para acessar o sistema de arquivos.

  Você pode usar a autenticação por senha ou a autenticação de chave pública SSH para usuários de domínio do Windows que acessam a ONTAP CLI ou a API REST.

Para obter os procedimentos que descrevem como usar para configurar a autenticação do Active Directory para administradores de sistemas de arquivos e SVM, consulte. Configurando a autenticação do Active Directory para ONTAP usuários

Criação de novos ONTAP usuários para administração do sistema de arquivos e do SVM

Cada ONTAP usuário está associado a uma SVM ou ao sistema de arquivos. Os usuários do sistema de arquivos com a `fsxadmin` função podem criar novas funções e usuários do SVM usando o comando `security login create`ONTAPCLI.

O `security login create` comando cria um método de login para o utilitário de gerenciamento. Um método de login consiste em um nome de usuário, um aplicativo (método de acesso) e um método de autenticação. Um nome de usuário pode ser associado a vários aplicativos. Opcionalmente, ele pode incluir um nome de função de controle de acesso. Se um nome de grupo do Active Directory, LDAP ou NIS for usado, o método de login concederá acesso aos usuários pertencentes ao grupo especificado. Se o usuário for membro de vários grupos provisionados na tabela de login de segurança, ele terá acesso a uma lista combinada dos comandos autorizados para os grupos individuais.

Para obter informações que descrevem como criar um novo ONTAP usuário, consulteCriando um novo usuário ONTAP.

Tópicos

- Criando um novo usuário ONTAP
- Criação de uma nova função SVM

- Configurando a autenticação do Active Directory para ONTAP usuários
- Como configurar a autenticação de chave pública
- Atualização dos requisitos de senha para funções de sistema de arquivos e SVM
- Falha na atualização fsxadmin da senha da conta

Criando um novo usuário ONTAP

Para criar um novo SVM ou usuário do sistema de arquivos (ONTAPCLI)

Somente usuários do sistema de arquivos com a `fsxadmin` função podem criar novos usuários do SVM e do sistema de arquivos.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Use o comando `security login create` ONTAP CLI para criar uma nova conta de usuário em seu FSx para sistema de arquivos ONTAP ou SVM.

   Insira seus dados para os espaços reservados no exemplo para definir as seguintes propriedades obrigatórias:

   - `-vserver`— Especifica o nome do SVM em que você deseja criar a nova função ou usuário do SVM. Se você estiver criando uma função ou usuário do sistema de arquivos, não especifique uma SVM.
   - `-user-or-group-name`— Especifica o nome de usuário ou o nome do grupo do Active Directory do método de login. O nome do grupo do Active Directory só pode ser especificado com o método de `domain` autenticação `ontapi` e os `ssh` aplicativos e.
   - `-application`— Especifica a aplicação do método de login. Os valores possíveis incluem http, ontapi e ssh.
   - `-authentication-method`— Especifica o método de autenticação para login. Os valores possíveis incluem o seguinte:

  - domínio — Use para autenticação do Active Directory
  - senha — Use para autenticação por senha
  - publickey — Usuário para autenticação de chave pública
- `-role`— Especifica o nome da função de controle de acesso para o método de login. No nível do sistema de arquivos, o único perfilo que pode ser especificada é `fsxadmin`.

(Opcional) Você também pode usar um ou mais dos seguintes parâmetros com o comando:

- `[-comment]`— Use para incluir uma anotação ou comentário para a conta do usuário. Por exemplo, **`Guest account`**. O tamanho máximo é 128 caracteres.
- `[-second-authentication-method {none|publickey|password|nsswitch}]`: especifica o método de autenticação de segundo fator. Você pode especificar os seguintes métodos:
  - senha — Use para autenticação por senha
  - publickey — Use para autenticação de chave pública
  - nsswitch — Use para autenticação NIS ou LDAP
  - none — O valor padrão se você não especificar um

```
Fsx0123456::> security login create -vserver vserver_name -user-or-group-
name user_or_group_name -application login_application -authentication-
method auth_method -role role_or_account_name
```

O comando a seguir cria um novo usuário do sistema de arquivos `new_fsxadmin` com a `fsxadmin-readonly` função atribuída, usando SSH com uma senha para fazer login. Quando solicitado, forneça uma senha para o usuário.

```
Fsx0123456::> security login create -user-or-group-name new_fsxadmin -application
 ssh -authentication-method password -role fsxadmin-readonly

Please enter a password for user 'new_fsxadmin':
Please enter it again:

Fsx0123456::>
```

3. O comando a seguir cria um novo usuário SVM `new_vsadmin` no `fsx` SVM com a `vsadmin_readonly` função, configurado para usar SSH com uma senha para fazer login. Quando solicitado, forneça uma senha para o usuário.

```
Fsx0123456::> security login create -vserver fsx  -user-or-group-name new_vsadmin -
application ssh -authentication-method password -role vsadmin-readonly

Please enter a password for user 'new_vsadmin':
Please enter it again:

Fsx0123456::>
```

4. O comando a seguir cria um novo usuário do sistema de arquivos somente para leitura `harvest2-user` que deve ser usado pelo aplicativo NetApp Harvest para coletar métricas de desempenho e capacidade. Para ter mais informações, consulte Monitorar sistemas de arquivos do FSx para ONTAP usando Harvest e Grafana.

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application
 ssh -role fsxadmin-readonly -authentication-method password
```

Para visualizar as informações de todos os usuários do sistema de arquivos e do SVM

- Use o comando a seguir para visualizar todas as informações de login do seu sistema de arquivos e SVMs.

```
Fsx0123456::> security login show

Vserver: Fsx0123456
                                                                  Second
User/Group                Authentication                 Acct   Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------ --------------
autosupport    console     password      autosupport      no     none
fsxadmin       http        password      fsxadmin         no     none
fsxadmin       ontapi      password      fsxadmin         no     none
fsxadmin       ssh         password      fsxadmin         no     none
fsxadmin       ssh         publickey     fsxadmin         -      none
new_fsxadmin   ssh         password      fsxadmin-readonly
                                                        no     none
```

```
Vserver: fsx
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------- ---------------- ------ --------------
new_vsadmin    ssh          password      vsadmin-readonly no     none
vsadmin        http         password      vsadmin          yes    none
vsadmin        ontapi       password      vsadmin          yes    none
vsadmin        ssh          password      vsadmin          yes    none
10 entries were displayed.

Fsx0123456::>
```

Criação de uma nova função SVM

Cada SVM que você cria tem um administrador de SVM padrão que tem a função `vsadmin` predefinida atribuída. Além do conjunto de funções de SVM predefinidas, você pode criar novas funções de SVM. Se você precisar criar novas funções para sua SVM, use o comando `security login role create` ONTAP CLI. Esse comando está disponível para administradores de sistemas de arquivos com a `fsxadmin` função.

Para criar uma nova função SVM (ONTAP CLI)

1. Você pode criar uma nova função SVM usando o `security login role create` ONTAP CLI comando:

   ```
   Fsx0123456::> security login role create -role vol_role -cmddirname volume
   ```

2. Especifique os seguintes parâmetros obrigatórios no comando:

   - `-role`: o nome do perfil.
   - `-cmddirname`: o comando ou diretório de comando ao qual o perfil fornece acesso. Coloque entre aspas duplas os nomes dos subdiretórios de comandos. Por exemplo, `"volume snapshot"`. Digite `DEFAULT` para especificar todos os diretórios de comando.

3. (Opcional) Você também pode adicionar qualquer um dos seguintes parâmetros ao comando:

   - `-vserver`: o nome da SVM que está associada ao perfil.
   - `-access`: o nível de acesso do perfil. Para diretórios de comandos, isso inclui:

- `none`: nega o acesso aos comandos do diretório. Este é o valor padrão dos perfis personalizados.
- `readonly`: concede acesso aos comandos show no diretório de comandos e nos subdiretórios.
- `all`: concede acesso a todos os comandos no diretório de comandos e nos subdiretórios. Para conceder ou negar acesso aos comandos intrínsecos, especifique o diretório de comandos.

Para comandos não intrínsecos (comandos que não terminam com `create`, `modify`, `delete` ou `show`):

- `none`: nega o acesso aos comandos do diretório. Este é o valor padrão dos perfis personalizados.
- `readonly`: não aplicável. Não use:
- `all`: concede acesso ao comando.

- `-query`: o objeto de consulta usado para filtrar o nível de acesso, que é especificado na forma de opção válida para o comando ou para um comando no diretório de comandos. Coloque entre aspas duplas o objeto de consulta.

4. Execute o comando `security login role create`.

O comando a seguir cria uma função de controle de acesso chamada “admin” para o Vserver vs1.example.com. A função tem todo o acesso ao comando “volume”, mas somente dentro do agregado “aggr0".

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-
aggr aggr0" -access all -vserver vs1.example.com
```

Configurando a autenticação do Active Directory para ONTAP usuários

Use a ONTAP CLI para configurar o uso da autenticação do Active Directory para usuários do sistema de ONTAP arquivos e do SVM.

Você deve ser um administrador do sistema de arquivos com a `fsxadmin` função de usar os comandos neste procedimento.

Para configurar a autenticação do Active Directory para ONTAP usuários (ONTAPCLI)

Os comandos desse procedimento estão disponíveis para usuários do sistema de arquivos com a `fsxadmin` função.

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. Use o `security login domain-tunnel create`comando conforme mostrado para estabelecer um túnel de domínio para autenticar usuários do Windows Active Directory. Substitua *`svm_name`* pelo nome do SVM que você está usando para o túnel do domínio.

   ```
   FsxId0123456::> security login domain-tunnel create -vserver svm_name
   ```

3. Use o `security login create`comando para criar contas de usuário de domínio do Active Directory que acessarão o sistema de arquivos.

   Especifique os seguintes parâmetros obrigatórios no comando:

   - `-vserver`— O nome do SVM configurado com o CIFS e associado ao seu Active Directory. Ele será usado como túnel para autenticar os usuários do domínio do Active Directory no sistema de arquivos, no qual a nova função ou usuário será criado.
   - `-user-or-group-name`: o nome de usuário ou nome do grupo do Active Directory do método de login. O nome do grupo do Active Directory só pode ser especificado com o método de autenticação `domain` e as aplicações `ontapi` e `ssh`.
   - `-application`: a aplicação do método de login. Os valores possíveis incluem http, ontapi e ssh.
   - `-authentication-method`— O método de autenticação usado para login. Os valores possíveis incluem o seguinte:
     - domínio — para autenticação do Active Directory
     - senha — para autenticação por senha
     - publickey — para autenticação de chave pública

- `-role`: o nome do perfil de controle de acesso para o método de login. No nível do sistema de arquivos, o único perfilo que pode ser especificada é `-role fsxadmin`.

O exemplo a seguir cria uma conta de usuário de domínio do Active Directory `CORP\Admin` para o sistema de `filesystem1` arquivos.

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
application ssh -authmethod domain -role fsxadmin
```

O exemplo a seguir cria a conta de `CORP\Admin` usuário com autenticação de chave pública.

```
FsxId0123456ab::> security login create -user-or-group-name "CORP\Admin" -
application ssh -authentication-method publickey -role fsxadmin
Warning: To use public-key authentication, you must create a public key for user
 "CORP\Admin".
```

Crie uma chave pública para o `CORP\Admin` usuário usando o seguinte comando:

```
FsxId0123456ab::> security login publickey create -username "CORP
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=
 cwaltham@b0be837a91bf.ant.amazon.com"
```

Para fazer login no sistema de arquivos usando SSH com credenciais do Active Directory

- O exemplo a seguir demonstra como efetuar SSH no sistema de arquivos com as credenciais do Active Directory, se você escolher `ssh` para o tipo `-application`. O `username` está no formato `"domain-name\user-name"`, que é o nome do domínio e o nome de usuário que você forneceu ao criar a conta, separados por uma barra invertida e entre aspas.

```
Fsx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
```

Quando solicitado a digitar uma senha, use a senha do usuário do Active Directory.

Como configurar a autenticação de chave pública

Para habilitar a autenticação de chave pública SSH, você deve primeiro gerar uma chave SSH e associá-la a uma conta de administrador usando o comando `security login publickey create`. Isso permite que a conta acesse a SVM. O comando `security login publickey create` aceita os seguintes parâmetros:

Parâmetro	Descrição
`-vserver` (Opcional)	O nome da SVM que a conta acessa. Se você estiver configurando a autenticação de chave pública SSH para usuários do sistema de arquivos, não inclua. `-versver`
`-username`	O nome de usuário da conta. O valor padrão, `admin`, é o nome padrão do administrador do cluster.
`-index`	O número de índice da chave pública. O valor padrão será 0 se a chave for a primeira criada para a conta. Caso contrário, o valor padrão será um a mais do que o maior número de índice existente para a conta.
`-publickey`	A chave pública OpenSSH. Coloque a chave entre aspas duplas.
`-role`	O perfil de controle de acesso atribuído à conta.
`-comment` (Opcional)	Texto descritivo da chave pública. Coloque o texto entre aspas duplas.

O exemplo a seguir associa uma chave pública à conta de administrador `svmadmin` da SVM `svm01`. A chave pública recebe o número de índice 5.

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J/
```

```
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

> **Important**
>
> Você deve ser administrador da SVM ou do sistema de arquivos para executar essa tarefa.

Atualização dos requisitos de senha para funções de sistema de arquivos e SVM

Você pode atualizar os requisitos de senha para uma função de sistema de arquivos ou SVM usando o comando `security login role config modify`ONTAPCLI. Esse comando só está disponível para contas de administrador do sistema de arquivos com a `fsxadmin` função. Ao modificar os requisitos de senha, o sistema avisará se há algum usuário existente com essa função que será afetado pela alteração.

O exemplo a seguir modifica o requisito de tamanho mínimo da senha para 12 caracteres para usuários com a `vsadmin-readonly` função no `fsx` SVM. Neste exemplo, existem usuários existentes com essa função.

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

O sistema exibe o seguinte aviso devido aos usuários existentes:

```
Warning: User accounts with this role exist. Modifications to the username/password
 restrictions on this role could result in non-compliant user
         accounts.
Do you want to continue? {y|n}:

FsxId0123456::>
```

Falha na atualização **fsxadmin** da senha da conta

Ao atualizar a senha do `fsxadmin` usuário, você pode receber um erro se ela não atender aos requisitos de senha definidos no sistema de arquivos. Você pode ver os requisitos de senha usando o comando da `security login role config show` ONTAP CLI ou da API REST.

Para visualizar os requisitos de senha para uma função de sistema de arquivos ou SVM

1. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

2. O `security login role config show` comando retorna os requisitos de senha para uma função de sistema de arquivos ou SVM.

   ```
   FsxId0123456::> security login role config show -role fsxadmin -
   fields password_requirement_fields
   ```

   Para o `-fields` parâmetro, especifique um ou todos os itens a seguir:

   - `passwd-minlength`: o tamanho mínimo da senha.
   - `passwd-min-special-chars`: o número mínimo de caracteres especiais na senha.
   - `passwd-min-lowercase-chars`: o número mínimo de letras minúsculas na senha.
   - `passwd-min-uppercase-chars`: o número mínimo de letras maiúsculas na senha.
   - `passwd-min-digits`: o número mínimo de dígitos na senha.
   - `passwd-alphanum`: informações sobre inclusão ou exclusão de caracteres alfanuméricos.
   - `passwd-expiry-time`: a data de validade da senha.
   - `passwd-expiry-warn-time`: o tempo do aviso de validade da senha.

3. Execute o comando a seguir para ver todos os requisitos de senha:

   ```
   FsxId0123456::> security login role config show -role fsxadmin -fields passwd-
   minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
   ```

```
digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
uppercase-chars

vserver                role     passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
---------------------- -------- ---------------- ---------------
 ------------------------ ------------------ --------------------------
 -------------------------- ------------------ ----------------------
FsxId0123456           fsxadmin 3                enabled         0
       unlimited          0                        0                        0
               unlimited
```

Migração para o Amazon NetApp FSx for ONTAP

As seções a seguir fornecem informações sobre como migrar seus sistemas de arquivos NetApp ONTAP existentes para o Amazon FSx for ONTAP. NetApp

> **Note**
>
> Se você planeja usar a política de divisão em níveis `All` para migrar seus dados para o nível do grupo de capacidade, tenha em mente que os metadados do arquivo são sempre armazenados no nível SSD e que todos os novos dados do usuário são gravados primeiro no nível SSD. Quando os dados são gravados no nível SSD, o processo de divisão em níveis em segundo plano começa a dividir seus dados no armazenamento do grupo de capacidade, mas esse processo não é imediato e consome recursos da rede. É necessário dimensionar seu nível SSD para contabilizar os metadados do arquivo (de 3 a 7% do tamanho dos dados do usuário), como um buffer para os dados do usuário, antes de serem divididos em níveis no armazenamento do grupo de capacidade. Recomendamos que não exceda 80% de utilização do nível SSD.
> Ao migrar dados, monitore sua camada de SSD usando métricas do sistema de CloudWatch arquivos para garantir que ela não seja preenchida mais rápido do que o processo de hierarquização pode mover os dados para o armazenamento do pool de capacidade.

Tópicos

- Migrando para FSx for ONTAP usando NetApp SnapMirror
- Como migrar para o FSx para ONTAP usando o AWS DataSync

Migrando para FSx for ONTAP usando NetApp SnapMirror

Você pode migrar seus sistemas de arquivos NetApp ONTAP para o Amazon FSx for ONTAP usando. NetApp NetApp SnapMirror

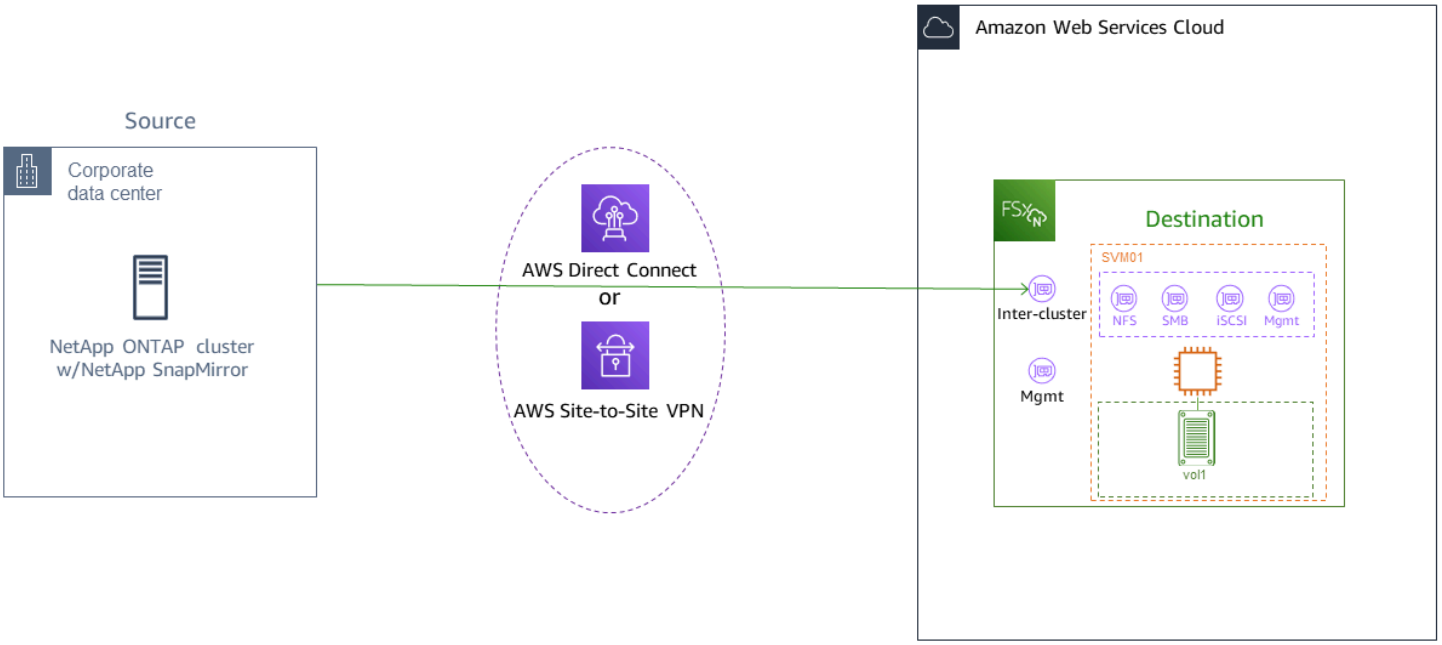
NetApp SnapMirror emprega replicação em nível de bloco entre dois sistemas de arquivos ONTAP, replicando dados de um volume de origem especificado para um volume de destino. Recomendamos usar SnapMirror para migrar sistemas de arquivos NetApp ONTAP locais para FSx for ONTAP. NetApp SnapMirrorA replicação em nível de bloco é rápida e eficiente até mesmo para sistemas de arquivos com:

- Estruturas complexas de diretórios
- Mais de 50 milhões de arquivos
- Arquivos muito pequenos (da ordem de kilobytes)

Quando você costuma migrar SnapMirror para o FSx for ONTAP, os dados desduplicados e compactados permanecem nesses estados, o que reduz os tempos de transferência e reduz a quantidade de largura de banda necessária para a migração. Os snapshots que existem nos volumes do ONTAP de origem são preservados quando migrados para os volumes de destino. A migração de seus sistemas de arquivos NetApp ONTAP locais para o FSx for ONTAP envolve as seguintes tarefas de alto nível:

1. Criar o volume de destino no Amazon FSx.
2. Reunir interfaces lógicas (LIFs) de origem e destino.
3. Estabelecer o emparelhamento de cluster entre os sistemas de arquivos de origem e destino.
4. Criar um relacionamento de emparelhamento com a SVM.
5. Crie o SnapMirror relacionamento.
6. Manter um cluster de destino atualizado.
7. Substituição para o sistema de arquivos do FSx para ONTAP.

O diagrama a seguir ilustra o cenário de migração descrito nesta seção.



Tópicos

Antes de começar

Antes de começar a usar os procedimentos descritos nas próximas seções, verifique se você atende aos pré-requisitos a seguir.

- O FSx para ONTAP prioriza o tráfego do cliente em relação às tarefas em segundo plano, incluindo divisão de dados em níveis, eficiência do armazenamento e backups. Ao migrar dados, e como prática recomendada geral, recomendamos que monitore a capacidade do nível SSD para garantir que não exceda 80% de utilização. Você pode monitorar a utilização do seu nível de SSD usando métricas do sistema de CloudWatch arquivos. Para ter mais informações, consulte Métricas de volume.
- Se você definir a política de divisão de dados em níveis do volume de destino para `All` ao migrar seus dados, todos os metadados do arquivo serão armazenados no nível de armazenamento SSD principal. Os metadados do arquivo são sempre armazenados no nível SSD principal, independentemente da política de divisão de dados em níveis do volume. Recomendamos assumir uma proporção de 1 : 10 para o nível principal : capacidade de armazenamento do nível do grupo de capacidade.
- Os sistemas de arquivos de origem e destino estão conectados na mesma VPC ou em redes emparelhadas usando emparelhamento da Amazon VPC, Transit Gateway, AWS Direct Connect ou AWS VPN. Para obter mais informações, consulte Acessando dados de dentro AWS e O que é emparelhamento de VPC? no Guia de emparelhamento da Amazon VPC.
- O grupo de segurança da VPC do sistema de arquivos do FSx para ONTAP tem regras de entrada e saída que permitem ICMP e TCP nas portas 443, 10000, 11104 e 11105 para os endpoints entre clusters (LIFs).

- Verifique se os volumes de origem e destino estão executando versões compatíveis do NetApp ONTAP antes de criar uma relação de proteção de SnapMirror dados. Para obter mais informações, consulte Versões compatíveis do ONTAP para SnapMirror relacionamentos na documentação do usuário NetApp do ONTAP. Os procedimentos apresentados aqui usam um sistema de arquivos NetApp ONTAP local para a fonte.
- Seu sistema de arquivos NetApp ONTAP local (de origem) inclui uma SnapMirror licença.
- Você criou um sistema de arquivos de destino do FSx para ONTAP com uma SVM, mas não um volume de destino. Para ter mais informações, consulte Como criar sistemas de arquivos do FSx para ONTAP.

Os comandos nesses procedimentos usam os aliases de cluster, SVM e volume a seguir.

- *FSx-Dest*— o ID do cluster de destino (FSx) (no formato F Sxldabcdef 1234567890a).
- *OnPrem-Source*: o ID do cluster de origem.
- *DestSVM*: o nome da SVM de destino.
- *SourceSVM*: o nome da SVM de origem.
- O nome do volume de origem e o de destino é `vol1`.

> **Note**
>
> Um sistema de arquivos do FSx para ONTAP é chamado de cluster em todos os comandos de CLI do ONTAP.

Os procedimentos nesta seção usam os seguintes comandos da CLI do NetApp ONTAP.

- comando volume create
- comandos cluster
- comandos vserver peer
- comandos snapmirror

Você usará a CLI do NetApp ONTAP para criar e gerenciar SnapMirror uma configuração em seu sistema de arquivos FSx for ONTAP. Para ter mais informações, consulte Usar a CLI do NetApp ONTAP.

Criar o volume de destino

Você pode criar um volume de destino de proteção de dados (DP) usando o console Amazon FSx, AWS CLI o e a API Amazon FSx, além da CLI e da API REST do NetApp ONTAP. Para obter informações sobre como criar um volume de destino usando o console do Amazon FSx e a AWS CLI, consulte Criação de volumes.

No procedimento a seguir, você usará a CLI do NetApp ONTAP para criar um volume de destino em seu sistema de arquivos FSx for ONTAP. Você precisará da senha de `fsxadmin` e do endereço IP ou nome DNS da porta de gerenciamento do sistema de arquivos.

1. Estabeleça uma sessão SSH com o sistema de arquivos de destino utilizando o usuário e a senha de `fsxadmin` definidos ao criar o sistema de arquivos.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Crie um volume no cluster de destino que tenha uma capacidade de armazenamento que seja, no mínimo, igual à capacidade de armazenamento do volume de origem. Use `-type DP` para designá-lo como destino para um SnapMirror relacionamento.

   Se você planeja usar a divisão de dados em níveis, recomendamos que defina a `-tiering-policy` como `all`. Isso garante que seus dados sejam imediatamente transferidos para o armazenamento do grupo de capacidade e evita que você fique sem capacidade no nível SSD. Após a migração, você pode mudar a `-tiering-policy` para `auto`.

   > **Note**
   >
   > Os metadados do arquivo são sempre armazenados no nível SSD principal, independentemente da política de divisão de dados em níveis do volume.

   ```
   FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
   type DP -tiering-policy all
   ```

Registrar as LIFs entre clusters de origem e destino

SnapMirror usa interfaces lógicas entre clusters (LIFs), cada uma com um endereço IP exclusivo, para facilitar a transferência de dados entre os clusters de origem e de destino.

1. Nos sistemas de arquivos de destino do FSx para ONTAP, você pode recuperar o os endereços IP do endpoint entre clusters do console do Amazon FSx navegando até a guia Administração na página de detalhes do sistema de arquivos.
2. Para o cluster NetApp ONTAP de origem, recupere os endereços IP LIF entre clusters usando a CLI ONTAP. Execute o seguinte comando:

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

> **Note**
>
> Para sistemas de arquivos escaláveis, há dois endereços IP entre clusters para cada par de alta disponibilidade (HA). Salve esses valores para mais tarde.

Salve os endereços IP `inter_1` e `inter_2`. Eles são referidos no `FSx-Dest` como `dest_inter_1` e `dest_inter_2` e em `OnPrem-Source` como `source_inter_1` e `source_inter_2`.

Estabelecer o emparelhamento de clusters entre a origem e o destino

Estabeleça uma relação entre pares de clusters no cluster de destino fornecendo os endereços IP entre clusters. Você também precisará criar uma senha que deverá ser inserida ao estabelecer o emparelhamento de clusters no cluster de origem.

1. Configure o peering no cluster de destino usando o comando a seguir. Para sistemas de arquivos escaláveis, você precisará fornecer cada endereço IP entre clusters.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
```

```
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. Em seguida, estabeleça o relacionamento entre pares do cluster no cluster de origem. Você precisará digitar a senha criada acima para se autenticar. Para sistemas de arquivos escaláveis, você precisará fornecer cada endereço IP entre clusters.

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. Verifique se o emparelhamento foi bem-sucedido usando o comando a seguir no cluster de origem. Na saída, `Availability` deve ser definida como `Available`.

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

Criar um relacionamento de emparelhamento entre SVMs

Com o emparelhamento de cluster estabelecido, a próxima etapa é emparelhar as SVMs. Crie um relacionamento de emparelhamento entre SVMs no cluster de destino (FSx-Dest) usando o comando `vserver peer`. Estes são os aliases adicionais usados nos comandos a seguir.

- `DestLocalName`: esse é o nome usado para identificar a SVM de destino ao configurar o emparelhamento entre SVMs na SVM de origem.
- `SourceLocalName`: esse é o nome usado para identificar a SVM de origem ao configurar o emparelhamento entre SVMs na SVM de destino.

1. Use o comando a seguir para criar um relacionamento de emparelhamento da SVM entre as SVMs de origem e de destino.

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName
```

```
 Info: [Job 207] 'vserver peer create' job queued
```

2. Aceite o relacionamento de emparelhamento no cluster de origem:

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. Verifique o status de emparelhamento da SVM usando o comando a seguir; `Peer State` deve ser definido como `peered` na resposta.

```
OnPrem-Source::> vserver peer show

Peer    Peer     Peer   Peering  Remote
vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------ ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

Crie o SnapMirror relacionamento

Agora que você emparelhou as SVMs de origem e destino, as próximas etapas são criar e inicializar o SnapMirror relacionamento no cluster de destino.

> **Note**
>
> Depois de criar e inicializar um SnapMirror relacionamento, os volumes de destino ficam somente para leitura até que o relacionamento seja interrompido.

- Use o `snapmirror create` comando para criar o SnapMirror relacionamento no cluster de destino. O comando `snapmirror create` deve ser usado na SVM de destino.

  Opcionalmente, você pode usar `-throttle` para definir a largura de banda máxima (em KB/s) para o relacionamento. SnapMirror

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
path DestSVM:vol1 -vserver DestSVM -throttle unlimited
```

```
Operation succeeded: snapmirror create for the relationship with destination
"DestSVM:vol1".
```

Transferir dados para o sistema de arquivos do FSx para ONTAP

Agora que você criou o SnapMirror relacionamento, você pode transferir dados para o sistema de arquivos de destino.

1. Você pode transferir dados para o sistema de arquivos de destino executando o comando a seguir no sistema de arquivos de destino.

   > **Note**
   >
   > Depois de executar esse comando, SnapMirror começa a transferir instantâneos de dados do volume de origem para o volume de destino.

   ```
   FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
   path SourceLocalName:vol1
   ```

2. Se estiver migrando dados que estão sendo usados ativamente, precisará atualizar seu cluster de destino para que permaneça sincronizado com o cluster de origem. Para executar uma atualização única no cluster de destino, execute o comando a seguir.

   ```
   FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
   ```

3. Você também pode programar atualizações de hora em hora ou diárias antes de concluir a migração e transferir seus clientes para o FSx para ONTAP. Você pode estabelecer um cronograma de SnapMirror atualização usando o `snapmirror modify`comando.

   ```
   FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
   ```

Substituição para o Amazon FSx

Prepare-se para a substituição pelo sistema de arquivos do FSx para ONTAP com os passos a seguir.

- Desconecte todos os clientes que gravam no cluster de origem.
- Execute uma SnapMirror transferência final para garantir que não haja perda de dados durante o recorte.
- Rompa o SnapMirror relacionamento.
- Conecte todos os clientes ao sistema de arquivos do FSx para ONTAP.

1. Para garantir que todos os dados do cluster de origem sejam transferidos para o sistema de arquivos do FSx para ONTAP, execute uma transferência final do Snapmirror.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. Certifique-se de que a migração dos dados esteja concluída verificando se o `Mirror State` está definido como `Snapmirrored` e se o `Relationship Status` está definido como `Idle`. Você também deve garantir que a data de `Last Transfer End Timestamp` seja a esperada, pois mostra quando ocorreu a última transferência para o volume de destino.
3. Execute o comando a seguir para mostrar o SnapMirror status.

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      ---------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. Desative quaisquer SnapMirror transferências futuras usando o `snapmirror quiesce` comando.

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. Verifique se o `Relationship Status` mudou para `Quiesced` usando `snapmirror show`.

```
FSx-Dest::> snapmirror show

Source           Destination   Mirror        Relationship
Path             Path          State         Status
-----------      ------------  ------------ --------
sourcesvm1:vol1  svm01:DestVol Snapmirrored  Quiesced
```

6. Durante a migração, o volume de destino é somente leitura. Para habilitar a leitura/gravação, você precisa romper o SnapMirror relacionamento e passar para o sistema de arquivos FSx for ONTAP. Quebre o SnapMirror relacionamento usando o comando a seguir.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. Depois que a SnapMirror replicação for concluída e você romper o SnapMirror relacionamento, você poderá montar o volume para disponibilizar os dados.

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

O volume já está disponível com os dados do volume de origem totalmente migrados para o volume de destino. O volume também está disponível para os clientes lerem e gravarem nele. Se você definiu anteriormente a `tiering-policy` desse volume como `all`, poderá alterá-la para `auto` ou `snapshot-only` e seus dados farão a transição automática entre os níveis de armazenamento de acordo com os padrões de acesso. Para tornar esses dados acessíveis a clientes e aplicações, consulte Acesso a dados do .

Como migrar para o FSx para ONTAP usando o AWS DataSync

Recomendamos usar o AWS DataSync para transferir dados entre os sistemas de arquivos do FSx para ONTAP e sistemas de arquivos que não sejam do ONTAP, incluindo FSx para Lustre, FSx para OpenZFS, FSx para Windows File Server, Amazon EFS, Amazon S3 e arquivadores on-premises. Se você estiver transferindo arquivos entre FSx for ONTAP NetApp e ONTAP, recomendamos usar. NetApp SnapMirror AWS DataSyncé 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 pela AWS Internet ou. AWS Direct Connect DataSync pode transferir dados e metadados do sistema de arquivos, como propriedade, registros de data e hora e permissões de acesso.

Você pode usar DataSync para transferir arquivos entre dois sistemas de arquivos FSx for ONTAP e também mover dados para um sistema de arquivos em uma conta ou diferenteRegião da AWS. AWS Você também pode usar DataSync com FSx for ONTAP sistemas de arquivos para outras tarefas. Por exemplo, você pode executar migrações de dados únicas, ingerir dados periodicamente para workloads distribuídas e programar a replicação para proteção e recuperação de dados.

Em DataSync, um local é um endpoint para um sistema de arquivos FSx for ONTAP. Para obter informações sobre cenários de transferência específicos, consulte Working with locations no Guia do usuário do AWS DataSync.

> **Note**
>
> Se você planeja usar a política de divisão em níveis `All` para migrar seus dados para o nível do grupo de capacidade, tenha em mente que os metadados do arquivo são sempre armazenados no nível SSD e que todos os novos dados do usuário são gravados primeiro no nível SSD. Quando os dados são gravados no nível SSD, o processo de divisão em níveis em segundo plano começa a dividir seus dados no armazenamento do grupo de capacidade, mas esse processo não é imediato e consome recursos da rede. É necessário dimensionar seu nível SSD para contabilizar os metadados do arquivo (de 3 a 7% do tamanho dos dados do usuário), como um buffer para os dados do usuário, antes de serem divididos em níveis no armazenamento do grupo de capacidade. Recomendamos que não exceda 80% de utilização do SSD.
> Ao migrar dados, monitore sua camada de SSD usando métricas do sistema de CloudWatch arquivos para garantir que ela não seja preenchida mais rápido do que o processo de hierarquização pode mover os dados para o armazenamento do pool de capacidade. Você também pode reduzir as DataSync transferências para uma taxa menor do que a taxa em que a hierarquização está ocorrendo para garantir que seu nível de SSD não exceda 80% de utilização. Por exemplo, em sistemas de arquivos com uma capacidade de throughput de, pelo menos, 512 MBps, um controle de utilização de 200 MBps normalmente equilibra as taxas de transferência de dados e de divisão de dados em níveis.

Pré-requisitos

Para migrar dados para a configuração do FSx for ONTAP, você precisa de um servidor e uma rede que atendam aos requisitos. DataSync Para saber mais, consulte os requisitos DataSync no Guia do AWS DataSync usuário.

Etapas básicas para migrar arquivos usando DataSync

A transferência de arquivos de uma origem para um destino usando DataSync envolve as seguintes etapas básicas:

- 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:

- Data transfer between self-managed storage and AWS
- Criação de um local para o Amazon FSx for ONTAP NetApp

Monitoramento do Amazon FSx para ONTAP NetApp

Você pode usar os seguintes serviços e ferramentas para monitorar o uso e a atividade do NetApp ONTAP no Amazon FSx:

- Amazon CloudWatch — Você pode monitorar sistemas de arquivos usando a Amazon CloudWatch, que coleta e processa automaticamente dados brutos do FSx for ONTAP em métricas legíveis. Essas estatísticas são retidas por um período de 15 meses para que seja possível acessar informações históricas e ver a performance do sistema de arquivos. Você também pode definir alarmes com base nas suas métricas ao longo de um período especificado e realizar uma ou mais ações com base no valor das métricas em relação aos limites definidos por você.
- Eventos do EMS do ONTAP: você pode monitorar o sistema de arquivos do FSx para ONTAP usando eventos gerados pelo Events Management System (EMS) do ONTAP. Os eventos do EMS são notificações de ocorrências no sistema de arquivos, como a criação de LUN de iSCSI ou o dimensionamento automático de volumes.
- NetApp Cloud Insights — Você pode monitorar as métricas de configuração, capacidade e desempenho de seus sistemas de arquivos FSx for ONTAP usando o serviço NetApp Cloud Insights. Você também pode criar alertas com base nas condições das métricas.
- NetApp Harvest e NetApp Grafana — Você pode monitorar seu sistema de arquivos FSx for ONTAP usando Harvest e Grafana. NetApp NetApp NetApp O Harvest monitora os sistemas de arquivos ONTAP coletando métricas de desempenho, capacidade e hardware do FSx para sistemas de arquivos ONTAP. O Grafana fornece um painel em que as métricas coletadas do Harvest podem ser exibidas.
- AWS CloudTrail— Você pode usar AWS CloudTrail para capturar todas as chamadas de API para o Amazon FSx como eventos. Esses eventos fornecem um registro de ações executadas por um usuário, um perfil ou um serviço da AWS no Amazon FSx.

Tópicos

- Registro em log de chamadas de API do FSx para ONTAP com AWS CloudTrail

Monitoramento com a Amazon CloudWatch

Você pode monitorar sistemas de arquivos usando a Amazon CloudWatch, que coleta e processa dados brutos do Amazon FSx NetApp for ONTAP em métricas legíveis e quase em tempo real. Essas estatísticas são retidas por um período de 15 meses para que seja possível acessar informações históricas a fim de determinar a performance do sistema de arquivos. Por padrão, os dados métricos do FSx for ONTAP são enviados automaticamente CloudWatch em períodos de 1 minuto. Para obter mais informações sobre CloudWatch, consulte O que é a Amazon CloudWatch? no Guia do CloudWatch usuário da Amazon.

> **Note**
>
> Por padrão, o FSx for ONTAP envia dados métricos para períodos de 1 minuto, exceto as seguintes métricas que são enviadas CloudWatch em intervalos de 5 minutos:
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch as métricas do FSx for ONTAP são organizadas em quatro categorias, que são definidas pelas dimensões usadas para consultar cada métrica. Para obter mais informações sobre dimensões, consulte Dimensões no Guia do CloudWatch usuário da Amazon.

- Métricas do sistema de arquivos: métricas de ile-system-level desempenho e capacidade de armazenamento F.
- Métricas detalhadas do sistema de arquivos: F métricas ile-system-level de armazenamento por nível de armazenamento (SSD e pool de capacidade).
- Métricas de volume: métricas de performance e capacidade de armazenamento por volume.
- Métricas detalhadas de volume: métricas de capacidade do armazenamento por volume pelo nível de armazenamento ou pelo tipo de dados (usuário, snapshot ou outro).

Todas as CloudWatch métricas do FSx for ONTAP são publicadas no namespace em. `AWS/FSx` CloudWatch

Tópicos

Como usar o FSx para métricas ONTAP CloudWatch

As CloudWatch métricas relatadas pelo Amazon FSx fornecem informações valiosas sobre seu FSx para sistemas de arquivos e volumes ONTAP.

Tópicos

Monitoramento de métricas do sistema de arquivos no console do Amazon FSx

Você pode usar o painel Monitoramento e performance, no painel do sistema de arquivos no console do Amazon FSx, para visualizar as métricas descritas na tabela a seguir. Para ter mais informações, consulte Acessando CloudWatch métricas.

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
Resumo	...determinar a quantidade da capacidade de armazenamento disponível no meu sistema de arquivos?	Capacidade de armazenamento principal disponível (bytes)	`StorageCapacity {SSD} - StorageUsed {SSD}`

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
	...determinar o throughput total do cliente do meu sistema de arquivos?	Throughput total do cliente (bytes por segundo)	SOMA(`DataReadBytes + DataWriteBytes`)/ PERÍODO (em segundos)
	...determinar o total de IOPS do cliente do meu sistema de arquivos?	Total de IOPS do cliente (operações por segundo)	SOMA(`DataRead0perations + DataWrite0perations + Metadata0perations`)/PERÍODO (em segundos)
	...determinar a latência média das operações de leitura, gravação e metadados do meu sistema de arquivos?	Latência média (ms/operação)	Latência média de leitura: `DataRead0perationTime` * 1.000/`DataRead0perations` Latência média de gravação: `DataWrite0perationTime` * 1.000/`DataWrite0perations` Latência média de metadados: `Metadata0perationTime` * 1.000/`Metadata0perations`

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
	...determinar a distribuição da capacidade de armazenamento usada e livre no meu sistema de arquivos?	Distribuição de armazenamento	Nível principal disponível: `StorageCapacity {SSD} - StorageUsed {SSD}` Nível principal usado: `StorageUsed {SSD}` Grupo de capacidade usado: `StorageUsed {StandardCapacityPool }`
	...determinar a economia com a eficiência do armazenamento (compressão, eliminação de duplicação e compactação)?	Economia com a eficiência do armazenamento	`StorageEfficiencySavings`
Armazenamento	...determinar a quantidade de armazenamento principal disponível?	Capacidade de armazenamento principal disponível (bytes)	`StorageCapacity {SSD} - StorageUsed {SSD}`

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
	...determinar a porcentagem de armazenamento principal usado do meu sistema de arquivos?	Utilização da capacidade de armazenamento principal (porcentagem)	`StorageUsed {SSD} * 100/StorageCapacity {SSD}`
Performance do servidor de arquivos	...determinar se meu sistema de arquivos está se aproximando do limite de throughput da rede?	Throughput da rede: utilização (porcentagem)	`NetworkThroughputUtilization`
	...determinar se meu sistema de arquivos está se aproximando do limite de throughput do disco?	Throughput do disco: utilização (porcentagem)	`FileServerDiskThroughputUtilization`
	...determinar se meu sistema de arquivos esgotou os créditos de intermitência permitidos para o throughput do disco?	Throughput de disco: equilíbrio de intermitência (porcentagem)	`FileServerDiskThroughputBalance`

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
	...determinar se meu sistema de arquivos está se aproximando do limite de IOPS de SSD dos servidores de arquivos?	IOPS de disco: utilização (porcentagem)	`FileServerDiskIopsUtilization`
	...determinar se meu sistema de arquivos esgotou os créditos de intermitência permitidos pelos servidores de arquivos para a IOPS de SSD de disco?	IOPS de disco: equilíbrio de intermitência (porcentagem)	`FileServerDiskIopsBalance`
	...determinar a utilização média da CPU do sistema de arquivos?	Utilização da CPU (porcentagem)	`CPUUtilization`
	...determinar se minha workload está usando a RAM e os caches de leitura da NVMe do meu sistema de arquivos de modo eficiente?	Proporção de ocorrência do cache (porcentagem)	`FileServerCacheHitRatio`

Monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
Performance do disco	...determinar se meu sistema de arquivos está se aproximando da capacidade de IOPS de SSD provisionada atualmente?	IOPS de disco: utilização (SSD) (porcentagem)	`DiskIopsUtilization`

> **Note**
>
> Recomendamos que você mantenha uma utilização média da capacidade de throughput de qualquer dimensão relacionada à performance, como utilização da rede, da CPU e da IOPS de SSD, abaixo de 50%. Isso garante que você tenha capacidade de throughput disponível suficiente para picos inesperados na sua workload, bem como para qualquer operação de armazenamento em segundo plano (como sincronização de armazenamento, divisão de dados em níveis ou backups).

Monitoramento de métricas de volume no console do Amazon FSx

No console do Amazon FSx, visualize o painel de Monitoramento no painel do seu volume para ver métricas de performance adicionais. Para ter mais informações, consulte Acessando CloudWatch métricas.

Monitoramento	Como faço para...	Gráfico	Métricas relevantes
	...determinar a capacidade de armazenamento disponível do meu volume?	Capacidade de armazenamento	`StorageCapacity`

Monitoramento	Como faço para...	Gráfico	Métricas relevantes
		disponível	
	...determinar o throughput total de clientes do meu volume?	Throughput total do cliente (bytes por segundo)	SOMA(`DataReadBytes + DataWriteBytes`)/ PERÍODO (em segundos)
	...determinar o total de IOPS do cliente do meu volume?	Total de IOPS do cliente (operações por segundo)	SOMA(`DataReadOperations + DataWriteOperations + MetadataOperations`)/PERÍODO (em segundos)
	...determinar quantas operações de leitura e gravação estão vindo do nível do grupo de capacidade ou indo para ele?	IOPS do grupo de capacidade (operações por segundo)	Operações de leitura: `CapacityPoolReadOperations` Operações de gravação: `CapacityPoolWriteOperations`

Monitoramento	Como faço para...	Gráfico	Métricas relevantes
	...determinar a latência média das operações de leitura, gravação e metadados do meu volume?	Latência média (ms/operação)	Latência média de leitura: `DataReadOperationTime * 1.000/DataReadOperations` Latência média de gravação: `DataWriteOperationTime * 1.000/DataWriteOperations` Latência média de metadados: `MetadataOperationTime * 1.000/MetadataOperations`
	...determinar a quantidade de arquivos ou inodes disponíveis no meu volume?	Arquivos disponíveis (inodes)	`FilesCapacity - FilesUsed`
	...determinar a distribuição da capacidade de armazenamento usada e livre no meu volume?	Distribuição de armazenamento	`StorageCapacity - StorageUsed`

Acessando CloudWatch métricas

Você pode ver CloudWatch as métricas da Amazon para o Amazon FSx das seguintes formas:

- O console do Amazon FSx
- O CloudWatch console da Amazon
- O AWS Command Line Interface (AWS CLI) para CloudWatch

- A CloudWatch API

O procedimento a seguir explica como visualizar as CloudWatch métricas do seu sistema de arquivos com o console Amazon FSx.

Para visualizar CloudWatch métricas para seu sistema de arquivos usando o console Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Sistemas de arquivos e selecione o sistema de arquivos cujas métricas você deseja visualizar.
3. Na página Resumo, escolha Monitoramento e performance no segundo painel para visualizar gráficos das métricas do sistema de arquivos.

Há quatro guias no painel Monitoramento e performance.

- Escolha Resumo (a guia padrão) para exibir quaisquer avisos, CloudWatch alarmes e gráficos ativos da atividade do sistema de arquivos.
- Escolha Armazenamento para visualizar a capacidade de armazenamento e as métricas de utilização.
- Escolha Performance para visualizar as métricas de performance do servidor de arquivos e do armazenamento.
- Escolha CloudWatch alarmes para ver gráficos de todos os alarmes configurados para seu sistema de arquivos.

O procedimento a seguir explica como visualizar as CloudWatch métricas do seu volume com o console Amazon FSx.

Para visualizar CloudWatch métricas do seu volume usando o console Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Volumes e selecione o volume cujas métricas você deseja visualizar.
3. Na página Resumo, escolha Monitoramento (a guia padrão) no segundo painel para visualizar gráficos com as métricas do volume.

O procedimento a seguir explica como visualizar as CloudWatch métricas do seu sistema de arquivos com o CloudWatch console da Amazon.

Para visualizar métricas usando o CloudWatch console da Amazon

1. Na página Resumo do sistema de arquivos, escolha Monitoramento e performance no segundo painel para visualizar gráficos das métricas do sistema de arquivos.
2. Escolha Visualizar em métricas no menu de ações no canto superior direito do gráfico que você deseja visualizar no CloudWatch console da Amazon. Isso abre a página Métricas no CloudWatch console da Amazon.

O procedimento a seguir explica como adicionar métricas do sistema de arquivos FSx for ONTAP a um painel no console da Amazon. CloudWatch

Para adicionar métricas a um CloudWatch console da Amazon

1. Escolha o conjunto de métricas (Resumo, Armazenamento ou Performance) no painel Monitoramento e performance do console do Amazon FSx.
2. Escolha Adicionar ao painel no canto superior direito do painel. Isso abre o CloudWatch console da Amazon.
3. Selecione um CloudWatch painel existente na lista ou crie um novo painel. Para obter mais informações, consulte Usando CloudWatch painéis da Amazon no Guia do CloudWatch usuário da Amazon.

O procedimento a seguir explica como acessar as métricas do sistema de arquivos com a AWS CLI.

Para acessar métricas do AWS CLI

- Use o comando da CloudWatch CLI list-metrics com o parâmetro. `--namespace "AWS/FSx"` Para obter mais informações, consulte Referência de comandos da AWS CLI.

O procedimento a seguir explica como acessar as métricas do seu sistema de arquivos com a CloudWatch API.

Para acessar métricas da CloudWatch API

- Chame a operação da API de GetMetricestatísticas. Para obter mais informações, consulte a Amazon CloudWatch API Reference.

Métricas do sistema de arquivos

As métricas do sistema de arquivos do Amazon FSx for NetApp ONTAP são classificadas como métricas do sistema de arquivos ou métricas detalhadas do sistema de arquivos.

- As Métricas do sistema de arquivos são métricas agregadas de performance e armazenamento para um único sistema de arquivos que assume uma única dimensão, `FileSystemId`. Essas métricas medem a performance da rede e o uso da capacidade de armazenamento do seu sistema de arquivos.
- As Métricas detalhadas do sistema de arquivos medem a capacidade de armazenamento do sistema de arquivos e o armazenamento usado em cada nível de armazenamento (por exemplo, armazenamento SSD e armazenamento em grupo de capacidade). Cada métrica inclui uma dimensão `FileSystemId`, `StorageTier` e `DataType`.

Observe o seguinte sobre quando o Amazon FSx publica pontos de dados para essas métricas para: CloudWatch

- Para as métricas de utilização (qualquer métrica cujo nome termine em Utilização, como`NetworkThroughputUtilization`), há um ponto de dados emitido a cada período para cada servidor de arquivos ativo ou agregado. Por exemplo, o Amazon FSx emite uma métrica minuciosa por servidor de arquivos ativo e uma métrica minuciosa por agregado para`FileServerDiskIopsUtilization`. `DiskIopsUtilization`
- Para todas as outras métricas, há um único ponto de dados emitido a cada período, correspondendo ao valor total da métrica em todos os seus servidores de arquivos ativos (como métricas `DataReadBytes` de servidores de arquivos) ou em todos os seus agregados (como métricas `DiskReadBytes` de armazenamento).

Tópicos

Métricas de E/S de rede

Todas essas métricas assumem uma dimensão, `FileSystemId`.

Métrica	Descrição
`NetworkThroughputUtilization`	O percentual de utilização do throughput de rede do sistema de arquivos. A estatística `Average` é a utilização média do throughput da rede do sistema de arquivos em um período especificado. A estatística `Minimum` é a menor utilização do throughput da rede do sistema de arquivos em um período especificado. A estatística `Maximum` é a maior utilização do throughput da rede do sistema de arquivos em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`NetworkSentBytes`	O número de bytes (E/S de rede) enviados pelo sistema de arquivos. A estatística `Sum` é o número total de bytes enviados pelo sistema de arquivos em um período especificado. Para calcular o throughput enviado (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período especific ado. Unidades: bytes

Métrica	Descrição
	Estatística válida: `Sum`
`NetworkReceivedBytes`	O número de bytes (E/S de rede) recebidos pelo sistema de arquivos. A estatística `Sum` é o número total de bytes recebidos pelo sistema de arquivos em um período especificado. Para calcular o throughput recebido (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período especific ado. Unidades: bytes Estatística válida: `Sum`
`DataReadBytes`	O número de bytes (E/S de rede) das leituras feitas por clientes no sistema de arquivos. A estatística `Sum` é o número total de bytes associados às operações de leitura no período especificado. Para calcular a média de throughput (bytes por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: bytes Estatística válida: `Sum`

Métrica	Descrição
`DataWriteBytes`	O número de bytes (E/S de rede) das gravações feitas por clientes no sistema de arquivos. A estatística `Sum` é o número total de bytes associados às operações de gravação no período especificado. Para calcular a média de throughput (bytes por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: bytes Estatística válida: `Sum`
`DataReadOperations`	A contagem das operações de leitura (E/S de rede) das leituras feitas por clientes no sistema de arquivos. A estatística `Sum` é o número total de operações de E/S que ocorreram em um período especificado. Para calcular a média de operações de leitura por segundo para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatística válida: `Sum`

Métrica	Descrição
`DataWriteOperations`	A contagem das operações de gravação (E/S de rede) das gravações feitas por clientes no sistema de arquivos. A estatística `Sum` é o número total de operações de E/S que ocorreram em um período especificado. Para calcular a média de operações de gravação por segundo para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatística válida: `Sum`
`MetadataOperations`	A contagem das operações de metadados (E/S de rede) feitas por clientes no sistema de arquivos. A estatística `Sum` é o número total de operações de E/S que ocorreram em um período especificado. Para calcular a média de operações de metadados por segundo para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatística válida: `Sum`

Métrica	Descrição
`DataReadOperationTime`	A soma do tempo total gasto no sistema de arquivos em operações de leitura (E/S de rede) feitas por clientes acessando dados no sistema de arquivos. A estatística `Sum` é o número total de segundos gastos pelas operações de leitura no período especificado. Para calcular a latência média de leitura de um período, divida a estatística `Sum` pela `Sum` da métrica `DataReadOperations` no mesmo período. Unidades: segundos Estatística válida: `Sum`
`DataWriteOperationTime`	A soma do tempo total gasto no sistema de arquivos para realizar operações de gravação (E/S de rede) feitas por clientes acessando dados no sistema de arquivos. A estatística `Sum` é o número total de segundos gastos pelas operações de gravação durante o período especificado. Para calcular a latência média de gravação em um período, divida a estatística `Sum` pela `Sum` da métrica `DataWriteOperations` no mesmo período. Unidades: segundos Estatística válida: `Sum`

Métrica	Descrição
`CapacityPoolReadBytes`	O número de bytes lidos (E/S de rede) do nível do grupo de capacidade do sistema de arquivos. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de bytes lidos do nível do grupo de capacidade do sistema de arquivos em um período especific ado. Para calcular os bytes do grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especific ado. Unidades: bytes Estatística válida: `Sum`

Métrica	Descrição
`CapacityPoolReadOperations`	O número de operações de leitura (E/S de rede) do nível do grupo de capacidade do sistema de arquivos. Isso se traduz em uma solicitação de leitura do grupo de capacidade. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de operações de leitura do nível do grupo de capacidade do sistema de arquivos em um período especificado. Para calcular as solicitações de grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especificado. Unidades: contagem Estatística válida: `Sum`

Métrica	Descrição
`CapacityPoolWriteBytes`	O número de bytes gravados (E/S de rede) no nível do grupo de capacidade do sistema de arquivos. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de bytes gravados no nível do grupo de capacidad e do sistema de arquivos em um período especificado. Para calcular os bytes do grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especific ado. Unidades: bytes Estatística válida: `Sum`

Métrica	Descrição
`CapacityPoolWriteOperations`	O número de operações de gravação (E/S de rede) no sistema de arquivos do nível do grupo de capacidade. Isso se traduz em uma solicitação de gravação. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de operações de gravação no nível do grupo de capacidade do sistema de arquivos em um período especificado. Para calcular as solicitações de grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especificado. Unidades: contagem Estatística válida: `Sum`

Métricas do servidor de arquivos

Todas essas métricas assumem uma dimensão, `FileSystemId`.

Métrica	Descrição
`CPUUtilization`	A porcentagem de utilização dos recursos de CPU do sistema de arquivos. A estatística `Average` é a utilização média da CPU do sistema de arquivos em um período especificado.

Métrica	Descrição
	A estatística `Minimum` é a menor utilização da CPU do sistema de arquivos em um período especificado. A estatística `Maximum` é a maior utilização da CPU do sistema de arquivos em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`FileServerDiskThroughputUtilization`	O throughput do disco entre o servidor de arquivos e a camada principal, como uma porcentagem do limite provisionado determinado pela capacidade de throughput. A estatística `Average` é a porcentagem média de utilização do throughput de disco dos servidores de arquivos em um período especificado. A estatística `Minimum` é a menor porcentagem de utilização do throughput de disco dos servidores de arquivos em um período especificado. A estatística `Maximum` é a maior utilização do throughput de disco dos servidores de arquivos em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerDiskThroughputBalance`	A porcentagem de créditos de intermitência disponíveis para throughput de disco entre o servidor de arquivos e o nível principal. Isso é válido para sistemas de arquivos provision ados com uma capacidade de throughput de 512 MBps ou menos. A estatística `Average` é o equilíbrio médio de intermitência disponível em um período especificado. A estatística `Minimum` é o equilíbrio mínimo de intermitência disponível em um período especificado. A estatística `Maximum` é o equilíbrio máximo de intermitência disponível em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerDiskIopsBalance`	A porcentagem de créditos de intermitência disponíveis para IOPS de disco entre o servidor de arquivos e o nível principal. Isso é válido para sistemas de arquivos provisionados com uma capacidade de throughput de 512 MBps ou menos. A estatística `Average` é o equilíbrio médio de intermitência disponível em um período especificado. A estatística `Minimum` é o equilíbrio mínimo de intermitência disponível em um período especificado. A estatística `Maximum` é o equilíbrio máximo de intermitência disponível em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerDiskIopsUtilization`	A porcentagem de utilização de IOPS da capacidade de IOPS de disco disponível para o servidor de arquivos. A estatística `Average` é a utilização média de IOPS de disco do sistema de arquivos em um período especificado. A estatística `Minimum` é a utilização mínima de IOPS de disco do sistema de arquivos em um período especificado. A estatística `Maximum` é a utilização máxima de IOPS de disco do sistema de arquivos em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerCacheHitRatio`	A porcentagem de todas as solicitações de leitura atendidas pelos dados nos caches da RAM e da NVMe do sistema de arquivos. Uma porcentagem maior significa que mais leituras são atendidas pelos caches de leitura do sistema de arquivos. Unidades: percentual A estatística `Average` é a porcentagem média de ocorrência do cache do sistema de arquivos em um período especificado. A estatística `Minimum` é a menor porcentagem de ocorrência do cache do sistema de arquivos em um período especificado. A estatística `Maximum` é a maior porcentagem de ocorrência do cache do sistema de arquivos em um período especificado. Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métricas de E/S de disco

Todas essas métricas assumem uma dimensão, `FileSystemId`.

Métrica	Descrição
`DiskReadBytes`	O número de bytes (E/S de disco) de qualquer leitura de disco na camada principal do sistema de arquivos.

Métrica	Descrição
	A estatística `Sum` é o número total de bytes lidos do sistema de arquivos em um período especificado. Para calcular o throughput de leitura do disco (bytes por segundo) para qualquer estatísti ca, divida a estatística `Sum` pelos segundos no período especificado. Unidades: bytes Estatística válida: `Sum`
`DiskWriteBytes`	O número de bytes (E/S de disco) de qualquer gravação do disco no nível principal do sistema de arquivos. A estatística `Sum` é o número total de bytes gravados do sistema de arquivos em um período especificado. Para calcular o throughput de gravação do disco (bytes por segundo) para qualquer estatística, divida a estatística `Sum` pelos segundos no período especificado. Unidades: bytes Estatística válida: `Sum`

Métrica	Descrição
`DiskIopsUtilization`	A IOPS de disco entre o servidor de arquivos e os volumes de armazenamento, como uma porcentagem do limite de IOPS do disco provisionado nos níveis principais. A estatística `Average` é a utilização média de IOPS de disco do sistema de arquivos em um período especificado. A estatística `Minimum` é a utilização mínima de IOPS de disco do sistema de arquivos em um período especificado. A estatística `Maximum` é a utilização máxima de IOPS de disco do sistema de arquivos em um período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`DiskReadOperations`	O número de operações de leitura (E/S de disco) da camada principal do sistema de arquivos. A estatística `Sum` é o número total de operações de leitura da camada principal em um período especificado. Unidades: contagem Estatística válida: `Sum`

Métrica	Descrição
`DiskWriteOperations`	O número de operações de gravação (E/S de disco) no nível principal do sistema de arquivos. A estatística `Sum` é o número total de operações de gravação na camada principal em um período especificado. Unidades: contagem Estatística válida: `Sum`

Métricas da capacidade de armazenamento

Todas essas métricas assumem uma dimensão, `FileSystemId`.

Métrica	Descrição
`StorageEfficiencySavings`	Os bytes economizados com os recursos de eficiência do armazenamento (compressão, eliminação de duplicação e compactação). A estatística `Average` é a economia média com a eficiência de armazenamento em um período especificado. Para calcular a economia com a eficiência do armazenamento como uma porcentagem de todos os dados armazenados, em um período de um minuto, divida `StorageEfficiencySavings` pela soma de `StorageEfficiencySavings` e pela métrica `StorageUsed` do sistema de arquivos, usando a estatística `Sum` para `StorageUsed` .

Métrica	Descrição
	A estatística `Minimum` é a economia mínima com a eficiência do armazenamento em um período especificado. A estatística `Maximum` é a economia máxima com a eficiência do armazenamento em um período especificado. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`StorageUsed`	A quantidade total de dados físicos armazenados no sistema de arquivos, tanto no nível principal (SSD) quanto no nível do grupo de capacidade. Essa métrica inclui economias com recursos de eficiência do armazenamento, como compressão e eliminação de duplicação dos dados. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`LogicalDataStored`	A quantidade total de dados lógicos armazenados no sistema de arquivos, considerando tanto o nível SSD quanto o nível do grupo de capacidade. Essa métrica inclui o tamanho lógico total dos instantâneos e FlexClones, mas não inclui a economia de eficiência de armazenamento obtida por meio da compactação, compactação e desduplicação. Para computar a economia com a eficiência do armazenamento em bytes, pegue a `Average` de `StorageUsed` em um determinado período e subtraia da `Average` de `LogicalDataStored` no mesmo período. Para computar a economia com a eficiência do armazenamento como uma porcentagem do tamanho lógico total dos dados, pegue a `Average` de `StorageUsed` em um determinado período e subtraia da `Average` de `LogicalDataStored` no mesmo período. Em seguida, divida a diferença pela `Average` de `LogicalDataStored` no mesmo período. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métricas detalhadas do sistema de arquivos

As métricas detalhadas do sistema de arquivos são métricas detalhadas de utilização do armazenamento para cada um dos seus níveis de armazenamento. Todas as métricas detalhadas do sistema de arquivos têm as dimensões `FileSystemId`, `StorageTier` e `DataType`.

- A dimensão `StorageTier` indica o nível de armazenamento medido pela métrica, com valores possíveis de `SSD` e `StandardCapacityPool`.
- A dimensão `DataType` indica o tipo de dados medidos pela métrica, com o valor possível de `All`.

Há uma linha para cada combinação exclusiva de um determinado par de chave-valor métrico e dimensional, com uma descrição do que essa combinação mede.

Métrica	Descrição
`StorageCapacityUtilization`	A utilização da capacidade de armazenamento para cada um dos agregados do seu sistema de arquivos. Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A `Average` estatística é a quantidade média de utilização da capacidade de armazenamento para o nível de desempenho do seu sistema de arquivos durante o período especificado. A `Minimum` estatística é a menor quantidad e de utilização da capacidade de armazenam ento para o nível de desempenho do seu sistema de arquivos durante o período especificado. A `Maximum` estatística é a maior quantidade de utilização da capacidade de armazenamento para o nível de desempenho do seu sistema de arquivos durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`StorageCapacity`	A capacidade total de armazenamento do nível principal (SSD).

Métrica	Descrição
	Unidades: bytes Estatística válida: `Maximum`

Métrica	Descrição
`StorageUsed`	A capacidade de armazenamento físico usada em bytes, específica do nível de armazenam ento. Esse valor inclui economias com recursos de eficiência do armazenamento, como compressão e eliminação de duplicação dos dados. Os valores de dimensão válidos para `StorageTier` são `SSD` e `StandardC apacityPool` , correspondendo ao nível de armazenamento medido por essa métrica. Essa métrica também exige a dimensão `DataType` com o valor de `All`. As estatísticas `Average`, `Minimum` e `Maximum` são o consumo de armazenamento por nível em bytes para o período determinado. Para calcular a utilização da capacidade de armazenamento do nível de armazenamento principal (SSD), divida qualquer uma dessas estatísticas pelo `Maximum` da `StorageCa pacity` no mesmo período, com a dimensão `StorageTier` igual ao `SSD`. Para calcular a capacidade de armazenam ento livre do nível de armazenamento principal (SSD) em bytes, subtraia qualquer uma dessas estatísticas do `Maximum` da `StorageCa pacity` no mesmo período, com a dimensão `StorageTier` igual ao `SSD`. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métricas escaláveis do sistema de arquivos

As métricas a seguir são fornecidas para sistemas de arquivos FSx for ONTAP com dois ou mais pares de alta disponibilidade (HA). Para as métricas, um ponto de dados é emitido para cada par de HA e para cada agregado (para métricas de utilização de armazenamento).

> **Note**
>
> Se você tiver um sistema de arquivos com vários pares de HA, também poderá usar as métricas do sistema de arquivos com um único par de HA e as métricas de volume.

Tópicos

Métricas de E/S de rede

Todas essas métricas assumem duas dimensões, `FileSystemId` e `FileServer`.

- `FileSystemId`— ID do AWS recurso do seu sistema de arquivos.
- `FileServer`— O nome de um servidor de arquivos (ou nó) no ONTAP (por exemplo,`FsxId01234567890abcdef-01`). Os servidores de arquivos com números ímpares são servidores de arquivos preferenciais (ou seja, eles atendem ao tráfego, a menos que o sistema de arquivos tenha passado para o servidor de arquivos secundário), enquanto os servidores de arquivos com números pares são servidores de arquivos secundários (ou seja, eles fornecem tráfego somente quando o parceiro não está disponível). Por esse motivo, os servidores de arquivos secundários geralmente mostram menos utilização do que os servidores de arquivos preferenciais.

Métrica	Descrição
`NetworkThroughputUtilization`	Utilização da taxa de transferência de rede como uma porcentagem da taxa de transferê

Métrica	Descrição
	ncia de rede disponível para seu sistema de arquivos. Essa métrica é equivalente ao máximo `NetworkSentBytes` e `NetworkReceivedBytes` como uma porcentagem da capacidade de taxa de transferência de rede de um par de HA para seu sistema de arquivos. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada servidor de arquivos do seu sistema de arquivos. A `Average` estatística é a utilização média da taxa de transferência da rede para um determinado servidor de arquivos durante o período especificado. A `Minimum` estatística é a menor utilização da taxa de transferência de rede para um determinado servidor de arquivos em um minuto, durante o período especificado. A `Maximum` estatística é a maior utilização da taxa de transferência de rede para um determinado servidor de arquivos em um minuto, durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`NetworkSentBytes`	O número de bytes (IO de rede) enviados pelo seu sistema de arquivos. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada servidor de arquivos do seu sistema de arquivos. A `Sum` estatística é o número total de bytes enviados pela rede pelo determinado servidor de arquivos durante o período especificado. A `Average` estatística é o número médio de bytes enviados pela rede pelo determinado servidor de arquivos durante o período especificado. A `Minimum` estatística é o menor número de bytes enviados pela rede pelo determinado servidor de arquivos durante o período especificado. A `Maximum` estatística é o maior número de bytes enviados pela rede pelo determinado servidor de arquivos durante o período especificado. Para calcular o throughput enviado (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período especificado. Unidades: bytes Estatísticas válidas:`Sum`,`Average`,`Minimum`, e `Maximum`

Métrica	Descrição
`NetworkReceivedBytes`	O número de bytes (IO de rede) recebidos pelo seu sistema de arquivos. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada servidor de arquivos do seu sistema de arquivos. A `Sum` estatística é o número total de bytes recebidos pela rede pelo determinado servidor de arquivos durante o período especificado. A `Average` estatística é o número médio de bytes recebidos pela rede pelo determinado servidor de arquivos a cada minuto durante o período especificado. A `Minimum` estatística é o menor número de bytes recebidos pela rede pelo determinado servidor de arquivos a cada minuto durante o período especificado. A `Maximum` estatística é o maior número de bytes recebidos pela rede pelo determinado servidor de arquivos a cada minuto durante o período especificado. Para calcular a taxa de transferência recebida (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período. Unidades: bytes Estatísticas válidas:`Sum`,`Average`,`Minimum`, e `Maximum`

Métricas do servidor de arquivos

Todas essas métricas assumem duas dimensões, `FileSystemId` e `FileServer`.

Métrica	Descrição
`CPUUtilization`	A porcentagem de utilização dos recursos de CPU do sistema de arquivos. Há uma métrica emitida a cada minuto para cada servidor de arquivos do seu sistema de arquivos. A estatística `Average` é a utilização média da CPU do sistema de arquivos em um período especificado. A `Minimum` estatística é a menor utilização da CPU para um determinado servidor de arquivos durante o período especificado. A `Maximum` estatística é a maior utilização da CPU para um determinado servidor de arquivos durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`FileServerDiskThroughputUtilization`	A taxa de transferência do disco entre o servidor de arquivos e o agregado, como uma porcentagem do limite provisionado determinado pela capacidade de taxa de transferência. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Essa métrica é equivalente à soma `DiskReadBytes` e `DiskWriteBytes` como uma porcentagem da capacidade de taxa de transferência de disco do servidor de arquivos

Métrica	Descrição
	de um par de HA para seu sistema de arquivos. Há uma métrica emitida a cada minuto para cada servidor de arquivos do seu sistema de arquivos. A `Average` estatística é a utilização média da taxa de transferência de disco do servidor de arquivos para um determinado servidor de arquivos durante o período especificado. A `Minimum` estatística é a menor utilização da taxa de transferência de disco do servidor de arquivos para um determinado servidor de arquivos durante o período especificado. A `Maximum` estatística é a maior utilização da taxa de transferência de disco do servidor de arquivos para um determinado servidor de arquivos durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerDiskIopsUtilization`	A utilização de IOPS da capacidade de IOPS de disco disponível para seu servidor de arquivos, como uma porcentagem do limite de IOPS de disco. Isso difere do `DiskIopsUtilization` fato de a utilização de IOPS de disco exceder o máximo que seu servidor de arquivos pode suportar, em oposição à IOPS de disco provisionada. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada servidor de arquivos do seu sistema de arquivos. A `Average` estatística é a utilização média de IOPS de disco para um determinado servidor de arquivos durante o período especificado. A `Minimum` estatística é a menor utilização de IOPS de disco para um determinado servidor de arquivos durante o período especificado. A `Maximum` estatística é a maior utilização de IOPS de disco para um determinado servidor de arquivos durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`FileServerCacheHitRatio`	A porcentagem de todas as solicitações de leitura atendidas pelos dados que residem nos caches RAM ou NVMe do seu sistema de arquivos para cada um dos seus pares de HA (por exemplo, o servidor de arquivos ativo em um par de HA). Uma porcentagem maior indica uma proporção maior de leituras em cache em relação ao total de leituras. Toda a I/O é considerada, inclusive tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada servidor de arquivos do seu sistema de arquivos. Unidades: percentual A `Average` estatística é a taxa média de acertos do cache para um dos pares de HA do seu sistema de arquivos durante o período especificado. A `Minimum` estatística é a menor taxa de acertos de cache para um dos pares de HA do seu sistema de arquivos durante o período especificado. A `Maximum` estatística é a maior taxa de acertos de cache para um dos pares de HA do seu sistema de arquivos durante o período especificado. Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métricas de E/S de disco

Todas essas métricas assumem duas dimensões, `FileSystemId` e `Aggregate`.

- `FileSystemId`— ID do AWS recurso do seu sistema de arquivos.
- `Aggregate`— O nível de desempenho do seu sistema de arquivos consiste em vários pools de armazenamento chamados agregados. Há um agregado para cada par de HA. Por exemplo, agregue `aggr1` mapas para o servidor de arquivos `FsxId01234567890abcdef-01` (o servidor de arquivos ativo) e o servidor de arquivos `FsxId01234567890abcdef-02` (o servidor de arquivos secundário) em um par de HA.

Métrica	Descrição
`DiskReadBytes`	O número de bytes (E/S do disco) de qualquer disco lido desse agregado. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A `Sum` estatística é o número total de bytes lidos a cada minuto de um determinado agregado durante o período especificado. A `Average` estatística é o número médio de bytes lidos a cada minuto de um determinado agregado durante o período especificado. A `Minimum` estatística é o menor número de bytes lidos a cada minuto de um determinado agregado durante o período especificado. A `Maximum` estatística é o maior número de bytes lidos a cada minuto de um determinado agregado durante o período especificado.

Métrica	Descrição
	Para calcular a taxa de transferência do disco de leitura (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período. Unidades: bytes Estatísticas válidas:`Sum`,`Average`,`Minimum`, e `Maximum`

Métrica	Descrição
`DiskWriteBytes`	O número de bytes (E/S do disco) de qualquer gravação em disco nesse agregado. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirro r hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A `Sum` estatística é o número total de bytes gravados em um determinado agregado durante o período especificado. A `Average` estatística é o número médio de bytes gravados em um determinado agregado a cada minuto durante o período especificado. A `Minimum` estatística é o menor número de bytes gravados em um determinado agregado a cada minuto durante o período especificado. A `Maximum` estatística é o maior número de bytes gravados em um determinado agregado a cada minuto durante o período especificado. Para calcular o throughput de gravação do disco (bytes por segundo) para qualquer estatística, divida a estatística pelos segundos no período especificado. Unidades: bytes Estatísticas válidas:`Sum`,`Average`,`Minimum`, e `Maximum`

Métrica	Descrição
`DiskIopsUtilization`	A utilização de IOPS em disco de um agregado, como uma porcentagem do limite de IOPS de disco do agregado (ou seja, o total de IOPS do sistema de arquivos dividido pelo número de pares de HA para seu sistema de arquivos). Isso difere do fato de ser a utilizaçã o de IOPS de disco provisionado `FileServe rDiskIopsUtilization` em relação ao limite de IOPS provisionado, em oposição ao máximo de IOPS de disco suportado pelo servidor de arquivos (ou seja, determinado pela capacidade de taxa de transferência configurada por par de HA). Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarqui zação e backups). Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A `Average` estatística é a utilização média de IOPS de disco para um determinado agregado durante o período especificado. A `Minimum` estatística é a menor utilização de IOPS de disco para um determinado agregado durante o período especificado. A `Maximum` estatística é a maior utilização de IOPS de disco para um determinado agregado durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`DiskReadOperations`	O número de operações de leitura (E/S de disco) desse agregado. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A `Sum` estatística é o número total de operações de leitura realizadas por um determinado agregado durante o período especificado. A `Average` estatística é o número médio de operações de leitura realizadas a cada minuto pelo agregado determinado durante o período especificado. A `Minimum` estatística é o menor número de operações de leitura realizadas a cada minuto pelo agregado determinado durante o período especificado. A `Maximum` estatística é o maior número de operações de leitura realizadas a cada minuto pelo agregado determinado durante o período especificado. Para calcular a média de IOPS do disco durante o período, use a `Average` estatística e divida o resultado por 60 (segundos). Unidades: contagem Estatísticas válidas:`Sum`,`Average`,`Minimum`, e `Maximum`

Métrica	Descrição
`DiskWriteOperations`	O número de operações de gravação (E/S de disco) nesse agregado. Todo o tráfego é considerado nessa métrica, incluindo tarefas em segundo plano (como SnapMirror hierarquização e backups). Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A `Sum` estatística é o número total de operações de gravação realizadas por um determinado agregado durante o período especificado. A `Average` estatística é o número médio de operações de gravação realizadas a cada minuto pelo agregado determinado durante o período especificado. Para calcular a média de IOPS do disco durante o período, use a `Average` estatística e divida o resultado por 60 (segundos). Unidades: contagem Estatísticas válidas: `Sum` e `Average`

Métricas detalhadas do sistema de arquivos

As métricas detalhadas do sistema de arquivos são métricas detalhadas de utilização do armazenamento para cada um dos seus níveis de armazenamento. As métricas detalhadas do sistema de arquivos têm `DataType` as dimensões `FileSystemIdStorageTier`, e ou as `FileSystemId` `Aggregate` dimensões `StorageTierDataType`,, e.

- Quando a `Aggregate` dimensão não é fornecida, as métricas são para todo o sistema de arquivos. As `StorageCapacity` métricas `StorageUsed` e têm um único ponto de dados a cada minuto correspondente ao armazenamento total consumido do sistema de arquivos (por nível de

armazenamento) e à capacidade total de armazenamento (para o nível SSD). Enquanto isso, a `StorageCapacityUtilization` métrica emite uma métrica a cada minuto para cada agregado.

- Quando a `Aggregate` dimensão é fornecida, as métricas são para cada agregado.

O significado das dimensões é o seguinte:

- `FileSystemId`— ID do AWS recurso do seu sistema de arquivos.
- `Aggregate`— O nível de desempenho do seu sistema de arquivos consiste em vários pools de armazenamento chamados agregados. Há um agregado para cada par de HA. Por exemplo, agregue `aggr1` mapas para o servidor de arquivos `FsxId01234567890abcdef-01` (o servidor de arquivos ativo) e o servidor de arquivos `FsxId01234567890abcdef-02` (o servidor de arquivos secundário) em um par de HA.
- `StorageTier`— Indica o nível de armazenamento que a métrica mede, com valores possíveis de `SSD` `StandardCapacityPool` e.
- `DataType`— Indica o tipo de dados que a métrica mede, com o valor possível`All`.

Há uma linha para cada combinação exclusiva de um determinado par de chave-valor métrico e dimensional, com uma descrição do que essa combinação mede.

Métrica	Descrição
`StorageCapacityUtilization`	A utilização da capacidade de armazenamento para um determinado agregado do sistema de arquivos. Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A `Average` estatística é a quantidade média de utilização da capacidade de armazenam ento de um determinado agregado durante o período especificado. A `Minimum` estatística é a quantidade mínima de utilização da capacidade de armazenam ento para um determinado agregado durante o período especificado.

Métrica	Descrição
	A `Maximum` estatística é a quantidade máxima de utilização da capacidade de armazenam ento para um determinado agregado durante o período especificado. Unidades: percentual Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`StorageCapacity`	A capacidade de armazenamento de um determinado agregado do sistema de arquivos. Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A `Average` estatística é a quantidade média de capacidade de armazenamento de um determinado agregado durante o período especificado. A `Minimum` estatística é a quantidade mínima de capacidade de armazenamento para um determinado agregado durante o período especificado. A `Maximum` estatística é a quantidade máxima de capacidade de armazenamento para um determinado agregado durante o período especificado. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métrica	Descrição
`StorageUsed`	A capacidade de armazenamento físico usada em bytes, específica do nível de armazenam ento. Esse valor inclui economias com recursos de eficiência do armazenamento, como compressão e eliminação de duplicação dos dados. Os valores de dimensão válidos para `StorageTier` são `SSD` e `StandardC apacityPool` , correspondendo ao nível de armazenamento medido por essa métrica. Há uma métrica emitida a cada minuto para cada agregado do seu sistema de arquivos. A `Average` estatística é a quantidade média de capacidade de armazenamento físico consumida em determinado nível de armazenamento por um determinado agregado durante o período especificado. A `Minimum` estatística é a quantidade mínima de capacidade de armazenamento físico consumida em determinado nível de armazenamento por um determinado agregado durante o período especificado. A `Maximum` estatística é a quantidade máxima de capacidade de armazenamento físico consumida em determinado nível de armazenamento por um determinado agregado durante o período especificado. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`

Métricas de volume

Seu sistema de arquivos Amazon FSx for NetApp ONTAP pode ter um ou mais volumes que armazenam seus dados. Cada um desses volumes tem um conjunto de métricas, classificadas como Métricas de volume ou Métricas detalhadas de volume.

- As Métricas de volume são métricas de performance e armazenamento por volume que assumem duas dimensões: `FileSystemId` e `VolumeId`. `FileSystemId` mapeia para o sistema de arquivos ao qual o volume pertence.
- Métricas de volume detalhadas são per-storage-tier métricas que medem o consumo de armazenamento por nível com a `StorageTier` dimensão (com valores possíveis de `SSD` e`StandardCapacityPool`) e por tipo de dados com a `DataType` dimensão (com valores possíveis de `UserSnapshot`, e`Other`). Essas métricas têm as dimensões `FileSystemId`, `VolumeId`, `StorageTier` e `DataType`.

Tópicos

Métricas de E/S de rede

Todas essas métricas assumem duas dimensões, `FileSystemId` e `VolumeId`.

Métrica	Descrição
`DataReadBytes`	O número de bytes (E/S de rede) lidos do volume pelos clientes. A estatística `Sum` é o número total de bytes associados às operações de leitura no período especificado. Para calcular a média de throughput (bytes por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: bytes

Métrica	Descrição
	Estatística válida: `Sum`
`DataWriteBytes`	O número de bytes (E/S de rede) gravados no volume pelos clientes. A estatística `Sum` é o número total de bytes associados às operações de gravação no período especificado. Para calcular a média de throughput (bytes por segundo) para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: bytes Estatística válida: `Sum`
`DataReadOperations`	O número de operações de leitura (E/S de rede) no volume feitas por clientes. A estatística `Sum` é o número total das operações de leitura no período especificado. Para calcular a média de operações de leitura por segundo para um período, divida a estatísti ca `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatística válida: `Sum`

Métrica	Descrição
`DataWriteOperations`	O número de operações de gravação (E/S de rede) no volume feitas por clientes. A estatística `Sum` é o número total das operações de gravação no período especific ado. Para calcular a média de operações de gravação por segundo para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatística válida: `Sum`
`MetadataOperations`	O número de operações de E/S (E/S de rede) das atividades de metadados feitas por clientes no volume. A estatística `Sum` é o número total das operações de metadados no período especific ado. Para calcular a média de operações de metadados por segundo para um período, divida a estatística `Sum` pelo número de segundos no período especificado. Unidades: contagem Estatística válida: `Sum`

Métrica	Descrição
`DataReadOperationTime`	A soma do tempo total gasto no volume para operações de leitura (E/S de rede) de clientes acessando dados no volume. A estatística `Sum` é o número total de segundos gastos pelas operações de leitura no período especificado. Para calcular a latência média de leitura de um período, divida a estatística `Sum` pela `Sum` da métrica `DataReadOperations` no mesmo período. Unidades: segundos Estatística válida: `Sum`
`DataWriteOperationTime`	A soma do tempo total gasto no volume para realizar operações de gravação (E/S de rede) de clientes acessando dados no volume. A estatística `Sum` é o número total de segundos gastos pelas operações de gravação durante o período especificado. Para calcular a latência média de gravação em um período, divida a estatística `Sum` pela `Sum` da métrica `DataWriteOperations` no mesmo período. Unidades: segundos Estatística válida: `Sum`

Métrica	Descrição
`MetadataOperationTime`	A soma do tempo total gasto no volume para realizar operações de metadados (E/S de rede) de clientes acessando dados no volume. A estatística `Sum` é o número total de segundos gastos pelas operações de leitura no período especificado. Para calcular a latência média de um período, divida a estatística `Sum` pela `Sum` das `MetadataOperations` no mesmo período. Unidades: segundos Estatística válida: `Sum`
`CapacityPoolReadBytes`	O número de bytes lidos (E/S de rede) do nível do grupo de capacidade do volume. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de bytes lidos do nível do grupo de capacidade do volume em um período especificado. Para calcular os bytes do grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especificado. Unidades: bytes Estatística válida: `Sum`

Métrica	Descrição
`CapacityPoolReadOperations`	O número de operações de leitura (E/S de rede) do nível do grupo de capacidade do volume. Isso se traduz em uma solicitação de leitura do grupo de capacidade. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de operações de leitura do nível do grupo de capacidade do volume em um período especific ado. Para calcular as solicitações de grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especific ado. Unidades: contagem Estatística válida: `Sum`

Métrica	Descrição
`CapacityPoolWriteBytes`	O número de bytes gravados (E/S de rede) no nível do grupo de capacidade do volume. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de bytes gravados no nível do grupo de capacidade do volume em um período especificado. Para calcular os bytes do grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especificado. Unidades: bytes Estatística válida: `Sum`

Métrica	Descrição
`CapacityPoolWriteOperations`	O número de operações de gravação (E/S de rede) no volume do nível do grupo de capacidade. Isso se traduz em uma solicitação de gravação. Para garantir a integridade dos dados, o ONTAP executa uma operação de leitura no grupo de capacidade imediatamente após realizar uma operação de gravação. A estatística `Sum` é o número total de operações de gravação no nível do grupo de capacidade do volume em um período especificado. Para calcular as solicitações de grupo de capacidade por segundo, divida a estatística `Sum` pelos segundos em um período especificado. Unidades: contagem Estatística válida: `Sum`

Métricas da capacidade de armazenamento

Todas essas métricas assumem duas dimensões, `FileSystemId` e `VolumeId`.

Métrica	Descrição
`StorageCapacity`	O tamanho do volume em bytes. Unidades: bytes Estatística válida: `Maximum`
`StorageUsed`	A capacidade de armazenamento lógico usada do volume.

Métrica	Descrição
	Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`StorageCapacityUtilization`	A utilização da capacidade de armazenamento do volume. Unidades: percentual Estatística válida: `Average`
`FilesUsed`	Os arquivos usados (número de arquivos ou inodes) no volume. Unidades: contagem Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`FilesCapacity`	O número total de inodes que podem ser criados no volume. Unidades: contagem Estatística válida: `Maximum`

Métricas detalhadas de volume

As métricas detalhadas de volume assumem mais dimensões do que as métricas de volume, permitindo medições mais granulares dos seus dados. Todas as métricas detalhadas de volume têm as dimensões `FileSystemId`, `VolumeId`, `StorageTier` e `DataType`.

- A dimensão `StorageTier` indica o nível de armazenamento medido pela métrica, com valores possíveis de `All`, `SSD` e `StandardCapacityPool`.
- A dimensão `DataType` indica o tipo de dados medidos pela métrica, com valores possíveis de `All`, `User`, `Snapshot` e `Other`.

A tabela a seguir define o que é medido pela métrica `StorageUsed` para as dimensões listadas.

Métrica	Descrição
`StorageUsed`	A quantidade de espaço lógico usado, em bytes. Essa métrica mede diferentes tipos de consumo de espaço, dependendo das dimensões usadas com ela. Ao definir o `StorageTier` como `SSD` ou `StandardCapacityPool` e configurar o `DataType` como `All`, essa métrica mede o uso do espaço lógico desse volume para os níveis de SSD e grupo de capacidade, respectivamente. Ao definir a dimensão `DataType` como `User`, `Snapshot` ou `Other` e configurar o `StorageTier` como `All`, essa métrica mede o uso do espaço lógico para cada tipo respectivo de dados. O consumo de dados do `Snapshot` inclui a reserva de snapshot, que é 5% do tamanho do volume por padrão. Unidades: bytes Estatísticas válidas: `Average`, `Minimum` e `Maximum`
`StorageCapacityUtilization`	A porcentagem do espaço físico em disco usado pelo volume. Unidades: percentual Estatística válida: `Maximum`

Avisos e recomendações de performance

O FSx for ONTAP exibe um aviso para CloudWatch métricas sempre que uma dessas métricas se aproxima ou ultrapassa um limite predeterminado para vários pontos de dados consecutivos. Esses

avisos fornecem recomendações práticas que você pode usar para otimizar a performance do seu sistema de arquivos.

Os avisos podem ser acessados em várias áreas do painel Monitoramento e performance. Todos os avisos de desempenho ativos ou recentes do Amazon FSx e quaisquer CloudWatch alarmes configurados para o sistema de arquivos que estejam em estado de ALARME aparecem no painel Monitoramento e desempenho na seção Resumo. O aviso também aparece na seção do painel onde o gráfico de métricas é exibido.

Você pode criar CloudWatch alarmes para qualquer uma das métricas do Amazon FSx. Para ter mais informações, consulte Criação de CloudWatch alarmes da Amazon para monitorar o Amazon FSx.

Use os avisos de performance para melhorar a performance do sistema de arquivos

O Amazon FSx fornece recomendações práticas que você pode usar para otimizar a performance do seu sistema de arquivos. Essas recomendações descrevem como lidar com um possível gargalo na performance. Você pode realizar a ação recomendada caso espere que a atividade continue ou se ela estiver causando um impacto na performance do seu sistema de arquivos. Dependendo da métrica que acionou um aviso, você pode resolvê-lo aumentando a capacidade de throughput ou a capacidade de armazenamento do sistema de arquivos, conforme descrito na tabela a seguir.

Seção Dashboard	Se houver um aviso para essa métrica	Faça o seguinte
Armazenamento	Utilização da capacidade de armazenamento primário	Aumente a capacidade de armazenamento primário do seu sistema de arquivos se ele ainda não estiver na capacidade máxima de armazenamento SSD. Para ter mais informações, consulte Modificando a capacidade de armazenamento SSD e o IOPS provisionado. Se seu sistema de arquivos tiver vários pares de HA e sua utilização da capacidade de armazenamento primário for apenas maior para um subconjunto dos agregados do sistema de arquivos (os pools de armazenamento que compõem seu nível de armazenamento primário), você também pode reequilibrar sua carga de trabalho para que a utilização da

Seção Dashboard	Se houver um aviso para essa métrica	Faça o seguinte
		capacidade de armazenamento principal seja distribuída de forma mais uniforme pelo sistema de arquivos. Para obter mais informações sobre como reequilibrar suas cargas de trabalho, consulte. Monitorando o FSx para balanceamento da carga de trabalho do ONTAP
Performance do servidor de arquivos	Throughput na rede	Aumente a capacidade de taxa de transferência do seu sistema de arquivos se ele ainda não estiver na capacidade máxima de taxa de transferência. Para obter mais informações sobre a atualização da capacidade de processamento, consulteComo modificar a capacidade de throughput. Se seu sistema de arquivos tiver vários pares de HA e a utilização for alta somente em um subconjunto de servidores de arquivos, você também poderá reequilibrar sua carga de trabalho para que ela utilize de forma mais uniforme os recursos de desempenho de cada um dos pares de HA do sistema de arquivos. Para obter mais informações sobre como reequilibrar suas cargas de trabalho, consulte. Monitorando o FSx para balanceamento da carga de trabalho do ONTAP
	Throughput do disco	
	IOPS de disco	
	Utilização da CPU	

Seção Dashboard	Se houver um aviso para essa métrica	Faça o seguinte
Performance do disco	IOPS de disco	Aumente o IOPS de SSD se seu sistema de arquivos ainda não estiver no máximo de IOPS de SSD para a capacidade de taxa de transferência atual do seu sistema de arquivos. Para obter mais informações sobre como atualizar as IOPS provisionadas do seu sistema de arquivos, consulte. Modificando a capacidade de armazenamento SSD e o IOPS provisionado Se seu sistema de arquivos tiver vários pares de HA e sua utilização de IOPS em disco for apenas maior para um subconjunto dos agregados do sistema de arquivos (os pools de armazenamento que compõem seu nível de armazenamento primário), você também pode reequilibrar sua carga de trabalho para que o IOPS de disco seja utilizado de forma mais uniforme em todo o sistema de arquivos. Para obter mais informações sobre como reequilibrar suas cargas de trabalho, consulte. Monitorando o FSx para balanceamento da carga de trabalho do ONTAP

Para obter mais informações sobre a performance do sistema de arquivos, consulte Amazon FSx para NetApp desempenho de ONTAP.

Criação de CloudWatch alarmes da Amazon para monitorar o Amazon FSx

Você pode criar um CloudWatch alarme que envia uma mensagem do Amazon Simple Notification Service (Amazon SNS) quando o alarme muda de estado. Um alarme observa uma única métrica por um período tempo que você especifica. Se necessário, o alarme realiza uma ou mais ações com base no valor da métrica relativa a um determinado limite durante vários períodos. A ação é uma notificação enviada a um tópico do Amazon SNS ou a uma política de Auto Scaling.

Os alarmes invocam ações somente para mudanças de estado sustentadas. CloudWatch os alarmes não invocam ações somente porque estão em um estado específico; o estado deve ter sido alterado

e mantido por um determinado número de períodos. Você pode criar um alarme no console Amazon FSx ou no console da Amazon CloudWatch .

Os procedimentos a seguir descrevem como criar alarmes usando o console do Amazon FSx, a AWS Command Line Interface (AWS CLI) e a API.

Definir alarmes usando o console do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação à esquerda, escolha Sistemas de arquivos e selecione o sistema de arquivos para o qual deseja criar o alarme.
3. Na página Resumo, escolha Monitoramento e performance no segundo painel.
4. Escolha a guia CloudWatch de alarmes.
5. Escolha Criar CloudWatch alarme. O sistema redireciona você para o console do CloudWatch.
6. Escolha Selecionar métrica.
7. Na seção Métricas, escolha FSx.
8. Escolha uma categoria de métrica:
   - Métricas do sistema de arquivos
   - Métricas detalhadas do sistema de arquivos
   - Métricas de volume
   - Métricas detalhadas de volume
9. Escolha a métrica para a qual você deseja definir o alarme e Selecionar métrica.
10. Na seção Condições, escolha as condições desejadas para o alarme e selecione Próximo.

> **Note**
>
> As métricas podem não ser publicadas durante a manutenção do sistema de arquivos. Para evitar alterações desnecessárias e enganosas nas condições de alarme e configurar seus alarmes para que sejam resilientes aos pontos de dados perdidos, consulte Como configurar como os CloudWatch alarmes tratam os dados perdidos no Guia do usuário da Amazon. CloudWatch

11. Se você quiser CloudWatch enviar um e-mail ou uma notificação ao Amazon SNS quando o estado do alarme iniciar a ação, escolha um estado de alarme para o gatilho do estado do alarme.

Em Enviar uma notificação ao seguinte tópico do SNS, escolha uma opção. 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. Essa lista é salva e aparece no campo para alarmes futuros. Selecione Next (Próximo).

> **Note**
>
> Se você usar Create topic (Criar tópico) para criar um novo tópico do Amazon SNS, os endereços de e-mail deverão ser verificados antes que eles recebam notificações. Os e-mails são enviados somente quando o alerta entra em um estado de alerta. Se essa alteração no status de alarme ocorrer antes que os endereços de e-mail sejam verificados, eles não receberão notificação.

12. Preencha os campos Nome do alarme e Descrição do alarme e selecione Próximo.
13. Na página Pré-visualizar e criar, revise o alarme que está prestes a criar e escolha Criar alarme.

Para definir alarmes usando o console CloudWatch

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Escolha Criar alarme para iniciar o Assistente de criação de alarmes.
3. Siga o procedimento em Para definir alarmes usando o console do Amazon FSx, começando com a etapa 6.

Para definir um alarme usando o AWS CLI

- Chame o comando da CLI put-metric-alarm. Para obter mais informações, consulte Referência de comandos da AWS CLI.

Para definir um alarme usando a CloudWatch API

- Chame a operação da API de PutMetricalarme. Para obter mais informações, consulte a Amazon CloudWatch API Reference.

Monitorando o FSx para balanceamento da carga de trabalho do ONTAP

Se você tem um sistema de arquivos com vários pares de HA, seu desempenho e taxa de transferência estão distribuídos por cada um dos pares de HA. O FSx for ONTAP equilibra automaticamente seus arquivos à medida que eles são gravados em seu sistema de arquivos, mas, em casos raros, é possível que os dados da carga de trabalho ou a E/S fiquem desequilibrados entre os pares de HA, o que pode afetar o desempenho geral da carga de trabalho. Você pode monitorar sua carga de trabalho para garantir que ela permaneça equilibrada em cada um dos pares de HA do seu sistema de arquivos (e seus servidores de arquivos e agregados proporcionais — os pools de armazenamento que compõem seu nível de armazenamento primário).

Tópicos

Equilíbrio de utilização do armazenamento primário

A capacidade de armazenamento principal do seu sistema de arquivos é dividida igualmente entre cada um dos seus pares de HA em pools de armazenamento chamados de agregados. Cada par de HA tem um agregado. Recomendamos que você mantenha uma utilização média não superior a 80% para seu nível de armazenamento primário de forma contínua. Para sistemas de arquivos com vários pares de HA, recomendamos que você mantenha uma utilização média de até 80% para cada agregado.

Manter 80% de utilização garante que haja espaço livre para novos dados recebidos e mantém uma sobrecarga saudável para as operações de manutenção, que podem temporariamente reivindicar espaço livre em seus agregados.

Se você perceber que seus agregados estão desequilibrados, você pode aumentar a capacidade de armazenamento primário do seu sistema de arquivos (aumentando proporcionalmente a capacidade de armazenamento de cada agregado) ou pode mover seus volumes entre agregados usando o comando volume move na CLI do ONTAP.

Desequilíbrio na utilização do desempenho do servidor de arquivos e do disco

Os recursos de desempenho total do seu sistema de arquivos (como taxa de transferência de rede, taxa de transferência de servidor para disco e IOPS e IOPS de disco) são divididos igualmente entre os pares de HA do sistema de arquivos. Recomendamos que você mantenha uma utilização média abaixo de 50% (e um pico máximo de utilização abaixo de 80%) para todos os limites de desempenho de forma contínua — isso vale tanto para a utilização geral dos recursos do servidor de arquivos do seu sistema de arquivos em todos os pares de HA quanto para cada servidor de arquivos.

Se você perceber que a utilização do desempenho do servidor de arquivos está desequilibrada — e os servidores de arquivos nos quais sua carga de trabalho está desequilibrada têm uma utilização contínua de mais de 80% — você pode usar a CLI e a API REST do ONTAP para diagnosticar ainda mais a causa do desequilíbrio de desempenho e corrigi-la. A seguir está uma tabela de possíveis indicadores de desequilíbrio e as próximas etapas para diagnósticos adicionais.

Se o seu sistema de arquivos for...	Então...
A taxa de transferência do disco do servidor de arquivos ou o IOPS do disco do servidor de arquivos estão desequilibrados	Você pode estar enfrentando pontos de acesso de E/S em um subconjunto de pares de HA (um subconjunto de seus volumes contendo uma grande quantidade de dados sendo acessados), o que pode limitar o desempenho geral de sua carga de trabalho porque está congestionado em relação a um subconjunto de pares de HA. Para cada servidor de arquivos altamente utilizado, verifique os volumes mais utilizados para ver quais volumes têm mais atividade em um agregado. Para obter mais informações sobre esse procedimento, consulte Rebalanceamento de volumes altamente utilizados.
A taxa de transferência da rede está desequilibrada, mas a taxa de transferência do disco do servidor de arquivos, o IOPS do disco do servidor	Seus dados são distribuídos uniformemente entre pares de HA, mas seus clientes não. Para os servidores de arquivos que utilizam mais a taxa de transferência da rede do que outros, verifique os principais clientes de cada servidor de arquivos e, em seguida, reequilibre esses clientes desmontando todos os volumes desses clientes e remontando-os usando um endpoint diferente em um par de HA diferente. Para obter

Se o seu sistema de arquivos for...	Então...
de arquivos ou o IOPS do disco não estão desequilibrados	mais informações sobre esse procedimento, consulte Reequilibrando clientes de alto tráfego.

Mapeamento de CloudWatch dimensões para recursos da CLI do ONTAP e da API REST

Seu sistema de arquivos escalável tem CloudWatch métricas da Amazon com a dimensão `FileServer` or`Aggregate`. Para diagnosticar ainda mais os casos de desequilíbrio, você precisa mapear esses valores de dimensão para servidores de arquivos específicos (ou nós) e agregados na CLI ou na API REST do ONTAP.

- Para servidores de arquivos, cada nome de servidor de arquivos é mapeado para um nome de servidor de arquivos (ou nó) no ONTAP (por exemplo,`FsxId01234567890abcdef-01`). Os servidores de arquivos com números ímpares são servidores de arquivos preferenciais (ou seja, eles atendem ao tráfego, a menos que o sistema de arquivos tenha passado para o servidor de arquivos secundário), enquanto os servidores de arquivos com números pares são servidores de arquivos secundários (ou seja, eles fornecem tráfego somente quando o parceiro não está disponível). Por esse motivo, os servidores de arquivos secundários normalmente mostram menos utilização do que os servidores de arquivos preferenciais.
- Para agregados, cada nome agregado é mapeado para um agregado no ONTAP (por exemplo,). `aggr1` Há um agregado para cada par de HA, ou seja, o agregado `aggr1` é compartilhado por servidores de arquivos `FsxId01234567890abcdef-01` (o servidor de arquivos ativo) e `FsxId01234567890abcdef-02` (o servidor de arquivos secundário) em um par de HA, o agregado `aggr2` é compartilhado por servidores de arquivos `FsxId01234567890abcdef-03` e assim por `FsxId01234567890abcdef-04` diante.

Você pode visualizar os mapeamentos entre todos os agregados e servidores de arquivos usando a CLI do ONTAP.

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar a CLI do NetApp ONTAP do usuário do Amazon FSx for ONTAP. NetApp

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Use o comando storage aggregate show, especificando o `-fields node` parâmetro.

```
::> storage aggregate show -fields node
aggregate                     node
----------------------------- ------------------------
aggr1                         FsxId01234567890abcdef-01
aggr2                         FsxId01234567890abcdef-03
aggr3                         FsxId01234567890abcdef-05
aggr4                         FsxId01234567890abcdef-07
aggr5                         FsxId01234567890abcdef-09
aggr6                         FsxId01234567890abcdef-11
6 entries were displayed.
```

Reequilibrando clientes de alto tráfego

Se você estiver enfrentando um desequilíbrio de E/S nos servidores de arquivos (especificamente com a utilização da taxa de transferência da rede), clientes de E/S elevados podem ser a causa. Para identificar clientes de alto tráfego, use a CLI do ONTAP.

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar a CLI do NetApp ONTAP do usuário do Amazon FSx for ONTAP. NetApp

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Para visualizar os clientes com maior tráfego, use o comando statistics top client show ONTAP CLI. Opcionalmente, você pode especificar o `-node` parâmetro para visualizar somente os principais clientes de um servidor de arquivos específico. Se você estiver diagnosticando um desequilíbrio em um servidor de arquivos específico, use o `-node` parâmetro, `node_name` substituindo-o pelo nome do servidor de arquivos (por exemplo,`FsxId01234567890abcdef-01`).

   Opcionalmente, você pode adicionar o `-interval` parâmetro, fornecendo o intervalo durante o qual medir (em segundos) antes da saída de cada relatório. Aumentar o intervalo (por exemplo, até o máximo de 300 segundos) fornece uma amostra de longo prazo da quantidade de tráfego direcionada para cada volume. O padrão é 5 (segundos).

```
::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
```

Na saída, os principais clientes são mostrados pelo endereço IP e pela porta.

```
                                                      *Total     Total
            Client   Vserver          Node                Ops     (Bps)
------------------ --------- ------------------------ ------ ---------
 172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
```

3. Você pode reequilibrar um subconjunto dos clientes de alto tráfego listados para outros servidores de arquivos. Para fazer isso, desmonte o volume do cliente e remonte-o usando o nome DNS do endpoint NFS/SMB do SVM. Isso retorna um endpoint aleatório correspondente a um par HA aleatório.

   Recomendamos que você reutilize o nome DNS, mas você tem a opção de escolher explicitamente qual par de HA um determinado cliente monta. Para garantir que você esteja montando um cliente em um endpoint diferente, você pode especificar um endereço IP de endpoint diferente daquele que corresponde ao nó com alto tráfego. Você pode fazer isso executando o seguinte comando:

   ```
   ::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
    address,curr-node
   vserver   lif                  address      curr-node
   --------- -------------------- ------------ ------------------------
   svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
   svm01 nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
   2 entries were displayed.
   ```

   De acordo com o exemplo de saída do `statistics top client show` comando, o cliente `172.17.236.53` está direcionando tráfego intenso para `FsxId01234567890abcdef-01` o. A saída do `network interface show` comando indica que esse é o endereço`172.31.15.89`. Para montar em um endpoint diferente, selecione qualquer outro endereço (neste exemplo, o único outro endereço é`172.31.8.112`, correspondente a`FsxId01234567890abcdef-03`).

Rebalanceamento de volumes altamente utilizados

Se você estiver enfrentando um desequilíbrio de E/S em seus volumes ou agregados, você pode reequilibrar os volumes para redistribuir o tráfego de E/S entre seus volumes.

> **Note**
>
> Se você estiver enfrentando um desequilíbrio na utilização do armazenamento em seus agregados, geralmente não há nenhum impacto no desempenho, a menos que a alta utilização esteja associada ao desequilíbrio de E/S. Embora você possa mover volumes entre agregados para equilibrar a utilização do armazenamento, recomendamos mover volumes somente se você estiver vendo um impacto no desempenho, pois a movimentação de volumes pode ter um impacto adverso no desempenho se você também não considerar a I/O direcionada para cada volume que você está pensando em mover.

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar a CLI do NetApp ONTAP do usuário do Amazon FSx for ONTAP. NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Use o comando da CLI statistics volume show ONTAP para visualizar os volumes de maior tráfego para um determinado agregado, com as seguintes alterações:

   - Substitua *`aggregate_name`* pelo nome do agregado (por exemplo,). `aggr1`
   - Opcionalmente, você pode adicionar o `-interval` parâmetro, fornecendo o intervalo durante o qual medir (em segundos) antes da saída de cada relatório. Aumentar o intervalo (por exemplo, até o máximo de 300 segundos) fornece uma amostra de longo prazo da quantidade de tráfego direcionada para cada volume. O padrão é 5 (segundos).

   ```
   ::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
    [5,300]]
   ```

   Dependendo do intervalo escolhido, pode levar até 5 minutos para mostrar os dados. O comando mostra todos os volumes no agregado, junto com a quantidade de tráfego direcionada para cada agregado.

```
                          *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (us)
---------- ------- --------- ------ ---- ----- ----- --------- ----- -------
vol1__0007    svm1     aggr1   4078 4078     0     0 267255808     0    1092
vol1__0005    svm1     aggr1   4078 4078     0     0 267255808     0    1086
vol1__0003    svm1     aggr1   4077 4077     0     0 267223040     0    1086
vol1__0001    svm1     aggr1   4077 4077     0     0 267239424     0    1087
vol1__0008    svm1     aggr2   2314 2314     0     0 151650304     0    1112
vol1__0006    svm1     aggr2   2144 2144     0     0 140509184     0    1104
vol1__0002    svm1     aggr2   2183 2183     0     0 143065088     0    1106
vol1__0004    svm1     aggr2   2183 2183     0     0 143065088     0    1103
```

As estatísticas de volume são mostradas por constituinte (por exemplo, `vol1__0015` é o 15º constituinte de). FlexGroup `vol1` Você pode ver na saída do exemplo que os constituintes de `aggr1` são mais utilizados do que os constituintes de. `aggr2` Para equilibrar o tráfego entre os agregados, você pode mover os volumes constituintes entre os agregados para que o tráfego seja distribuído de forma mais uniforme.

3. Para mover um volume entre agregados, use o comando volume move start ONTAP CLI, substituindo os seguintes valores:

   - Substitua *`svm_name pelo nome`* da SVM que hospeda o volume que você está movendo.
   - Substitua *`volume_name`* pelo nome do componente do volume (por exemplo,). `vol1__0001`
   - Substitua *`aggregate_name`* pelo nome do agregado de destino do volume.

   > **Important**
   >
   > A movimentação de volumes consome recursos de rede e disco para os servidores de arquivos de origem e de destino. Como resultado, o desempenho de sua carga de trabalho pode ser afetado por qualquer movimentação de volume em andamento. Além disso, há uma fase de transição do processo de movimentação do volume que pausa temporariamente a E/S de qualquer tráfego para o volume.

```
::> volume move start -vserver svm_name -volume volume_name -
destination aggregate_name -foreground false
[Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".
```

```
Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the
 status of this operation.
```

Para verificar o status da operação de movimentação de volume, use o comando `volume move show` ONTAP CLI.

```
::> volume move show -vserver svm_name -volume volume_name
                          Vserver Name: svm01
                           Volume Name: vol1__0001
                  Actual Completion Time: -
                         Bytes Remaining: 1.00TB
           Specified Action For Cutover: retry_on_failure
         Specified Cutover Time Window: 30
                 Destination Aggregate: aggr2
                      Destination Node: FsxId01234567890abcdef-03
                       Detailed Status: Transferring data: 12.23GB sent.
                    Percentage Complete: 1%
                             Move Phase: replicating
               Prior Issues Encountered: -
           Estimated Remaining Duration: 00:40:25
                 Replication Throughput: 434.3MB/s
                      Duration of Move: 00:00:27
                      Source Aggregate: aggr2
                           Source Node: FsxId01234567890abcdef-01
                            Move State: healthy
```

Esse comando mostra o tempo estimado para concluir a movimentação, como um dos campos de informação. Quando a operação for concluída, o mesmo comando mostrará que o `Move Phase` campo foi preenchido.

Você deve garantir que cada um FlexGroup seja distribuído uniformemente em seus agregados, de preferência com os 8 constituintes recomendados por agregado. Se você mover um volume constituinte para outro agregado para obter um equilíbrioFlexGroup, deverá, por sua vez, mover outro volume constituinte (menos utilizado) para o agregado de origem para manter o equilíbrio.

Monitoramento de eventos EMS do FSx para ONTAP

Você pode monitorar os eventos do sistema de arquivos do FSx para ONTAP usando o sistema de gerenciamento de eventos (EMS) nativo do NetApp ONTAP. Você pode visualizar esses eventos usando a CLI do NetApp ONTAP.

Tópicos

Visão geral dos eventos EMS

Os eventos do EMS são notificações geradas automaticamente que alertam você quando uma condição predefinida ocorre em seu sistema de arquivos FSx for ONTAP. Essas notificações mantêm você informado para que você possa evitar ou corrigir problemas que podem levar a problemas maiores, como aqueles de autenticação de máquina virtual de armazenamento (SVM) ou volumes cheios.

Por padrão, os eventos são registrados no log do sistema de gerenciamento de eventos. Usando o EMS, você pode monitorar eventos como alterações na senha do usuário, um componente com capacidade quase FlexGroup total, um número de unidade lógica (LUN) colocado manualmente on-line ou off-line ou um volume redimensionado automaticamente.

Para obter mais informações sobre eventos do ONTAP EMS, consulte Referência do ONTAP EMS no Centro de Documentação do NetApp ONTAP. Para exibir as categorias de eventos, use o painel de navegação esquerdo do documento.

> **Note**
>
> Somente algumas mensagens do EMS do ONTAP estão disponíveis para sistemas de arquivos do FSx para ONTAP. Para ver uma lista das mensagens do ONTAP EMS disponíveis, use o comando show do catálogo de eventos do NetApp ONTAP CLI.

As descrições de eventos EMS contêm nomes de eventos, gravidade, possíveis causas, mensagens de log e ações corretivas que podem ajudar você a decidir como responder. Por exemplo, um evento wafl.vol.autosize.Fail ocorre quando o dimensionamento automático de um volume falha. De acordo com a descrição do evento, a ação corretiva é aumentar o tamanho máximo do volume ao definir o tamanho automático.

Visualização de eventos EMS

Use o comando NetApp ONTAP CLI event log show para exibir o conteúdo do registro de eventos. Esse comando estará disponível se você tiver o perfil `fsxadmin` em seu sistema de arquivos. A sintaxe do comando é a seguinte:

```
event log show [event_options]
```

Os eventos mais recentes são listados primeiro. Por padrão, esse comando exibe os eventos de nível de gravidade `EMERGENCY`, `ALERT` e `ERROR` com as seguintes informações:

- Hora: a hora do evento.
- Nó: o nó em que o evento ocorreu.
- Gravidade: o nível de gravidade do evento. Para exibir os eventos de nível de gravidade `NOTICE`, `INFORMATIONAL` ou `DEBUG`, use a opção `-severity`.
- Evento: o nome e a mensagem do evento.

Para exibir informações detalhadas sobre eventos, use uma ou mais das opções de eventos listadas na tabela a seguir.

Opção de evento	Descrição
`-detail`	Exibe informações adicionais sobre o evento.
`-detailtime`	Exibe informações detalhadas do evento em ordem cronológica inversa.
`-instance`	Exibe informações detalhadas sobre todos os campos.
`-node` *`nodename`*`|local`	Exibe uma lista de eventos para o nó que você especifica. Use essa opção com `-seqnum` para exibir informações detalhadas.

Opção de evento	Descrição
`-seqnum` *sequence_number*	Seleciona os eventos que correspondem a esse número na sequência. Use com `-node` para exibir informações detalhadas.

Opção de evento	Descrição

`-time MM/DD/YYYY HH:MM:SS`	Seleciona os eventos que aconteceram nesse horário específico. Use o formato: MM/DD/AAAA HH:MM:SS [+-HH:MM]. Você pode especificar um intervalo de tempo usando o operador `..` entre duas declarações de tempo.
	`event log show -time "04/17/2023 05:55:00".."04/17/2023 06:10:00"`
	Os valores comparativos de tempo são relativos à hora atual quando você executa o comando. O exemplo a seguir mostra como exibir apenas eventos que ocorreram no último minuto:
	`event log show -time >1m`
	Os campos de mês e data dessa opção não são preenchidos com zero. Esses campos podem ter dígito únicos; por exemplo, `4/1/2023 06:45:00`.

Opção de evento	Descrição
`-severity sev_level`	Seleciona os eventos que correspondem ao valor *sev_level* , que deve ser um dos seguintes: • EMERGENCY : interrupção • ALERT: único ponto de falha • ERROR: redução • NOTICE: informações • INFORMATIONAL : informações • DEBUG: informações de depuração Para exibir todos os eventos, especifique a gravidade da seguinte forma: `event log show -severity <=DEBUG`

Opção de evento	Descrição
`-ems-severity` *ems_sev_level*	Seleciona os eventos que correspondem ao valor *ems_sev_level* , que deve ser um dos seguintes: • `NODE_FAULT` : a corrupção de dados é detectada ou o nó não consegue fornecer atendimento ao cliente. • `SVC_FAULT` : uma perda temporária de serviço, normalmente uma falha transitória, é detectada. • `NODE_ERROR` : um erro de hardware que não é imediatamente fatal é detectado. • `SVC_ERROR` : um erro de software que não é imediatamente fatal é detectado. • `WARNING`: uma mensagem de alta prioridade que não indica uma falha. • `NOTICE`: uma mensagem de prioridade normal que não indica uma falha. • `INFO`: uma mensagem de baixa prioridade que não indica uma falha. • `DEBUG`: uma mensagem de depuração.

Opção de evento	Descrição
	• VAR: uma mensagem com gravidade variável, selecionada no runtime. Para exibir todos os eventos, especifique a gravidade da seguinte forma: `event log show -ems-severity <=DEBUG`
`-source` *text*	Seleciona os eventos que correspondem ao valor *text*. Normalmente, a fonte é um módulo de software.
`-message-name` *message_name*	Seleciona os eventos que correspondem ao valor *message_name* . Os nomes das mensagens são descritivos; portanto, a filtragem da saída por nome da mensagem exibe mensagens de um tipo específico.
`-event` *text*	Seleciona os eventos que correspondem ao valor *text*. O campo `event` contém o texto completo do evento, incluindo todos os parâmetros.

Opção de evento	Descrição
`-kernel-generation-num` *integer*	Seleciona os eventos que correspondem ao valor *integer*. Somente eventos provenientes do kernel têm números de geração do kernel.
`-kernel-sequence-num` *integer*	Seleciona os eventos que correspondem ao valor *integer*. Somente eventos provenientes do kernel têm números de sequência do kernel.
`-action` *text*	Seleciona os eventos que correspondem ao valor *text*. O campo `action` descreve qual ação corretiva , se houver, você deve tomar para remediar a situação.
`-description` *text*	Seleciona os eventos que correspondem ao valor *text*. O campo `description` descreve por que o evento aconteceu e o que isso significa.
`-filter-name` *filter_name*	Seleciona os eventos que correspondem ao valor *filter_name* . Somente os eventos incluídos pelos filtros existentes que correspondem a esse valor são exibidos.

Opção de evento	Descrição
`-fields fieldname ,...`	Indica que a saída do comando também inclui os campos especificados. Você pode usar `-fields ?` para escolher os campos que deseja especificar.

Visualizar eventos EMS

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar a CLI do NetApp ONTAP do usuário do Amazon FSx for ONTAP. NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Use o comando `event log show` para exibir o conteúdo do log de eventos.

   ```
   ::> event log show
   Time                Node          Severity      Event
   ------------------- ------------- ------------- -------------------------
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0a.
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0d.
   ```

Para obter informações sobre os eventos do EMS retornados pelo `event log show` comando, consulte a Referência do ONTAP EMS no Centro de Documentação do NetApp ONTAP.

Encaminhamento de eventos do EMS para um servidor Syslog

Você pode configurar eventos do EMS para encaminhar notificações para um servidor Syslog. O encaminhamento de eventos do EMS é usado para monitorar em tempo real seu sistema de arquivos para determinar e isolar as causas-raiz de uma ampla variedade de problemas. Se o seu ambiente ainda não tiver um servidor Syslog para notificações de eventos, você deverá primeiro criar um. O DNS deve ser configurado no sistema de arquivos para resolver o nome do servidor Syslog.

Para configurar eventos do EMS para encaminhar notificações para um servidor Syslog

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar a CLI do NetApp ONTAP do usuário do Amazon FSx for ONTAP. NetApp

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Use o comando event notification destination create para criar um destino de notificação de eventos do tipo`syslog`, especificando os seguintes atributos:

   - *`dest_name`*— O nome do destino da notificação que deve ser criado (por exemplo,`syslog-ems`). O nome do destino de uma notificação de evento deve ter de 2 a 64 caracteres. Os caracteres válidos são os seguintes caracteres ASCII: A-Z, a-z, 0-9, “_” e “-”. O nome deve começar e terminar com: A-Z, a-z ou 0-9.
   - *`syslog_name`*— O nome do host ou endereço IP do servidor Syslog para o qual as mensagens do Syslog são enviadas.
   - *`transport_protocol`*— O protocolo usado para enviar os eventos:
     - `udp-unencrypted`— Protocolo de datagrama de usuário sem segurança. Esse é o protocolo padrão.
     - `tcp-unencrypted`— Protocolo de controle de transmissão sem segurança.
     - `tcp-encrypted`— Protocolo de controle de transmissão com Transport Layer Security (TLS). Quando essa opção é especificada, o FSx for ONTAP verifica a identidade do host de destino validando seu certificado.
   - *`port_number`*— A porta do servidor Syslog para a qual as mensagens do Syslog são enviadas. O `syslog-port` parâmetro de valor padrão depende da configuração do `syslog-transport` parâmetro. Se `syslog-transport` estiver definido como`tcp-encrypted`, o valor `syslog-port` padrão será`6514`. Se `syslog-transport` estiver definido como`tcp-unencrypted`, `syslog-port` tem o valor padrão`601`. Caso contrário, a porta padrão será definida como`514`.

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. Use o comando event notification create para criar uma nova notificação de um conjunto de eventos definido por um filtro de eventos para o destino da notificação criado na etapa anterior, especificando os seguintes atributos:

   - *node_name*— O nome do filtro de eventos. Os eventos incluídos no filtro de eventos são encaminhados para os destinos especificados no `-destinations` parâmetro.
   - *dest_name*— O nome do destino de notificação existente para o qual as notificações de eventos são enviadas.

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. Use o `event notification destination check` comando para gerar uma mensagem de teste e verificar se sua configuração funciona. Especifique os seguintes atributos com o comando:

   - *node_name*— O nome do nó (por exemplo,`FsxId07353f551e6b557b4-01`).
   - *dest_name*— O nome do destino de notificação existente para o qual as notificações de eventos são enviadas.

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

Monitoramento com o Cloud Insights

NetApp O Cloud Insights é um NetApp serviço que você pode usar para monitorar seus sistemas de arquivos Amazon FSx for NetApp ONTAP junto com suas outras NetApp soluções de armazenamento. Com o Cloud Insights, você pode monitorar as métricas de configuração, capacidade e performance ao longo do tempo para entender as tendências da sua workload e planejar as necessidades futuras de performance e capacidade de armazenamento. Você também pode criar alertas com base nas condições de métricas que podem ser integradas aos seus fluxos de trabalho e ferramentas de produtividade existentes.

> **Note**
>
> O Cloud Insights não é compatível com sistemas de arquivos escaláveis.

O Cloud Insights fornece:

- Uma variedade de métricas e logs: colete métricas de configuração, capacidade e performance. Entenda a tendência da sua workload com painéis, alertas e relatórios predefinidos.
- Análise do usuário e proteção contra ransomware: com os snapshots do Cloud Secure e do ONTAP, você pode auditar, detectar, interromper e reparar incidentes de erro do usuário e ransomware.
- SnapMirror relatórios — entenda seus SnapMirror relacionamentos e defina alertas sobre problemas de replicação.
- Planejamento de capacidade: entenda os requisitos de recursos das workloads on-premises para ajudar você a migrar sua workload para uma configuração mais eficiente do FSx para ONTAP. Você também pode usar esses insights para planejar quando será necessário mais performance ou capacidade para a implantação do FSx para ONTAP.

Para obter mais informações sobre o Cloud Insights, consulte NetApp Cloud Insights no NetApp Cloud Central.

Monitorar sistemas de arquivos do FSx para ONTAP usando Harvest e Grafana

NetApp O Harvest é uma ferramenta de código aberto para coletar métricas de desempenho e capacidade dos sistemas ONTAP e é compatível com o FSx for ONTAP. Você pode usar o Harvest com Grafana para uma solução de monitoramento de código aberto.

Começando com Harvest e Grafana

A seção a seguir detalha como você pode instalar e configurar o Harvest e o Grafana para medir seu FSx para o desempenho e a utilização da capacidade de armazenamento do sistema de arquivos ONTAP.

Você pode monitorar seu sistema de arquivos Amazon FSx for NetApp ONTAP usando o Harvest e o Grafana. NetApp O Harvest monitora os data centers ONTAP coletando métricas de desempenho,

capacidade e hardware do FSx para sistemas de arquivos ONTAP. O Grafana fornece um painel em que as métricas coletadas do Harvest podem ser exibidas.

Painéis compatíveis do Harvest

O Amazon FSx for NetApp ONTAP expõe um conjunto de métricas diferente do ONTAP local. NetApp Portanto, somente os seguintes painéis do out-of-the-box Harvest marcados com `fsx` são atualmente suportados para uso com FSx for ONTAP. Alguns desses painéis podem não apresentar as informações que não são compatíveis.

- ONTAP: conformidade
- ONTAP: snapshots de proteção de dados
- ONTAP: segurança
- ONTAP: SVM
- ONTAP: volume

AWS CloudFormation modelo

Para começar, você pode implantar um AWS CloudFormation modelo que inicia automaticamente uma instância do Amazon EC2 executando Harvest e Grafana. Como entrada para o AWS CloudFormation modelo, você especifica o `fsxadmin` usuário e o endpoint de gerenciamento do Amazon FSx para o sistema de arquivos que será adicionado como parte dessa implantação. Depois que a implantação for concluída, você poderá fazer login no painel do Grafana para monitorar seu sistema de arquivos.

Essa solução é usada AWS CloudFormation para automatizar a implantação da solução Harvest e Grafana. O modelo cria uma instância do Linux do Amazon EC2 e instala os softwares Harvest e Grafana. Para usar essa solução, baixe o modelo AWS CloudFormation fsx-ontap-harvest-grafana.template.

> **Note**
>
> A implementação dessa solução gera cobrança pelos serviços associados AWS . Para obter mais informações, consulte as páginas de detalhes de preços desses serviços.

Tipos de instância do Amazon EC2

Ao configurar o modelo, você fornece o tipo de instância do Amazon EC2. NetAppA recomendação da para o tamanho da instância depende de quantos sistemas de arquivos você monitora e do número de métricas que você escolhe coletar. Com a configuração padrão, para cada 10 sistemas de arquivos que você monitora, NetApp recomenda:

- CPU: dois núcleos
- Memória: 1 GB
- Disco: 500 MB (usado principalmente por arquivos de log)

Veja a seguir alguns exemplos de configurações e o tipo de instância `t3` que você pode escolher.

Sistemas de arquivos	CPU	Disk	Tipo de instância
Menos de 10	2 núcleos	500 MB	`t3.micro`
De 10 a 40	4 núcleos	1.000 MB	`t3.xlarge`
40+	8 núcleos	2.000 MB	`t3.2xlarge`

Para obter mais informações sobre os tipos de instância do Amazon EC2, consulte Instâncias de uso geral no Guia do usuário do Amazon EC2.

Regras de porta para instância

Ao configurar sua instância do Amazon EC2, certifique-se de que as portas 3000 e 9090 estejam abertas para tráfego de entrada do grupo de segurança em que as instâncias do Harvest e Grafana do Amazon EC2 estão. Como a instância iniciada se conecta a um endpoint via HTTPS, ela precisa resolver o endpoint, que precisa da porta 53 TCP/UDP para DNS. Além disso, para alcançar o endpoint, ele precisa da porta 443 TCP para HTTPS e acesso à Internet.

Procedimento de implantação

O procedimento a seguir configura e implanta a solução Harvest e Grafana. A implantação demora cerca de cinco minutos. Antes de começar, você deve ter um sistema de arquivos FSx for ONTAP em execução em uma Amazon Virtual Private Cloud (Amazon VPC) em sua AWS conta e as

informações de parâmetros do modelo listado abaixo. Para obter mais informações sobre como criar um sistema de arquivos, consulte Como criar sistemas de arquivos do FSx para ONTAP.

Executar a pilha de soluções Harvest e Grafana

1. Baixe o modelo AWS CloudFormation fsx-ontap-harvest-grafana.template. Para obter mais informações sobre como criar uma AWS CloudFormation pilha, consulte Como criar uma pilha no AWS CloudFormation console no Guia do AWS CloudFormation usuário.

   > **Note**
   >
   > Por padrão, esse modelo é iniciado na AWS região Leste dos EUA (Norte da Virgínia). Você deve iniciar essa solução em um Região da AWS local onde o Amazon FSx esteja disponível. Para obter mais informações, consulte Amazon FSx endpoints and quotas 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
InstanceType	`t3.micro`	O tipo de instância do Amazon EC2. A seguir, estão os tipos de instância `t3`. • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` Para obter a lista completa dos valores de tipo de

Parâmetro	Padrão	Descrição
		instância do Amazon EC2 permitidos para esse parâmetro, consulte o fsx-ontap-harvest-grafana .template.
KeyPair	Nenhum valor padrão	O par de chaves que é usado para acessar a instância do Amazon EC2.
SecurityGroup	Nenhum valor padrão	O ID do grupo de segurança da instância do Harvest e Grafana. Certifique-se de que as portas de entrada 3000 e 9090, além das portas 53 e 443, estejam abertas pelos clientes que você deseja usar para acessar seu painel da Grafana.
Tipo de sub-rede	Nenhum valor padrão	Especifique o tipo de sub-rede, `public` ou `private`. Use uma sub-rede `public` para recursos que devem estar conectados à Internet e uma sub-rede privada para recursos que não estarão conectados à Internet. Para obter mais informações, consulte Tipos de sub-redes no Guia do usuário da Amazon VPC.

Parâmetro	Padrão	Descrição
Sub-rede	Nenhum valor padrão	Especifique a mesma sub-rede do Amazon FSx NetApp para a sub-rede preferencial do sistema de arquivos ONTAP. Você pode encontrar o ID da sub-rede preferencial do sistema de arquivos no console do Amazon FSx, na guia Rede e segurança da página de detalhes do sistema de arquivos do FSx para ONTAP
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	A versão mais recente da AMI do Amazon Linux 2 em uma determinada Região da AWS.
SxEndPonto F	Nenhum valor padrão	O endereço IP do endpoint de gerenciamento do sistema de arquivos. Você pode encontrar o endereço IP do endpoint de gerenciamento do sistema de arquivos no console do Amazon FSx, na guia Administração da página de detalhes do sistema de arquivos do FSx para ONTAP.

Parâmetro	Padrão	Descrição
SecretName	Nenhum valor padrão	AWS Secrets Manager nome secreto contendo a senha do `fsxadmin` usuário do sistema de arquivos. Essa é a senha que você forneceu ao criar o sistema de arquivos.

3. Selecione Next (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 ver o status da pilha no AWS CloudFormation console na coluna Status. Você deverá visualizar um status CREATE_COMPLETE em cerca de cinco minutos.

Fazer login no Grafana

Após a conclusão da implantação, use seu navegador para fazer login no painel do Grafana no IP e na porta 3000 da instância do Amazon EC2:

```
http://EC2_instance_IP:3000
```

Quando solicitado, use o nome de usuário (`admin`) e a senha (`pass`) padrão do Grafana. Recomendamos que você altere sua senha assim que fizer login.

Para obter mais informações, consulte a página NetApp Harvest em GitHub.

Solução de problemas de Harvest e Grafana

Se você encontrar algum dado ausente mencionado nos painéis do Harvest e do Grafana ou estiver tendo problemas para configurar o Harvest e o Grafana com o FSx for ONTAP, consulte os tópicos a seguir para ver uma possível solução.

Tópicos

Os painéis de SVM e volume estão em branco

Se a AWS CloudFormation pilha foi implantada com sucesso e puder entrar em contato com a Grafana, mas os painéis de SVM e volume estiverem em branco, use o procedimento a seguir para solucionar problemas em seu ambiente. Você precisará de acesso SSH à instância do Amazon EC2 na qual o Harvest e o Grafana estão implantados.

1. Faça o SSH na instância do Amazon EC2 na qual seus clientes Harvest e Grafana estão sendo executados.

```
[~]$ ssh ec2-user@ec2_ip_address
```

2. Use o comando a seguir para abrir o `harvest.yml` arquivo e:
   - Verifique se uma entrada foi criada para sua instância FSx for ONTAP como. `Cluster-2`
   - Verifique se as entradas de nome de usuário e senha correspondem às suas `fsxadmin` credenciais.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/
harvest.yml
```

3. Se o campo de senha estiver em branco, abra o arquivo em um editor e atualize-o com a `fsxadmin` senha, da seguinte forma:

```
[ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
harvest.yml
```

4. Certifique-se de que as credenciais `fsxadmin` do usuário estejam armazenadas no Secrets Manager no formato a seguir para qualquer implantação futura, *`fsxadmin_password`* substituindo-as pela sua senha.

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

CloudFormation pilha revertida após o tempo limite

Se você não conseguir implantar a CloudFormation pilha com êxito e ela estiver sendo revertida com erros, use o procedimento a seguir para resolver o problema. Você precisará de acesso SSH à instância EC2 implantada pela pilha. CloudFormation

1. Reimplante a CloudFormation pilha, certificando-se de que a reversão automática esteja desativada.
2. Faça o SSH na instância do Amazon EC2 na qual seus clientes Harvest e Grafana estão sendo executados.

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. Verifique se os contêineres do docker foram iniciados com sucesso usando o comando a seguir.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

Na resposta, você deve ver cinco contêineres da seguinte forma:

```
CONTAINER ID   IMAGE                    COMMAND                  CREATED
 STATUS                          PORTS                     NAMES
6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
 Restarting (1) 20 seconds ago                             harvest_cluster-2
3cf3e3623fde   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago   Up
 About a minute                                            harvest_cluster-1
708f3b7ef6f8   grafana/grafana         "/run.sh"                8 minutes ago   Up
 8 minutes                   0.0.0.0:3000->3000/tcp   harvest_grafana
0febee61cab7   prom/alertmanager       "/bin/alertmanager -…"   8
 minutes ago   Up 8 minutes                    0.0.0.0:9093->9093/tcp
 harvest_prometheus_alertmanager
1706d8cd5a0c   prom/prometheus         "/bin/prometheus --c…"   8 minutes ago   Up
 8 minutes                   0.0.0.0:9090->9090/tcp   harvest_prometheus
```

4. Se os contêineres do docker não estiverem em execução, verifique se há falhas no `/var/log/cloud-init-output.log` arquivo da seguinte maneira.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
     PLAY [Manage Harvest]
 ****************************************************

TASK [Gathering Facts] ********************************************************
```

```
ok: [localhost]

TASK [Verify images] ************************************************************
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
 "changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
 ('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
 "changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP **********************************************************************
localhost                  : ok=1    changed=0    unreachable=0    failed=1
 skipped=0    rescued=0    ignored=0
```

5. Se houver falhas, execute os comandos a seguir para implantar os contêineres Harvest e Grafana.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
     [ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml --tags api
```

6. Valide os contêineres iniciados com sucesso executando sudo docker ps e conectando-se à sua URL do Harvest e da Grafana.

Registro em log de chamadas de API do FSx para ONTAP com AWS CloudTrail

O Amazon FSx é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um serviço da AWS no Amazon FSx. O CloudTrail captura todas as chamadas de API do Amazon FSx para o Amazon FSx para NetApp ONTAP como eventos. As chamadas capturadas incluem as do console do Amazon FSx e as de código para as operações da API do Amazon FSx.

Caso crie uma trilha, você poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos do Amazon FSx. 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 feita ao Amazon FSx. 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 sobre o Amazon FSx no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre uma atividade de API no Amazon FSx, ela é registrada em um evento do CloudTrail com outros eventos de serviço da AWS no Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte Viewing events with CloudTrail Event history (Como visualizar eventos com o histórico de eventos do CloudTrail).

Para obter um registro contínuo de eventos na conta da AWS, incluindo eventos do Amazon FSx, 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:

- Criar uma trilha para a sua Conta da AWS
- Integrações de serviços da AWS com logs do 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 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 Guia do usuário do AWS CloudTrail.

Noções básicas sobre entradas de arquivos de log do Amazon FSx

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"
}
```

Cotas

A seguir, você pode descobrir mais sobre cotas ao trabalhar com o Amazon FSx NetApp for ONTAP.

Tópicos

Cotas que podem ser aumentadas

A seguir estão as cotas do Amazon FSx NetApp for ONTAP para Conta da AWS cada, Região da AWS por, que você pode aumentar.

Recurso	Padrão	Descrição
Sistemas de arquivos do ONTAP	100	O número máximo de sistemas de arquivos Amazon FSx for NetApp ONTAP que você pode criar nessa conta.
ONTAPCapacidade de armazenamento SSD	524.288	A quantidade máxima de capacidade de armazenam ento SSD (em GiB) para todos os sistemas de arquivos Amazon FSx NetApp for ONTAP que você pode ter nessa conta.
ONTAPcapacidade de produção	10,240	A quantidade máxima de capacidade de transferência (em MBps) para todos os sistemas de arquivos Amazon FSx for NetApp ONTAP que você pode ter nessa conta.

Recurso	Padrão	Descrição
ONTAPSSD IOPS	1.000.000	A quantidade máxima de SSD IOPS para todos os sistemas de arquivos Amazon FSx for NetApp ONTAP que você pode ter nessa conta.
ONTAPbackups por sistema de arquivos	10.000	O número máximo de backups de volume iniciados pelo usuário para todos os sistemas de arquivos Amazon FSx NetApp for ONTAP que você pode ter nessa conta.

Para solicitar um aumento da cota

1. Abra a página AWS Support, faça login se necessário e escolha Create case (Criar caso).
2. Em Criar caso, escolha Suporte para conta e faturamento.
3. No painel Detalhes do caso, faça as seguintes entradas:
   - Em Tipo, escolha Conta.
   - Em Categoria, escolha Outros problemas de conta.
   - Em Assunto, insira **`Amazon FSx for NetApp ONTAP service limit increase request`**.
   - Forneça uma Descrição detalhada de sua solicitação, incluindo:
     - A cota do FSx que você deseja aumentar e o valor para o qual deseja aumentá-la, se conhecido.
     - O motivo de estar buscando o aumento da cota.
     - O ID do sistema de arquivos e a região de cada sistema de arquivos para o qual você está solicitando um aumento.
4. Forneça suas Opções de contato preferenciais e escolha Enviar.

Cotas de recursos para cada sistema de arquivos

A tabela a seguir lista as cotas no Amazon FSx NetApp para recursos ONTAP para cada sistema de arquivos em um. Região da AWS

Recurso	Limite por sistema de arquivos
Capacidade mínima de armazenamento SSD	1.024 GiB por par de alta disponibilidade (HA)
Capacidade máxima de armazenamento SSD	• Escalabilidade horizontal: 512 TiB por par de HA, até 1 PiB • Aumento de escala: 192 TiB
IOPS de SSD máxima	Expansão: • 200.000 por par de HA (até 12 pares) Aumento de escala: • 160.000 na região Leste dos EUA (Ohio), Região Leste dos EUA (Norte da Virgínia), Região Oeste dos EUA (Oregon) e Europa (Irlanda) • 80.000 em todos os outros Regiões da AWS lugares onde o FSx for ONTAP está disponível
Capacidade de throughput mínima	• Expansão: 3.072 MBps por par de HA • Aumento de escala: 128 MBps
Capacidade de throughput máxima	Expansão: • 73.728 Mbps 1

Recurso	Limite por sistema de arquivos
	Aumento de escala: • 4.096 MBps [2] na região Leste dos EUA (Ohio), Região Leste dos EUA (Norte da Virgínia), Região Oeste dos EUA (Oregon) e Europa (Irlanda) • 2.048 MBps em todos os outros em que o Regiões da AWS FSx for ONTAP está disponível
Número máximo de volumes	• Expansão: 1.000 • Aumento de escala: 500
Número máximo de snapshots	1.023 por volume 3
Número máximo de backups	4.091 por volume 4

Recurso	Limite por sistema de arquivos
Número máximo de SVMs	Expansão: • 5 Aumento de escala: • 6 (capacidade de throughput de 128 MBps) • 6 (capacidade de throughput de 256 MBps) • 14 (capacidade de throughput de 512 MBps) • 14 (capacidade de throughput de 1.024 MBps) • 24 (capacidade de throughput de 2.048 MBps) • 24 (capacidade de throughput de 4.096 MBps)
Número máximo de tags	50
Período máximo de retenção para backups automatizados	90 dias
Período máximo de retenção para backups iniciados pelo usuário	Sem limite de retenção
Número máximo de rotas suportadas por sistema de arquivos	50 [5]

Note

[1] Em um sistema de arquivos escalável com 12 pares de HA (6.144 MBps por par de HA). Para ter mais informações, consulte Pares de alta disponibilidade (HA).

[2] Para provisionar 4 GBps de capacidade de taxa de transferência, seu sistema de arquivos escalável FSx for ONTAP requer uma configuração de IOPS SSD máxima (160.000) e um mínimo de 5.120 GiB de capacidade de armazenamento SSD em um suporte. Região da AWS Para obter mais informações sobre quais Regiões da AWS suportam 4.096 MBps de capacidade de taxa de transferência, consulte. Impacto da capacidade de throughput na performance

[3] Você pode armazenar até 1.023 instantâneos por volume a qualquer momento. Após atingir esse limite, você deverá excluir um snapshot existente antes que um novo snapshot do volume possa ser criado.

[4] Você pode armazenar até 4.091 backups por volume a qualquer momento. Depois de atingir esse limite, você deve excluir um backup existente antes que um novo backup do seu volume possa ser criado.

[5] Você pode configurar até 50 rotas por sistema de arquivos a qualquer momento. Depois de atingir esse limite, você deve excluir uma rota existente antes que uma nova rota possa ser configurada. O número de rotas do seu sistema de arquivos é determinado pelo número de SVMs que ele tem e pelo número de tabelas de rotas associadas a ele. Você pode determinar o número existente de rotas para um sistema de arquivos usando a seguinte equação: (1 + número de SVMs no sistema de arquivos) * (tabelas de rotas associadas ao sistema de arquivos).

Solução de problemas do Amazon FSx para ONTAP NetApp

Use as seções a seguir para solucionar problemas que possam surgir com o FSx para ONTAP.

Tópicos

Meu sistema de arquivos Multi-AZ está em um estado `MISCONFIGURED`

Há várias causas possíveis para um sistema de arquivos estar em um `MISCONFIGURED` estado, cada uma com sua própria resolução, conforme a seguir.

Tópicos

A conta do proprietário da VPC desativou o compartilhamento de VPC Multi-AZ

Os sistemas de arquivos Multi-AZ criados por um participante Conta da AWS em uma sub-rede VPC compartilhada entrarão em `MISCONFIGURED` um estado por um dos seguintes motivos:

- A conta do proprietário que compartilhou a sub-rede VPC desativou o suporte ao compartilhamento de VPC Multi-AZ para sistemas de arquivos FSx for ONTAP.
- A conta do proprietário descompartilhou a sub-rede VPC.

Se a conta do proprietário tiver descompartilhado a sub-rede VPC, você verá a seguinte mensagem no console desse sistema de arquivos:

```
The vpc ID vpc-012345abcde does not exist
```

Você precisa entrar em contato com a conta do proprietário que compartilhou a sub-rede VPC com você para resolver o problema. Para obter mais informações, consulte Criação de FSx para sistemas de arquivos ONTAP em sub-redes compartilhadas para obter mais informações.

Você não pode criar uma nova SVM em um sistema de arquivos Multi-AZ

Para sistemas de arquivos Multi-AZ criados por um participante Conta da AWS em uma VPC compartilhada, você não conseguirá criar uma nova SVM por um dos seguintes motivos:

- A conta do proprietário que compartilhou a sub-rede VPC desativou o suporte ao compartilhamento de VPC Multi-AZ para sistemas de arquivos FSx for ONTAP.
- A conta do proprietário descompartilhou a sub-rede VPC.

Você precisa entrar em contato com a conta do proprietário que compartilhou a sub-rede VPC com você para resolver o problema. Para obter mais informações, consulte Criação de FSx para sistemas de arquivos ONTAP em sub-redes compartilhadas para obter mais informações.

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.

Tópicos

- Não é possível acessar um sistema de arquivos por meio do iSCSI de um cliente em outra VPC
- A conta proprietária cancelou o compartilhamento da sub-rede VPC
- Não é possível acessar um sistema de arquivos por meio de NFS, SMB, CLI do ONTAP ou API REST do ONTAP de um cliente em outra VPC ou on-premises

A interface de rede elástica do sistema de arquivos foi modificada ou excluída

Você não deve modificar nem excluir nenhuma das interfaces de rede elástica do sistema de arquivos. Modificar ou excluir uma interface de rede pode causar uma perda permanente de conexão entre a nuvem privada virtual (VPC) e o sistema de arquivos. Crie um sistema de arquivos e não modifique nem exclua a interface de rede do Amazon FSx. Para ter mais informações, consulte Controle de acesso ao sistema de arquivos com a Amazon VPC.

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. Para ter mais informações, consulte Clientes compatíveis.

O grupo de segurança VPC do sistema de arquivos não tem as regras de entrada necessárias

Analise as regras de entrada especificadas em Grupos de segurança da Amazon VPC e certifique-se de que o grupo de segurança associado ao seu sistema de arquivos tenha as regras de entrada correspondentes.

O grupo de segurança VPC da instância de computação não tem as regras de saída necessárias

Analise as regras de saída especificadas em Grupos de segurança da Amazon VPC e certifique-se de que o grupo de segurança associado à sua instância de computação tenha as regras de saída correspondentes.

A sub-rede da instância de computação não usa nenhuma das tabelas de rotas associadas ao seu sistema de arquivos

O FSx para ONTAP cria endpoints para acessar seu sistema de arquivos em uma tabela de rotas de VPC. Recomendamos que configure o sistema de arquivos para usar todas as tabelas de rotas da VPC associadas às sub-redes nas quais seus clientes estão localizados. Por padrão, o Amazon FSx usa a tabela de rotas principal da VPC. Opcionalmente, você pode especificar uma ou mais tabelas de rotas para o Amazon FSx usar ao criar seu sistema de arquivos.

Se você consegue fazer ping no endpoint intercluster do sistema de arquivos, mas não no endpoint de gerenciamento do sistema de arquivos (consulte Recursos do sistema de arquivos para obter mais informações), é provável que seu cliente não esteja em uma sub-rede associada a uma das tabelas de rotas do sistema de arquivos. Para acessar seu sistema de arquivos, associe uma das tabelas de rotas do sistema de arquivos à sub-rede do seu cliente. Para obter informações sobre como atualizar tabelas de rotas da Amazon VPC do sistema de arquivos, consulte Atualização de um sistema de arquivos.

O Amazon FSx não pode atualizar a tabela de rotas para sistemas de arquivos Multi-AZ criados usando AWS CloudFormation

O Amazon FSx gerencia tabelas de rotas de VPC para sistemas de arquivos Multi-AZ usando autenticação baseada em tags. Essas tabelas de rotas estão marcadas com`Key: AmazonFSx; Value: ManagedByAmazonFSx`. Ao criar ou atualizar o FSx para sistemas de arquivos ONTAP Multi-AZ usando, AWS CloudFormation recomendamos que você adicione a tag manualmente. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Se você não conseguir acessar seu sistema de arquivos Multi-AZ, verifique se as tabelas de rotas da VPC associadas ao sistema de arquivos estão marcadas com. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Caso contrário, o Amazon FSx não poderá atualizar essas tabelas de rotas para rotear os endereços IP flutuantes das portas de gerenciamento e de dados para o servidor de arquivos ativo quando ocorrer um evento de failover. Para obter informações sobre como atualizar tabelas de rotas da Amazon VPC do sistema de arquivos, consulte Atualização de um sistema de arquivos.

Não é possível acessar um sistema de arquivos por meio do iSCSI de um cliente em outra VPC

Para acessar um sistema de arquivos por meio do protocolo Internet Small Computer Systems Interface (iSCSI) de um cliente em outra VPC, você pode configurar o emparelhamento da Amazon VPC ou o AWS Transit Gateway entre a VPC associada ao seu sistema de arquivos e a VPC na qual seu cliente reside. Para obter mais informações, consulte Criar e aceitar conexões de emparelhamento da VPC no guia da Amazon Virtual Private Cloud.

A conta proprietária cancelou o compartilhamento da sub-rede VPC

Se você criou seu sistema de arquivos em uma sub-rede VPC que foi compartilhada com você, a conta proprietária pode ter cancelado o compartilhamento da sub-rede VPC.

Se a conta do proprietário tiver descompartilhado a sub-rede VPC, você verá a seguinte mensagem no console desse sistema de arquivos:

```
The vpc ID vpc-012345abcde does not exist
```

Você precisará entrar em contato com a conta proprietária para que eles possam compartilhar novamente a sub-rede com você.

Não é possível acessar um sistema de arquivos por meio de NFS, SMB, CLI do ONTAP ou API REST do ONTAP de um cliente em outra VPC ou on-premises

Para acessar um sistema de arquivos via Network File System (NFS), Server Message Block (SMB) ou NetApp ONTAP CLI e REST API de um cliente em outra VPC ou no local, você deve configurar o roteamento usando AWS Transit Gateway entre a VPC associada ao seu sistema de arquivos e a rede na qual seu cliente reside. Para ter mais informações, consulte Acesso a dados do .

Não é possível associar uma máquina virtual de armazenamento (SVM) ao Active Directory

Se você não conseguir associar uma SVM a um Active Directory (AD), primeiro analise Junção de SVMs com um Microsoft Active Directory. Problemas comuns que impedem uma SVM de se associar

ao Active Directory estão listados nas seções a seguir, incluindo as mensagens de erro geradas para cada circunstância.

Tópicos

O nome NetBIOS da SVM é igual ao nome NetBIOS do domínio inicial.

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

Amazon FSx is unable to establish a connection with your Active Directory. Isso ocorre porque o nome do servidor especificado é o nome NetBIOS do domínio inicial. Para corrigir esse problema, escolha um nome NetBIOS para a sua SVM que seja diferente do nome NetBIOS do domínio inicial. Em seguida, tente associar novamente a SVM ao Active Directory.

Para resolver esse problema, siga o procedimento descrito em Unindo uma SVM a um Active Directory usando a API AWS Management Console, AWS CLI e para tentar associar novamente a SVM ao AD. Certifique-se de usar um nome NetBIOS para a SVM que seja diferente do nome NetBIOS do domínio inicial do Active Directory.

A SVM já está associada a outro Active Directory

Ocorre uma falha ao associar uma SVM a um Active Directory com a seguinte mensagem de erro:

Amazon FSx is unable to establish a connection to your Active Directory. Isso ocorre porque a SVM já está associada a um domínio. Para associar essa SVM a um domínio diferente, você pode usar a CLI do ONTAP ou a API REST para desassociá-la do Active Directory. Em seguida, tente associar novamente a SVM a um Active Directory diferente.

Para resolver o problema, faça o seguinte:

1. Use a CLI do NetApp ONTAP para desassociar o SVM do Active Directory atual. Para ter mais informações, consulte Desassocie um Active Directory do seu SVM usando a CLI do NetApp ONTAP.
2. Siga o procedimento descrito em Unindo uma SVM a um Active Directory usando a API AWS Management Console, AWS CLI e para tentar associar novamente a SVM ao novo AD.

O Amazon FSx não consegue se conectar aos controladores de domínio do Active Directory porque o nome NetBIOS da SVM já está em uso

Ocorre uma falha ao criar uma SVM associada ao AD autogerenciado com a seguinte mensagem de erro:

Amazon FSx is unable to establish a connection with your Active Directory. Isso ocorre porque o nome NetBIOS (computador) especificado já está em uso no Active Directory. Para corrigir esse problema, escolha um nome NetBIOS para a SVM que não esteja em uso no Active Directory, especificando um NetBIOS (computador). Em seguida, tente associar novamente a SVM ao Active Directory.

Para resolver esse problema, siga o procedimento descrito em Unindo uma SVM a um Active Directory usando a API AWS Management Console, AWS CLI e para tentar associar novamente a SVM ao AD. Certifique-se de usar um nome NetBIOS para a SVM que seja exclusivo e ainda não esteja em uso no Active Directory.

O Amazon FSx não consegue se comunicar com os controladores de domínio do Active Directory

Ocorre uma falha ao associar uma SVM ao AD autogerenciado com a seguinte mensagem de erro:

Amazon FSx is unable to communicate with your Active Directory. Para corrigir esse problema, certifique-se de que o tráfego de rede seja permitido entre o Amazon FSx e os controladores de domínio. Em seguida, tente associar novamente a SVM ao Active Directory.

Para resolver esse problema, faça o seguinte:

1. Analise os requisitos descritos em Requisitos de configuração de rede e faça as alterações necessárias para permitir a comunicação de rede entre o Amazon FSx e o AD.
2. Quando o Amazon FSx conseguir se comunicar com o AD, siga o procedimento descrito em Unindo uma SVM a um Active Directory usando a API AWS Management Console, AWS CLI e tente associar novamente a SVM ao AD.

O Amazon FSx não consegue se conectar ao Active Directory devido a requisitos da porta ou permissões da conta de serviço não atendidos

Ocorre uma falha ao associar uma SVM ao AD autogerenciado com a seguinte mensagem de erro:

Amazon FSx is unable to establish a connection with your Active Directory. Isso se deve ao fato de os requisitos de porta do Active Directory não serem atendidos ou a conta de serviço fornecida não ter permissões para associar a máquina virtual de armazenamento ao domínio com a unidade organizacional especificada. Para corrigir esse problema, atualize a configuração do Active Directory da sua máquina virtual de armazenamento depois de resolver qualquer problema de permissão com portas e contas de serviço, conforme recomendado no guia do usuário do Amazon FSx.

Para resolver esse problema, faça o seguinte:

1. Analise os requisitos descritos em Requisitos de configuração de rede e faça as alterações necessárias para atender aos requisitos de rede e garantir que as comunicações estejam habilitadas nas portas necessárias
2. Analise os requisitos da conta de serviço descritos em Requisitos de conta de serviço do Active Directory. Certifique-se de que a conta de serviço tenha as permissões delegadas necessárias para associar a SVM ao domínio do AD usando a unidade organizacional especificada.

3. Depois de fazer alterações nas permissões de porta ou na conta de serviço, siga o procedimento descrito em Unindo uma SVM a um Active Directory usando a API AWS Management Console, AWS CLI e e tente associar novamente a SVM ao AD.

O Amazon FSx não consegue se conectar aos controladores de domínio do Active Directory porque as credenciais da conta de serviço não são válidas

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

O Amazon FSx não consegue estabelecer uma conexão com os controladores de domínio do Active Directory porque as credenciais fornecidas da conta de serviço são inválidas. Para corrigir esse problema, atualize a configuração do Active Directory da sua máquina virtual de armazenamento com uma conta de serviço válida.

Para resolver esse problema, use o procedimento descrito em Atualização de uma configuração existente do SVM Active Directory usando a AWS Management Console API, AWS CLI, e para atualizar as credenciais da conta de serviço da SVM. Ao inserir o nome de usuário da conta de serviço, inclua somente o nome do usuário (por exemplo, `ServiceAcct`) e não inclua nenhum prefixo de domínio (por exemplo, `corp.com\ServiceAcct`) ou sufixo de domínio (por exemplo, `ServiceAcct@corp.com`). Não use o nome distinto (DN) ao inserir o nome de usuário da conta de serviço (por exemplo, `CN=ServiceAcct,OU=example,DC=corp,DC=com`).

O Amazon FSx não consegue se conectar aos controladores de domínio do Active Directory devido à insuficiência de credenciais da conta de serviço

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

O Amazon FSx não consegue estabelecer uma conexão com os controladores de domínio do Active Directory. Isso se deve ao fato de os requisitos de porta do Active Directory não terem sido atendidos ou a conta de serviço fornecida não ter permissão para associar a máquina virtual de armazenamento ao domínio com a unidade organizacional especificada.

Para resolver esse problema, certifique-se de ter delegado as permissões necessárias à conta de serviço fornecida. A conta de serviço deve ser capaz de criar e excluir objetos de computador na UO no domínio ao qual você está associando o sistema de arquivos. A conta de serviço também precisa, no mínimo, ter permissões para fazer o seguinte:

- Redefinir senhas
- Restringir contas de ler e gravar dados
- Capacidade validada para gravar no nome do host DNS
- Capacidade validada para gravar no nome da entidade principal de serviço
- Capacidade para criar e excluir objetos de computador
- Capacidade validada para ler e gravar restrições de conta

Para obter mais informações sobre como criar uma conta de serviço com as permissões corretas, consulte Requisitos de conta de serviço do Active Directory e Delegar permissões à conta de serviço do Amazon FSx.

O Amazon FSx não consegue se comunicar com os servidores DNS ou controladores de domínio do Active Directory

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

Amazon FSx is unable to communicate with your Active Directory. Isso ocorre porque o Amazon FSx não consegue acessar os servidores DNS fornecidos ou os controladores de domínio do seu domínio. Para corrigir esse problema, atualize a configuração do Active Directory da sua máquina virtual de armazenamento com servidores DNS válidos e uma configuração de rede que permita que o tráfego flua da máquina virtual de armazenamento para o controlador de domínio.

Para resolver esse problema, use o seguinte procedimento:

1. Se somente alguns dos controladores de domínio no Active Directory estiverem acessíveis, por exemplo, devido a limitações geográficas ou firewalls, você poderá adicionar controladores de domínio preferenciais. Usando essa opção, o Amazon FSx tenta entrar em contato com os controladores de domínio preferenciais. Adicione controladores de domínio preferenciais usando o comando `vserver cifs domain preferred-dc add` NetApp ONTAP CLI, da seguinte forma:

    a. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

b. Insira o seguinte comando no qual:

- `-vserver vserver_name` especifica o nome da máquina virtual de armazenamento (SVM).
- `-domain domain_name` especifica o nome de domínio totalmente qualificado (FQDN) do Active Directory ao qual os controladores de domínio especificados pertencem.
- `-preferred-dc IP_address,…` especifica um ou mais endereços IP dos controladores de domínio preferenciais, como uma lista delimitada por vírgulas, por ordem de preferência.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_name -
domain domain_name -preferred-dc IP_address, …+
```

O comando a seguir adiciona os controladores de domínio 172.17.102.25 e 172.17.102.24 à lista de controladores de domínio preferenciais que o servidor SMB na SVM vs1 usa para gerenciar o acesso externo ao domínio cifs.lab.example.com.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
 cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. Verifique se o seu controlador de domínio pode ser resolvido com o DNS. Use o comando `vserver services access-check dns forward-lookup` NetApp ONTAP CLI para retornar o endereço IP de um nome de host com base na pesquisa no servidor DNS especificado ou na configuração DNS do vserver.

a. Para acessar a CLI do NetApp ONTAP, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos Amazon FSx NetApp for ONTAP executando o seguinte comando. Substitua *`management_endpoint_ip`* pelo endereço IP da porta de gerenciamento do sistema de arquivos.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Para ter mais informações, consulte Gerenciando sistemas de arquivos com a ONTAP CLI.

b. Entre no modo avançado da CLI do ONTAP usando o comando a seguir.

```
FsxId123456789::> set adv
```

c. Insira o seguinte comando no qual:

- `-vserver vserver_name` especifica o nome da máquina virtual de armazenamento (SVM).
- `-hostname host_name` especifica o nome do host a ser pesquisado no servidor DNS.
- `-node node_name` especifica o nome do nó no qual o comando é executado.
- `-lookup-type` especifica o tipo de endereço IP a ser pesquisado no servidor DNS, o padrão é `all`.

```
FsxId123456789::> vserver services access-check dns forward-lookup \
-vserver vserver_name -node node_name \
-domains domain_name -name-servers dns_server_ip_address \
-hostname host_name
```

3. Analise as informações que você precisa ter ao associar uma SVM a um AD.
4. Analise os requisitos de rede ao associar uma SVM a um AD.
5. Use o procedimento descrito em Requisitos de configuração de rede para atualizar a configuração do AD da SVM usando os endereços IP corretos para os servidores DNS do AD.

O Amazon FSx não consegue se comunicar com o Active Directory devido a um nome de domínio inválido do Active Directory.

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

O Amazon FSx detectou que o FQDN fornecido é inválido. Para corrigir esse problema, atualize a configuração do Active Directory da sua máquina virtual de armazenamento com um FQDN que atenda aos requisitos de configuração.

Para resolver esse problema, use o seguinte procedimento:

1. Analise os requisitos de nome de domínio do Active Directory on-premises descritos em Informações necessárias ao unir uma SVM a um Active Directory. Certifique-se de que o AD que você está tentando associar atenda a esses requisitos.
2. Use o procedimento descrito em Unindo uma SVM a um Active Directory usando a API AWS Management Console, AWS CLI e e tente associar novamente a SVM a um AD. Certifique-se de usar o formato correto para o FQDN do domínio do AD.

A conta de serviço não consegue acessar o grupo de administradores especificado na configuração do Active Directory da SVM

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

O Amazon FSx não consegue aplicar a configuração do Active Directory. Isso ocorre porque o grupo de administradores fornecido não existe ou não está acessível à conta de serviço fornecida. Para corrigir esse problema, certifique-se de que sua configuração de rede permita o tráfego da SVM para os controladores de domínio e servidores DNS do Active Directory. Em seguida, atualize a configuração do Active Directory da SVM, fornecendo os servidores DNS do Active Directory e especificando um grupo de administradores no domínio que possa ser acessado pela conta de serviço fornecida.

Para resolver esse problema, faça o seguinte:

1. Analise as informações sobre como fornecer um grupo de domínio para realizar ações administrativas na SVM. Verifique se está usando o nome correto do grupo de administradores de domínio do AD.
2. Use o procedimento descrito em Unindo uma SVM a um Active Directory usando a API AWS Management Console, AWS CLI e e tente associar novamente a SVM a um AD.

O Amazon FSx não consegue se conectar aos controladores de domínio do Active Directory porque a unidade organizacional especificada não existe ou não está acessível

Ocorre uma falha ao associar uma SVM ao Active Directory autogerenciado com a seguinte mensagem de erro:

Amazon FSx is unable to establish a connection with your Active Directory. Isso ocorre porque a unidade organizacional especificada não existe ou não está acessível à conta de serviço fornecida. Para corrigir esse problema, atualize a configuração do Active Directory da sua máquina virtual de armazenamento, especificando uma unidade organizacional à qual a conta de serviço tem permissões para se associar.

Para resolver esse problema, faça o seguinte:

1. Analise os pré-requisitos para associar uma SVM a um AD.
2. Analise as informações que você precisa ter ao associar uma SVM a um AD.
3. Tente associar novamente a SVM ao AD usando este procedimento com a unidade organizacional correta.

Não é possível excluir um volume ou uma máquina virtual de armazenamento

Cada sistema de arquivos do FSx para ONTAP pode conter uma ou mais máquinas virtuais de armazenamento (SVMs), e cada SVM pode conter um ou mais volumes. Ao excluir um recurso, você deve primeiro garantir que todos os recursos secundários tenham sido excluídos. Por exemplo, antes de excluir uma SVM, você deve primeiro excluir todos os volumes não raiz na SVM.

> **Important**
>
> Você só pode excluir máquinas virtuais de armazenamento usando o console, a API e a CLI do Amazon FSx. Você só pode excluir volumes usando o console do Amazon FSx, a API ou a CLI se o volume tiver os backups do Amazon FSx habilitados.

Para ajudar a proteger seus dados e sua configuração, o Amazon FSx impede a exclusão de SVMs e volumes em determinadas circunstâncias. Se você tentar excluir uma SVM ou volume e sua solicitação de exclusão não for bem-sucedida, o Amazon FSx fornecerá informações no AWS console, AWS Command Line Interface (AWS CLI) e na API sobre o motivo pelo qual o recurso não foi excluído. Depois de resolver a causa da falha de exclusão, você poderá repetir a solicitação de exclusão.

Tópicos

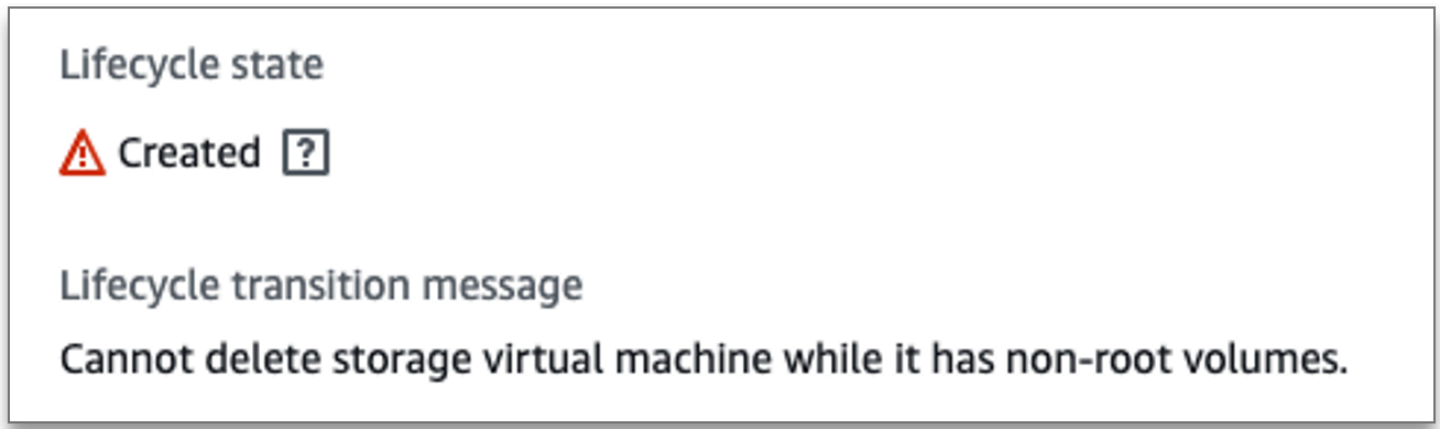
- Identificar falhas em exclusões

- Exclusão de SVM: tabelas de rotas inacessíveis
- Exclusão da SVM: relacionamento entre pares
- SVM ou exclusão de volume: SnapMirror
- Exclusão de SVM: LIF habilitada pelo Kerberos
- Exclusão de SVM: outro motivo
- Exclusão de volume: relacionamento FlexCache

Identificar falhas em exclusões

Ao excluir uma SVM ou volume do Amazon FSx, você normalmente vê a transição de estado do `Lifecycle` do recurso para `DELETING` por até alguns minutos antes que o recurso desapareça do console do Amazon FSx, da CLI e da API.

Se você tentar excluir um recurso e o estado de `Lifecycle` mudar para `DELETING` e depois voltar para `CREATED`, esse comportamento indica que o recurso não foi excluído com êxito. Nesse caso, o Amazon FSx relata um ícone de alerta no console ao lado do estado `CREATED` do ciclo de vida. Escolher o ícone de alerta exibe o motivo da exclusão malsucedida, conforme mostrado no exemplo a seguir.



Os motivos mais comuns pelos quais o Amazon FSx impede a exclusão de SVM e volume são fornecidos nas seções a seguir, com step-by-step instruções sobre como resolver esses problemas.

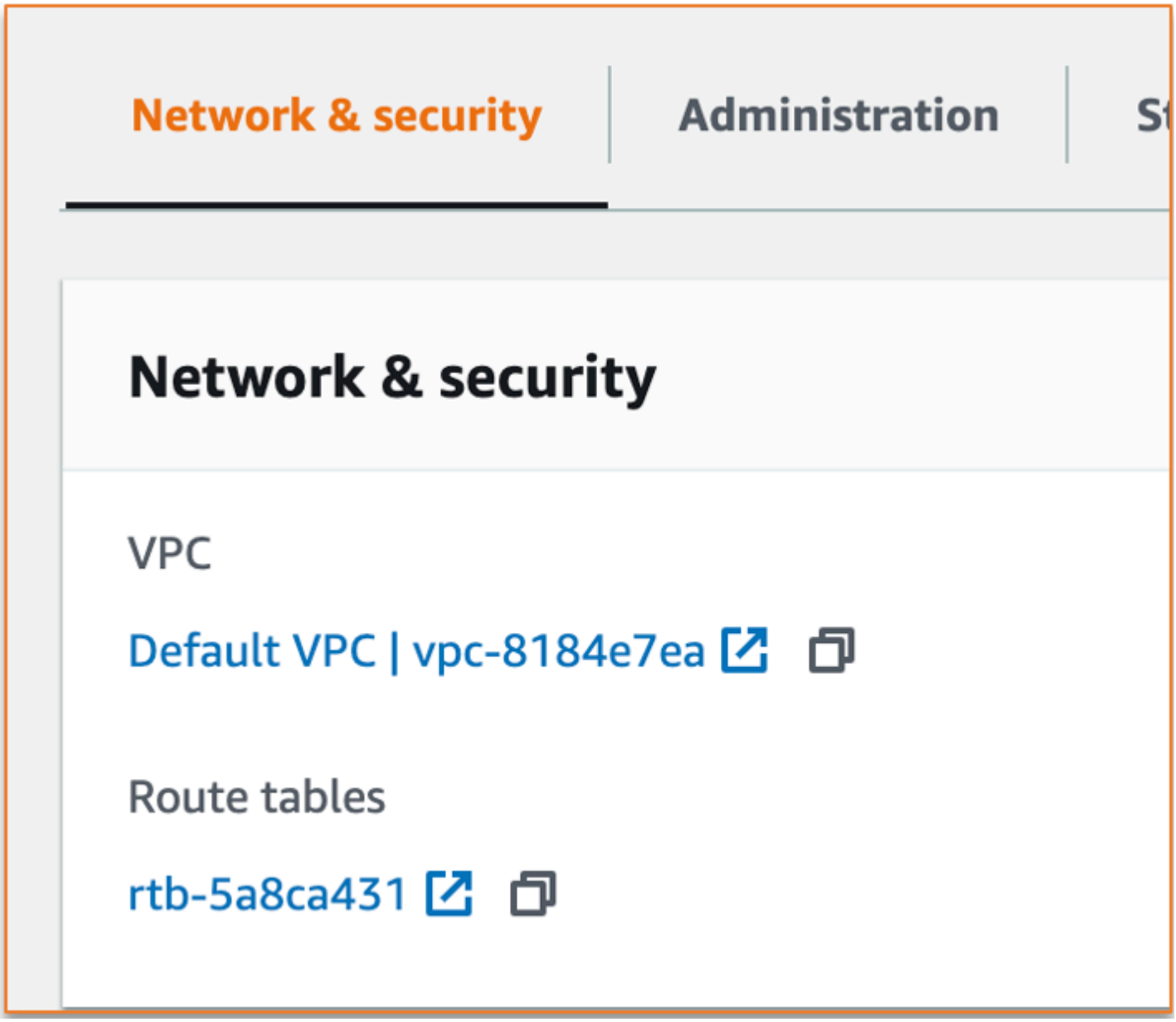
Exclusão de SVM: tabelas de rotas inacessíveis

Cada sistema de arquivos do FSx para ONTAP cria uma ou mais entradas da tabela de rotas para fornecer failover e failback automáticos nas zonas de disponibilidade. Por padrão, essas entradas da tabela de rotas são criadas na tabela de rotas padrão da VPC. Opcionalmente, você pode especificar

uma ou mais tabelas de rotas não padrão nas quais as interfaces do FSx para ONTAP podem ser criadas. O Amazon FSx marca cada tabela de rotas associada a um sistema de arquivos com uma tag `AmazonFSx` que, se for removida, poderá impedir que o Amazon FSx exclua recursos. Se essa situação ocorrer, você verá o seguinte `LifecycleTransitionReason`:

```
Amazon FSx is unable to complete the requested storage virtual machine
operation because of an inability to access one or more of the route tables
associated with your file system. Please contact AWS Support.
```

Você encontra as tabelas de rotas do seu sistema de arquivos no console do Amazon FSx navegando até a página de resumo do sistema de arquivos, na guia Rede e segurança:



Escolher o link das tabelas de rotas leva você às suas tabelas de rotas. Em seguida, verifique se cada uma das tabelas de rotas associadas ao seu sistema de arquivos está marcada com esse par de chave-valor:

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

Se essa tag não estiver presente, recrie-a e tente excluir a SVM novamente.

Exclusão da SVM: relacionamento entre pares

Se estiver tentando excluir uma SVM ou um volume que faça parte de um relacionamento entre pares, primeiro exclua o relacionamento entre pares antes de excluir a SVM ou o volume. Esse requisito evita que as SVMs emparelhadas se tornem não íntegras. Se a SVM não puder ser excluída por causa de um relacionamento entre pares, você verá o seguinte `LifecycleTransitionReason`:

O Amazon FSx não consegue excluir a máquina virtual de armazenamento porque ela faz parte de um relacionamento entre pares de SVM ou pares de transição. Exclua o relacionamento e tente novamente.

Você pode excluir relacionamentos entre pares de SVM por meio da CLI do ONTAP. Para acessar a CLI do ONTAP, siga as etapas em Gerenciando sistemas de arquivos com a ONTAP CLI. Usando a CLI do ONTAP, siga as etapas a seguir.

1. Verifique os relacionamentos entre pares de SVM usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

Se esse comando for executado com êxito, você verá uma saída semelhante à:

```
            Peer        Peer                          Peering        Remote
Vserver     Vserver     State        Peer Cluster     Applications   Vserver
----------- ----------- ------------ ----------------- -------------- ---------
svm_name    test2       peered       FsxId02d81fef0d84734b6
                                                       snapmirror     fsxDest
svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                       snapmirror     fsxDest
2 entries were displayed.
```

2. Exclua cada relacionamento entre pares de SVM usando o comando a seguir. Substitua *svm_name* e *remote_svm_name* pelos seus valores reais.

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

Se esse comando for executado com êxito, você verá a seguinte saída:

```
Info: 'vserver peer delete' command is successful.
```

SVM ou exclusão de volume: SnapMirror

Assim como você não pode excluir uma SVM com um relacionamento entre pares sem primeiro excluir o relacionamento entre pares (consulteExclusão da SVM: relacionamento entre pares), você não pode excluir um SVM que tenha um SnapMirror relacionamento sem primeiro excluir o relacionamento. SnapMirror Para excluir o SnapMirror relacionamento, use a CLI do ONTAP para seguir as etapas a seguir no sistema de arquivos que é o destino do SnapMirror relacionamento. Para acessar a CLI do ONTAP, siga as etapas em Gerenciando sistemas de arquivos com a ONTAP CLI.

> **Note**
>
> Os backups do Amazon FSx são usados SnapMirror para criar point-in-time backups incrementais dos volumes do seu sistema de arquivos. Você não pode excluir essa SnapMirror relação para seus backups na CLI do ONTAP. No entanto, esse relacionamento

é excluído automaticamente ao excluir um volume por meio da CLI, da API ou do console da AWS .

1. Liste seus SnapMirror relacionamentos no sistema de arquivos de destino usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

Se esse comando for executado com êxito, você verá uma saída semelhante à:

```
Source            Destination    Mirror  Relationship   Total             Last
Path        Type  Path           State   Status         Progress  Healthy Updated
----------- ---- ------------    ------- -------------- --------- ------- --------
sourceSvm:sourceVol
            XDP  destSvm:destVol Snapmirrored
                                       Idle           -         true    -
```

2. Exclua seu SnapMirror relacionamento executando o comando a seguir no sistema de arquivos de destino.

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

Exclusão de SVM: LIF habilitada pelo Kerberos

Se estiver tentando excluir uma SVM que tenha uma interface lógica (LIF) com o Kerberos habilitado, primeiro desative o Kerberos nessa LIF antes de excluir a SVM.

Você pode desabilitar o Kerberos em uma LIF por meio da CLI do ONTAP. Para acessar a CLI do ONTAP, siga as etapas em Gerenciando sistemas de arquivos com a ONTAP CLI.

1. Entre no modo de diagnóstico na CLI do ONTAP usando o comando a seguir.

```
FsxId123456789abcdef::> set diag
```

Quando for solicitado que continue, insira **y**.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
```

```
Do you want to continue? {y|n}: y
```

2. Verifique quais interfaces têm o Kerberos habilitado. Substitua *svm_name* pelo nome da sua SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Se esse comando for executado com êxito, você verá uma saída semelhante à:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    enabled
5 entries were displayed.
```

3. Desabilite a LIF do Kerberos usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM. Você precisará fornecer o nome de usuário e a senha do Active Directory usados para associar essa SVM ao Active Directory.

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

Se esse comando for executado com êxito, você verá a saída a seguir. Forneça o nome de usuário e a senha do Active Directory usados para associar essa SVM ao Active Directory. Quando for solicitado que continue, insira **y**.

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *************

Warning: This command deletes the service principal name from the machine account
 on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. Verifique se o Kerberos está desabilitado na SVM usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Se esse comando for executado com êxito, você verá uma saída semelhante à:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    disabled
5 entries were displayed.
```

5. Se a interface for mostrada como`disabled`, tente excluir a SVM novamente por meio da AWS CLI, da API ou do console.

   Se você não conseguiu excluir a LIF usando os comandos anteriores, poderá forçar a exclusão da LIF do Kerberos usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

   > **Important**
   >
   > O comando a seguir pode prender o objeto computacional da SVM no Active Directory.

   ```
   FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
    nfs_smb_management_1 -force true
   ```

   Se esse comando for executado com êxito, você verá uma saída semelhante à mostrada a seguir. Quando for solicitado que continue, insira **y**.

   ```
   (vserver nfs kerberos interface disable)

   Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver
    "svm_name" will be deleted.
   The corresponding account on the KDC will not be deleted. Do you want to continue?
    {y|n}: y
   ```

Exclusão de SVM: outro motivo

As SVMs do FSx para ONTAP criam um objeto de computador no Active Directory quando se associam a ele. Em alguns casos, talvez você queira desassociar manualmente uma SVM do Active Directory usando a CLI do ONTAP. Para acessar a CLI do ONTAP, siga as etapas em Gerenciando sistemas de arquivos com a ONTAP CLI, fazendo login na CLI do ONTAP no nível do sistema de arquivos com as credenciais de `fsxadmin`. Usando a CLI do ONTAP, siga as etapas a seguir para desassociar uma SVM do Active Directory.

> **Important**
>
> Esse procedimento pode prender o objeto computacional da SVM no Active Directory.

1. Entre no modo avançado na CLI do ONTAP usando o comando a seguir.

   ```
   FsxId123456789abcdef::> set adv
   ```

   Após executar esse comando, você verá essa saída. Insira **y** para continuar.

   ```
   Warning: These advanced commands are potentially dangerous; use them only when
         directed to do so by NetApp personnel.
         Do you want to continue? {y|n}: y
   ```

2. Exclua o DNS do Active Directory usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

   ```
   FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
    delete -vserver svm_name -lif nfs_smb_management_1
   ```

   > **Note**
   >
   > Se o registro DNS já tiver sido excluído ou se o servidor DNS estiver inacessível, esse comando falhará. Se isso acontecer, prossiga para a próxima etapa.

3. Desabilite o DNS usando o comando a seguir. Substitua *svm_name* pelo nome da sua SVM.

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
vserver svm_name -is-enabled false -use-secure false
```

Se esse comando for executado com êxito, você verá a seguinte saída:

```
Warning: DNS updates for Vserver "svm_name" are now disabled.
     Any LIFs that are subsequently modified or deleted
     can result in a stale DNS entry on the DNS server,
     even when DNS updates are enabled again.
```

4. Desassocie o dispositivo do Active Directory. Substitua *svm_name* pelo nome da sua SVM.

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

Após executar esse comando, você verá a saída a seguir, na qual *CORP.EXAMPLE.COM* é substituído pelo nome do seu domínio. Quando for solicitado, insira o nome de usuário e senha. Quando perguntado se deseja excluir o servidor, digite **y**.

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
     Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
 server.
     Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

Exclusão de volume: relacionamento FlexCache

Você não pode excluir volumes que são os volumes de origem de um FlexCache relacionamento, a menos que primeiro exclua o relacionamento de cache. Para determinar quais volumes têm uma FlexCache relação, você pode usar a CLI do ONTAP. Para acessar a CLI do ONTAP, siga as etapas em Gerenciando sistemas de arquivos com a ONTAP CLI.

1. Verifique os FlexCache relacionamentos usando o comando a seguir.

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. Exclua qualquer relacionamento de cache usando o comando a seguir. Substitua *dest_svm_name* e *dest_vol_name* pelos seus valores reais.

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. Após excluir o relacionamento do cache, tente excluir a SVM por meio da CLI, da API ou do console da AWS novamente.

Os backups diários automáticos falham devido à capacidade de volume insuficiente

Os backups diários automáticos do seu volume falham com a seguinte mensagem:

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

Os backups diários automáticos estão falhando porque não há capacidade de armazenamento livre suficiente no volume. Para mitigar essa condição, você precisará liberar a capacidade de armazenamento no volume. Você pode fazer isso usando uma ou mais das seguintes opções, dependendo da sua situação:

- Aumente a capacidade de armazenamento do volume
- Aumente a reserva de instantâneos do volume
- Desativar a exclusão automática de instantâneos
- Não exclua o instantâneo de backup usando a CLI do ONTAP

Você não tem capacidade de volume suficiente

Se estiver ficando sem espaço nos seus volumes, poderá usar os procedimentos mostrados aqui para diagnosticar e resolver a situação.

Tópicos

- Determine como a capacidade de armazenamento do volume está sendo usada

- Como aumentar a capacidade de armazenamento de um volume
- Como usar o dimensionamento automático de volume
- O armazenamento principal do sistema de arquivos está cheio
- Exclusão de snapshots
- Como aumentar a capacidade máxima de arquivos de um volume

Determine como a capacidade de armazenamento do volume está sendo usada

Você pode ver como a capacidade de armazenamento do seu volume está sendo consumida usando o comando `volume show-space` NetApp ONTAP CLI. Essas informações podem ajudar a tomar decisões sobre como recuperar ou conservar a capacidade de armazenamento do volume. Para ter mais informações, consulte Para monitorar a capacidade de armazenamento de um volume (console).

Como aumentar a capacidade de armazenamento de um volume

Você pode aumentar a capacidade de armazenamento de um volume usando o console Amazon FSx e a API AWS CLI Amazon FSx. Para obter mais informações sobre como atualizar um volume com maior capacidade, consulte Atualizar um volume.

Como alternativa, você pode aumentar a capacidade de armazenamento de um volume usando o comando `volume modify` NetApp ONTAP CLI. Para ter mais informações, consulte Para alterar a capacidade de armazenamento de um volume (console).

Como usar o dimensionamento automático de volume

Você pode usar o dimensionamento automático de volume para que um volume cresça automaticamente em uma quantidade especificada ou até um tamanho especificado quando atingir um limite de espaço usado. Você pode fazer isso para tipos de FlexVol volume, que é o tipo de volume padrão para FSx for ONTAP, usando o comando ONTAP CLI. `volume autosize` NetApp Para ter mais informações, consulte Habilitando o dimensionamento automático de volume.

O armazenamento principal do sistema de arquivos está cheio

Se o armazenamento principal do sistema de arquivos do FSx para ONTAP estiver cheio, você não poderá adicionar mais dados aos volumes do sistema de arquivos, mesmo que um volume mostre

que há capacidade de armazenamento disponível suficiente. Você pode visualizar a quantidade da capacidade de armazenamento principal disponível na guia Monitoramento e performance na página de detalhes do sistema de arquivos no console do Amazon FSx. Para obter mais informações, consulte Monitorando a utilização do armazenamento SSD.

Para resolver esse problema, você pode aumentar o tamanho do nível de armazenamento principal do sistema de arquivos. Para ter mais informações, consulte Atualizando o armazenamento SSD e o IOPS do sistema de arquivos.

Exclusão de snapshots

Os snapshots são habilitados por padrão nos volumes, usando a política de snapshots padrão. Os snapshots são armazenados no diretório `.snapshot` na raiz de um volume. Você pode gerenciar a capacidade de armazenamento de volumes em relação aos snapshots das seguintes maneiras:

- Excluir os snapshots manualmente: recupere a capacidade de armazenamento excluindo os snapshots manualmente.
- Criar uma política de exclusão automática de snapshots: crie uma política que exclua os snapshots de forma mais agressiva do que a política de snapshots padrão.
- Desativar os snapshots automáticos: conserve a capacidade de armazenamento desativando os snapshots automáticos.

Para obter mais informações sobre como excluir snapshots e gerenciar políticas de snapshots para conservar a capacidade de armazenamento, consulte Exclusão de snapshots.

Como aumentar a capacidade máxima de arquivos de um volume

Um volume do FSx para ONTAP pode ficar sem capacidade de arquivo quando o número de inodes ou ponteiros de arquivo disponíveis estiver esgotado. Por padrão, o número de inodes disponíveis em um volume é de 1 para cada 32 KiB de tamanho do volume. Para ter mais informações, consulte Capacidade do arquivo de volumes.

O número de inodes em um volume aumenta proporcionalmente à capacidade de armazenamento do volume, até um limite de 648 GiB. Por padrão, todos os volumes com capacidade de armazenamento de 648 GiB ou mais têm o mesmo número de inodes, 21.251.126. Para visualizar a capacidade máxima de arquivos de um volume, consulte Visualizar a capacidade de arquivos de um volume.

Se você criar um volume maior que 648 GiB e quiser ter mais de 21.251.126 inodes, deverá aumentar o número máximo de arquivos no volume manualmente. Se a capacidade de armazenamento do volume estiver acabando, você poderá verificar a capacidade máxima de arquivos. Se estiver se aproximando da capacidade de arquivos, você poderá aumentá-la manualmente. Para ter mais informações, consulte Para aumentar o número máximo de arquivos em um volume (ONTAPCLI).

Corrigir problemas de rede

Se estiver enfrentando problemas de rede, poderá usar os procedimentos mostrados aqui para diagnosticar o problema.

Você deseja capturar um rastreamento de pacote

O rastreamento de pacotes é o processo de verificar o caminho de um pacote pelas camadas até seu destino. Você controla o processo de rastreamento de pacotes com os seguintes comandos do NetApp ONTAP CLI:

- network tcpdump start: inicia o rastreamento de pacotes
- network tcpdump show: mostra os rastreamentos de pacotes atualmente em execução
- network tcpdump stop: interrompe um rastreamento de pacotes em execução

Esses comandos estão disponíveis para usuários que tenham o perfil `fsxadmin` no sistema de arquivos.

Capturar um rastreamento de pacotes do sistema de arquivos

1. Para entrar via SSH na NetApp CLI do ONTAP do seu sistema de arquivos, siga as etapas documentadas na seção do Guia Usar a CLI do NetApp ONTAP do usuário do Amazon FSx for ONTAP. NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Insira o nível de privilégio do diagnóstico na CLI do ONTAP usando o comando a seguir.

   ```
   ::> set diag
   ```

   Quando for solicitado que continue, insira `y`.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

3. Identifique o local no sistema de arquivos onde deseja salvar o rastreamento de pacotes. O volume deve estar on-line e montado no namespace com um caminho de junção válido. Use o seguinte comando para verificar se há volumes que atendem a esses critérios:

```
::*> volume show -junction-path !- -fields junction-path
vserver volume    junction-path
------- --------- -------------
fsx     test_vol1 /test_vol1
fsx     test_vol2 /test_vol2
fsx     test_vol2 /test_vol3
```

4. Inicie o rastreamento com os argumentos mínimos necessários. Substitua o seguinte:

   - Substitua *node_name* pelo nome do nó (por exemplo,). `FsxId01234567890abcdef-01`
   - Substitua *svm_name* pelo nome da sua máquina virtual de armazenamento (por exemplo,). `fsx`
   - Substitua *junction_path_name pelo nome* do volume (por exemplo,). `test-vol1`

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
 e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
 packet traces are occurring. Use the
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
 disable Snapshots on the
tcpdump destination volume.
```

> **Important**
>
> Os rastreamentos de pacotes só podem ser capturados na interface `e0e` e no espaço `Default` de IP. No FSx para ONTAP, todo o tráfego de rede usa a interface `e0e`.

Ao usar o rastreamento de pacotes, lembre-se dos seguintes pontos:

- *Ao iniciar um rastreamento de pacotes, você deve incluir o caminho para onde deseja armazenar os arquivos de rastreamento, neste formato: /clus/ svm_name/junction-path-name*
- Opcionalmente, forneça o nome do arquivo para o rastreamento do pacote. *Se o nome_filtro não for especificado, ele será gerado automaticamente no formato: node-name _ port-name _ yyyymmdd_hhmmss .trc*
- Se rastreamentos cumulativos forem especificados, o filter_name será sufixado com um número que indica a posição na sequência de rotação.
- A CLI do ONTAP também aceita os seguintes argumentos -pass-through opcionais:

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
<filter-expression>
```

- Para obter informações sobre expressões de filtro, consulte a página inicial de pcap-filter(7).

5. Veja os rastreamentos em andamento:

```
::*> debug network tcpdump show
Node                    IPspace  Port     Filename
----------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. Pare o rastreamento:

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

7. Retorne ao nível de privilégio de administrador:

```
::*> set -priv admin
::>
```

8. Acesse os rastreamentos de pacotes.

   Seus rastreamentos de pacotes são armazenados no volume especificado usando o comando debug network tcpdump start e podem ser acessados por meio da exportação de NFS ou de um compartilhamento SMB que corresponda a esse volume.

Para obter mais informações sobre a captura de rastreamentos de pacotes, consulte Como usar o debug network tcpdump no ONTAP 9.10+ na Base de Conhecimento. NetApp

Histórico de documentos do Amazon FSx for ONTAP NetApp

- Versão da API: 1/3/2018
- Última atualização da documentação: 30 de abril de 2024

A tabela a seguir descreve mudanças importantes no Guia do usuário do Amazon FSx NetApp ONTAP. Para receber notificações sobre atualizações da documentação, inscreva-se no feed RSS.

Alteração	Descrição	Data
Support adicionado para a `fsxadmin-readonly` função de usuários administrativos do sistema de arquivos	A `fsxadmin-readonly` função agora está disponível para usuários administrativos do sistema de ONTAP arquivos e pode ser usada para aplicativos de monitoramento do sistema de arquivos, comoNetApp Harvest. Para obter mais informações, consulte Funções e usuários do administrador do sistema de arquivos.	30 de abril de 2024
Support adicionado para autenticação de chave pública SSH para usuários administrativos de domínio do Windows	Agora você pode usar a autenticação de chave pública SSH com o sistema de arquivos de domínio do Active Directory e usuários SVM. Para ter mais informações, consulte https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/set-up-ad-auth.html.	30 de abril de 2024

Support adicionado para 12 pares de HA em sistemas de arquivos escaláveis	O Amazon FSx for NetApp ONTAP adicionou suporte para 12 pares de HA em sistemas de arquivos escaláveis. Sistemas de arquivos com 12 pares de HA podem fornecer até 72 GBps de capacidade de taxa de transferência e 2.400.000 SSD IOPS em 12 pares de alta disponibilidade (HA). Para obter mais informaçõ es, consulte Pares de alta disponibilidade (HA) e Amazon FSx NetApp for ONTAP performance.	4 de março de 2024
Support adicionado para o modo de gravação em nuvem	O Amazon FSx for NetApp ONTAP adicionou suporte ao modo de gravação em nuvem para volumes. Para obter mais informações, consulte Habilitar o modo de gravação na nuvem em um volume.	6 de fevereiro de 2024
Support adicionado para backup de FlexGroup volumes com AWS Backup	Agora você pode usar AWS Backup para fazer backup e restaurar FlexGroup volumes em seus sistemas de arquivos FSx for ONTAP. Para obter mais informações, consulte Usando AWS Backup com o Amazon FSx.	11 de janeiro de 2024

O Amazon FSx atualizou as políticas gerenciadas do AmazonFSxFullAccess, AmazonF, AmazonFSx ConsoleFullAccess, AmazonF e SxReadOnlyAccess AmazonF SxConsole ReadOnlyAccess SxService RolePolicy AWS	O Amazon FSx atualizou as políticas AmazonF, AmazonFSxFullAccess, AmazonFSxConsoleFullAccess, AmazonF e AmazonF para SxReadOnlyAccess adicionar a permissãoSxConsole ReadOnlyAccess. SxService RolePolicy `ec2:GetSecurityGroupsForVpc` Para obter mais informações, consulte as atualizações do Amazon FSx para políticas AWS gerenciadas.	9 de janeiro de 2024
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 açãoSxConsoleFullAccess . `ManageCrossAccountDataReplication` Para obter mais informações, consulte as atualizações do Amazon FSx para políticas AWS gerenciadas.	20 de dezembro de 2023
Support adicionado para métricas de expansão	O FSx for ONTAP agora fornece CloudWatch métricas da Amazon para sistemas de arquivos com vários pares de HA. Para obter mais informações, consulte Métricas escaláveis do sistema de arquivos.	26 de novembro de 2023

Support adicionado para sistemas de arquivos escaláveis	O Amazon FSx for NetApp ONTAP adicionou suporte para sistemas de arquivos escaláveis que podem fornecer até 36 GBps de capacidade de taxa de transferência e 1.200.000 IOPS de SSD em seis pares de alta disponibilidade (HA). Para obter mais informaçõ es, consulte Pares de alta disponibilidade (HA) e Amazon FSx NetApp for ONTAP performance.	26 de novembro de 2023
Support adicionado para FlexGroup volumes	O Amazon FSx for NetApp ONTAP adicionou suporte para volumes. FlexGroup Para obter mais informações, consulte Estilos de volume.	26 de novembro de 2023
Suporte compartilhado para VPC adicionado para sistemas de arquivos Multi-AZ	Agora, as contas dos participa ntes podem criar sistemas de arquivos Multi-AZ em uma VPC que foi compartil hada com elas. As contas do proprietário podem gerenciar esse recurso no console, na CLI e na API do Amazon FSx. Para obter mais informações, consulte Criação de FSx para sistemas de arquivos ONTAP em sub-redes compartilhadas	26 de novembro 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
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 criar perfis e usuários adicionais do ONTAP	O Amazon FSx for NetApp ONTAP agora oferece suporte à criação de funções e usuários adicionais do ONTAP para definir capacidades e privilégios do usuário ao usar a CLI e a API REST do ONTAP. Para obter mais informações, consulte Funções e usuários no Amazon FSx for NetApp ONTAP.	6 de setembro de 2023
Support adicionado para CloudWatch métricas adicionais e um painel de monitoramento aprimorado	O FSx para ONTAP agora fornece métricas de performance adicionais e um painel de monitoramento aprimorado para melhorar a visibilidade da atividade do sistema de arquivos. Para obter mais informações, consulte Monitoramento com CloudWatch.	17 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

Support adicionado para usar o NetApp System Manager diretamente	Você pode gerenciar seus sistemas de arquivos do FSx para ONTAP usando o System Manager diretamente do NetApp BlueXP. Para obter mais informações, consulte Usando o NetApp System Manager com o BlueXP.	13 de julho de 2023
Suporte adicionado para monitorar eventos do EMS	Você pode monitorar os eventos do sistema de arquivos do FSx para ONTAP usando o Events Management System (EMS) nativo do NetApp ONTAP. Você pode visualizar eventos do EMS usando a CLI do NetApp ONTAP. Para obter mais informações, consulte Monitoramento de eventos de EMS do FSx para ONTAP.	13 de julho de 2023

Suporte adicionado para o SnapLock	O FSx para ONTAP agora oferece suporte aos volumes do SnapLock. O SnapLock permite proteger seus arquivos fazendo a transição deles para um estado de gravação única e várias leituras (WORM), o que impede modificações ou exclusões dentro de um período de retenção especific ado. O FSx for ONTAP suporta os modos de retenção Compliance e Enterprise com. SnapLock Para obter mais informações, consulte Trabalhando com SnapLock.	13 de julho de 2023
Suporte adicionado para criptografia IPsec de dados em trânsito	O FSx para ONTAP agora suporta o uso da criptografia IPsec para criptografar dados em trânsito entre sistemas de arquivos e clientes conectado s. Para obter mais informaçõ es, consulte Configurando IPsec usando autenticação PSK e Configurando IPsec usando autenticação de certificado.	13 de julho de 2023

O tamanho máximo do volume aumentou	O FSx for ONTAP atualizou o tamanho máximo de um volume de 100 TB para 300 TB. Para obter mais informações, consulte Ativar o dimensionamento automático de volumes.	13 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
Suporte adicionado para unir máquinas virtuais de armazenamento existentes a um Active Directory	Você pode unir máquinas virtuais de armazenam ento existentes a um Active Directory usando a AWS Management Console API AWS CLI e. Para obter mais informações, consulte Junção de uma SVM com um Active Directory.	13 de junho de 2023

Suporte para cache de leitura NVMe adicionado para sistemas de arquivos com uma única AZ	O cache de leitura NVMe agora conta com suporte nos sistemas de arquivos com uma única AZ criados após 28 de novembro de 2022, com pelo menos 2 GBps de capacidade de throughput, na região Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda). Para obter mais informações, consulte Impacto do tipo de implantação na performance.	28 de novembro de 2022
Suporte adicionado para o uso de intervalos de endereços IP na VPC para criar sistemas de arquivos com várias AZs	Agora você pode criar sistemas de arquivos do FSx para ONTAP com várias AZs especificando endpoints que estão dentro do intervalo de endereços IP da VPC. Para obter mais informações, consulte Criação de sistemas de arquivos do FSx para ONTAP.	28 de novembro de 2022

Suporte adicionado para atualizar tabelas de rotas de VPC em sistemas de arquivos com várias AZs	Agora você pode associar (adicionar) uma nova tabela de rotas da VPC a um sistema de arquivos existente do FSx para ONTAP com várias AZs ou desassociar (remover) uma tabela de rotas da VPC existente de um sistema de arquivos existente do FSx para ONTAP com várias AZs. Para obter mais informações, consulte Atualização de um sistema de arquivos.	28 de novembro de 2022
Support adicionado para criptografia de dados em trânsito com o AWS Nitro System	Os dados em trânsito são criptografados automatic amente quando acessados de instâncias do Amazon EC2 com suporte, na região Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia) , Oeste dos EUA (Oregon) e Europa (Irlanda). Para obter mais informações, consulte Criptografando dados em trânsito com o AWS Nitro System.	28 de novembro de 2022

Suporte adicionado para criar volumes DP	Agora você pode criar volumes DP (proteção de dados) usando o console Amazon FSx ou a API AWS CLI Amazon FSx. Você pode usar volumes DP como destino de um SnapVault relacionamento NetApp SnapMirror ou quando quiser migrar ou proteger os dados de um único volume. Para obter mais informações, consulte Tipos de volume.	28 de novembro de 2022
Suporte adicionado para copiar tags de volume para backups	Agora você pode habilitar `CopyTagsToBackups` na AWS CLI ou na API do Amazon FSx para copiar automaticamente tags dos volumes para backups. Para obter mais informações, consulte Cópia de tags para backups.	28 de novembro de 2022

Suport adicionado para escolher uma política de snapshot	Agora você pode escolher entre três políticas de snapshot integradas ao criar ou atualizar um volume usando o console AWS CLI do Amazon FSx ou a API do Amazon FSx. Você também pode selecionar uma política de snapshot personalizada que criou na CLI ou na API REST do ONTAP. Para obter mais informações, consulte Políticas de snapshot.	28 de novembro de 2022
Suporte adicionado para mais opções de capacidade de throughput do sistema de arquivos	O FSx para ONTAP agora oferece suporte a 4.096 MBps de capacidade de throughpu t para sistemas de arquivos criados após 28 de novembro de 2022 na região Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda). Para obter mais informações, consulte Impacto da capacidade de throughput na performance.	28 de novembro de 2022

Suporte adicionado para mais IOPS de SSD	O FSx para ONTAP agora oferece suporte a 160.000 IOPS de SSD para sistemas de arquivos criados após 28 de novembro de 2022 na região Leste dos EUA (Ohio), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon) e Europa (Irlanda) . Para obter mais informaçõ es, consulte Impacto da capacidade de throughput na performance.	28 de novembro de 2022
Support adicionado para o uso do FSx for ONTAP como um armazenamento de dados externo para o VMware Cloud on AWS	Você pode usar o FSx for ONTAP como um armazenam ento de dados externo para o VMware Cloud on AWS Software-Defined Data Centers (SDDCs). Esse suporte adicional fornece flexibilidade para aumentar ou diminuir o armazenam ento, independentemente dos recursos de computação para cargas de trabalho do VMware Cloud on. AWS Para obter mais informações, consulte Uso do VMware Cloud com o FSx para ONTAP.	30 de agosto de 2022

Aumentar automaticamente a capacidade de armazenamento de um sistema de arquivos	Use um AWS CloudFormation modelo personalizável AWS desenvolvido para aumentar automaticamente a capacidade de armazenamento do seu sistema de arquivos quando a quantidade de capacidade de armazenamento SSD usada exceder um limite especificado por você. Para obter mais informações, consulte Aumento da capacidade de armazenamento SSD dinamicamente.	3 de junho de 2022
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 Usando AWS Backup com o Amazon FSx.	18 de maio de 2022
Suporte adicionado para implantações de sistemas de arquivos do ONTAP com uma única zona de disponibilidade	Você pode criar sistemas de arquivos do FSx para ONTAP com uma única AZ, projetados para fornecer alta disponibilidade e durabilidade em uma única Zona de Disponibilidade (AZ). Para obter mais informações, consulte Escolha da implantação do sistema de arquivos.	13 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 modificar a capacidade de throughput dos sistemas de arquivos do ONTAP existentes	Agora você pode modificar a capacidade de throughput que está disponível para seus sistemas de arquivos do ONTAP existentes. Para obter mais informações, consulte Como gerenciar a capacidade de throughput.	30 de março de 2022
Suporte adicionado para capacidade de armazenamento SSD e escala de IOPS provisionadas	Agora é possível aumentar a capacidade de armazenamento SSD e IOPS provisionadas nos sistemas de arquivos do FSx para ONTAP existentes à medida que seus requisitos de armazenamento e IOPS evoluem. Para obter mais informações, consulte Gerenciamento da capacidade de armazenamento e IOPS provisionadas	25 de janeiro de 2022

Support adicionado para CloudWatch métricas da Amazon	Você pode monitorar seu sistema de arquivos usando a Amazon CloudWatch, que coleta e processa dados brutos do FSx for ONTAP em métricas legíveis e quase em tempo real. Para obter mais informações, consulte Monitoramento com a Amazon CloudWatch.	19 de janeiro de 2022
Suporte adicionado para mais opções de throughput do sistema de arquivos	O FSx para ONTAP agora suporta opções de 128 MB/s e 256 MB/s para throughput do sistema de arquivos. Para obter mais informações, consulte Impacto da capacidade de throughput na performance.	30 de novembro de 2021
O Amazon FSx for NetApp ONTAP agora está disponível ao público em geral	O FSx for ONTAP é um serviço totalmente gerenciado que fornece armazenamento de arquivos altamente confiável, escalável, de alto desempenho e rico em recursos, incorporado no sistema de arquivos ONTAP. NetApp Ele fornece os recursos, o desempenho, os recursos e as APIs familiares dos sistemas de NetApp arquivos com a agilidade, a escalabilidade e a simplicidade de um serviço totalmente gerenciado. AWS	2 de setembro de 2021

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.