aws

Guia do usuário do Windows

Amazon FSx para Windows File Server

Amazon FSx para Windows File Server: Guia do usuário do Windows

Table of Contents

O que é o FSx para Windows File Server?

O Amazon FSx para Windows File Server fornece servidores de arquivos Microsoft Windows totalmente gerenciados, baseados em um sistema de arquivos Windows totalmente nativo. O FSx para Windows File Server possui os atributos, a performance e a compatibilidade necessários para mover sem alterações (lift-and-shift) facilmente as aplicações corporativas para a Nuvem AWS.

O Amazon FSx é compatível com um amplo conjunto de workloads corporativas do Windows com armazenamento de arquivos totalmente gerenciado criado no Microsoft Windows Server. O Amazon FSx tem suporte nativo para recursos do sistema de arquivos Windows e para o protocolo SMB (Server Message Block) padrão do setor para acessar o armazenamento de arquivos em uma rede. O Amazon FSx é otimizado para aplicativos corporativos no Nuvem AWS, com compatibilidade nativa do Windows, desempenho e recursos corporativos e latências consistentes de menos de um milissegundo.

Com o armazenamento de arquivos no Amazon FSx, o código, as aplicações e as ferramentas que os desenvolvedores e administradores do Windows usam hoje em dia podem continuar a funcionar sem alterações. As aplicações e workloads do Windows ideais para o Amazon FSx incluem aplicações de negócios, diretórios pessoais, serviço na Web, gerenciamento de conteúdo, análise de dados, configurações de criação de software e workloads de processamento de mídia.

Como um serviço totalmente gerenciado, o FSx para Windows File Server elimina os custos administrativos indiretos de configurar e provisionar servidores de arquivos e volumes de armazenamento. Além disso, o Amazon FSx mantém o software Windows atualizado, detecta e soluciona falhas de hardware e realiza backups. Ele também fornece uma integração avançada com outros AWS serviços AWS Directory Service for Microsoft Active Directory, como AWS IAM WorkSpaces AWS Key Management Service, Amazon AWS CloudTraile.

Recursos do FSx para Windows File Server: sistemas de arquivos, backups e compartilhamentos de arquivos

Os principais recursos do Amazon FSx são sistemas de arquivos e backups. Um sistema de arquivos é o local onde você armazena e acessa seus arquivos e pastas. Um sistema de arquivos é composto por um ou mais servidores de arquivos do Windows e volumes de armazenamento. Ao criar um sistema de arquivos, você especifica uma quantidade de capacidade de armazenamento (em GiB), IOPS de SSD e capacidade de throughput (em MB/s). Você pode modificar essas propriedades à

medida que suas necessidades mudarem após a criação do sistema de arquivos. Para obter mais informações, consulte Como gerenciar a capacidade de armazenamento, Como gerenciar IOPS de SSD e Como gerenciar a capacidade de throughput.

Os backups do FSx for Windows File Server file-system-consistent são altamente duráveis e incrementais. Para garantir a consistência do sistema de arquivos, o Amazon FSx usa o Volume Shadow Copy Service (VSS) no Microsoft Windows. Os backups diários automáticos são ativados por padrão quando você cria um sistema de arquivos, e você também pode fazer backups manuais adicionais a qualquer momento. Para ter mais informações, consulte Trabalhar com backups.

Um compartilhamento de arquivos do Windows é uma pasta específica (e suas subpastas) dentro do seu sistema de arquivos que você torna acessível às suas instâncias de computação com o SMB. Seu sistema de arquivos já vem com um compartilhamento de arquivos padrão do Windows chamado `\share`. Você pode criar e gerenciar quantos compartilhamentos de arquivos do Windows você quiser ao usar a ferramenta de interface gráfica do usuário (GUI) de Pastas compartilhadas no Windows. Para ter mais informações, consulte Como usar compartilhamentos de arquivos do Microsoft Windows.

Os compartilhamentos de arquivos são acessados usando o nome DNS do sistema de arquivos ou os aliases de DNS que você associa ao sistema de arquivos. Para ter mais informações, consulte Como gerenciar aliases de DNS.

Como acessar compartilhamentos de arquivos

O Amazon FSx pode ser acessado nas instâncias de computação com o protocolo SMB (compatível com as versões 2.0 a 3.1.1). Você pode acessar seus compartilhamentos de todas as versões do Windows, a partir do Windows Server 2008 e do Windows 7, e também das versões atuais do Linux. Você pode mapear seus compartilhamentos de arquivos do Amazon FSx em instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e em instâncias, instâncias AppStream Amazon 2.0 e WorkSpaces VMware Cloud em VMs. AWS

Você pode acessar seus compartilhamentos de arquivos nas instâncias de computação on-premises usando o AWS Direct Connect ou a AWS VPN. Além de acessar compartilhamentos de arquivos que estão na mesma VPC, AWS conta e AWS região do sistema de arquivos, você também pode acessar seus compartilhamentos em instâncias computacionais que estão em uma Amazon VPC, conta ou região diferente. Isso é feito com o uso do emparelhamento de VPCs ou gateways de trânsito. Para ter mais informações, consulte Métodos de acesso compatíveis.

Segurança e proteção de dados

O Amazon FSx oferece vários níveis de segurança e conformidade para ajudar a garantir que seus dados estejam protegidos. Ele criptografa automaticamente os dados em repouso (para sistemas de arquivos e backups) usando chaves que você gerencia em AWS Key Management Service (AWS KMS). Os dados em trânsito também são criptografados automaticamente usando chaves de sessão SMB do Kerberos. Ele foi avaliado para estar em conformidade com as certificações ISO, PCI-DSS e SOC, e é elegível para HIPAA.

O Amazon FSx fornece controle de acesso no nível de arquivos e pastas com listas de controle de acesso (ACLs) do Windows. Ele fornece controle de acesso no nível do sistema de arquivos usando grupos de segurança da Amazon Virtual Private Cloud (Amazon VPC). Além disso, ele fornece controle de acesso no nível da API usando políticas de acesso do AWS Identity and Access Management (IAM). Os usuários que acessam os sistemas de arquivos são autenticados com o Microsoft Active Directory. O Amazon FSx se integra AWS CloudTrail para monitorar e registrar suas chamadas de API, permitindo que você veja as ações realizadas pelos usuários em seus recursos do Amazon FSx.

Além disso, ele protege seus dados fazendo backups altamente duráveis do seu sistema de arquivos automaticamente, todos os dias, e permite que você faça backups adicionais a qualquer momento. Para ter mais informações, consulte Segurança no Amazon FSx.

Disponibilidade e durabilidade

O FSx para Windows File Server oferece sistemas de arquivos com dois níveis de disponibilidade e durabilidade. Os arquivos single-AZ garantem alta disponibilidade em uma única zona de disponibilidade (AZ), detectando e tratando automaticamente as falhas dos componentes. Além disso, os sistemas de arquivos Multi-AZ fornecem alta disponibilidade e suporte de failover em várias zonas de disponibilidade, provisionando e mantendo um servidor de arquivos em espera em uma zona de disponibilidade separada dentro de uma região. AWS Para saber mais sobre as implantações de sistemas de arquivos single-AZ e multi-AZ, consulte Disponibilidade e durabilidade: sistemas de arquivos single-AZ e multi-AZ.

Como gerenciar sistemas de arquivos

Você pode administrar seus sistemas de arquivos FSx for Windows File Server usando comandos personalizados de PowerShell gerenciamento remoto ou usando a GUI nativa do Windows em

alguns casos. Para saber mais sobre o gerenciamento de sistemas de arquivos do Amazon FSx, consulte Como administrar sistemas de arquivos.

Flexibilidade de preço e performance

O FSx para Windows File Server oferece a flexibilidade de preço e performance ao oferecer os tipos de armazenamento de unidade de estado sólido (SSD) e unidade de disco rígido (HDD). O armazenamento em HDD foi projetado para um amplo espectro de workloads, incluindo diretórios pessoais, compartilhamentos de usuários e departamentos e sistemas de gerenciamento de conteúdo. O armazenamento SSD foi projetado para as workloads de mais alta performance e mais sensíveis à latência, incluindo bancos de dados, workloads de processamento de mídia e aplicações de análise de dados.

Com o FSx para Windows File Server, você pode fornecer armazenamento do sistema de arquivos, IOPS de SSD e throughput de forma independente para obter a combinação certa de custo e performance. Você pode modificar o armazenamento, IOPS de SSD e as capacidades de throughput do seu sistema de arquivos para atender às necessidades de workloads em constante mudança, de modo que você pague apenas o necessário. Para ter mais informações, consulte Como otimizar os custos com o Amazon FSx.

Preços do Amazon FSx

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

Suposições

Para usar o Amazon FSx, você precisa de uma AWS conta com uma instância, instância WorkSpaces AppStream , instância 2.0 ou VM do Amazon EC2 em execução na nuvem AWS VMware em ambientes do tipo suportado.

Neste guia, fazemos as seguintes suposições:

- Se você estiver usando o Amazon EC2, presumimos que você já tenha familiaridade com o Amazon EC2. Para obter mais informações sobre o Amazon EC2, consulte a Documentação do Amazon Elastic Compute Cloud.

- Se você estiver usando WorkSpaces, presumimos que você esteja familiarizado com WorkSpaces. Para obter mais informações sobre como usar WorkSpaces, consulte o Guia WorkSpaces do usuário da Amazon.
- Se você estiver usando o VMware Cloud on AWS, presumimos que você esteja familiarizado com ele. Para obter mais informações, consulte VMware Cloud na AWS.
- Presumimos que você tenha familiaridade com os conceitos do Microsoft Active Directory.

Pré-requisitos

Para criar um sistema de arquivos do Amazon FSx, você precisa do seguinte:

- Uma AWS conta com as permissões necessárias para criar um sistema de arquivos Amazon FSx e uma instância do Amazon EC2. Para ter mais informações, consulte Configurando seu Conta da AWS.
- Uma instância do Amazon EC2 executando o Microsoft Windows Server na nuvem privada virtual (VPC) com base no serviço Amazon VPC que você deseja associar ao seu sistema de arquivos do Amazon FSx. Para obter informações sobre como criar uma, consulte Conceitos básicos das instâncias Windows do Amazon EC2 no Guia do usuário do Amazon EC2.
- O Amazon FSx trabalha com o Microsoft Active Directory para realizar a autenticação de usuários e o controle de acesso. Você associa seu sistema de arquivos do Amazon FSx a um Microsoft Active Directory ao criá-lo. Para ter mais informações, consulte Trabalhar com o Microsoft Active Directory no FSx para Windows File Server.
- Este guia pressupõe que você não alterou as regras do grupo de segurança padrão para sua VPC com base no serviço Amazon VPC. Caso tenha feito isso, é preciso garantir que você adicione as regras necessárias para permitir o tráfego de rede da instância do Amazon EC2 para o sistema de arquivos do Amazon FSx. Para obter mais detalhes, consulte Segurança no Amazon FSx.
- Instale e configure o AWS Command Line Interface (AWS CLI). As versões compatíveis são a 1.9.12 e as mais recentes. Para obter mais informações, consulte Como instalar, atualizar e desinstalar a AWS CLI no Guia do usuário da AWS Command Line Interface .

> **Note**
>
> Você pode verificar a versão do AWS CLI que você está usando com o `aws --version` comando.

Fóruns do Amazon FSx para Windows File Server

Caso você encontre problemas ao usar o Amazon FSx, use os fóruns.

É a primeira vez que você usa o Amazon FSx?

Se for você estiver usando o Amazon FSx pela primeira vez, recomendamos que você leia as seções a seguir na ordem.

1. Caso esteja tudo pronto para criar seu primeiro sistema de arquivos do Amazon FSx, experimente o Introdução ao Amazon FSx para Windows File Server.
2. Para obter mais informações sobre performance, consulte Performance do FSx para Windows File Server.
3. Para obter detalhes de segurança do Amazon FSx, consulte Segurança no Amazon FSx.
4. Para obter informações sobre a API do Amazon FSx, consulte Amazon FSx API Reference.

Práticas recomendadas para FSx para Windows File Server

Recomendamos que você siga estas práticas recomendadas quando trabalhar com o Amazon FSx para Windows File Server. Siga os links abaixo para saber mais sobre os tópicos discutidos.

Tópicos

Práticas recomendadas gerais

Como testar as workloads antes de passar para a produção

Recomendamos usar um ambiente de preparação com as mesmas configurações que o seu ambiente de produção para testar suas workloads. Por exemplo, use as mesmas configurações do Active Directory (AD) e de rede, tamanho e configuração do sistema de arquivos e recursos do Windows, como eliminação de duplicação de dados e cópias de sombra. A execução de workloads de teste em um ambiente de preparação que simula o tráfego de produção desejado ajuda a garantir que o processo seja executado sem problemas.

Também recomendamos revisar o modelo de disponibilidade do seu sistema de arquivos e garantir que sua workload seja resiliente ao comportamento de recuperação esperado para seu tipo de sistema de arquivos durante eventos como manutenção do sistema de arquivos, alterações na capacidade de throughput e interrupções não planejadas do serviço. Para ter mais informações, consulte Disponibilidade e durabilidade: sistemas de arquivos single-AZ e multi-AZ.

Como criar um plano de monitoramento

Você pode usar métricas do sistema de arquivos para monitorar seu uso de armazenamento e performance, entender seus padrões de uso e acionar notificações quando seu uso se aproximar dos limites de armazenamento ou performance do sistema de arquivos. O monitoramento de seus sistemas de arquivos do Amazon FSx junto com o resto do seu ambiente de aplicações permite que você depure rapidamente quaisquer problemas que possam afetar a performance.

Garantir que seus sistemas de arquivos tenham recursos suficientes

Ter recursos insuficientes pode resultar em maior latência e filas para solicitações de E/S, o que pode parecer indisponibilidade total ou parcial do seu sistema de arquivos. Para obter mais informações sobre como monitorar a performance e acessar os avisos e recomendações de performance, consulte Como monitorar o FSx para Windows File Server.

Fazer backup de seus sistemas de arquivos regularmente

Os backups regulares permitem que você atenda às suas necessidades de retenção de dados, negócios e conformidade. Recomendamos usar os backups diários automáticos que são ativados por padrão para seu sistema de arquivos e usar AWS Backup uma solução de backup centralizada em todo Serviços da AWS o sistema. AWS Backup permite que você configure planos de backup adicionais com diferentes frequências (por exemplo, várias vezes ao dia, diariamente ou semanalmente) e períodos de retenção.

Melhores práticas de segurança

Recomendamos que você siga estas práticas recomendadas para administrar os controles de segurança e acesso do sistema de arquivos. Para obter informações mais detalhadas sobre como configurar o Amazon FSx para atender aos objetivos de segurança e compatibilidade, consulte. Segurança no Amazon FSx

Segurança de rede

Não modifique nem exclua a ENI associada ao seu sistema de arquivos

Seu sistema de arquivos do Amazon FSx é acessado por meio de uma interface de rede elástica (ENI) que reside na nuvem privada virtual (VPC) associada 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.

Uso de grupos de segurança e network ACLs

É possível usar grupos de segurança e listas de controle de acesso (ACLs) à rede para limitar o acesso aos sistemas de arquivos. Para grupos de segurança da VPC, o grupo de segurança padrão já está adicionado ao seu sistema de arquivos no console. Garanta que o grupo de segurança e as

ACLs de rede das sub-redes em que você cria seu sistema de arquivos permitam tráfego nas portas. Para ter mais informações, consulte Grupos de segurança da Amazon VPC.

Active Directory

Ao criar um sistema de arquivos do Amazon FSx, você pode associá-lo ao seu domínio do Microsoft AD para fornecer autenticação de usuário e autorização de controle de acesso em nível de compartilhamento, arquivo e pasta. Seus usuários podem usar suas contas existentes do AD para se conectar a compartilhamentos de arquivos e acessar arquivos e pastas dentro deles. Além disso, você pode migrar a configuração atual da ACL de segurança para o Amazon FSx sem nenhuma modificação. O Amazon FSx oferece duas opções para o Active Directory: AWS Managed Microsoft AD ou Microsoft AD autogerenciado.

Se você estiver usando um AWS Managed Microsoft AD, recomendamos deixar as configurações padrão do seu grupo de segurança do AD. Se você modificar essas configurações, certifique-se de manter uma configuração de rede que atenda aos requisitos de rede. Para ter mais informações, consulte Pré-requisitos de rede.

Se você estiver usando um Microsoft AD autogerenciado, você tem opções adicionais para configurar seu sistema de arquivos. Recomendamos as práticas recomendadas a seguir para configuração inicial quando usar o Amazon FSx com seu Microsoft AD autogerenciado:

- Atribuir sub-redes a um único site do AD: se seu ambiente do AD tiver um grande número de controladores de domínio, use os sites e serviços do Active Directory para atribuir as sub-redes usadas pelos sistemas de arquivos do Amazon FSx a um único site do AD com a maior disponibilidade e confiabilidade. Certifique-se de que o grupo de segurança da VPC, a ACL da rede VPC, as regras de firewall do Windows em seus DCs e quaisquer outros controles de roteamento de rede que você tenha em sua infraestrutura do AD permitam a comunicação do Amazon FSx nas portas necessárias. Isso permite que o Windows reverta para outros DCs, se não puder usar o site do AD atribuído. Para ter mais informações, consulte Controle de acesso ao sistema de arquivos com a Amazon VPC.
- Usar uma unidade organizacional (UO) separada: use uma UO para seus sistemas de arquivos do Amazon FSx que seja separada de qualquer outra unidade organizacional que você possa ter.
- Configurar sua conta de serviço com os privilégios mínimos necessários: configure ou delegue a conta de serviço que você fornece ao Amazon FSx com os privilégios mínimos necessários. Para obter mais informações, consulte Pré-requisitos para usar um Microsoft Active Directory autogerenciado e Delegar privilégios à conta de serviço Amazon FSx .

- Verificar continuamente sua configuração do AD: execute a ferramenta de validação do Active Directory do Amazon FSx em relação à sua configuração do AD, antes de criar seu sistema de arquivos do Amazon FSx para verificar se sua configuração é válida para uso com o Amazon FSx e para descobrir quaisquer avisos e erros que a ferramenta possa expor.

Evitar perder a disponibilidade devido à configuração incorreta do AD

Ao usar o Amazon FSx com seu Microsoft AD autogerenciado, é importante ter uma configuração válida do AD não apenas durante a criação do seu sistema de arquivos, mas também para operações e disponibilidade contínuas. Durante eventos de recuperação de falhas, eventos de manutenção de rotina e ações de atualização da capacidade de throughput, o Amazon FSx reúne os recursos do servidor de arquivos ao seu Active Directory. Se a configuração do AD não for válida durante um evento, seu sistema de arquivos será alterado para o status de Configurado incorretamente e corre o risco de ficar indisponível. Aqui estão algumas maneiras de evitar a perda de disponibilidade:

- Mantenha sua configuração do AD atualizada com o Amazon FSx: se você fizer alterações, como redefinir a senha da sua conta de serviço, certifique-se de atualizar a configuração de qualquer sistema de arquivos usando essa conta de serviço.
- Monitore a configuração incorreta do AD: defina notificações de status de configuração incorreta para que você possa redefinir a configuração do AD do seu sistema de arquivos, se necessário. Para ver um exemplo que usa uma solução baseada em Lambda para conseguir isso, consulte Monitoramento da integridade dos sistemas de arquivos Amazon FSx usando Amazon e. EventBridge AWS Lambda
- Valide sua configuração do AD regularmente: se você quiser detectar proativamente configurações incorretas do AD, recomendamos que você execute a ferramenta de validação do Active Directory em sua configuração do AD de forma contínua. Se você receber avisos ou erros ao executar a ferramenta de validação, isso significa que seu sistema de arquivos corre o risco de ser configurado incorretamente.
- Não mova nem modifique objetos de computador criados pelo FSx: o Amazon FSx cria e gerencia objetos de computador em seu AD, usando a conta de serviço e as permissões que você fornece. Mover ou modificar esses objetos do computador pode resultar na configuração incorreta do sistema de arquivos.

ACLs do Windows

Com o Amazon FSx, você usa listas de controle de acesso (ACLs) padrão do Windows para um controle de acesso refinado em nível de compartilhamento, arquivo e pasta. Os sistemas de arquivos do Amazon FSx verificam automaticamente as credenciais dos usuários que acessam os dados do sistema de arquivos para aplicar essas ACLs do Windows.

- Não altere as permissões de ACL de NTFS para o usuário SYSTEM: o Amazon FSx exige que o usuário SYSTEM tenha controle total das permissões de ACL de NTFS em todas as pastas do seu sistema de arquivos. Alterar as permissões de ACL de NTFS para o usuário SYSTEM pode fazer com que seu sistema de arquivos fique inacessível e que futuros backups do sistema de arquivos se tornem inutilizáveis.

Como configurar e dimensionar corretamente seu sistema de arquivos

Selecionar um tipo de implantação

O Amazon FSx oferece duas opções de implantação: single-AZ e multi-AZ. Recomendamos o uso de sistemas de arquivos multi-AZ para a maioria das workloads de produção que exigem alta disponibilidade para dados de arquivos compartilhados do Windows. Para ter mais informações, consulte Disponibilidade e durabilidade: sistemas de arquivos single-AZ e multi-AZ.

Selecionar um tipo de armazenamento

O armazenamento SSD é apropriado para a maioria das workloads de produção que têm requisitos de alta performance e sensibilidade à latência. Exemplos dessas workloads incluem bancos de dados, análise de dados, processamento de mídia e aplicações de negócios. Também recomendamos o SSD para casos de uso que envolvam um grande número de usuários finais, altos níveis de E/S ou conjuntos de dados que tenham um grande número de arquivos pequenos. Por fim, recomendamos o uso de armazenamento SSD se você planeja habilitar cópias de sombra. Você pode configurar e escalar IOPS de SSD para sistemas de arquivos com armazenamento SSD, mas não armazenamento em HDD.

Se você decidir usar o armazenamento em HDD, teste seu sistema de arquivos para garantir que ele atenda aos seus requisitos de performance. O armazenamento em HDD tem um custo menor em relação ao armazenamento SSD, mas com latências mais altas e níveis mais baixos de taxa

de throughput e IOPS de disco por unidade de armazenamento. Ele pode ser adequado para compartilhamentos de usuários de uso geral e diretórios de base com baixos requisitos de E/S, grandes sistemas de gerenciamento de conteúdo (CMS) em que os dados são recuperados com pouca frequência ou conjuntos de dados com pequenos números de arquivos grandes. Para ter mais informações, consulte Configuração e performance do armazenamento.

Você pode atualizar seu tipo de armazenamento de HDD para SSD a qualquer momento usando o console Amazon FSx ou a API do Amazon FSx. Para ter mais informações, consulte Como gerenciar o tipo de armazenamento.

Seleção de uma capacidade de throughput

Configure seu sistema de arquivos com capacidade de throughput suficiente para atender não apenas ao tráfego esperado de sua workload, mas também aos recursos adicionais de performance necessários para oferecer suporte aos recursos que você deseja habilitar em seu sistema de arquivos. Por exemplo, se você estiver executando a eliminação de duplicação de dados, a capacidade de throughput selecionada deverá fornecer memória suficiente para executar a eliminação de duplicação com base no armazenamento que você tem. Se você estiver usando cópias de sombra, aumente a capacidade de throughput para um valor que seja pelo menos três vezes o valor esperado de sua workload para evitar que o Windows Server exclua suas cópias de sombra. Para ter mais informações, consulte Impacto da capacidade de throughput na performance.

Como aumentar a capacidade de armazenamento e a de throughput

Aumente a capacidade de armazenamento do seu sistema de arquivos quando ele estiver com pouco espaço livre ou quando você esperar que seus requisitos de armazenamento aumentem mais do que o limite de armazenamento atual. Recomendamos manter pelo menos 10% da capacidade de armazenamento livre em todos os momentos em seu sistema de arquivos. Também recomendamos aumentar a capacidade de armazenamento em pelo menos 20% antes da escalabilidade do armazenamento, pois você não poderá aumentá-la enquanto o processo estiver em andamento. Você pode usar a CloudWatch métrica FreeStorageCapacidade para monitorar a quantidade de armazenamento gratuito disponível e entender suas tendências. Para ter mais informações, consulte Como gerenciar a capacidade de armazenamento.

Você também deverá aumentar a capacidade de throughput do sistema de arquivos se sua workload estiver limitada pelos limites de performance atuais. Você pode usar a página Monitoramento e performance no console FSx para ver quando as demandas de workload se aproximaram ou excederam os limites de performance e determinar se seu sistema de arquivos está subprovisionado para sua workload.

Para minimizar a duração da escalabilidade do armazenamento e evitar a redução na performance de gravação, recomendamos aumentar a capacidade de throughput do seu sistema de arquivos antes de aumentar a capacidade de armazenamento e, em seguida, reduzir a capacidade de throughput após a conclusão do aumento da capacidade de armazenamento. A maioria das workloads tem um impacto mínimo na performance durante a escalabilidade do armazenamento, mas aplicações com muita gravação e grandes conjuntos de dados ativos podem experimentar temporariamente uma redução de até metade na performance de gravação.

Modificar a capacidade de throughput durante períodos de inatividade

A atualização da capacidade de throughput interrompe a disponibilidade por alguns minutos para sistemas de arquivos single-AZ e causa failover e failback para sistemas de arquivos multi-AZ. Para sistemas de arquivos multi-AZ, se houver tráfego contínuo durante o failover e o failback, todas as alterações de dados feitas durante esse período precisarão ser sincronizadas entre os servidores de arquivos. O processo de sincronização de dados pode levar até várias horas para workload com muita gravação e IOPS. Embora seu sistema de arquivos continue disponível durante esse período, recomendamos programar janelas de manutenção e realizar atualizações da capacidade de throughput durante os períodos de inatividade, quando há uma carga mínima no sistema de arquivos, para reduzir a duração da sincronização de dados. Para saber mais, consulte Como gerenciar a capacidade de throughput.

Introdução ao Amazon FSx para Windows File Server

A seguir, você pode aprender como começar a usar o FSx for Windows File Server. Este exercício sobre os conceitos básicos inclui as etapas apresentadas a seguir.

1. Inscreva-se Conta da AWS e crie um usuário administrativo na conta.
2. Crie um Microsoft AD Active Directory AWS gerenciado usando AWS Directory Service o. Você unirá seu sistema de arquivos e sua instância de computação ao Active Directory.
3. Crie uma instância de computação Amazon Elastic Compute Cloud executando o Microsoft Windows Server. Você usará essa instância para acessar seu sistema de arquivos.
4. Crie um sistema de arquivos Amazon FSx for Windows File Server usando o console Amazon FSx.
5. Mapeie seu sistema de arquivos para sua instância do EC2
6. Grave dados em seu sistema de arquivos.
7. Faça backup do seu sistema de arquivos.
8. Limpe os recursos que você criou.

Tópicos

Configurando seu Conta da AWS

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

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 prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem 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 Início de Sessão da AWS .
2. Ative a autenticação multifator (MFA) para seu 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 IAM Identity Center, use a URL de login enviada ao seu endereço de e-mail quando você criou o usuário IAM Identity Center user.

  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 a 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 .

Crie seu sistema de arquivos

Para criar seu sistema de arquivos Amazon FSx, você deve criar sua instância Windows Amazon Elastic Compute Cloud (Amazon EC2) e o diretório. AWS Directory Service Se você ainda não tiver isso configurado, consulte Passo a passo 1: pré-requisitos para começar.

Para criar seu sistema de arquivos (console)

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 FSx for Windows File Server e, em seguida, selecione Next (Avançar). A página Criar sistema de arquivos é exibida.
4. Em Método de criação, escolha Criação padrão.

Detalhes do sistema de arquivos

1. Na seção Detalhes do sistema de arquivos, forneça um nome para o 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, espaços em branco e números, além dos caracteres especiais + - = . _ : /
2. Em Tipo de implantação, escolha Multi-AZ ou Single-AZ.

   - Escolha Multi-AZ para implantar um sistema de arquivos que seja tolerante à indisponibilidade da zona de disponibilidade. Essa opção é compatível com armazenamento SSD e HDD.
   - Escolha Single-AZ para implantar um sistema de arquivos em uma única zona de disponibilidade. Single-AZ 2 é a geração mais recente de sistemas de arquivos de zona de disponibilidade única. É compatível com armazenamento SSD e HDD.

   Para ter mais informações, consulte Disponibilidade e durabilidade: sistemas de arquivos single-AZ e multi-AZ.
3. Em Tipo de armazenamento, você pode escolher SSD ou HDD.

   O FSx para Windows File Server oferece tipos de armazenamento em unidade de estado sólido (SSD) e em unidade de disco rígido (HDD). O armazenamento SSD foi projetado para as workloads de mais alta performance e mais sensíveis à latência, incluindo bancos de dados, workloads de processamento de mídia e aplicações de análise de dados. O armazenamento HDD foi projetado para um amplo espectro de workloads, incluindo diretórios iniciais, compartilhamentos de arquivos de usuários e departamentos e sistemas de gerenciamento de conteúdo. Para ter mais informações, consulte Como otimizar os custos usando tipos de armazenamento.

4. Em IOPS SSD provisionado, você pode escolher o modo Automático ou Provisionado pelo usuário.

   Se você escolher o modo Automático, o FSx para Windows File Server escalará automaticamente o IOPS SSD para manter 3 IOPS SSD por GiB de capacidade de armazenamento. Se você escolher o modo provisionado pelo usuário, insira qualquer número inteiro no intervalo de 96 a 400.000. A escalabilidade de IOPS SSD acima de 80 mil está disponível no Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Leste dos EUA (Ohio), Europa (Irlanda), Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Singapura). Para ter mais informações, consulte Como gerenciar IOPS de SSD.

5. Em Capacidade de armazenamento, insira a capacidade de armazenamento do sistema de arquivos, em GiB. Se você estiver usando o armazenamento SSD, insira qualquer número inteiro no intervalo entre 32 e 65.536. Se você estiver usando o armazenamento em HDD, insira qualquer número inteiro no intervalo entre 2.000 e 65.536. 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.

6. Mantenha a Capacidade de Throughput na configuração padrão. Capacidade de throughput: é a velocidade sustentada na qual o servidor de arquivos que hospeda o sistema de arquivos pode fornecer dados. A configuração da capacidade de throughput recomendada é baseada na quantidade de capacidade de armazenamento que você escolher. Se você precisar de mais do que a capacidade de throughput recomendada, escolha Especificar capacidade de throughput e, em seguida, escolha um valor. Para ter mais informações, consulte Performance do FSx para Windows File Server.

   > **Note**
   >
   > Se você quiser habilitar a auditoria de acesso a arquivos, deverá escolher uma capacidade de throughput de 32 MB/s ou mais. Para ter mais informações, consulte Auditoria de acesso a arquivos.

   Você pode modificar a capacidade de throughput, conforme necessário, a qualquer momento depois de criar o sistema de arquivos. Para ter mais informações, consulte Como gerenciar a capacidade de throughput.

Rede e segurança

1. Na seção Rede e segurança, escolha a Amazon VPC que você deseja associar ao sistema de arquivos. Para este exercício de introdução, escolha a mesma Amazon VPC que você escolheu para seu AWS Directory Service diretório e sua instância do Amazon EC2.
2. Em Grupos de segurança da VPC, o grupo de segurança padrão para a Amazon VPC padrão já está adicionado ao sistema de arquivos no console. Se você não estiver usando o grupo de segurança padrão, verifique se o grupo de segurança escolhido está no Região da AWS mesmo do seu sistema de arquivos. Para garantir que você possa conectar uma instância do EC2 ao seu sistema de arquivos, você precisará adicionar as seguintes regras ao grupo de segurança escolhido:

   a. Adicione as regras de entrada e saída a seguir para permitir as portas a seguir.

Regras	Portas
UDP	53, 88, 123, 389, 464
TCP	53, 88, 135, 389, 445, 464, 636, 3268, 3269, 5985, 9389, 49152-65535

   Adicione endereços IP de entrada e saída ou IDs de grupos de segurança associados às instâncias de computação nas quais você deseja acessar o sistema de arquivos.

   b. Adicione regras de saída para permitir todo o tráfego para o Active Directory ao qual você está associando o sistema de arquivos. Para isso, execute um dos seguintes procedimentos:

      - Permita tráfego de saída para o ID do grupo de segurança associado ao diretório do AWS Managed AD.
      - Permita tráfego de saída para os endereços IP associados aos controladores de domínio do Active Directory autogerenciado.

> **Note**
>
> Em alguns casos, você pode ter modificado as regras do seu grupo de AWS Managed Microsoft AD segurança a partir das configurações padrão. Nesse caso, certifique-se de que esse grupo de segurança tenha as regras de entrada necessárias para permitir tráfego proveniente do sistema de arquivos do Amazon FSx. Para obter mais informações sobre as regras de entrada necessárias, consulte Pré-requisitos do AWS Managed Microsoft AD no Guia de Administração do AWS Directory Service .

Para ter mais informações, consulte Controle de acesso ao sistema de arquivos com a Amazon VPC.

3. Os sistemas de arquivos Multi-AZ têm um servidor de arquivos primário e um em espera, cada um em sua própria zona de disponibilidade e sub-rede. Se você estiver criando um sistema de arquivos Multi-AZ (consulte a etapa 5), escolha um valor de sub-rede preferencial para o servidor de arquivos principal e um valor de sub-rede em espera para o servidor de arquivos em espera.

   Se você estiver criando um sistema de arquivos Single-AZ, escolha a sub-rede para seu sistema de arquivos.

autenticação do Windows

- Em autenticação do Windows, você tem as seguintes opções:

  Escolha Microsoft Active Directory AWS Gerenciado se quiser unir seu sistema de arquivos a um domínio do Microsoft Active Directory gerenciado por e AWS, em seguida, escolha seu AWS Directory Service diretório na lista. Para ter mais informações, consulte Trabalhar com o Microsoft Active Directory no FSx para Windows File Server.

  Escolha Microsoft Active Directory autogerenciado se quiser unir seu sistema de arquivos a um domínio autogerenciado do Microsoft Active Directory e forneça os seguintes detalhes para seu Active Directory. Para obter mais informações, consulte Como usar o Amazon FSx com seu Microsoft Active Directory autogerenciado.

  - O nome totalmente qualificado do domínio do Active Directory.

> **Important**
>
> Para sistemas de arquivos single-AZ 2 e todos os sistemas de arquivos multi-AZ, o nome de domínio do Active Directory não pode exceder 47 caracteres. Essa limitação se aplica tanto aos nomes AWS Directory Service de domínio autogerenciados do Active Directory.
> O Amazon FSx exige uma conexão direta para tráfego interno com seu endereço IP DNS. A conexão por meio de um gateway da Internet não é compatível. Em vez disso AWS Virtual Private Network, use emparelhamento de VPC ou AWS Direct Connect associação. AWS Transit Gateway

- Endereços IP de servidor DNS: os endereços IPv4 dos servidores DNS do seu domínio

> **Note**
>
> O servidor DNS deve ter o Extension Mechanisms for DNS (EDNS - Mecanismos de extensão para DNS) habilitado. Se o EDNS estiver desativado, seu sistema de arquivos pode falhar na criação.

- Nome de usuário da conta de serviço: o nome de usuário da conta de serviço no Active Directory atual. Não inclua um prefixo ou sufixo de domínio.
- Senha da conta de serviço: a senha da conta de serviço.
- (Opcional) Unidade organizacional (UO): o nome distinto do caminho da unidade organizacional à qual você deseja associar o sistema de arquivos.
- (Opcional) Grupo de administradores delegado do sistema de arquivos: o nome do grupo do Active Directory que pode administrar o sistema de arquivos. O grupo padrão é “Administradores de domínio”. Para ter mais informações, consulte Delegar privilégios à conta de serviço Amazon FSx .

Criptografia, auditoria e acesso (aliases de DNS)

1. Em Criptografia, escolha a chave de AWS KMS key criptografia usada para criptografar os dados em seu sistema de arquivos em repouso. Você pode escolher o aws/fsx padrão (padrão) que é gerenciado por AWS KMS, uma chave existente ou uma chave gerenciada pelo cliente especificando o ARN da chave. Para ter mais informações, consulte Criptografia em repouso.

2. Em Auditoria - opcional, a auditoria de acesso a arquivos está desabilitada por padrão. Para obter informações sobre a habilitação e a configuração da auditoria de acesso a arquivos, consulte Habilitar a auditoria de acesso a arquivos ao criar um sistema de arquivos (console).
3. Em Acesso: opcional, insira qualquer alias de DNS que você deseja associar ao sistema de arquivos. Cada nome de alias deve ser formatado como nome de domínio totalmente qualificado (FQDN). Para ter mais informações, consulte Como gerenciar aliases de DNS.

Backup e manutenção

Para obter mais informações sobre backups diários automáticos e as configurações desta seção, consulteTrabalhar com backups.

1. Para backup automático diário, está habilitado por padrão. Você pode desativar essa configuração se não quiser que o Amazon FSx faça backups do seu sistema de arquivos automaticamente diariamente.
2. Se os backups automáticos estiverem habilitados, eles ocorrerão dentro de um período conhecido como janela de backup. Você pode usar a janela padrão ou escolher um horário de início da janela de backup automático.
3. Para o período de retenção automática de backup, você pode usar a configuração padrão de 30 dias ou definir um valor entre 1 e 90 dias pelo qual o Amazon FSx reterá backups diários automáticos do seu sistema de arquivos. Essa configuração não se aplica ao backup iniciado pelo usuário ou aos backups feitos pelo AWS Backup.
4. Em Tags: opcional, insira 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. Para ter mais informações, consulte Marcar os recursos do Amazon FSx.

   Escolha Próximo.

Revise sua configuração e crie

1. Verifique a configuração do sistema de arquivos mostrada na página Criar sistema de arquivos. Para sua referência, você pode ver quais configurações do sistema de arquivos você pode e não pode modificar após a criação do sistema de arquivos. Escolha Create file system (Criar sistema de arquivos).

2. Depois que o Amazon FSx criar o sistema de arquivos, escolha o ID do sistema de arquivos na lista no painel de sistemas de arquivos para ver os detalhes. Escolha Anexar e anote o nome DNS do seu sistema de arquivos na guia Rede e segurança. Você precisará dela no procedimento a seguir para mapear um compartilhamento para uma instância do EC2.

Mapeie seu compartilhamento de arquivos para uma instância do EC2 executando o Windows Server

Agora você pode montar seu sistema de arquivos Amazon FSx na sua instância do Amazon EC2 baseada no Microsoft Windows associada ao seu diretório. AWS Directory Service O nome do compartilhamento de arquivos não é igual ao nome do sistema de arquivos.

Mapear um compartilhamento de arquivos em uma instância do Windows do Amazon EC2 usando a GUI

1. Antes de montar um compartilhamento de arquivos em uma instância do Windows, você deve iniciar a instância do EC2 e associá-la a um AWS Directory Service for Microsoft Active Directory. Para executar essa ação, 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 à sua instância. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
3. Quando estiver conectado, abra o Explorador de Arquivos.
4. No painel de navegação, abra o menu de contexto (clique com o botão direito do mouse) em Rede e escolha Mapear unidade de rede.
5. Escolha a letra de unidade preferencial em Unidade.
6. Você pode mapear o sistema de arquivos usando o nome DNS padrão atribuído pelo Amazon FSx ou usando um alias de DNS de sua escolha. Esse procedimento descreve o mapeamento de um compartilhamento de arquivos usando o nome DNS padrão. Se você quiser mapear um compartilhamento de arquivos usando um alias de DNS, consulte Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos.

   Em Pasta, insira o nome DNS do sistema de arquivos e o nome do compartilhamento. O compartilhamento padrão do Amazon FSx é denominado `\share`. Você pode encontrar

o nome DNS no console do Amazon FSx, https://console.aws.amazon.com/fsx/, na seção Windows File Server > Rede e segurança ou na resposta do comando CreateFileSystem ou DescribeFileSystems da API.

- Para um sistema de arquivos Single-AZ associado a um Microsoft Active Directory AWS gerenciado, o nome DNS se parece com o seguinte.

```
fs-0123456789abcdef0.ad-domain.com
```

- Para um sistema de arquivos single-AZ associado a um Active Directory autogerenciado, e para qualquer sistema de arquivos multi-AZ, o nome DNS seria como a seguir.

```
amznfsxaa11bb22.ad-domain.com
```

Por exemplo, digite `\\fs-0123456789abcdef0.ad-domain.com\share`.

7. Escolha se o compartilhamento de arquivos deve Reconectar-se no login e, em seguida, escolha Concluir.

Grave dados em seu compartilhamento de arquivos

Agora que você mapeou o compartilhamento de arquivos para a instância, você pode usá-lo como qualquer outro diretório no ambiente Windows.

Gravar dados no compartilhamento de arquivos

1. Abra o editor de texto Notepad.
2. Escreva algum conteúdo no editor de texto. Por exemplo: *Olá, mundo!*
3. Salve o arquivo na letra da unidade do compartilhamento de arquivos.
4. Usando o Explorador de Arquivos, navegue até o compartilhamento de arquivos e encontre o arquivo de texto que você acabou de salvar.

Faça backup do seu sistema de arquivos

Agora que você teve a oportunidade de usar o sistema de arquivos do Amazon FSx e os compartilhamentos de arquivos, pode fazer backup. Por padrão, os backups diários são criados automaticamente durante a janela de backup de 30 minutos do sistema de arquivos. No entanto,

você pode criar um backup iniciado pelo usuário a qualquer momento. Os backups têm custos adicionais associados a eles. Para obter mais informações sobre preços de backup, consulte Preços.

Criar um backup do sistema de arquivos no console

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel do console, escolha o nome do sistema de arquivos que você criou para este exercício.
3. Na guia Visão geral do sistema de arquivos, escolha Criar backup.
4. Na caixa de diálogo Criar backup que é aberta, forneça um nome para o backup. Esse nome pode conter no máximo 256 letras Unicode e incluir espaços em branco, números e os seguintes caracteres especiais: + - = . _ : /
5. Escolha Create backup.
6. Para visualizar todos os backups em uma lista, para que você possa restaurar o sistema de arquivos ou excluir o backup, escolha Backups.

Quando você cria um backup, o status dele é definido como CRIANDO enquanto ele está sendo criado. Isso pode levar alguns minutos. Quando o backup está disponível para uso, o status muda para DISPONÍVEL.

Limpar recursos

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

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. No console do Amazon FSx, exclua o sistema de arquivos. Todos os backups automáticos são excluídos automaticamente. No entanto, você ainda precisa excluir os backups criados manualmente. As seguintes etapas resumem este processo:
    a. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
    b. No painel do console, escolha o nome do sistema de arquivos que você criou para este exercício.

c. Para Ações, escolha Excluir sistema de arquivos.

d. Na caixa de diálogo Excluir sistema de arquivos que é aberta, decida se você deseja criar um backup final. Caso deseje, forneça um nome para o backup final. Todos os backups criados automaticamente também são excluídos.

> **Important**
>
> Sistemas de arquivos podem ser criados de backups. Recomendamos que você crie um backup final como prática recomendada. Se você achar que não precisa dele depois de um determinado período, poderá excluir esse e outros backups criados manualmente.

e. Insira o ID do sistema de arquivos que você deseja excluir na caixa ID do sistema de arquivos.

f. Escolha Excluir sistema de arquivos.

g. O sistema de arquivos agora está sendo excluído e o status dele no painel muda para EXCLUINDO. Quando o sistema de arquivos é excluído, não aparece mais no painel.

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

i. No painel, escolha os backups que têm o mesmo ID de sistema de arquivos que o sistema de arquivos que você excluiu e escolha Excluir backup.

j. A caixa de diálogo Excluir backups é aberta. Deixe a caixa de seleção marcada para o ID do backup selecionado e escolha Excluir backups.

O sistema de arquivos do Amazon FSx e os backups automáticos relacionados agora estão excluídos.

3. Se você criou um AWS Directory Service diretório para este exercício emPasso a passo 1: pré-requisitos para começar, você pode excluí-lo agora. Para obter mais informações, consulte Excluir diretório no Guia de Administração do AWS Directory Service .

Status do sistema de arquivos do Amazon FSx

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 está em um estado íntegro e está acessível e disponível para uso.
CRIANDO	O Amazon FSx está criando um novo sistema de arquivos.
EXCLUINDO	O Amazon FSx está excluindo um sistema de arquivos existente.
ATUALIZANDO	O sistema de arquivos está passando por uma atualização iniciada pelo cliente.
CONFIGURAÇÃO INCORRETA	O sistema de arquivos está danificado devido a uma alteração no ambiente do Active Directory . O sistema de arquivos está indisponível no momento ou corre o risco de perder a disponibilidade, e os backups podem não ser bem-sucedidos. Para obter informações sobre a restauração da disponibilidade, consulte O sistema de arquivos está em um estado de configuração incorreta.
MISCONFIGURED_UNAVAILABLE	O sistema de arquivos não está disponível no momento devido a uma alteração no ambiente do Active Directory. Para obter informaçõ es sobre a restauração da disponibilidade, consulte O sistema de arquivos está em um estado de configuração incorreta.
COM FALHA	• O Amazon FSx não conseguiu criar o sistema de arquivos. • O sistema de arquivos não está disponível. • O sistema de arquivos falhou e o Amazon FSx não consegue recuperá-lo. • O Amazon FSx não consegue criar backups.

Clientes, métodos de acesso e ambientes compatíveis com o Amazon FSx para Windows File Server

Você pode acessar seus sistemas de arquivos do Amazon FSx usando uma variedade de clientes e métodos compatíveis, tanto de ambientes da AWS quanto on-premises.

Tópicos

Clientes compatíveis

O Amazon FSx é compatível com a conexão ao seu sistema de arquivos de uma ampla variedade de instâncias de computação e sistemas operacionais. Ele é compatível com o acesso por meio do protocolo Server Message Block (SMB), versões 2.0 a 3.1.1.

As seguintes instâncias de computação da AWS são compatíveis para uso com o Amazon FSx:

- Instâncias do Amazon Elastic Compute Cloud (Amazon EC2), incluindo instâncias do Microsoft Windows, Mac, Amazon Linux e Amazon Linux 2. Para obter mais informações, consulte Como acessar compartilhamentos de arquivos.
- Contêineres do Amazon Elastic Container Service (Amazon ECS). Para obter mais informações, consulte Volumes do FSx para Windows File Server no Guia do desenvolvedor do Amazon Elastic Container Service.
- Instâncias do WorkSpaces: para saber mais, consulte a postagem do blog da AWS Using FSx para Windows File Server with Amazon WorkSpaces.
- Instâncias do Amazon AppStream 2.0: para saber mais, consulte a postagem do blog da AWS Using Amazon FSx with Amazon AppStream 2.0.
- VMs em execução em ambientes do VMware Cloud na AWS: para saber mais, consulte a postagem do blog da AWS Storing and Sharing Files with FSx para Windows File Server in a VMware Cloud on AWS Environment.

Os seguintes sistemas operacionais são compatíveis para uso com o Amazon FSx:

- Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 e Windows Server 2022.
- Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 (incluindo as experiências de desktop do WorkSpaces no Windows 7 e no Windows 10) e Windows 11.
- Linux, usando a ferramenta `cifs-utils`.
- macOS

Métodos de acesso compatíveis

Você pode usar os seguintes métodos e abordagens de acesso com o Amazon FSx:

Como acessar sistemas de arquivos usando seus nomes DNS padrão

O FSx para Windows File Server fornece um nome do Sistema de Nomes de Domínio (DNS) para cada sistema de arquivos. Você acessa seu sistema de arquivos do FSx para Windows File Server ao mapear uma letra de drive em sua instância de computação para o compartilhamento de arquivos do Amazon FSx usando esse nome DNS. Para saber mais, consulte Como usar compartilhamentos de arquivos do Microsoft Windows.

> **Important**
>
> O Amazon FSx somente grava registros DNS para um sistema de arquivos se você estiver usando o DNS da Microsoft como DNS padrão. Caso esteja usando um DNS de terceiros, você deverá configurar manualmente as entradas de DNS para seus sistemas de arquivos do Amazon FSx. Para obter informações sobre como escolher os endereços IP corretos a serem usados para o sistema de arquivos, consulte Como obter os endereços IP corretos do sistema de arquivos para usar no DNS.

Para localizar o nome DNS:

- No console do Amazon FSx, escolha Sistemas de arquivos e, em seguida, Detalhes. Visualize o nome DNS na seção Rede e segurança.
- Ou visualize-o na resposta do comando da API CreateFileSystem ou DescribeFileSystems.

Para todos os sistemas de arquivos single-AZ associados a um AWS Managed Microsoft Active Directory, o nome DNS é semelhante ao seguinte: `fs-0123456789abcdef0.`*`ad-dns-domain-name`*

Para todos os sistemas de arquivos single-AZ unidos a um Active Directory autogerenciado e para qualquer sistema de arquivos multi-AZ, o nome DNS é semelhante ao seguinte: `amznfsxaa11bb22.`*`ad-domain`*`.com`

Como usar nomes DNS com autenticação do Kerberos

Recomendamos que você use autenticação e criptografia baseadas no Kerberos em trânsito com o Amazon FSx. O Kerberos oferece a autenticação mais segura para clientes que acessam o sistema de arquivos. Para ativar a autenticação baseada no Kerberos e a criptografia de dados em trânsito para suas sessões SMB, use o nome DNS do sistema de arquivos fornecido pelo Amazon FSx para acessar o sistema de arquivos.

Se você tiver uma confiança externa configurada entre o AWSManaged Microsoft Active Directory e o Active Directory on-premises para usar o PowerShell remoto do Amazon FSx com autenticação do Kerberos, será necessário configurar uma política de grupo local no cliente para a ordem de pesquisa na floresta. Para obter mais informações, consulte Configurar o Kerberos Forest Search Order (KFSO) na documentação da Microsoft.

Como acessar sistemas de arquivos usando aliases de DNS

O FSx para Windows File Server fornece um nome DNS para cada sistema de arquivos que você pode usar para acessar seus compartilhamentos de arquivos. Você também pode habilitar o acesso ao Amazon FSx de nomes DNS diferentes do nome DNS padrão que o Amazon FSx cria, registrando aliases para os sistemas de arquivos do FSx para Windows File Server.

Com o uso de aliases de DNS, é possível mover os dados de compartilhamento de arquivos do Windows para o Amazon FSx e continuar usando os nomes DNS existentes para acessar os dados no Amazon FSx. Os aliases de DNS também permitem o uso de nomes significativos que facilitam a administração de ferramentas e aplicações para conexão com os sistemas de arquivos do Amazon FSx. Para obter mais informações, consulte Como gerenciar aliases de DNS.

Como usar aliases de DNS com autenticação Kerberos

Recomendamos que você use autenticação e criptografia baseadas no Kerberos em trânsito com o Amazon FSx. O Kerberos oferece a autenticação mais segura para clientes que acessam o sistema de arquivos. Para ativar a autenticação do Kerberos para clientes que acessam o Amazon FSx

usando um alias de DNS, você deve adicionar nomes das entidades principais de serviço (SPNs) que correspondam ao alias de DNS no objeto de computador do Active Directory do sistema de arquivos do Amazon FSx.

Opcionalmente, você pode impor que os clientes que acessam o sistema de arquivos usando um alias de DNS usem a autenticação e a criptografia do Kerberos configurando os seguintes Objetos de Política de Grupo (GPOs) em seu Active Directory:

- Restringir NTLM: tráfego NTLM de saída para servidores remotos: use essa configuração de política para negar ou auditar o tráfego NTLM de saída de um computador para qualquer servidor remoto que esteja executando o sistema operacional Windows.
- Restringir NTLM: adicionar exceções de servidor remoto para autenticação NTLM: use essa configuração de política para criar uma lista de exceções de servidores remotos para os quais os dispositivos clientes têm permissão de usar a autenticação NTLM se a configuração de política Segurança de rede: restringir NTLM: tráfego NTLM de saída para servidores remotos estiver configurada.

Para obter mais informações, consulte Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos.

Como trabalhar com sistemas de arquivos do FSx para Windows File Server e namespaces do DFS

O FSx para Windows File Server é compatível com o uso de namespaces do Sistema de Arquivos Distribuído (DFS) da Microsoft. Você pode usar os namespaces do DFS para organizar os compartilhamentos de arquivos em vários sistemas de arquivos em uma estrutura de pastas comum (um namespace) que você usa para acessar todo o conjunto de dados dos arquivos. Você pode usar um nome no namespace do DFS para acessar o sistema de arquivos do Amazon FSx ao configurar o destino do link para ser o nome DNS do sistema de arquivos. Para obter mais informações, consulte Agrupar vários sistemas de arquivos com namespaces do DFS.

Ambientes compatíveis

Você pode acessar seu sistema de arquivos de recursos que estão na mesma VPC que seu sistema de arquivos. Para obter mais informações e instruções detalhadas, consulte Passo a passo 1: pré-requisitos para começar.

Você também pode acessar sistemas de arquivos criados após 22 de fevereiro de 2019 de recursos on-premises e de recursos que estão em outra VPC, conta da AWS ou região da AWS. A tabela a seguir ilustra os ambientes nos quais o Amazon FSx é compatível com o acesso de clientes em cada um dos ambientes compatíveis, dependendo de quando o sistema de arquivos foi criado.

Clientes localizados em…	Acesso a sistemas de arquivos criados antes de 22 de fevereiro de 2019	Acesso a sistemas de arquivos criados antes de 17 de dezembro de 2020	Acesso a sistemas de arquivos criados após 17 de dezembro de 2020
Sub-redes nas quais o sistema de arquivos é criado	✓	✓	✓
Blocos CIDR primários da VPC em que o sistema de arquivos foi criado	✓	✓	✓
CIDRs secundários da VPC na qual o sistema de arquivos foi criado		Clientes com endereços IP em um intervalo de endereços IP privados do RFC 1918: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Clientes com endereços IP fora do seguinte intervalo de blocos CIDR: 198.19.0.0/16
Outros CIDRs ou redes emparelhados			

> **Note**
>
> Em alguns casos, você pode querer acessar um sistema de arquivos que foi criado antes de 17 de dezembro de 2020 on-premises usando um intervalo de endereços IP não privado. Para fazer isso, crie um novo sistema de arquivos de um backup do sistema de arquivos. Para obter mais informações, consulte Trabalhar com backups.

A seguir, você encontrará informações sobre como acessar os sistemas de arquivos do FSx para Windows File Server on-premises e de diferentes VPCs, contas da AWS ou regiões da AWS.

Como acessar os sistemas de arquivos do FSx para Windows File Server on-premises

O FSx para Windows File Server é compatível com o uso do AWS Direct Connect ou AWS VPN para acessar seus sistemas de arquivos nas instâncias de computação on-premises. Compatível com o AWS Direct Connect, o FSx para Windows File Server permite que você acesse seu sistema de arquivos por meio de uma conexão de rede dedicada a partir do seu ambiente on-premises. Compatível com o AWS VPN, o FSx para Windows File Server permite que você acesse seu sistema de arquivos de dispositivos on-premises por meio de um túnel seguro e privado.

Depois de conectar seu ambiente on-premises à VPC associada ao seu sistema de arquivos do Amazon FSx, você pode acessar seu sistema de arquivos usando seu nome DNS ou um alias de DNS. Você faz isso da mesma forma que faz com as instâncias de computação dentro da VPC. Para obter mais informações em AWS Direct Connect, consulte o Guia do usuário AWS Direct Connect. Para obter mais informações sobre a configuração de conexões da AWS VPN, consulte Conexões VPN no Guia do usuário da Amazon VPC.

O FSx para Windows File Server também é compatível com o uso do Gateway de Arquivos do Amazon FSx para fornecer baixa latência e acesso contínuo aos compartilhamentos de arquivos do FSx para Windows File Server na nuvem nas suas instâncias de computação on-premises. Para obter mais informações, consulte o Guia do usuário do Gateway de Arquivos do Amazon FSx.

Como acessar os sistemas de arquivos do FSx para Windows File Server de outra VPC, conta ou Região da AWS

Você pode acessar seu sistema de arquivos do FSx para Windows File Server nas instâncias de computação em uma VPC, conta da AWS ou região da AWS diferente daquela associada ao seu

sistema de arquivos. Para fazer isso, você pode usar o emparelhamento da VPC ou gateways de trânsito. Quando você usa uma conexão de emparelhamento da VPC ou um gateway de trânsito para conectar VPCs, as instâncias de computação que estão em uma VPC podem acessar os sistemas de arquivos do Amazon FSx em outra VPC. Esse acesso é possível mesmo que as VPCs pertençam a contas diferentes e mesmo que as VPCs residam em regiões da AWS diferentes.

Uma conexão de emparelhamento da VPC é uma conexão de rede entre duas VPCs que você pode usar para rotear o tráfego entre elas usando endereços IPv4 ou IP versão 6 (IPv6) privados. Você pode usar o emparelhamento da VPC para conectar VPCs na mesma região da AWS ou entre 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.

Um gateway de trânsito é um hub de trânsito de rede que pode ser usado para interconectar as VPCs e as redes on-premises. Para obter mais informações sobre o uso de gateways de trânsito da VPC, consulte Conceitos básicos de gateways de trânsito nos Gateways de trânsito da Amazon VPC.

Depois de configurar uma conexão de emparelhamento da VPC ou de gateway de trânsito, você poderá acessar seu sistema de arquivos usando o nome DNS. Isso é feito da mesma forma que nas instâncias de computação dentro da VPC associada.

Disponibilidade e durabilidade: sistemas de arquivos single-AZ e multi-AZ

O Amazon FSx para Windows File Server oferece dois tipos de implantação de sistema de arquivos: single-AZ e multi-AZ. As seções a seguir fornecem informações para ajudá-lo a escolher o tipo de implantação certo para suas cargas de trabalho. Para obter informações sobre o SLA (Acordo de Nível de Serviço) de disponibilidade do serviço, consulte Amazon FSx Service Level Agreement.

Os sistemas de arquivos single-AZ são compostos por uma única instância do servidor de arquivos do Windows e um conjunto de volumes de armazenamento em uma única zona de disponibilidade (AZ). Com os sistemas de arquivos single-AZ, os dados são replicados automaticamente para protegê-los contra a falha de um único componente na maioria dos casos. O Amazon FSx monitora continuamente a existência de falhas de hardware e se recupera automaticamente de eventos de falha, substituindo o componente de infraestrutura com falha. Os sistemas de arquivos Single-AZ ficam off-line, normalmente por menos de 20 minutos, durante esses eventos de recuperação de falhas e durante a manutenção planejada do sistema de arquivos dentro da janela de manutenção que você configura para o seu sistema de arquivos. Com os sistemas de arquivos single-AZ, a falha do sistema de arquivos pode ser irrecuperável em casos raros, como devido a falhas de vários componentes ou devido a uma falha não progressiva do servidor de arquivos único que deixa o sistema de arquivos em um estado inconsistente. Nesse caso, é possível recuperar o sistema de arquivos a partir do backup mais recente.

Os sistemas de arquivos multi-AZ são compostos por um cluster de alta disponibilidade de servidores de arquivos do Windows espalhados por duas AZs (uma AZ preferencial e uma AZ em espera), aproveitando a tecnologia de cluster de failover do Windows Server (WSFC) e um conjunto de volumes de armazenamento em cada uma das duas AZs. Os dados são replicados de forma síncrona em cada AZ individual e entre as duas AZs. Em relação à implantação single-AZ, as implantações multi-AZ oferecem durabilidade aprimorada por meio da replicação adicional de dados entre AZs e disponibilidade aprimorada durante a manutenção planejada do sistema e a interrupção não planejada do serviço por meio de failover automático para a AZ em espera. Isso permite que você continue acessando seus dados e ajuda a protegê-los contra falhas de instância e interrupção da AZ.

Como escolher a implantação do sistema de arquivos single-AZ ou multi-AZ

Recomendamos o uso de sistemas de arquivos multi-AZ para a maioria das workloads de produção, dado o modelo de alta disponibilidade e durabilidade que ele oferece. A implantação do single-AZ foi projetada como uma solução econômica para workloads de teste e desenvolvimento, determinadas workloads de produção que têm replicação incorporada à camada de aplicações e não exigem redundância adicional no nível de armazenamento, além de workloads de produção que têm disponibilidade reduzida e necessidades de objetivo de ponto de recuperação (RPO). Cargas de trabalho com necessidades de disponibilidade relaxadas podem tolerar a perda temporária de disponibilidade por até 20 minutos no caso de manutenção planejada do sistema de arquivos ou interrupção não planejada do serviço, e cargas de trabalho com necessidades relaxadas de RPO podem tolerar, em casos raros, a perda de atualizações de dados desde o backup mais recente.

Suporte a recursos por tipo de implantação

A tabela a seguir resume os recursos compatíveis com os tipos de implantação do sistema de arquivos do FSx para Windows File Server.

Tipo de implantação	Armazenamento em SSD	Armazenamento em HDD	Namespaces DFS	Replicação do DFS	Nomes DNS personalizados	Compartilhamentos CA
Single-AZ 1	✓		✓	✓	✓	
Single-AZ 2	✓	✓	✓		✓	✓*
Multi-AZ	✓	✓	✓		✓	✓*

> **Note**
>
> * Embora seja possível criar compartilhamentos continuamente disponíveis (CA) em sistemas de arquivos single-AZ 2, você deve usar compartilhamentos CA em sistemas de arquivos multi-AZ para implantações de HA do SQL Server.

Processo de failover para o FSx para Windows File Server

Os sistemas de arquivos multi-AZ fazem failover automaticamente do servidor de arquivos preferencial para o servidor de arquivos em espera se ocorrer alguma das seguintes condições:

- Ocorre uma interrupção na zona de disponibilidade.
- O servidor de arquivos preferencial fica indisponível.
- O servidor de arquivos preferencial passa por manutenção planejada.

Ao fazer o failover de um servidor de arquivos para outro, o novo servidor de arquivos ativo começa automaticamente a atender a todas as solicitações de leitura e gravação do sistema de arquivos. Quando os recursos na sub-rede preferencial estão disponíveis, o Amazon FSx automaticamente retorna ao servidor de arquivos preferencial na sub-rede preferencial. Normalmente, um failover é concluído em menos de 30 segundos, desde a detecção da falha no servidor de arquivos ativo até a promoção do servidor de arquivos em espera para o status ativo. O failback para a configuração original do multi-AZ também é concluído em menos de 30 segundos e só ocorre quando o servidor de arquivos na sub-rede preferencial é totalmente recuperado.

Durante o breve período em que seu sistema de arquivos está falhando e retornando, a E/S pode ser pausada e as métricas da CloudWatch Amazon podem ficar temporariamente indisponíveis.

Para sistemas de arquivos multi-AZ, se houver tráfego contínuo durante o failover e o failback, todas as alterações de dados feitas durante esse período precisarão ser sincronizadas entre os servidores de arquivos. Esse processo pode levar até várias horas para workloads com alto índice de gravação e IOPS. Recomendamos testar o impacto dos failovers em sua aplicação enquanto o sistema de arquivos estiver sob uma carga mais leve.

Experiência de failover em clientes Windows

Ao fazer o failover de um servidor de arquivos para outro, o novo servidor de arquivos ativo começa automaticamente a atender a todas as solicitações de leitura e gravação do sistema de arquivos.

Depois que os recursos na sub-rede preferencial estiverem disponíveis, o Amazon FSx passa por failback automaticamente ao servidor de arquivos preferencial na sub-rede preferencial. Como o nome DNS do sistema de arquivos permanece o mesmo, os failovers são transparentes para as aplicações do Windows, que retomam as operações do sistema de arquivos sem intervenção manual. Normalmente, um failover é concluído em menos de 30 segundos, desde a detecção da falha no servidor de arquivos ativo até a promoção do servidor de arquivos em espera para o status ativo. O failback para a configuração original do multi-AZ também é concluído em menos de 30 segundos e só ocorre depois que o servidor de arquivos na sub-rede preferencial é totalmente recuperado.

Experiência de failover em clientes Linux

Os clientes Linux não são compatíveis com failover automático baseado em DNS. Portanto, eles não se conectam automaticamente ao servidor de arquivos em espera durante um failover. Eles retomarão automaticamente as operações do sistema de arquivos depois que o sistema de arquivos multi-AZ falhar e voltar para o servidor de arquivos na sub-rede preferencial.

Como testar o failover em um sistema de arquivos

Você pode testar o failover do seu sistema de arquivos multi-AZ modificando sua capacidade de throughput. Quando você modifica a capacidade de throughput do seu sistema de arquivos, o Amazon FSx alterna o servidor de arquivos do sistema de arquivos. Os sistemas de arquivos multi-AZ fazem failover automaticamente para o servidor secundário, enquanto o Amazon FSx substitui primeiro o servidor de arquivos do servidor preferencial. Em seguida, o sistema de arquivos volta automaticamente 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. Após a conclusão bem-sucedida da atualização, o sistema de arquivos passou por failover para o servidor secundário e passou por failover de volta ao servidor primário. 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.

Como trabalhar com recursos do sistema de arquivos single e multi-AZ

Subredes

Quando você cria uma VPC, ela abrange todas as zonas de disponibilidade (AZs) da região. As zonas de disponibilidade são locais distintos projetados para serem isolados de falhas em outras zonas de disponibilidade. Depois de criar uma VPC, você pode adicionar uma ou mais sub-redes em cada zona de disponibilidade. A VPC padrão possui uma sub-rede em cada zona de disponibilidade. Cada sub-rede deve residir inteiramente dentro de uma zona de disponibilidade e não pode abranger zonas. Ao criar um sistema de arquivos single-AZ do Amazon FSx, 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 que você escolher devem estar em zonas de disponibilidade diferentes na mesma AWS região.

Para AWS aplicativos internos, recomendamos que você inicie seus clientes na mesma zona de disponibilidade do servidor de arquivos de sua preferência para minimizar a latência.

Interfaces de rede elástica do sistema de arquivos

Quando você cria um sistema de arquivos do Amazon FSx, o Amazon FSx provisiona uma ou mais interfaces de rede elástica na nuvem privada virtual (VPC) da Amazon que você associa ao seu sistema de arquivos. A interface de rede permite que seu cliente se comunique com o sistema de arquivos do FSx para Windows File Server. A interface de rede é considerada como estando dentro do escopo de serviço do Amazon FSx, apesar de fazer parte da VPC de sua conta. Os sistemas de arquivos multi-AZ têm duas interfaces de rede elástica, uma para cada servidor de arquivos. Os sistemas de arquivos single-AZ têm uma interface de rede elástica.

> **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.

A tabela a seguir resume a sub-rede, a interface de rede elástica e os recursos de endereço IP para os tipos de implantação do sistema de arquivos do FSx para Windows File Server.

Tipo de implantação do sistema de arquivos	Número de sub-redes	Número de interfaces de rede elástica	Número de endereços IP
Single-AZ 2	1	1	2
Single-AZ 1	1	1	1
Multi-AZ	2	2	4

Depois que um sistema de arquivos é criado, seus 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 do sistema de arquivos à Internet pública. Se um endereço IP elástico, que é um endereço IP público acessível pela Internet, for anexado à interface de rede elástica de um sistema de arquivos, o Amazon FSx o desconectará automaticamente.

Como otimizar os custos com o Amazon FSx

O FSx para Windows File Server oferece vários recursos que ajudam você a otimizar o custo total de propriedade (TCO) com base nas necessidades da sua aplicação. Você pode escolher o tipo de armazenamento (HDD ou SSD) para obter o equilíbrio certo entre as necessidades de custo e performance da sua aplicação. Você tem a flexibilidade de escolher a capacidade de throughput separadamente da quantidade de capacidade de armazenamento para otimizar seus custos. Além disso, você pode usar a eliminação de duplicação dos dados para otimizar os custos de armazenamento, eliminando dados redundantes em seu sistema de arquivos.

Tópicos

Flexibilidade para escolher o armazenamento e o throughput de forma independente

Com o FSx para Windows File Server, você pode configurar as capacidades de armazenamento, IOPS de SSD e throughput do seu sistema de arquivos de forma independente. Isso lhe dá flexibilidade para obter a combinação certa de custo e performance. Por exemplo, você pode optar por ter uma grande quantidade de armazenamento com uma quantidade relativamente pequena de capacidade de throughput para workloads frios (geralmente inativos) para economizar em custos de throughput desnecessários. Ou, como outro exemplo, você poderia optar por ter uma grande quantidade de capacidade de throughput por uma quantidade relativamente pequena de capacidade de armazenamento. A capacidade de throughput mais alta vem com quantidades maiores de memória para armazenamento em cache no servidor de arquivos. Você pode aproveitar o cache rápido no servidor de arquivos para otimizar a performance dos dados acessados ativamente. Para obter mais informações, consulte Performance do FSx para Windows File Server.

Você pode aumentar a quantidade de capacidade de armazenamento a qualquer momento após criar um sistema de arquivos. Para obter mais informações, consulte Como gerenciar a capacidade de armazenamento. Você pode escalar a IOPS do SSD independentemente da capacidade de armazenamento a qualquer momento depois de criar um sistema de arquivos. Para obter mais informações, consulte Como gerenciar IOPS de SSD. Você pode aumentar ou diminuir a quantidade

de capacidade de throughput a qualquer momento, proporcionando a flexibilidade necessária para atender às necessidades de performance em constante mudança. Para obter mais informações, consulte Como gerenciar a capacidade de throughput.

Otimizar custos do armazenamento

Você pode otimizar seus custos de armazenamento com o Amazon FSx de várias maneiras, descritas a seguir.

Como otimizar os custos usando tipos de armazenamento

O FSx para Windows File Server oferece dois tipos de armazenamento: unidades de disco rígido (HDD) e unidades de estado sólido (SSD), para que você possa otimizar o custo/performance e atender às suas necessidades de workload. O armazenamento em HDD foi projetado para um amplo espectro de workloads, incluindo diretórios pessoais, compartilhamentos de usuários e departamentos e sistemas de gerenciamento de conteúdo. O armazenamento SSD foi projetado para as workloads de mais alta performance e mais sensíveis à latência, incluindo bancos de dados, workloads de processamento de mídia e aplicações de análise de dados. Para obter mais informações, consulte Latência e os Preços do Amazon FSx para Windows File Server.

Como otimizar os custos de armazenamento usando a eliminação de duplicação dos dados

Conjuntos de dados grandes geralmente têm dados redundantes, o que aumenta os custos de armazenamento de dados. Por exemplo, os compartilhamentos de arquivos do usuário podem ter várias cópias do mesmo arquivo, armazenadas por vários usuários. Os compartilhamentos de desenvolvimento de software podem conter muitos binários que permanecem inalterados de uma compilação para outra. Você pode reduzir seus custos de armazenamento de dados ativando a eliminação de duplicação dos dados no sistema de arquivos. Quando ativada, a eliminação de duplicação dos dados reduz ou elimina automaticamente os dados redundantes, armazenando as partes duplicadas do conjunto de dados apenas uma vez. Para obter mais informações sobre a eliminação de duplicação dos dados e como ativá-la facilmente em seu sistema de arquivos do Amazon FSx, consulte Eliminação de duplicação de dados.

Como analisar o uso e o faturamento

Você pode analisar o uso do sistema de arquivos, incluindo a capacidade de armazenamento, a capacidade de throughput, o backup e a transferência de dados, usando o painel do AWS Billing ou

o AWS Cost Explorer. Essas ferramentas permitem que você analise o uso de seus recursos e filtre e agrupe por tipo de uso, região e outros critérios relevantes. Observe que, para visualizar o uso de um sistema de arquivos único ou de um backup de sistema de arquivos único, você precisará ativar as tags para esse recurso específico e ativar o relatório de faturamento baseado em tags. Para obter mais informações, consulte Uso de tags de alocação de custos da AWS no guia do usuário do AWS Billing.

Trabalhar com o Microsoft Active Directory no FSx para Windows File Server

O Amazon FSx trabalha com o Microsoft Active Directory para se integrar aos seus ambientes Microsoft Windows existentes. O Active Directory é o serviço de diretório da Microsoft usado para armazenar informações sobre objetos na rede e facilitar a localização e o uso dessas informações por administradores e usuários. Esses objetos geralmente incluem recursos compartilhados, como servidores de arquivos e contas de usuários e computadores da rede.

Ao criar um sistema de arquivos com o Amazon FSx, você o associa ao seu domínio do Active Directory para fornecer autenticação de usuário e controle de acesso em nível de arquivo e pasta. Seus usuários podem então usar suas identidades de usuário existentes no Active Directory para se autenticar e acessar o sistema de arquivos do Amazon FSx. Os usuários também podem usar suas identidades existentes para controlar o acesso a arquivos e pastas individuais. Além disso, você pode migrar seus arquivos e pastas existentes e a configuração da lista de controle de acesso (ACL) desses itens para o Amazon FSx sem nenhuma modificação.

O Amazon FSx oferece duas opções para usar seu sistema de arquivos do FSx para Windows File Server com o Active Directory: Usando o Amazon FSx com AWS Directory Service for Microsoft Active Directory e Como usar o Amazon FSx com seu Microsoft Active Directory autogerenciado.

> **Note**
>
> O Amazon FSx oferece suporte ao Serviços de domínio do Microsoft Azure Active Directory que você pode associar a um Microsoft Azure Active Directory.

Depois de criar uma configuração associada do Active Directory para um sistema de arquivos, você pode atualizar somente as seguintes propriedades:

- Credenciais do usuário de serviço
- Endereços IP do servidor DNS

Você não pode alterar as seguintes propriedades do Microsoft AD associado depois de criar o sistema de arquivos:

- DomainName

- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

No entanto, você pode criar um novo sistema de arquivos a partir de um backup e alterar essas propriedades na configuração de integração do Microsoft Active Directory para o novo sistema de arquivos. Para ter mais informações, consulte Passo a passo 2: criar um sistema de arquivos de um backup.

> **Note**
>
> O Amazon FSx não oferece suporte ao Active Directory Connector e ao Simple Active Directory.

Seu FSx para Windows File Server pode ficar mal configurado, se houver uma alteração na configuração do Active Directory que interrompa a conexão com seu sistema de arquivos. Para retornar seu sistema de arquivos ao estado Disponível, selecione o botão Tentativa de recuperação no console do Amazon FSx ou use o comando `StartMisconfiguredStateRecovery` na API ou no console do Amazon FSx. Para obter mais informações, consulte O sistema de arquivos está em um estado de configuração incorreta.

Tópicos

- Usando o Amazon FSx com AWS Directory Service for Microsoft Active Directory
- Como usar o Amazon FSx com seu Microsoft Active Directory autogerenciado

Usando o Amazon FSx com AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) fornece diretórios reais do Active Directory totalmente gerenciados e altamente disponíveis na nuvem. Você pode usar esses diretórios do Active Directory em sua implantação de carga de trabalho.

Se sua organização estiver usando AWS Managed Microsoft AD para gerenciar identidades e dispositivos, recomendamos que você integre seu sistema de arquivos Amazon FSx com o. AWS Managed Microsoft AD Ao fazer isso, você obtém uma solução pronta para uso usando o Amazon AWS Managed Microsoft AD FSx com. AWS lida com a implantação, operação, alta disponibilidade,

confiabilidade, segurança e integração perfeita dos dois serviços, permitindo que você se concentre em operar sua própria carga de trabalho de forma eficaz.

Para usar o Amazon FSx com sua AWS Managed Microsoft AD configuração, você pode usar o console do Amazon FSx. Ao criar um novo sistema de arquivos FSx for Windows File Server no console, AWS escolha Managed Active Directory na seção Autenticação do Windows. Você também escolhe o diretório específico que deseja usar. Para ter mais informações, consulte Crie seu sistema de arquivos.

Sua organização pode gerenciar identidades e dispositivos em um domínio do Active Directory autogerenciado (on-premises ou na nuvem). Nesse caso, você pode unir seu sistema de arquivos Amazon FSx diretamente ao seu domínio existente e autogerenciado do Active Directory. Para ter mais informações, consulte Como usar o Amazon FSx com seu Microsoft Active Directory autogerenciado.

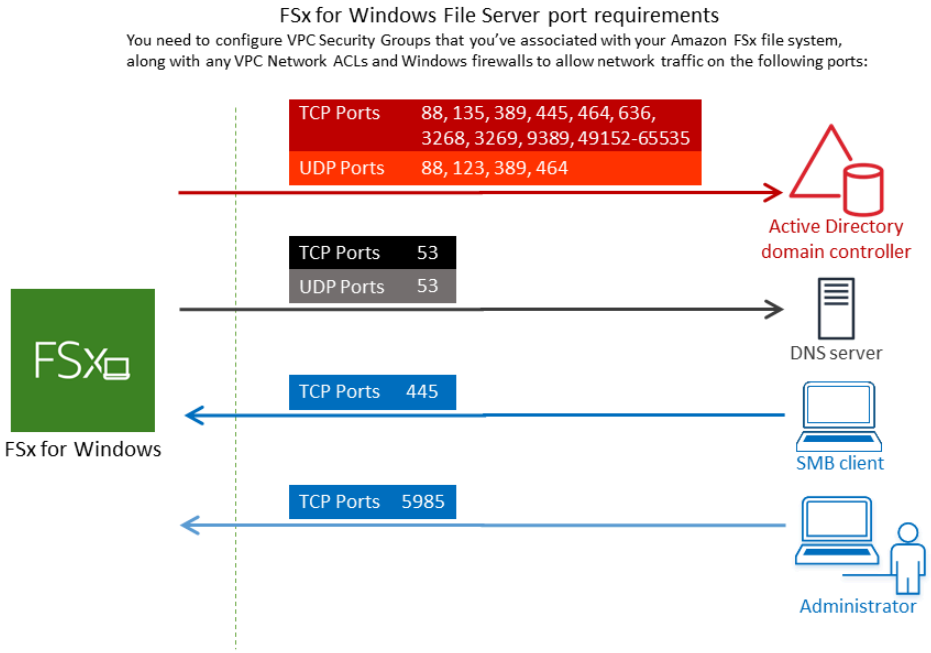
Além disso, você também pode configurar seu sistema para se beneficiar de um modelo de isolamento de floresta de recursos. Nesse modelo, você isola seus recursos, incluindo seus sistemas de arquivos Amazon FSx, em uma floresta separada do Active Directory daquela em que seus usuários estão.

> **Important**
>
> Para sistemas de arquivos single-AZ 2 e todos os sistemas de arquivos multi-AZ, o nome de domínio do Active Directory não pode exceder 47 caracteres.

Pré-requisitos de rede

Antes de criar um sistema de arquivos FSx for Windows File Server associado ao seu domínio AWS Microsoft Managed Active Directory, verifique se você criou e configurou as seguintes configurações de rede:

- Em Grupos de segurança da VPC, o grupo de segurança padrão para a Amazon VPC padrão já está adicionado ao sistema de arquivos no console. Certifique-se de que o grupo de segurança e as ACLs de rede da VPC para as sub-redes nas quais você vai criar seu sistema de arquivos do FSx permite tráfego nas portas e nas direções mostradas no diagrama a seguir.



A tabela a seguir identifica o perfil de cada porta.

Protocolo	Portas	Funçã
TCP/UDP	53	Doma Name Syste (DNS)
TCP/UDP	88	Auten ção de Kerbe
TCP/UDP	464	Altera d efinir senha

Protocolo	Portas	Funçã
TCP/UDP	389	Lightw ht Direct Acces Protoc (LDAP
UDP	123	Netwo Time Protoc (NTP)
TCP	135	Distrib ed Comp Enviro nt/ End Point Mappe (DCE/ EPMA P)
TCP	445	Comp hamer de arquiv de SMB para serviç de diretó

Protocolo	Portas	Funçã
TCP	636	Lightw ht Direct Acces Protoc over TLS/ SSL (LDAP
TCP	3268	Catálo global da Micros
TCP	3269	Catálo global da Micros sobre SSL
TCP	5985	WinRI 2.0 (Gere mento Remo do Micros Windo

Protocolo	Portas	Funçã
TCP	9389	Serviç Web do Micros AD DS, Power
TCP	49152 – 65535	Portas efême para RPC

> **Important**
>
> É necessário permitir o tráfego de saída na porta TCP 9389 para implantações de sistemas de arquivos single-AZ 2 e todas as implantações de sistemas de arquivos multi-AZ.

> **Note**
>
> Se estiver usando ACLs de rede de VPC, você também deverá permitir tráfego de saída em portas dinâmicas (49152-65535) do sistema de arquivos do FSx.

- Se você estiver conectando seu sistema de arquivos Amazon FSx a um AWS Microsoft Active Directory gerenciado em uma VPC ou conta diferente, garanta a conectividade entre essa VPC e a Amazon VPC onde você deseja criar o sistema de arquivos. Para ter mais informações, consulte Usando o Amazon FSx AWS Managed Microsoft AD em uma VPC ou conta diferente.

> **Important**
>
> Embora os grupos de segurança da Amazon VPC exijam que as portas sejam abertas somente na direção em que o tráfego de rede é iniciado, as ACLs da rede VPC exigem que as portas sejam abertas nas duas direções.

Use a ferramenta de validação de rede do Amazon FSx para validar a conectividade com seus controladores de domínio do Active Directory.

Como usar um modelo de isolamento de floresta de recursos

Você associa seu sistema de arquivos a uma configuração do AWS Managed Microsoft AD . Em seguida, você estabelece uma relação unidirecional de confiança florestal entre um AWS Managed Microsoft AD domínio criado por você e seu domínio autogerenciado existente do Active Directory. Para a autenticação do Windows no Amazon FSx, você só precisa de uma relação de confiança direcional unidirecional na floresta, na qual a floresta AWS gerenciada confia na floresta de domínio corporativo.

Seu domínio corporativo assume o papel de domínio confiável, e o domínio AWS Directory Service gerenciado assume o papel de domínio confiável. As solicitações de autenticação validadas percorrem os domínios em apenas uma direção, permitindo que as contas em seu domínio corporativo se autentiquem em relação aos recursos compartilhados no domínio gerenciado. Nesse caso, o Amazon FSx interage somente com o domínio gerenciado. O domínio gerenciado então passa as solicitações de autenticação para seu domínio corporativo.

Testar sua configuração do Active Directory

Antes de criar seu sistema de arquivos do Amazon FSx, recomendamos que você valide a conectividade com seus controladores de domínio do Active Directory usando a ferramenta de validação de rede do Amazon FSx. Para ter mais informações, consulte Como validar a conectividade com seus controladores de domínio do Active Directory.

Os seguintes recursos relacionados podem ajudá-lo a usar o AWS Directory Service for Microsoft Active Directory FSx for Windows File Server:

- O que é AWS Directory Service no Guia de AWS Directory Service Administração
- Crie seu Active Directory AWS gerenciado no Guia de AWS Directory Service Administração

- Quando criar uma relação de confiança no Guia de administração do AWS Directory Service
- Passo a passo 1: pré-requisitos para começar

Usando o Amazon FSx AWS Managed Microsoft AD em uma VPC ou conta diferente

Você pode unir seu sistema de arquivos FSx for Windows File Server a AWS Managed Microsoft AD um diretório que esteja em uma VPC diferente dentro da mesma conta usando o emparelhamento de VPC. Você também pode unir seu sistema de arquivos a um AWS Managed Microsoft AD diretório que esteja em uma AWS conta diferente usando o compartilhamento de diretórios.

> **Note**
>
> Você só pode selecionar um AWS Managed Microsoft AD dentro do Região da AWS mesmo sistema de arquivos. Se você quiser usar uma configuração de emparelhamento de VPC entre regiões, use um Microsoft Active Directory autogerenciado. Para ter mais informações, consulte Como usar o Amazon FSx com seu Microsoft Active Directory autogerenciado.

O fluxo de trabalho para unir seu sistema de arquivos a um AWS Managed Microsoft AD que está em uma VPC diferente envolve as seguintes etapas:

1. Configurar o ambiente de rede.
2. Compartilhar seu diretório.
3. Associe seu sistema de arquivos ao diretório compartilhado.

Para obter mais informações, consulte Compartilhar seu diretório no Guia de administração do AWS Directory Service .

Para configurar seu ambiente de rede, você pode usar AWS Transit Gateway o Amazon VPC e criar uma conexão de emparelhamento de VPC. Além disso, certifique-se de que o tráfego de rede seja permitido entre as duas VPCs.

Um gateway de trânsito é um hub de trânsito de rede que pode ser usado para interconectar as VPCs e as redes on-premises. Para obter mais informações sobre como usar os gateways de trânsito da VPC, consulte Conceitos básicos de gateways de trânsito no Guia de gateways de trânsito da Amazon VPC.

Uma conexão de emparelhamento de VPC é uma conexão de rede entre duas VPCs. Esta conexão permite rotear o tráfego entre eles usando endereços privados do protocolo da internet, versão 4 (IPv4) ou protocolo da internet, versão 6 (IPv6). Você pode usar o emparelhamento de VPC para conectar VPCs dentro da mesma AWS região ou entre regiões. AWS Para mais informações sobre emparelhamento de VPC, consulte O que é emparelhamento de VPC? no Guia de emparelhamento da Amazon VPC.

Há outro pré-requisito quando você associa seu sistema de arquivos a um AWS Managed Microsoft AD diretório em uma conta diferente daquela do seu sistema de arquivos. Você também precisa compartilhar seu Microsoft Active Directory com a outra conta. Para fazer isso, você pode usar o recurso de compartilhamento de diretórios AWS gerenciado do Microsoft Active Directory. Para saber mais, consulte Compartilhar seu diretório no Guia de administração do AWS Directory Service .

Como validar a conectividade com seus controladores de domínio do Active Directory

Antes de criar um sistema de arquivos do FSx para Windows File Server associado ao seu Active Directory, use a ferramenta Active Directory Validation do Amazon FSx para validar a conectividade com seu domínio do Active Directory. Você pode usar esse teste se estiver usando o FSx for Windows File Server AWS com Microsoft Active Directory gerenciado ou com uma configuração autogerenciada do Active Directory. O teste de conectividade de rede do controlador de domínio (Test-FSxADControllerConnection) não executa o conjunto completo de verificações de conectividade de rede em cada controlador de domínio no domínio. Em vez disso, use esse teste para executar a validação da conectividade de rede em um conjunto específico de controladores de domínio.

Validar a conectividade com seus controladores de domínio do Active Directory

1. Execute uma instância do Windows do Amazon EC2 na mesma sub-rede e com os mesmos grupos de segurança da Amazon VPC que você usará para seu sistema de arquivos do FSx para Windows File Server. Para tipos de implantação multi-AZ, use a sub-rede para o servidor de arquivos ativo preferencial.
2. Associe sua instância do EC2 do Windows ao seu Active Directory. Para obter mais informações, consulte Manually Join a Windows Instance no Guia de administração do AWS Directory Service .
3. Conecte-se à sua instância do EC2. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.

4. Abra uma PowerShell janela do Windows (usando Executar como administrador) na instância do EC2.

   Para testar se o módulo necessário do Active Directory para Windows PowerShell está instalado, use o comando de teste a seguir.

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   Se a mensagem acima retornar um erro, instale-o usando o comando a seguir.

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```

5. Baixe a ferramenta de validação de rede usando o comando a seguir.

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

6. Faça download do arquivo zip usando o comando a seguir.

   ```
   PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
   ```

7. Adicionar o módulo AmazonFSxADValidation à sessão atual.

   ```
   PS C:\> Import-Module .\AmazonFSxADValidation
   ```

8. Defina o valor para o endereço IP do controlador de domínio do Active Directory e execute o teste de conectividade usando os seguintes comandos:

   ```
   $ADControllerIp = '10.0.75.243'
   $Result = Test-FSxADControllerConnection -ADControllerIp $ADControllerIp
   ```

9. O exemplo a seguir demonstra a recuperação da saída do teste, com os resultados de um teste de conectividade bem-sucedido.

   ```
   PS C:\AmazonFSxADValidation> $Result

   Name                           Value
   ----                           -----
   ```

```
TcpDetails                      {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                          10.0.75.243
UdpDetails                      {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                         True


PS C:\AmazonFSxADValidation> $Result.TcpDetails

Port Result    Description
---- ------    -----------
  88 Listening Kerberos authentication
 135 Listening DCE / EPMAP (End Point Mapper)
 389 Listening Lightweight Directory Access Protocol (LDAP)
 445 Listening Directory Services SMB file sharing
 464 Listening Kerberos Change/Set password
 636 Listening Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
3268 Listening Microsoft Global Catalog
3269 Listening Microsoft Global Catalog over SSL
9389 Listening Microsoft AD DS Web Services, PowerShell
```

O exemplo a seguir mostra a execução do teste e a obtenção de um resultado com falha.

```
PS C:\AmazonFSxADValidation> $Result = Test-FSxADControllerConnection -
ADControllerIp $ADControllerIp
WARNING: TCP 9389 failed to connect. Required for Microsoft AD DS Web Services,
 PowerShell.
Verify security group and firewall settings on both client and directory
 controller.
WARNING: 1 ports failed to connect to 10.0.75.243. Check pre-requisites in
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html#self-
manage-prereqs

PS C:\AmazonFSxADValidation> $Result

Name                            Value
----                            -----
TcpDetails                      {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                          10.0.75.243
UdpDetails                      {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
```

```
Success                         False
FailedTcpPorts                  {9389}


PS C:\AmazonFSxADValidation> $Result.FailedTcpPorts
9389
```

```
Windows socket error code mapping

https://msdn.microsoft.com/en-us/library/ms740668.aspx
```

Como usar o Amazon FSx com seu Microsoft Active Directory autogerenciado

Se a sua organização gerencia identidades e dispositivos em um Active Directory autogerenciado on-premises ou na nuvem, você pode associar o sistema de arquivos do Amazon FSx diretamente ao domínio do Active Directory autogerenciado existente. Para usar o Amazon FSx com AWS Managed Microsoft AD, você pode usar o console do Amazon FSx. Ao criar um novo sistema de arquivos do FSx para Windows File Server no console, selecione Microsoft Active Directory autogerenciado em Autenticação do Windows. Forneça os seguintes detalhes para seu Active Directory autogerenciado:

- Um nome de domínio totalmente qualificado para seu diretório autogerenciado.

> **Note**
>
> O nome de domínio não deve estar no formato de domínio de rótulo único (SLD). Atualmente, o Amazon FSx não é compatível com domínios de SLD.

> **Note**
>
> Para sistemas de arquivos single-AZ 2 e multi-AZ, o nome de domínio do Active Directory não pode exceder 47 caracteres.

- Endereços IP do servidor DNS para seu domínio

Os endereços IP do servidor DNS, os endereços IP do controlador de domínio do Active Directory e a rede do cliente devem atender aos seguintes requisitos:

Para sistemas de arquivos criados antes de 17 de dezembro de 2020	Para sistemas de arquivos criados após 17 de dezembro de 2020
Os endereços IP devem estar em um intervalo de endereços IP privados do RFC 1918: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Os endereços IP podem estar em qualquer intervalo, exceto: • Endereços IP que entram em conflito com os endereços IP de propriedade da Amazon Web Services nessa AWS região. Para obter uma lista de endereços IP AWS próprios por região, consulte os intervalos de endereços AWS IP. • Endereços IP no seguinte intervalo de blocos CIDR: 198.19.0.0/16

> **Note**
>
> Seus controladores de domínio do Active Directory devem ser graváveis.

- Nome de usuário e senha de uma conta de serviço no seu domínio do Active Directory, para que o Amazon FSx use para unir o sistema de arquivos ao seu domínio do Active Directory
- (Opcional) A Unidade Organizacional (UO) em seu domínio na qual você deseja que seu sistema de arquivos seja associado
- (Opcional) O grupo de domínio ao qual você deseja delegar autoridade para executar ações administrativas no sistema de arquivos. Por exemplo, esse grupo de domínio pode gerenciar compartilhamentos de arquivos do Windows, gerenciar listas de controle de acesso (ACLs) na pasta raiz do sistema de arquivos, 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.

> **Note**
>
> O nome do grupo de domínio fornecido deve ser exclusivo no Active Directory. O FSx for Windows File Server não criará o grupo de domínio nas seguintes circunstâncias:
>
> - Se já existir um grupo com o nome que você especificar
> - Se você não especificar um nome e um grupo chamado “Administradores de domínio” já existir no seu Active Directory.

Para ter mais informações, consulte Associar um sistema de arquivos do Amazon FSx a um domínio do Microsoft Active Directory autogerenciado.

> **Important**
>
> O Amazon FSx só registra registros DNS para um sistema de arquivos se você estiver usando o Microsoft DNS como o serviço DNS padrão. Se estiver usando um DNS de terceiros, será necessário configurar manualmente as entradas de DNS para os sistemas de arquivos do Amazon FSx depois de criá-los.

Quando você associa o sistema de arquivos diretamente ao Active Directory autogerenciado, o FSx para Windows File Server reside na mesma floresta do Active Directory (o contêiner lógico superior 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).

> **Note**
>
> Você pode isolar seus recursos, incluindo os sistemas de arquivos do Amazon FSx, em uma floresta do Active Directory separada daquela em que residem seus usuários. Para fazer isso, associe seu sistema de arquivos a um Active Directory AWS gerenciado e estabeleça uma relação unidirecional de confiança florestal entre um Active Directory AWS gerenciado que você cria e seu Active Directory autogerenciado existente.

Tópicos

Pré-requisitos para usar um Microsoft Active Directory autogerenciado

Antes de criar um sistema de arquivos do Amazon FSx associado ao seu domínio autogerenciado do Microsoft Active Directory, examine os seguintes pré-requisitos:

Tópicos

Configurações on-premises

Certifique-se de que você tenha um Microsoft Active Directory on-premises ou outro Microsoft Active Directory autogerenciado ao qual possa associar o sistema de arquivos do Amazon FSx. Seu Active Directory on-premises deve ter a seguinte configuração:

- Seu controlador de domínio do Active Directory possui um nível funcional de domínio no Windows Server 2008 R2 ou superior.
- Os endereços IP do servidor DNS e os endereços IP do controlador de domínio do Active Directory são os seguintes, dependendo de quando o sistema de arquivos foi criado:

Para sistemas de arquivos criados antes de 17 de dezembro de 2020	Para sistemas de arquivos criados após 17 de dezembro de 2020
Os endereços IP devem estar em um intervalo de endereços IP privados do RFC 1918:	Os endereços IP podem estar em qualquer intervalo, exceto:

Para sistemas de arquivos criados antes de 17 de dezembro de 2020	Para sistemas de arquivos criados após 17 de dezembro de 2020
• 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	• Endereços IP que entram em conflito com os endereços IP de propriedade da Amazon Web Services nessa AWS região. Para obter uma lista de endereços IP AWS próprios por região, consulte os intervalos de endereços AWS IP. • Endereços IP no seguinte intervalo de blocos CIDR: 198.19.0.0/16

Se você precisar acessar um sistema de arquivos do FSx para Windows File Server que foi criado antes de 17 de dezembro de 2020 usando um intervalo de endereços IP não privado, você pode criar um novo sistema de arquivos restaurando um backup do sistema de arquivos. Para ter mais informações, consulte Trabalhar com backups.

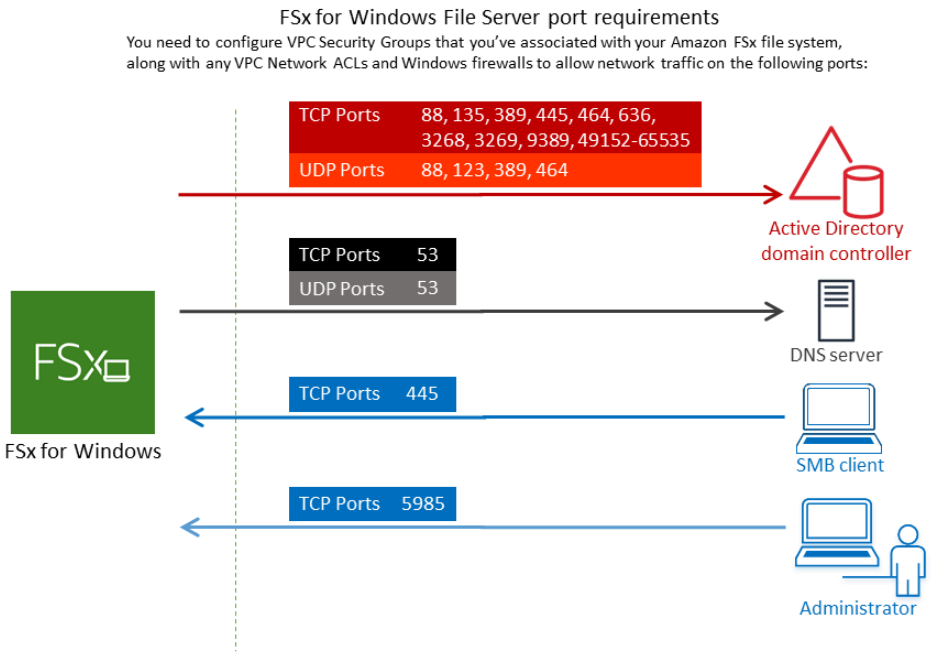
- Um nome de domínio que não está no formato de domínio de rótulo único (SLD). O Amazon FSx não é compatível com domínios de SLD.
- Para sistemas de arquivos single-AZ 2 e todos os sistemas de arquivos multi-AZ, o nome de domínio do Active Directory não pode exceder 47 caracteres.
- Se os sites do Active Directory estiverem definidos, as sub-redes da VPC associadas ao sistema de arquivos do Amazon FSx deverão ser definidas em um site do Active Directory e não deverão existir conflitos entre as sub-redes da VPC e as sub-redes dos outros sites.
- Talvez seja necessário adicionar regras ao seu firewall para permitir o tráfego ICMP entre seus controladores de domínio do Active Directory e o Amazon FSx.

Configurações de rede

Esta seção descreve as configurações de rede necessárias para unir um sistema de arquivos ao seu Active Directory autogerenciado.

Recomendamos que você use a ferramenta de validação Amazon FSx Active Directory para testar suas configurações de rede antes de tentar unir seu sistema de arquivos ao seu Active Directory autogerenciado.

- A conectividade deve ser configurada entre a Amazon VPC na qual você deseja criar o sistema de arquivos e o seu Active Directory autogerenciado. Você pode configurar essa conectividade usando AWS Direct Connect, AWS Virtual Private Network, VPC peering ou. AWS Transit Gateway
- Para grupos de segurança da VPC, o grupo de segurança padrão da sua Amazon VPC padrão deve ser adicionado ao seu sistema de arquivos no console. Certifique-se de que o grupo de segurança e as ACLs da rede da VPC para as sub-redes em que você criou o sistema de arquivos do FSx permitam o tráfego nas portas e nas direções mostradas no diagrama a seguir.



A tabela a seguir identifica o perfil de cada porta.

Protocolo	Portas	Função
TCP/UDP	53	Domain Name System (DNS)
TCP/UDP	88	Autenticação de Kerberos
TCP/UDP	464	Alterar/definir senha
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)

Protocolo	Portas	Função
UDP	123	Network Time Protocol (NTP)
TCP	135	Distributed Computing Environment/End Point Mapper (DCE/EPMAP)
TCP	445	Compartilhamento de arquivos de SMB para serviços de diretório
TCP	636	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
TCP	3268	Catálogo global da Microsoft
TCP	3269	Catálogo global da Microsoft sobre SSL
TCP	5985	WinRM 2.0 (Gerenciamento Remoto do Microsoft Windows)
TCP	9389	Serviços Web do Microsoft Active Directory DS, PowerShell
TCP	49152 – 65535	Portas efêmeras para RPC

Certifique-se de que essas regras de tráfego também sejam espelhadas nos firewalls que se aplicam a cada um dos controladores de domínio do Active Directory, servidores DNS, clientes do FSx e administradores do FSx.

> **Important**
>
> A permissão do tráfego de saída na porta TCP 9389 é necessária para implantações de sistemas de arquivos single-AZ 2 e multi-AZ.

> **Note**
>
> Se estiver usando ACLs de rede de VPC, você também deverá permitir tráfego de saída em portas dinâmicas (49152-65535) do sistema de arquivos do 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.

Permissões da conta de serviço

Certifique-se de ter uma conta de serviço em seu Microsoft Active Directory autogerenciado com permissões delegadas para associar computadores ao domínio. Uma conta de serviço é uma conta de usuário no Microsoft Active Directory autogerenciado à qual foram delegadas determinadas tarefas.

A conta de serviço precisa, no mínimo, receber as seguintes permissões na UO à qual você está ingressando no sistema de arquivos:

- Capacidade de redefinir senhas
- Capacidade de 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 (pode ser delegada) de criar e excluir objetos de computador
- Capacidade validada para ler e gravar restrições de conta
- Capacidade de modificar permissões

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 Microsoft Windows Server Erro: o acesso é negado quando usuários não administradores aos quais foi delegado o controle tentam associar computadores a um controlador de domínio.

Para obter mais informações sobre como criar uma conta de serviço com as permissões corretas, consulte Delegar privilégios à conta de serviço Amazon FSx .

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 realizar tarefas que exijam a desvinculação e a reintegração do seu domínio do Active Directory usando a conta de serviço. Essas tarefas incluem a substituição de um servidor de arquivos com falha ou a correção do software Windows Server. É fundamental que você mantenha a configuração do Active Directory, incluindo as credenciais da conta de serviço, atualizada com o Amazon FSx. Para ter mais informações, consulte Mantendo sua configuração do Active Directory atualizada.

O Amazon FSx requer conectividade com todos os controladores de domínio em seu ambiente do Active Directory. Se você tiver vários controladores de domínio, certifique-se de que todos eles atendam aos requisitos acima e de que todas as alterações na sua conta de serviço sejam propagadas para todos os controladores de domínio.

Você pode validar a configuração do Active Directory, inclusive testar a conectividade de vários controladores de domínio, usando a Ferramenta de validação do Active Directory do Amazon FSx. Para limitar o número de controladores de domínio que exigem conectividade, você também pode criar uma relação de confiança entre os controladores de domínio on-premises e o AWS Managed Microsoft AD. Para ter mais informações, consulte Como usar um modelo de isolamento de floresta de recursos.

> **Important**
>
> Não mova objetos de computador criados pelo Amazon FSx na UO depois da criação do sistema de arquivos. Isso fará com que o sistema de arquivos fique configurado incorretamente.

Práticas recomendadas para associar sistemas de arquivos do FSx para Windows File Server a um domínio de Microsoft Active Directory autogerenciado

Essas práticas são recomendadas na associação de sistemas de arquivos do Amazon FSx para Windows File Server ao Microsoft Active Directory autogerenciado.

Delegar privilégios à conta de serviço Amazon FSx

Certifique-se de configurar a conta de serviço fornecida ao Amazon FSx com os privilégios mínimos necessários. Além disso, separe a unidade organizacional (UO) de outras preocupações do controlador de domínio.

Para associar sistemas de arquivos do Amazon FSx ao seu domínio, certifique-se de que a conta de serviço tenha privilégios delegados. Os membros do grupo Administradores de domínio têm privilégios suficientes para realizar essa tarefa. No entanto, como prática recomendada, use uma conta de serviço que tenha apenas os privilégios mínimos necessários para isso. Os procedimentos a seguir demonstram como delegar apenas os privilégios necessários para unir sistemas de arquivos Amazon FSx ao seu domínio.

Você usa o Controle Delegado ou os Recursos Avançados no snap-in MMC de Usuários e Computadores do Active Directory para atribuir essas permissões.

Execute qualquer um desses procedimentos em uma máquina que esteja associada ao seu diretório ativo e tenha o Active Directory User and Computers MMC snap-in instalado.

Para atribuir permissões a uma conta de serviço ou grupo usando o Controle Delegado

1. Faça login no seu sistema como administrador de domínio do seu domínio do 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 o nome da conta de serviço ou grupo do Amazon FSx e, em seguida, escolha Avançar.
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 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

11. Escolha Next (Próximo) e, em seguida, escolha Finish (Concluir).
12. Feche o snap-in do MMC de Computadores e Usuários do Active Directory.

Para atribuir permissões usando recursos avançados

1. Faça login no seu sistema como administrador de domínio do seu domínio do Active Directory.
2. Abra o snap-in do MMC de Computadores e Uuários do Active Directory.
3. Selecione Visualizar na barra de menu e certifique-se de que a opção Recursos avançados esteja habilitada (uma marca de seleção aparecerá ao lado dela se o recurso estiver habilitado).
4. No painel de tarefas, expanda o nó do domínio.
5. Localize e abra o menu de contexto (clique com o botão direito do mouse) da UO que você deseja modificar e escolha Propiedades.
6. No painel Propriedades da UO, selecione a guia Segurança.
7. Na guia Segurança, selecione Avançado. Em seguida, selecione Adicionar.
8. Na página Entrada de permissão, escolha Selecionar uma entidade principal e insira o nome da conta de serviço ou grupo do Amazon FSx. Em Aplica-se a:, escolha Objetos de computador descendentes. Certifique-se de que o seguinte esteja selecionado:

   - Modificar permissões
   - Criar objetos de computador
   - Excluir objetos de computador

9. Selecione Aplicar e, em seguida, selecione OK.
10. Feche o snap-in do MMC de Computadores e Usuários do Active Directory.

> **Important**
>
> Não mova objetos de computador criados pelo Amazon FSx na UO depois da criação do sistema de arquivos. Isso fará com que o sistema de arquivos fique configurado incorretamente. Se você atualizar o sistema de arquivos com uma nova conta de serviço,

certifique-se de que a nova conta de serviço tenha permissões de Controle total para os objetos de computador atuais associados ao sistema de arquivos.

Mantendo sua configuração do Active Directory atualizada

Para ajudar a garantir a disponibilidade contínua e ininterrupta do seu sistema de arquivos Amazon FSx, você precisa atualizar a configuração do Active Directory do sistema de arquivos sempre que fizer alterações na configuração autogerenciada do Active Directory.

Por exemplo, se o Active Directory usa uma política de redefinição de senha com base no tempo, assim que a senha for redefinida, certifique-se de atualizar a senha da conta de serviço com o Amazon FSx. Da mesma forma, se os endereços IP do servidor DNS mudarem no domínio do Active Directory, atualize os endereços IP do servidor DNS com o Amazon FSx assim que a alteração ocorrer. Para ter mais informações, consulte Como atualizar a configuração do Active Directory autogerenciado.

Quando você atualiza a configuração do Active Directory autogerenciado para o sistema de arquivos do Amazon FSx, o estado do sistema de arquivos muda de Disponível para Atualizado enquanto a atualização é aplicada. Verifique se o estado volta para Disponível após a aplicação da atualização. A atualização pode levar alguns minutos para ser concluída. Para ter mais informações, consulte Como monitorar as atualizações do Active Directory autogerenciado.

Se houver algum problema com a configuração atualizada do Active Directory autogerenciado, o estado do sistema de arquivos mudará para Configurado incorretamente. Esse estado mostra uma mensagem de erro e uma ação corretiva recomendada ao lado da descrição do sistema de arquivos no console, na API e na CLI. Depois de executar a ação corretiva recomendada, verifique se o estado do sistema de arquivos muda para Disponível.

Para saber mais sobre a solução de possíveis problemas de configurações incorretas do Active Directory autogerenciado, consulte O sistema de arquivos está em um estado de configuração incorreta.

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 os privilégios 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 tráfego de saída somente para os controladores de domínios do Microsoft Active Directory 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.

Como validar a configuração do Active Directory

Antes de criar um sistema de arquivos do FSx para Windows File Server associado ao seu Active Directory, recomendamos que você valide a configuração do Active Directory usando a Ferramenta de validação do Active Directory do Amazon FSx. Observe que a conectividade de saída com a Internet é necessária para validar com êxito a configuração do Active Directory.

Validar a configuração do Active Directory

1. Inicie uma instância do Amazon EC2 do Windows na mesma sub-rede e com os mesmos grupos de segurança da Amazon VPC que você usa para o sistema de arquivos do FSx para Windows File Server. Certifique-se de que sua instância do EC2 tenha as permissões `AmazonEC2ReadOnlyAccess` do IAM necessárias. Você pode validar as permissões de perfil da instância do EC2 usando o simulador de políticas do IAM. Para obter mais informações, consulte Testar as políticas do IAM com o simulador de políticas do IAM no Guia do usuário do IAM.
2. Associe sua instância do EC2 do Windows ao seu Active Directory. Para obter mais informações, consulte Manually Join a Windows Instance no Guia de administração do AWS Directory Service .
3. Conecte-se à sua instância do EC2. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
4. Abra uma PowerShell janela do Windows (usando Executar como administrador) na instância do EC2.

   Para testar se o módulo necessário do Active Directory para Windows PowerShell está instalado, use o comando de teste a seguir.

```
PS C:\> Import-Module ActiveDirectory
```

Se a mensagem acima retornar um erro, instale-o usando o comando a seguir.

```
PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
```

5. Baixe a ferramenta de validação de rede usando o comando a seguir.

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

6. Faça download do arquivo zip usando o comando a seguir.

```
PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
```

7. Adicione o módulo `AmazonFSxADValidation` à sessão atual.

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. Defina os parâmetros necessários substituindo-os no comando a seguir.

   - Nome de domínio do Active Directory (*DOMAINNAME.COM*)
   - Prepare o objeto `$Credential` para a senha da conta de serviço usando uma das seguintes opções:
     - Para gerar o objeto de credencial de forma interativa, use o comando a seguir.

       ```
       $Credential = Get-Credential
       ```

     - Para gerar o objeto de credencial usando um AWS Secrets Manager recurso, use o comando a seguir.

       ```
       $Secret = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
        $AdminSecret).SecretString
       $Credential = (New-Object PSCredential($Secret.UserName,(ConvertTo-SecureString
        $Secret.Password -AsPlainText -Force)))
       ```

   - *Endereços IP do servidor DNS (IP_ADDRESS_1, IP_ADDRESS_2)*

- ID(s) de sub-rede para sub-redes nas quais você planeja criar seu sistema de arquivos do Amazon FSx (*SUBNET_1*, *SUBNET_2*, por exemplo, `subnet-04431191671ac0d19`).

```
PS C:\>
$FSxADValidationArgs = @{
    # DNS root of ActiveDirectory domain
    DomainDNSRoot = 'DOMAINNAME.COM'

    # IP v4 addresses of DNS servers
    DnsIpAddresses = @('IP_ADDRESS_1', 'IP_ADDRESS_2')

    # Subnet IDs for Amazon FSx file server(s)
    SubnetIds = @('SUBNET_1', 'SUBNET_2')

    Credential = $Credential
}
```

9. (Opcional) Defina a unidade organizacional, o grupo de administradores delegados e habilite a validação da permissão da conta de serviço seguindo as instruções no `README.md` arquivo incluído antes de executar a ferramenta de validação. DomainControllersMaxCount

> **Note**
>
> O grupo `Domain Admins` tem um nome diferente se o sistema operacional não estiver em inglês. Por exemplo, o grupo é denominado `Administrateurs du domaine` na versão francesa do OS. Se você não especificar um valor, o nome de grupo padrão `Domain Admins` será usado e a criação do sistema de arquivos falhará.

10. Execute a ferramenta de validação usando este comando.

```
PS C:\> $Result = Test-FSxADConfiguration @FSxADValidationArgs
```

11. A seguir, um exemplo de um resultado de teste bem-sucedido.

```
Test 1 - Validate EC2 Subnets ...
...
Test 17 - Validate 'Delete Computer Objects' permission ...

Test computer object amznfsxtestd53f deleted!
...
```

```
SUCCESS - All tests passed! Please proceed to creating an Amazon FSx file system.
 For your convenience, SelfManagedActiveDirectoryConfiguration of result can be
 used directly in CreateFileSystemWindowsConfiguration for New-FSXFileSystem
PS C:\AmazonFSxADValidation> $Result.Failures.Count
0
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

A seguir, um exemplo de um resultado de teste com erros.

```
Test 1 - Validate EC2 Subnets ...
...
Test 7 - Validate that provided EC2 Subnets belong to a single AD Site ...

Name          DistinguishedName
     Site
----          -----------------
     ----
10.0.0.0/19   CN=10.0.0.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local   CN=SiteB,CN=Sites,CN=Configu...
10.0.128.0/19 CN=10.0.128.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local CN=Default-First-Site-Name,C...
10.0.64.0/19  CN=10.0.64.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local  CN=SiteB,CN=Sites,CN=Configu...



Best match for EC2 subnet subnet-092f4caca69e360e7 is AD site CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=te
st-ad,DC=local
Best match for EC2 subnet subnet-04431191671ac0d19 is AD site
 CN=SiteB,CN=Sites,CN=Configuration,DC=test-ad,DC=local
WARNING: EC2 subnets subnet-092f4caca69e360e7 subnet-04431191671ac0d19 matched to
 different AD sites! Make sure they
are in a single AD site.
...
9 of 16 tests skipped.
FAILURE - Tests failed. Please see error details below:

Name                          Value
----                          -----
SubnetsInSeparateAdSites      {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}
```

```
Please address all errors and warnings above prior to re-running validation to
 confirm fix.
PS C:\AmazonFSxADValidation> $Result.Failures.Count
1
PS C:\AmazonFSxADValidation> $Result.Failures

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}


PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

Se você receber avisos ou erros ao executar a ferramenta de validação, consulte o Guia de solução de problemas incluído no pacote da ferramenta de validação (`TROUBLESHOOTING.md`) e Solução de problemas do Amazon FSx.

Associar um sistema de arquivos do Amazon FSx a um domínio do Microsoft Active Directory autogerenciado

Ao criar um novo sistema de arquivos ao FSx para Windows File Server, você pode configurar a integração do Microsoft Active Directory para que ela se associe ao seu domínio do Microsoft Active Directory autogerenciado. Para fazer isso, forneça as seguintes informações para o Microsoft Active Directory:

- O nome de domínio totalmente qualificado do diretório on-premises do Microsoft Active Directory.

> **Note**
>
> No momento, o Amazon FSx não oferece suporte a domínios de rótulo único (SLD).

- Os endereços IP de servidores DNS para o seu domínio.
- Credenciais para uma conta de serviço em seu domínio on-premises do Microsoft Active Directory. O Amazon FSx usa essas credenciais para associar a um Active Directory autogerenciado.

Opcionalmente, também é possível especificar as seguintes opções:

- Uma Unidade Organizacional (UO) específica dentro do domínio ao qual você deseja que seu sistema de arquivos do Amazon FSx se associe.
- (Opcional) O nome do grupo de domínios cujos membros têm privilégios administrativos para o sistemas de arquivos do Amazon FSx.

> **Note**
>
> O nome do grupo de domínio fornecido deve ser exclusivo no Active Directory. O FSx for Windows File Server não criará o grupo de domínio nas seguintes circunstâncias:
>
> - Se já existir um grupo com o nome que você especificar
> - Se você não especificar um nome e um grupo chamado “Administradores de domínio” já existir no seu Active Directory.

Depois de especificar essas informações, o Amazon FSx associa seu novo sistema de arquivos ao seu domínio do Active Directory autogerenciado usando a conta de serviço que você forneceu.

> **Important**
>
> O Amazon FSx só marca registros DNS para um sistema de arquivos, se o domínio do Active Directory ao qual você está se associando estiver usando o Microsoft DNS como o DNS padrão. Se você estiver usando um DNS de terceiros, precisará configurar manualmente as entradas de DNS para seus sistemas de arquivos do Amazon FSx depois de criar seu sistema de arquivos. Para obter mais informações sobre como escolher os endereços IP corretos a serem usados no sistema de arquivos, consulte Como obter os endereços IP corretos do sistema de arquivos para usar no DNS.

Antes de começar

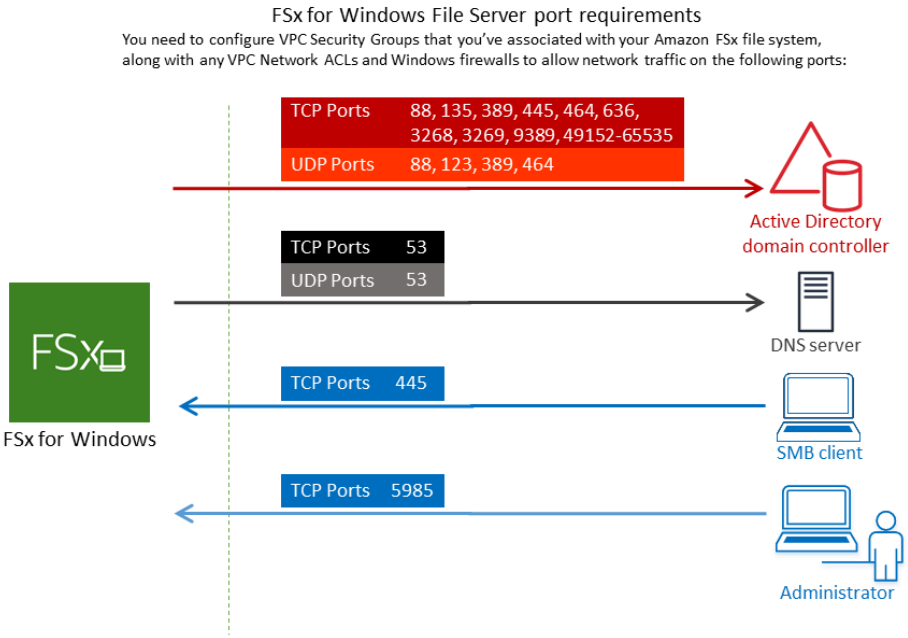
Garanta que concluiu o Pré-requisitos para usar um Microsoft Active Directory autogerenciado detalhado no Como usar o Amazon FSx com seu Microsoft Active Directory autogerenciado.

Para criar um sistema de arquivos do FSx para Windows File Server associado a um Active Directory autogerenciado (Console)

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. Escolha FSx para Windows File Server e, em seguida, escolha Próximo. A página Criar sistema de arquivos é exibida.
4. Forneça um nome para o sistema de arquivos. Você pode usar no máximo 256 letras Unicode, espaços em branco e números, além dos caracteres especiais + - = . _ : /
5. Em Capacidade de armazenamento, insira a capacidade de armazenamento do sistema de arquivos, em GiB. Se você estiver usando o armazenamento SSD, insira qualquer número inteiro no intervalo entre 32 e 65.536. Se você estiver usando o armazenamento em HDD, insira qualquer número inteiro no intervalo entre 2.000 e 65.536. 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.
6. Mantenha a Capacidade de Throughput na configuração padrão. Capacidade de throughput: é a velocidade sustentada na qual o servidor de arquivos que hospeda o sistema de arquivos pode fornecer dados. A configuração da capacidade de throughput recomendada é baseada na quantidade de capacidade de armazenamento que você escolher. Se você precisar de mais do que a capacidade de throughput recomendada, escolha Especificar capacidade de throughput e, em seguida, escolha um valor. Para ter mais informações, consulte Performance do FSx para Windows File Server.

   Você pode modificar a capacidade de throughput, conforme necessário, a qualquer momento depois de criar o sistema de arquivos. Para ter mais informações, consulte Como gerenciar a capacidade de throughput.
7. Escolha a VPC que você deseja associar a um sistema de arquivos. Para fins deste exercício de introdução, escolha a mesma VPC do seu AWS Directory Service diretório e da instância do Amazon EC2.
8. Escolha qualquer valor para zonas de disponibilidade e sub-rede.
9. Em Grupos de segurança da VPC, o grupo de segurança padrão para a Amazon VPC padrão já está adicionado ao sistema de arquivos no console. Certifique-se de que o grupo de segurança e as ACLs de rede da VPC para as sub-redes nas quais você vai criar seu sistema de arquivos do FSx permite tráfego nas portas e nas direções mostradas no diagrama a seguir.



A tabela a seguir identifica o perfil de cada porta.

Protocolo	Portas	Funçã
TCP/UDP	53	Doma Name Syste (DNS)
TCP/UDP	88	Auten ção de Kerbe
TCP/UDP	464	Altera d efinir senha

Protocolo	Portas	Funçã
TCP/UDP	389	Lightw ht Direct Acces Protoc (LDAP
UDP	123	Netwo Time Protoc (NTP)
TCP	135	Distrib ed Comp Enviro nt/ End Point Mappe (DCE/ EPMA P)
TCP	445	Comp hame de arquiv de SMB para serviç de diretó

Protocolo	Portas	Funçã
TCP	636	Lightw ht Direct Acces Protoc over TLS/ SSL (LDAP
TCP	3268	Catálo global da Micros
TCP	3269	Catálo global da Micros sobre SSL
TCP	5985	WinRI 2.0 (Gere mento Remo do Micros Windo

Protocolo	Portas	Funçã
TCP	9389	Serviç Web do Micros Active Direct DS, Powe l
TCP	49152 – 65535	Portas efême para RPC

> **Important**
>
> É necessário permitir o tráfego de saída na porta TCP 9389 para implantações de sistemas de arquivos single-AZ 2 e todas as implantações de sistemas de arquivos multi-AZ.

> **Note**
>
> Se estiver usando ACLs de rede de VPC, você também deverá permitir tráfego de saída em portas dinâmicas (49152-65535) do sistema de arquivos do FSx.

- Regras de saída para permitir todo o tráfego para os endereços IP associados aos servidores DNS e controladores de domínio do seu domínio do Microsoft Active Directory autogerenciado. Para obter mais informações, consulte a documentação da Microsoft sobre como configurar seu firewall para comunicação com o Active Directory.

- Confira se essas regras de tráfego também são refletidas nos firewalls que se aplicam a cada um dos controladores do domínio do Active Directory, servidores DNS, clientes do FSx e administradores do FSx.

> **Note**
>
> Se tiver sites do Active Directory definidos, você deve verificar se as sub-redes na VPC associada ao sistema de arquivos do Amazon FSx estão definidas em um site do Active Directory e se não existem conflitos entre as sub-redes em sua VPC e as sub-redes em seus outros sites. Você pode exibir e alterar essas configurações usando o snap-in do MMC de Serviços e Sites do Active Directory.

> **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.

10. Para Autenticação do Windows, escolha Microsoft Active Directory autogerenciado.
11. Insira um valor para o Nome de domínio totalmente qualificado para o diretório do Microsoft Active Directory autogerenciado.

> **Note**
>
> Seu nome de domínio de AD não pode estar no formato de domínio de rótulo único (SLD). No momento, o Amazon FSx não oferece suporte a domínios do SLD.

> **Important**
>
> Para sistemas de arquivos single-AZ 2 e todos os sistemas de arquivos multi-AZ, o nome de domínio do Active Directory não pode exceder 47 caracteres.

12. Insira um valor de unidade organizacional para o diretório do Microsoft Active Directory autogerenciado.

> **Note**
>
> Certifique-se de que a conta de serviço que você forneceu tenha permissões delegadas à UO especificada aqui ou à UO padrão, se você não especificar uma.

13. Insira pelo menos um, e não mais do que dois, valores para Endereços IP do servidor DNS para o diretório do Microsoft Active Directory autogerenciado.
14. Insira um valor de string para o Nome de usuário da conta de serviço para a conta em seu domínio do Active Directory autogerenciado, como `ServiceAcct`. O Amazon FSx usa esse nome de usuário para se associar ao seu domínio do Microsoft Active Directory.

> **Important**
>
> NÃO inclua um prefixo de domínio (`corp.com\ServiceAcct`) ou sufixo de domínio (`ServiceAcct@corp.com`) ao inserir o Nome de usuário da conta de serviço.
> NÃO use o Nome Distinto (DN) ao inserir o Nome de usuário da conta de serviço (`CN=ServiceAcct,OU=example,DC=corp,DC=com`).

15. Insira um valor para a Senha da conta de serviço para a conta em seu domínio do Active Directory autogerenciado. O Amazon FSx usa essa senha para se associar ao seu domínio do Microsoft Active Directory.
16. Digite novamente a senha para confirmá-la em Confirmar senha.
17. Para o Grupo de administradores delegado do sistema de arquivos, especifique o grupo `Domain Admins` ou um grupo personalizado delegado de administradores do sistema de arquivos (se você tiver criado um). O grupo que você especificar deve ter a autoridade delegada para realizar tarefas administrativas em seu sistema de arquivos. Se você não fornecer um valor, o Amazon FSx usa o grupo de `Domain Admins` incorporado. Observe que o Amazon FSx não oferece suporte para ter um `Delegated file system administrators group` (o `Domain Admins` grupo ou um grupo personalizado que você especificar) localizado no contêiner embutido.

> **Important**
>
> Se você não fornecer um Grupo de administradores delegado do sistema de arquivos, por padrão, o Amazon FSx tentará usar o grupo `Domain Admins` integrado em seu domínio do Active Directory. Se o nome desse grupo incorporado tiver sido alterado ou se você estiver usando um grupo diferente para administração de domínio, forneça esse nome para o grupo aqui.

> **Important**
>
> NÃO inclua um prefixo de domínio (corp.com\ FSxAdmins) ou sufixo de domínio (F SxAdmins @corp .com) ao fornecer o parâmetro do nome do grupo.
> NÃO use o Nome distinto (DN) para o grupo. Um exemplo de nome distinto é CN=FSxAdmins, OU=example, DC=corp, DC=com.

Criar um sistema de arquivos do Amazon FSx para Windows File Server associado a uma (AWS CLI) do Active Directory autogerenciado

O exemplo a seguir cria um sistema de arquivos do FSx para Windows File Server com um `SelfManagedActiveDirectoryConfiguration` na zona de disponibilidade `us-east-2`.

```
aws fsx --region us-east-2 \
create-file-system \
--file-system-type WINDOWS \
--storage-capacity 300 \
--security-group-ids security-group-id \
--subnet-ids subnet-id\
--windows-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAdmini
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',ThroughputCapacity=8
```

> **Important**
>
> Não mova objetos de computador criados pelo Amazon FSx na UO depois da criação do sistema de arquivos. Isso fará com que o sistema de arquivos fique configurado incorretamente.

Como obter os endereços IP corretos do sistema de arquivos para usar no DNS

O Amazon FSx só registra registros DNS para um sistema de arquivos se você estiver usando o Microsoft DNS como o serviço DNS padrão. Se estiver usando um DNS de terceiros, será necessário configurar manualmente as entradas de DNS para os sistemas de arquivos do Amazon FSx. Esta seção descreve como obter os endereços IP corretos do sistema de arquivos a serem usados se for necessário adicionar manualmente o sistema de arquivos ao seu DNS. Observe que, depois que um sistema de arquivos é criado, seus endereços IP não mudam até que o sistema de arquivos seja excluído.

Como obter endereços IP do sistema de arquivos para usar nas entradas DNS A

1. Em https://console.aws.amazon.com/fsx/, escolha o sistema de arquivos do qual você deseja obter o endereço IP para exibir a página de detalhes do sistema de arquivos.
2. Na guia Rede e segurança, siga um destes procedimentos:

   - Para sistemas de arquivos single-AZ 1:
     - No painel Sub-rede, selecione a interface de rede elástica mostrada em Interface de rede para abrir a página Interfaces de rede no console do Amazon EC2.
     - O endereço IP do sistema de arquivos single-AZ 1 a ser usado é mostrado na coluna IP IPv4 privado primário.
   - Para sistemas de arquivos single-AZ 2 ou multi-AZ:
     - No painel Sub-rede preferencial, escolha a interface de rede elástica mostrada em Interface de rede para abrir a página Interfaces de rede no console do Amazon EC2.
     - O endereço IP da sub-rede preferencial a ser usada é mostrado na coluna IP IPv4 privado secundário.

- No painel Sub-rede em espera do Amazon FSx, escolha a interface de rede elástica mostrada em Interface de rede para abrir a página Interfaces de rede no console do Amazon EC2.
- O endereço IP da sub-rede em espera a ser usado é mostrado na coluna IP IPv4 privado secundário.

> **Note**
>
> Se precisar configurar entradas de DNS para seu PowerShell Endpoint Remoto do Windows para sistemas de arquivos Single-AZ 2 ou Multi-AZ, use o endereço IPv4 privado primário para a interface de rede elástica de sua sub-rede preferencial. Para ter mais informações, consulte Usando a CLI do Amazon FSx para PowerShell.

Como atualizar a configuração do Active Directory autogerenciado

Você pode usar a AWS Management Console API Amazon FSx ou atualizar o nome de usuário e AWS CLI a senha da conta de serviço e os endereços IP do servidor DNS da configuração autogerenciada do Active Directory de um sistema de arquivos. Você pode acompanhar o progresso de uma atualização de configuração autogerenciada do Active Directory a qualquer momento usando a AWS Management Console CLI e a API. Para ter mais informações, consulte Como monitorar as atualizações do Active Directory autogerenciado.

Atualizar a configuração do Active Directory autogerenciado (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Navegue até Sistemas de arquivos e selecione o sistema de arquivos do Windows para o qual você deseja atualizar a configuração do Active Directory autogerenciado.
3. Na guia Rede e segurança, selecione Atualizar para os endereços IP do servidor DNS ou para o nome de usuário da conta de serviço, dependendo das propriedades do Active Directory que você está atualizando.
4. Insira os novos endereços IP do servidor DNS ou as credenciais da nova conta de serviço na caixa de diálogo exibida.
5. Selecione Atualizar para iniciar a atualização da configuração do Active Directory.

Você pode monitorar o progresso da atualização usando o AWS Management Console ou AWS CLI o.

Atualizar a configuração do Active Directory autogerenciado (CLI)

- Para atualizar a configuração autogerenciada do Active Directory de um sistema de arquivos FSx for Windows File Server, use AWS CLI o comando update-file-system. Defina os seguintes parâmetros:
  - `--file-system-id` para o ID do sistema de arquivos que você está atualizando.
  - `UserName`: o novo nome de usuário para a conta de serviço do Active Directory autogerenciado.
  - `Password`: a nova senha da conta de serviço do Active Directory autogerenciado.
  - `DnsIps`: os endereços IP dos servidores DNS do Active Directory autogerenciado.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 'SelfManagedActiveDirectoryConfiguration={UserName=username,Password=password,\
    DnsIps=[192.0.2.0,192.0.2.24]}'
```

Se a ação de atualização for bem-sucedida, o serviço enviará de volta uma resposta HTTP 200. O `AdminstrativeActions` objeto na resposta descreve a solicitação e seu status.

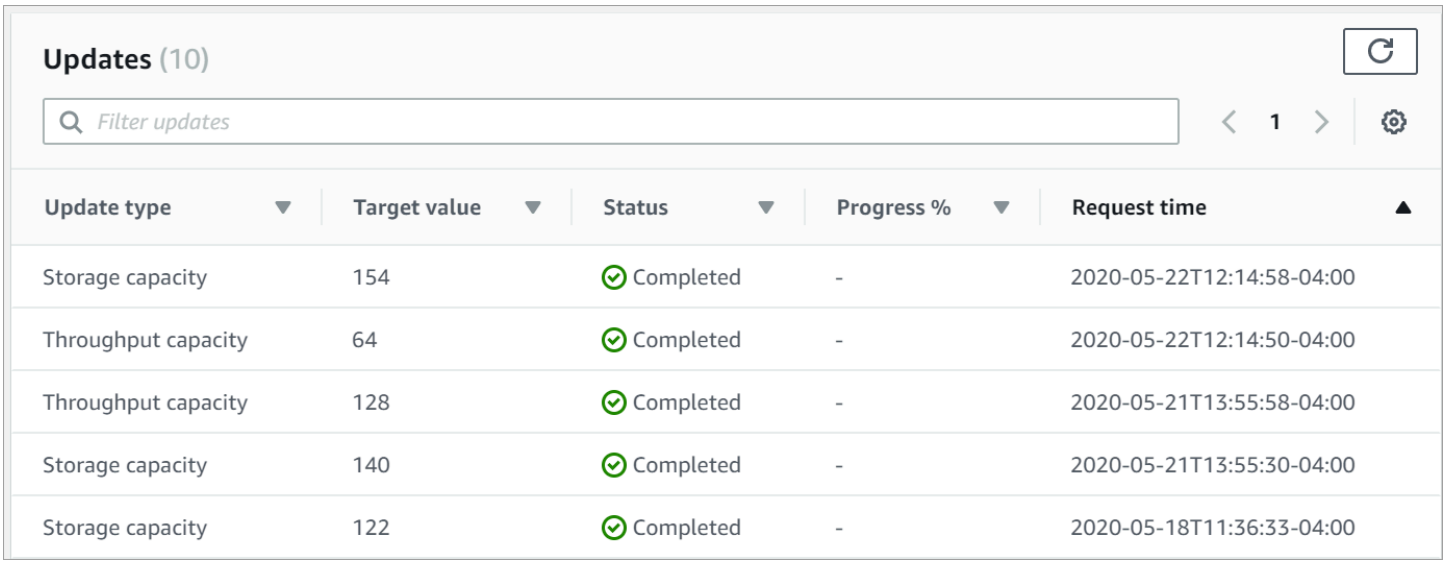
Como monitorar as atualizações do Active Directory autogerenciado

Quando você atualiza a configuração autogerenciada do Active Directory do seu sistema de arquivos, o estado do sistema de arquivos muda de Disponível para Atualizado enquanto a atualização é aplicada. Depois que a atualização for concluída, o estado volta para Disponível — observe que a atualização pode levar vários minutos para ser concluída.

Você pode monitorar o progresso de uma atualização de configuração autogerenciada do Active Directory usando a AWS Management Console, a API ou a AWS CLI, descrita nas seções a seguir.

Como monitorar as atualizações no console

Na guia Atualizações na janela Detalhes do sistema de arquivos, você pode ver as dez atualizações mais recentes para cada tipo de atualização.



Para atualizações do Active Directory autogerenciado, você pode visualizar as seguintes informações:

Tipo de atualização

Os tipos compatíveis são os seguintes:

- Endereço IP do servidor DNS
- Credenciais da conta de serviço

Target value (Valor de destino)

O valor desejado para atualizar a propriedade do sistema de arquivos. Para atualizações de Credenciais da conta de serviço, somente o nome de usuário é mostrado. As senhas da conta de serviço nunca são incluídas nesse campo.

Status

O status atual da atualização. Para atualizações do Active Directory autogerenciado, os valores possíveis são os seguintes:

- 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.

- Concluída: a atualização do sistema de arquivos foi concluída com êxito.
- Com falha: a atualização do sistema de arquivos falhou. Selecione o ponto de interrogação (?) para ver os detalhes sobre a falha.

% de progresso

Exibe o progresso da atualização do sistema de arquivos como porcentagem concluída.

Horário da solicitação

O horário em que o Amazon FSx recebeu a solicitação de ação de atualização.

Monitorando atualizações usando a API AWS CLI e

Você pode visualizar e monitorar as solicitações de atualização do sistema de arquivos que estão em andamento usando o AWS CLI comando describe-file-systems e a ação da API Systems. DescribeFile A matriz `AdministrativeActions` lista as dez ações de atualização mais recentes para cada tipo de ação administrativa.

O exemplo a seguir mostra um trecho da resposta de um comando da CLI describe-file-systems que mostra duas atualizações do sistema de arquivos do Active Directory autogerenciado.

```
{
    "OwnerId": "111122223333",
    .
    .
    .
    "StorageCapacity": 1000,
    "AdministrativeActions": [
        {
            "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
            "RequestTime": 1581694766.757,
            "Status": "PENDING",
            "TargetFileSystemValues": {
                "WindowsConfiguration": {
                    "SelfManagedActiveDirectoryConfiguration": {
                        "UserName": "serviceUser",
                    }
                }
            }
        },
        {
```

```
                "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                "RequestTime": 1619032957.759,
                "Status": "FAILED",
                "TargetFileSystemValues": {
                    "WindowsConfiguration": {
                        "SelfManagedActiveDirectoryConfiguration": {
                        "DnsIps": [
                                "10.0.138.161"
                            ]
                        }
                    }
                },
                "FailureDetails": {
                    "Message": "Failure details message."
                }
            }
        ],
    .
    .
    .
```

Como usar compartilhamentos de arquivos do Microsoft Windows

Um compartilhamento de arquivos do Microsoft Windows é uma pasta específica em seu sistema de arquivos. Ele inclui as subpastas dessa pasta, as quais você torna acessíveis às suas instâncias de computação com o protocolo SMB (Server Message Block). Seu sistema de arquivos vem com um compartilhamento de arquivos padrão do Windows, chamado `share`. Você pode criar e gerenciar quantos compartilhamentos de arquivos do Windows quiser usando a ferramenta de interface gráfica do usuário (GUI) do Windows chamada Pastas compartilhadas.

Como acessar compartilhamentos de arquivos

Para acessar seus compartilhamentos de arquivos, use a funcionalidade Mapear unidade de rede do Windows para mapear uma letra de drive em sua instância de computação para o compartilhamento de arquivos do Amazon FSx. O processo de mapeamento de um compartilhamento de arquivos para uma unidade em sua instância de computação é conhecido como montagem de um compartilhamento de arquivos no Linux. Esse processo difere de acordo com o tipo de instância de computação e o sistema operacional. Depois que o compartilhamento de arquivos for mapeado, suas aplicações e usuários poderão acessar arquivos e pastas no compartilhamento de arquivos como se fossem arquivos e pastas locais.

Veja a seguir os procedimentos para mapear um compartilhamento de arquivos nas diferentes instâncias de computação compatíveis.

Tópicos

Como mapear um compartilhamento de arquivos em uma instância do Amazon EC2 do Windows

Você pode mapear um compartilhamento de arquivos em uma instância do EC2 do Windows usando o Explorador de Arquivos do Windows ou o prompt de comando.

Mapear um compartilhamento de arquivos em uma instância do Amazon EC2 do Windows (console)

1. Inicie a instância do EC2 do Windows e conecte-a ao Microsoft Active Directory ao qual você associou seu sistema de arquivos do Amazon FSx. 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 à instância do Windows do EC2. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
3. Depois de se conectar, abra o Explorador de Arquivos.
4. No painel de navegação, abra o menu de contexto (clique com o botão direito do mouse) em Rede e escolha Mapear unidade de rede.
5. Em Drive, escolha uma letra de drive.
6. Em Pasta, insira o nome DNS do sistema de arquivos ou um alias de DNS associado ao sistema de arquivos e o nome do compartilhamento.

   > **Important**
   >
   > Usar um endereço IP em vez do nome DNS pode resultar em indisponibilidade durante o processo de failover do sistema de arquivos multi-AZ. Além disso, nomes DNS ou aliases de DNS associados são necessários para a autenticação baseada em Kerberos em sistemas de arquivos multi-AZ e single-AZ.

   Você pode encontrar o nome de DNS do sistema de arquivos e quaisquer aliases de DNS associados no console do Amazon FSx, selecionando Windows File Server, Rede e segurança. Ou você pode encontrá-los na resposta da operação do CreateFileSistema ou da API de DescribeFileSistemas. Para obter mais informações sobre o uso de aliases de DNS, consulte Como gerenciar aliases de DNS.

- Para um sistema de arquivos Single-AZ associado a um Microsoft Active Directory AWS gerenciado, o nome DNS se parece com o seguinte.

  ```
  fs-0123456789abcdef0.ad-domain.com
  ```

- Para um sistema de arquivos single-AZ associado a um Active Directory autogerenciado, e para qualquer sistema de arquivos multi-AZ, o nome DNS seria como a seguir.

  ```
  amznfsxaa11bb22.ad-domain.com
  ```

Por exemplo, para usar o nome DNS de um sistema de arquivos single-AZ, insira o seguinte em Pasta:

```
\\fs-0123456789abcdef0.ad-domain.com\share
```

Para usar o nome DNS de um sistema de arquivos multi-AZ, insira o seguinte em Pasta:

```
\\famznfsxaa11bb22.ad-domain.com\share
```

Para usar um alias de DNS associado ao sistema de arquivos, insira o seguinte em Pasta:

```
\\fqdn-dns-alias\share
```

7. Escolha uma opção para Reconectar no login, a qual indica se o compartilhamento de arquivos deve se reconectar no login e, em seguida, selecione Concluir.

Mapear um compartilhamento de arquivos em uma instância do Amazon EC2 do Windows (prompt de comando)

1. Inicie a instância do EC2 do Windows e conecte-a ao Microsoft Active Directory ao qual você associou seu sistema de arquivos do Amazon FSx. 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 à sua instância do EC2 Windows como usuário em seu AWS Managed Microsoft AD diretório. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
3. Depois de se conectar, abra uma janela do prompt de comando.
4. Monte o compartilhamento de arquivos usando uma letra de drive de sua escolha, o nome DNS do sistema de arquivos e o nome do compartilhamento. Você pode encontrar o nome DNS usando o console do Amazon FSx, selecionando Windows File Server, Rede e segurança. Ou você pode encontrá-lo na resposta do `CreateFileSystem` ou na operação da API `DescribeFileSystems`.

   - Para um sistema de arquivos Single-AZ associado a um Microsoft Active Directory AWS gerenciado, o nome DNS se parece com o seguinte.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - Para um sistema de arquivos single-AZ associado a um Active Directory autogerenciado, e para qualquer sistema de arquivos multi-AZ, o nome DNS seria como a seguir.

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   A seguir, um exemplo de comando para montar o compartilhamento de arquivos.

   ```
   $ net use H: \\amzfsxaa11bb22.ad-domain.com\share /persistent:yes
   ```

   Em vez do `net use` comando, você também pode usar qualquer PowerShell comando compatível para montar um compartilhamento de arquivos.

Como montar um compartilhamento de arquivos em uma instância do Amazon EC2 do Mac

Você pode montar um compartilhamento de arquivos em uma instância do Amazon EC2 do Mac que esteja associada ou não ao seu Active Directory. Se a instância não estiver associada ao seu Active Directory, certifique-se de atualizar as opções de DHCP definidas para a Amazon Virtual Private

Cloud (Amazon VPC) na qual a instância reside para incluir os servidores de nomes DNS do seu domínio do Active Directory. Em seguida, reinicie a instância.

Montar um compartilhamento de arquivos em uma instância do Amazon EC2 do Mac (GUI)

1. Inicie a instância do EC2 no Mac. Para fazer isso, escolha um dos seguintes procedimentos no Guia do usuário do Amazon EC2:

   - Executar uma instância do Mac usando o console
   - Execute uma instância do Mac usando o AWS CLI

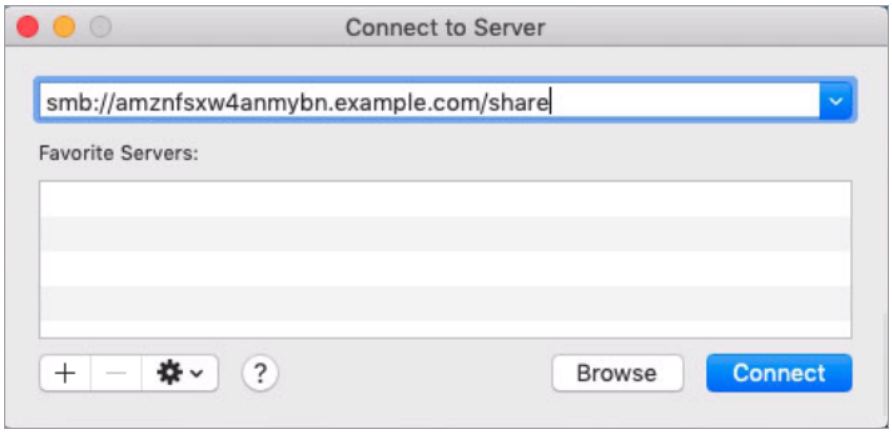
2. Conecte-se à sua instância do EC2 do Mac usando a computação de rede virtual (VNC). Para obter mais informações, consulte Conecte-se à sua instância usando VNC no Guia do usuário do Amazon EC2.

3. Em sua instância do EC2 do Mac, conecte-se ao compartilhamento de arquivos do Amazon FSx, como segue:

   a. Abra o Finder, selecione Ir e, em seguida, selecione Conectar ao servidor.

   b. Na caixa de diálogo Conectar ao servidor, insira o nome DNS do sistema de arquivos ou um alias de DNS associado ao sistema de arquivos e o nome do compartilhamento. Depois, escolha Conectar.

      Você pode encontrar o nome de DNS do sistema de arquivos e quaisquer aliases de DNS associados no console do Amazon FSx, selecionando Windows File Server, Rede e segurança. Ou você pode encontrá-los na resposta da operação do CreateFileSistema ou da API de DescribeFileSistemas. Para obter mais informações sobre o uso de aliases de DNS, consulte Como gerenciar aliases de DNS.

   c. Na tela seguinte, selecione Conectar para continuar.

d. Insira suas credenciais do Microsoft Active Directory (AD) para a conta de serviço do Amazon FSx, conforme mostrado no exemplo a seguir. Depois, escolha Conectar.

e. Se a conexão for bem-sucedida, você poderá visualizar o compartilhamento do Amazon FSx, em Locais, na janela do Finder.

Montar um compartilhamento de arquivos em uma instância do Amazon EC2 do Mac (linha de comando)

1. Inicie a instância do EC2 no Mac. Para fazer isso, escolha um dos seguintes procedimentos no Guia do usuário do Amazon EC2:

   - Executar uma instância do Mac usando o console
   - Execute uma instância do Mac usando o AWS CLI

2. Conecte-se à sua instância do EC2 do Mac usando a computação de rede virtual (VNC). Para obter mais informações, consulte Conecte-se à sua instância usando VNC no Guia do usuário do Amazon EC2.

3. Monte o compartilhamento de arquivos com o seguinte comando:

   ```
   mount_smbfs //file_system_dns_name/file_share mount_point
   ```

   Você pode encontrar o nome DNS no console do Amazon FSx escolhendo Windows File Server, Rede e segurança. Ou você pode encontrá-lo na resposta do `CreateFileSystem` ou na operação da API `DescribeFileSystems`.

- Para um sistema de arquivos Single-AZ associado a um Microsoft Active Directory AWS gerenciado, o nome DNS se parece com o seguinte.

```
fs-0123456789abcdef0.ad-domain.com
```

- Para um sistema de arquivos single-AZ associado a um Active Directory autogerenciado, e para qualquer sistema de arquivos multi-AZ, o nome DNS seria como a seguir.

```
amznfsxaa11bb22.ad-domain.com
```

O comando de montagem usado nesse procedimento executa o seguinte nos pontos indicados:

- *//file_system_dns_name/file_share*: especifica o nome DNS e o compartilhamento do sistema de arquivos a ser montado.
- *mount_point*: o diretório na instância do EC2 em que você está montando o sistema de arquivos.

Como montar um compartilhamento de arquivos em uma instância do Amazon EC2 do Linux

Você pode montar um compartilhamento de arquivos do FSx para Windows File Server em uma instância do Amazon EC2 do Linux que esteja associada ou não ao Active Directory.

> **Note**
>
> - Os comandos a seguir especificam parâmetros como o protocolo SMB, o cache e o tamanho do buffer de leitura e gravação apenas como exemplos. As escolhas de parâmetros para o comando `cifs` do Linux, bem como a versão do kernel do Linux utilizada, podem afetar o throughput e a latência das operações de rede entre o cliente e o sistema de arquivos do Amazon FSx. Para obter mais informações, consulte a documentação do `cifs` do ambiente Linux que você está usando.
> - Os clientes Linux não são compatíveis com failover automático baseado em DNS. Para ter mais informações, consulte Experiência de failover em clientes Linux.

Montar um compartilhamento de arquivos em uma instância do Amazon EC2 do Linux associada ao Active Directory

1. Se você ainda não tiver uma instância do EC2 do Linux em execução associada ao Microsoft Active Directory, consulte Associar manualmente uma instância do Linux no Guia de administração do AWS Directory Service para obter instruções sobre como fazer isso.
2. Conecte-se à sua instância do EC2 do Linux. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
3. Execute o seguinte comando para instalar o pacote `cifs-utils`: Esse pacote é usado para montar sistemas de arquivos de rede como o Amazon FSx no Linux.

   ```
   $ sudo yum install cifs-utils
   ```

4. Crie o diretório do ponto de montagem **`/mnt/fsx`**. É nele que você montará o sistema de arquivos do Amazon FSx.

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

5. Faça a autenticação com o kerberos usando o comando a seguir.

   ```
   $ kinit
   ```

6. Monte o compartilhamento de arquivos com o seguinte comando:

   ```
   $ sudo mount -t cifs //file_system_dns_name/file_share mount_point --verbose -o
    vers=SMB_version,sec=krb5,cruid=ad_user,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=no
   file-server-Ip
   ```

   Você pode encontrar o nome DNS no console do Amazon FSx escolhendo Windows File Server, Rede e segurança. Ou você pode encontrá-los na resposta do `CreateFileSystem` ou com a operação da API `DescribeFileSystems`.

   - Para um sistema de arquivos Single-AZ associado a um Microsoft Active Directory AWS gerenciado, o nome DNS se parece com o seguinte.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - Para um sistema de arquivos single-AZ associado a um Active Directory autogerenciado, e para qualquer sistema de arquivos multi-AZ, o nome DNS seria como a seguir.

```
amznfsxaa11bb22.ad-domain.com
```

Substitua *CIFSMaxBufSize* pelo maior valor permitido pelo seu kernel. Execute o seguinte comando para obter esse valor:

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

A saída mostra que o tamanho máximo do buffer é 130048.

7. Verifique se o sistema de arquivos está montado executando o comando a seguir, que retorna apenas sistemas de arquivos do tipo Common Internet File System (CIFS).

```
$ mount -l -t cifs
//fs-0123456789abcdef0/share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=krb5,cache=cache_mode,username=user1@CORP.NETWORK.COM,ui
```

O comando de montagem usado nesse procedimento executa o seguinte nos pontos indicados:

- *//file_system_dns_name/file_share*: especifica o nome DNS e o compartilhamento do sistema de arquivos a ser montado.
- *mount_point*: o diretório na instância do EC2 em que você está montando o sistema de arquivos.
- `-t cifs vers=`*SMB_version*: especifica o tipo de sistema de arquivos como o CIFS e a versão do protocolo SMB. O Amazon FSx para Windows File Server é compatível com as versões 2.0 a 3.1.1 do SMB.
- `sec=krb5`: especifica o uso do Kerberos versão 5 para autenticação.
- `cache=`*cache_mode*: define o modo de cache. Essa opção para o cache CIFS pode afetar a performance, e você deve testar quais configurações funcionam melhor (e analisar a documentação do Linux) para seu kernel e sua workload. As opções `strict` e `none` são recomendadas, pois a opção `loose` pode causar inconsistência de dados devido à semântica mais flexível do protocolo.
- `cruid=`*ad_user*: define o uid do proprietário do cache de credenciais como o administrador do diretório do AD.

- */mnt/fsx*: especifica o ponto de montagem para o compartilhamento de arquivos do Amazon FSx em sua instância do EC2.
- `rsize=`*CIFSMaxBufSize*`,wsize=`*CIFSMaxBufSize*: especifica o tamanho do buffer de leitura e gravação como o máximo permitido pelo protocolo CIFS. Substitua *CIFSMaxBufSize* pelo maior valor permitido pelo seu kernel. Determine o `CIFSMaxBufSize` ao executar o comando a seguir.

  ```
  $ modinfo cifs | grep CIFSMaxBufSize
  parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
   16384 Range: 8192 to 130048 (uint)
  ```

  A saída mostra que o tamanho máximo do buffer é 130048.
- `ip=`*preferred-file-server-Ip*: define o endereço IP de destino como o do servidor de arquivos preferencial do sistema de arquivos.

  É possível recuperar o endereço IP do servidor de arquivos preferencial do sistema de arquivos da seguinte forma:
  - Usando o console do Amazon FSx, na guia Rede e segurança da página Detalhes do sistema de arquivos.
  - Na resposta do comando `describe-file-systems` CLI ou do comando equivalente da API de DescribeFilesistemas.

Montar um compartilhamento de arquivos em uma instância do Amazon EC2 do Linux não associada ao seu Active Directory

O procedimento a seguir permite a montagem de um compartilhamento de arquivos do Amazon FSx em uma instância do Amazon EC2 do Linux que não está associada ao seu Active Directory (AD). Para uma instância do EC2 do Linux que não está associada ao seu AD, somente é possível montar um compartilhamento de arquivo do FSx para Windows File Server usando seu endereço IP privado. Você pode obter o endereço IP privado do sistema de arquivos usando o console do Amazon FSx, na guia Rede e segurança, em Endereço IP do servidor de arquivos preferencial.

Este exemplo usa a autenticação NTLM. Para fazer isso, monte o sistema de arquivos como um usuário que seja membro do domínio do Microsoft Active Directory ao qual o sistema de arquivos do FSx para Windows File Server está associado. As credenciais da conta de usuário são fornecidas em um arquivo de texto que você cria na instância do EC2, `creds.txt`. Esse arquivo contém o nome de usuário, a senha e o domínio do usuário.

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

Executar e configurar a instância do Amazon EC2 do Linux

1. Execute uma instância do Amazon EC2 do Linux usando o console do Amazon EC2. Para obter mais informações, consulte Iniciar uma instância no Guia do usuário do Amazon EC2.
2. Conecte-se à sua instância do Amazon EC2 do Linux. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
3. Execute o seguinte comando para instalar o pacote `cifs-utils`: Esse pacote é usado para montar sistemas de arquivos de rede como o Amazon FSx no Linux.

   ```
   $ sudo yum install cifs-utils
   ```
4. Crie o ponto de montagem **`/mnt/fsxx`** no qual você planeja montar o sistema de arquivos do Amazon FSx.

   ```
   $ sudo mkdir -p /mnt/fsx
   ```
5. Crie o arquivo de credenciais `creds.txt` no diretório `/home/ec2-user` usando o formato mostrado anteriormente.
6. Defina as permissões do arquivo `creds.txt` para que somente você (o proprietário) possa ler e gravar no arquivo, executando o seguinte comando:

   ```
   $ chmod 700 creds.txt
   ```

Para montar o sistema de arquivos.

1. Você monta um compartilhamento de arquivos não associado ao Active Directory usando seu endereço IP privado. Você pode obter o endereço IP privado do sistema de arquivos usando o console do Amazon FSx, na guia Rede e segurança, em Endereço IP do servidor de arquivos preferencial.
2. Monte o sistema de arquivos usando o seguinte comando:

```
$ sudo mount -t cifs //file-system-IP-address/file_share /mnt/fsx
 --verbose -o vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

Substitua *CIFSMaxBufSize* pelo maior valor permitido pelo seu kernel. Execute o seguinte comando para obter esse valor:

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

A saída mostra que o tamanho máximo do buffer é 130048.

3. Verifique se o sistema de arquivos está montado executando o comando a seguir, que retorna apenas sistemas de arquivos CIFS.

```
$ mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_mode,username=user1,domain=CORP.EXA
```

O comando de montagem usado nesse procedimento executa o seguinte nos pontos indicados:

- *//file-system-IP-address/file_share*: especifica o endereço IP e o compartilhamento do sistema de arquivos que você está montando.
- `-t cifs vers=`*SMB_version*: especifica o tipo de sistema de arquivos como o CIFS e a versão do protocolo SMB. O Amazon FSx para Windows File Server é compatível com as versões 2.0 a 3.1.1 do SMB.
- `sec=ntlmsspi`: especifica o uso da interface do provedor de suporte de segurança do NT LAN Manager (NTLMSSPI) para a autenticação.
- `cache=`*cache_mode*: define o modo de cache. Essa opção para o cache CIFS pode afetar a performance, e você deve testar quais configurações funcionam melhor (e analisar a documentação do Linux) para seu kernel e sua workload. As opções `strict` e none são recomendadas, pois a opção `loose` pode causar inconsistência de dados devido à semântica mais flexível do protocolo.
- `cred=/home/ec2-user/creds.txt`: especifica onde obter as credenciais do usuário.

- */mnt/fsx*: especifica o ponto de montagem para o compartilhamento de arquivos do Amazon FSx em sua instância do EC2.
- `rsize=`*CIFSMaxBufSize*`,wsize=`*CIFSMaxBufSize*: especifica o tamanho do buffer de leitura e gravação como o máximo permitido pelo protocolo CIFS. Substitua *CIFSMaxBufSize* pelo maior valor permitido pelo seu kernel. Determine o `CIFSMaxBufSize` ao executar o comando a seguir.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

Montagem automática de compartilhamentos de arquivos em uma instância do Amazon EC2 do Linux não associada ao Active Directory

Você pode montar automaticamente o compartilhamento de arquivos do FSx para Windows File Server sempre que a instância do Amazon EC2 do Linux na qual ele está montado for reinicializada. Para fazer isso, adicione uma entrada ao arquivo `/etc/fstab` na instância do EC2. 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 no arquivo `/etc/fstab`.

Para uma instância do Amazon EC2 do Linux que não esteja associada ao seu Active Directory, somente é possível montar um compartilhamento de arquivo do FSx para Windows File Server usando seu endereço IP privado. Você pode obter o endereço IP privado do sistema de arquivos usando o console do Amazon FSx, na guia Rede e segurança, em Endereço IP do servidor de arquivos preferencial.

O procedimento a seguir usa a autenticação Microsoft NTLM. Você monta o sistema de arquivos como um usuário que é membro do domínio do Microsoft Active Directory ao qual o sistema de arquivos do FSx para Windows File Server está associado. As credenciais da conta de usuário são fornecidas no arquivo de texto `creds.txt`. Esse arquivo contém o nome de usuário, a senha e o domínio do usuário.

```
$ cat creds.txt
username=user1
```

```
password=Password123
domain=EXAMPLE.COM
```

Montar automaticamente um compartilhamento de arquivos em uma instância do Amazon EC2 do Linux não associada ao Active Directory

Executar e configurar a instância do Amazon EC2 do Linux

1. Execute uma instância do Amazon EC2 do Linux usando o console do Amazon EC2. Para obter mais informações, consulte Iniciar uma instância no Guia do usuário do Amazon EC2.
2. Conecte-se à sua instância. Para obter mais informações, consulte Connect to your Linux instance no Amazon EC2 User Guide.
3. Execute o seguinte comando para instalar o pacote `cifs-utils`: Esse pacote é usado para montar sistemas de arquivos de rede como o Amazon FSx no Linux.

   ```
   $ sudo yum install cifs-utils
   ```
4. Crie o diretório `/mnt/fsx`. É nele que você montará o sistema de arquivos do Amazon FSx.

   ```
   $ sudo mkdir /mnt/fsx
   ```
5. Crie o arquivo de credenciais `creds.txt` no diretório `/home/ec2-user`.
6. Defina as permissões do arquivo de modo que somente você (o proprietário) possa ler o arquivo ao executar o seguinte comando:

   ```
   $ sudo chmod 700 creds.txt
   ```

Montar automaticamente o sistema de arquivos

1. Você monta automaticamente um compartilhamento de arquivos não associado ao Active Directory usando seu endereço IP privado. Você pode obter o endereço IP privado do sistema de arquivos usando o console do Amazon FSx, na guia Rede e segurança, em Endereço IP do servidor de arquivos preferencial.
2. Para montar automaticamente o compartilhamento de arquivos usando seu endereço IP privado, adicione a seguinte linha ao arquivo `/etc/fstab`.

```
//file-system-IP-address/file_share /mnt/fsx cifs
 vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

Substitua *CIFSMaxBufSize* pelo maior valor permitido pelo seu kernel. Execute o seguinte comando para obter esse valor:

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

A saída mostra que o tamanho máximo do buffer é 130048.

3. Teste a entrada `fstab` usando o comando `mount` com a opção 'fake' em conjunto com as opções 'all' e 'verbose'.

```
$ sudo mount -fav
home/ec2-user/fsx      : successfully mounted
```

4. Para montar o compartilhamento de arquivos, reinicie a instância do Amazon EC2.
5. Quando a instância estiver disponível novamente, verifique se o sistema de arquivos está montado executando o seguinte comando:

```
$ sudo mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_code,username=user1,domain=CORP.EXA
```

A linha adicionada ao arquivo `/etc/fstab` nesse procedimento executa o seguinte nos pontos indicados:

- *//file-system-IP-address/file_share*: especifica o endereço IP e o compartilhamento do sistema de arquivos do Amazon FSx que você está montando.
- `/mnt/fsx`: especifica o ponto de montagem do sistema de arquivos do Amazon FSx em sua instância do EC2.
- `cifs vers=`*SMB_version*: especifica o tipo de sistema de arquivos como o CIFS e a versão do protocolo SMB. O Amazon FSx para Windows File Server é compatível com as versões 2.0 a 3.1.1 do SMB.

- `sec=ntlmsspi`: especifica o uso da interface do provedor de suporte de segurança do NT LAN Manager para facilitar a autenticação NTLM de desafio-resposta.
- `cache=`*`cache_mode`*: define o modo de cache. Essa opção para o cache CIFS pode afetar a performance, e você deve testar quais configurações funcionam melhor (e analisar a documentação do Linux) para seu kernel e sua workload. As opções `strict` e `none` são recomendadas, pois a opção `loose` pode causar inconsistência de dados devido à semântica mais flexível do protocolo.
- `cred=/home/ec2-user/creds.txt`: especifica onde obter as credenciais do usuário.
- `_netdev`: informa ao sistema operacional que o sistema de arquivos reside em um dispositivo que requer acesso à rede. O uso dessa opção impede que a instância monte o sistema de arquivos até que o serviço de rede seja habilitado no cliente.
- `0`: indica que o backup do sistema de arquivos deve ser feito pelo `dump`, caso seja um valor diferente de zero. Para o Amazon FSx, esse valor deve ser `0`.
- `0`: especifica a ordem em que o `fsck` verifica os sistemas de arquivos na inicialização. Para sistemas de arquivos do Amazon FSx, esse valor deve ser `0` para indicar que o `fsck` não deve ser executado na inicialização.

Como migrar o armazenamento de arquivos atual para o Amazon FSx

O FSx para Windows File Server possui os recursos, a performance e a compatibilidade para facilmente mover sem alterações (lift-and-shift) aplicações empresariais para a Nuvem Amazon Web Services. O processo de migração para o FSx para Windows File Server envolve as seguintes etapas:

1. Migre seus arquivos para o FSx para Windows File Server. Para ter mais informações, consulte Como migrar o armazenamento de arquivos atual para o FSx para Windows File Server.
2. Migre sua configuração de compartilhamento de arquivos para o FSx para Windows File Server. Para ter mais informações, consulte Como migrar configurações de compartilhamento de arquivos para o Amazon FSx.
3. Associe seu nome DNS atual como um alias de DNS para seu sistema de arquivos do Amazon FSx. Para obter mais informações, consulte Associar um alias de DNS ao Amazon FSx.
4. Mude para o FSx para Windows File Server. Para ter mais informações, consulte Substituição para o Amazon FSx.

Você pode encontrar os detalhes de cada etapa do processo nas seções a seguir.

Tópicos

Como migrar o armazenamento de arquivos atual para o FSx para Windows File Server

Para migrar seus arquivos existentes para os sistemas de arquivos FSx for Windows File Server, recomendamos o AWS DataSync uso de um serviço de transferência de dados on-line projetado para simplificar, automatizar e acelerar a cópia de grandes quantidades de dados de e AWS para serviços de armazenamento. DataSync copia dados pela internet ou AWS Direct Connect. Como

um serviço totalmente gerenciado, DataSync elimina grande parte da necessidade de modificar aplicativos, desenvolver scripts ou gerenciar a infraestrutura. Para ter mais informações, consulte Como migrar arquivos atuais para o FSx para Windows File Server usando o AWS DataSync.

Como solução alternativa, você pode usar o Robust File Copy, ou Robocopy, que é um diretório de linha de comando e um conjunto de comandos de replicação de arquivos para o Microsoft Windows. Para conhecer os procedimentos detalhados sobre como usar o Robocopy para migrar o armazenamento de arquivos para o FSx para Windows File Server, consulte Como migrar arquivos atuais para o FSx para Windows File Server usando o Robocopy.

Práticas recomendadas para migrar o armazenamento de arquivos atual para o FSx para Windows File Server

Para migrar grandes quantidades de dados para o FSx para Windows File Server o mais rápido possível, use sistemas de arquivos do Amazon FSx configurados com armazenamento em unidade de estado sólido (SSD). Após a migração, você pode mover os dados para sistemas de arquivos do Amazon FSx usando armazenamento em unidade de disco rígido (HDD), se esta for a melhor solução para sua aplicação.

Para mover dados de um sistema de arquivos do Amazon FSx usando armazenamento SDD para armazenamento em HDD, execute as etapas a seguir. (Observe que os sistemas de arquivos HDD têm uma capacidade mínima de armazenamento de 2 TB e não é possível alterar a capacidade de armazenamento ao ser feita a restauração com base em um backup.)

1. Faça um backup do sistema de arquivos SSD. Para ter mais informações, consulte Como criar backups iniciados pelo usuário.
2. Restaure o backup em um sistema de arquivos usando o armazenamento HDD. Para ter mais informações, consulte Como restaurar backups.

Como migrar arquivos atuais para o FSx para Windows File Server usando o AWS DataSync

Recomendamos usar AWS DataSync para transferir dados entre sistemas de arquivos FSx for Windows File Server. DataSync é um serviço de transferência de dados que simplifica, automatiza e acelera a movimentação e a replicação de dados entre sistemas de armazenamento locais e outros serviços de AWS armazenamento pela 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.

DataSync suporta a cópia de listas de controle de acesso (ACLs) NTFS e também suporta a cópia de informações de controle de auditoria de arquivos, também conhecidas como listas de controle de acesso (SACLs) do sistema NTFS, que são usadas pelos administradores para controlar o registro de auditoria das tentativas do usuário de acessar arquivos.

Você pode usar DataSync para transferir arquivos entre dois sistemas de arquivos FSx for Windows File Server e também mover dados para um sistema de arquivos em uma conta AWS ou Região da AWS diferente. Você pode usar DataSync com o FSx for Windows File Server 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 AWS DataSync, um local para FSx for Windows File Server é um endpoint para um FSx for Windows File Server. Você pode transferir arquivos entre um local para o FSx para Windows e um local para outros sistemas de arquivos. Para obter informações, consulte Trabalhar com locais no Guia do usuário do AWS DataSync .

DataSync acessa seu FSx for Windows File Server usando o protocolo Server Message Block (SMB). Ele se autentica com o nome de usuário e a senha que você configura no AWS DataSync console ou AWS CLI.

Pré-requisitos

Para migrar dados para a configuração do Amazon FSx for Windows File Server, 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.

Se você estiver realizando uma grande migração de dados ou uma migração envolvendo muitos arquivos pequenos, recomendamos usar um sistema de arquivos do Amazon FSx com tipo de armazenamento SSD. Isso ocorre porque DataSync as tarefas envolvem varreduras de metadados de arquivos que podem esgotar os limites de IOPS de disco dos sistemas de arquivos HDD, causando migrações de longa duração e impacto no desempenho do sistema de arquivos. Para obter mais informações, consulte: Práticas recomendadas para migrar o armazenamento de arquivos atual para o FSx para Windows File Server.

Se seu conjunto de dados consistir principalmente em arquivos pequenos, contagens de arquivos na casa dos milhões ou se você tiver mais largura de banda de rede disponível do que uma única

DataSync tarefa do que consumir, você também poderá acelerar suas transferências de dados com uma arquitetura escalável. Para obter mais informações, consulte: Como acelerar suas transferências de dados com arquiteturas de AWS DataSync expansão horizontal.

Você pode monitorar a utilização de E/S de disco do sistema de arquivos usando Métricas de performance do FSx.

Etapas básicas para migrar arquivos usando DataSync

Para transferir arquivos de um local de origem para um local de destino usando DataSync, siga as seguintes etapas básicas:

- Faça download e implante um agente em seu ambiente e ative-o.
- Crie e configure um local de origem e destino.
- Crie e configure uma tarefa.
- Execute a tarefa para transferir arquivos da origem para o destino.

Para saber como transferir arquivos de um sistema de arquivos local existente para seu FSx for Windows File Server, consulte Transferência de dados entre armazenamento autogerenciado e, Criação de um local para SMB AWS e Criação de um local para o Amazon FSx for Windows File Server no Guia do usuário.AWS DataSync

Para saber como transferir arquivos de um sistema de arquivos atual na nuvem para o FSx para Windows File Server, consulte Implantar o agente como uma instância do Amazon EC2 no Guia do usuário do AWS DataSync .

Como migrar entre dois sistemas de arquivos do Amazon FSx

Você pode usar DataSync para migrar dados entre dois sistemas de arquivos Amazon FSx. Isso pode ser útil se você precisar mover sua workload de um sistema de arquivos atual para um novo sistema de arquivos com uma configuração diferente, como de uma configuração single-AZ para uma configuração multi-AZ. Você também pode usar DataSync para dividir sua carga de trabalho entre dois sistemas de arquivos.

Veja um exemplo de visão geral do processo de migração:

1. Crie DataSync locais para os sistemas de arquivos de origem e destino. A origem e o destino precisam pertencer ao mesmo domínio do Active Directory (AD) ou ter uma relação de confiança do AD entre seus domínios.

2. Crie e configure uma DataSync tarefa para transferir dados da origem para o destino. Você pode executar a tarefa como uma instância única ou definir a tarefa para ser executada automaticamente de acordo com uma programação configurada por você.
3. Depois que a tarefa for concluída com êxito, os dados do sistema de arquivos de destino serão uma cópia exata da origem. Você precisará pausar temporariamente qualquer atividade de gravação ou de atualização de arquivos no sistema de arquivos de origem para concluir a tarefa. Em seguida, você pode mudar para o sistema de arquivos de destino e excluir o sistema de arquivos de origem.

Antes de migrar do seu sistema de arquivos de produção, você pode testar o processo de migração em um sistema de arquivos restaurado com base em um backup recente. Isso permite estimar quanto tempo leva o processo de transferência de dados e solucionar DataSync erros com antecedência.

Para minimizar o tempo de transição, você pode executar DataSync tarefas com antecedência, movendo a maioria dos dados do sistema de arquivos de origem para o sistema de arquivos de destino. Depois de interromper o tráfego para o sistema de arquivos de origem, você pode executar uma transferência de tarefa final para sincronizar todos os dados que foram atualizados recentemente desde que você interrompeu o tráfego e, em seguida, mudar para o sistema de arquivos de destino.

Você pode configurar DataSync tarefas para serem executadas somente em determinados diretórios ou para incluir ou excluir determinados caminhos. Isso pode ser útil se você estiver executando várias tarefas em paralelo ou se quiser migrar um subconjunto dos dados.

Você pode criar um alias de DNS no sistema de arquivos de destino que seja igual ao nome DNS do sistema de arquivos de origem. Isso permite que os usuários finais e as aplicações continuem acessando os dados do arquivo usando o nome DNS do sistema de arquivos de origem. Para obter mais informações sobre como configurar um alias de DNS, consulte: Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos.

Ao realizar esse tipo de migração, recomendamos o seguinte:

- Programe a migração para evitar backups do sistema de arquivos, a janela de manutenção semanal e trabalhos `Data Deduplication`. Especificamente, recomendamos desativar o trabalho `Data Deduplication GarbageCollection` se ele coincidir com a migração planejada.

- Use um tipo de armazenamento SSD para os sistemas de arquivos de origem e de destino. Você pode alternar entre os tipos de armazenamento HDD e SSD ao restaurar com base em backup. Para obter mais informações, consulte: Como migrar o armazenamento de arquivos atual para o FSx para Windows File Server.
- Configure os sistemas de arquivos de origem e destino com capacidade de throughput suficiente para a quantidade de dados que você precisa transferir. Durante os processos de DataSync tarefas, monitore a utilização do desempenho dos sistemas de arquivos de origem e de destino. Para obter mais informações, consulte: Monitoramento de métricas com a Amazon CloudWatch.
- Configure o DataSync monitoramento para ajudar você a entender o progresso das tarefas em andamento. Você também pode enviar DataSync registros para o grupo Amazon CloudWatch Logs para ajudá-lo a depurar suas tarefas caso encontre algum erro.

Como migrar arquivos atuais para o FSx para Windows File Server usando o Robocopy

Deenvolvido no Microsoft Windows Server, o Amazon FSx para Windows File Server permite que você migre totalmente conjuntos de dados atuais para sistemas de arquivos do Amazon FSx. Você pode migrar os dados de cada arquivo. Você também pode migrar todos os metadados de arquivos relevantes, incluindo atributos, carimbos de data e hora, listas de controle de acesso (ACLs), informações do proprietário e informações de auditoria. Com esse suporte total à migração, o Amazon FSx permite a transferência de workloads e aplicações baseadas no Windows que dependem desses conjuntos de dados de arquivos para a Nuvem Amazon Web Services.

Use os tópicos a seguir como guia no processo de cópia de dados de arquivos atuais. Ao realizar essa cópia, você preserva todos os metadados de arquivos dos datacenters on-premises ou dos servidores de arquivos autogerenciados no Amazon EC2.

Pré-requisitos

Antes de começar, faça o seguinte:

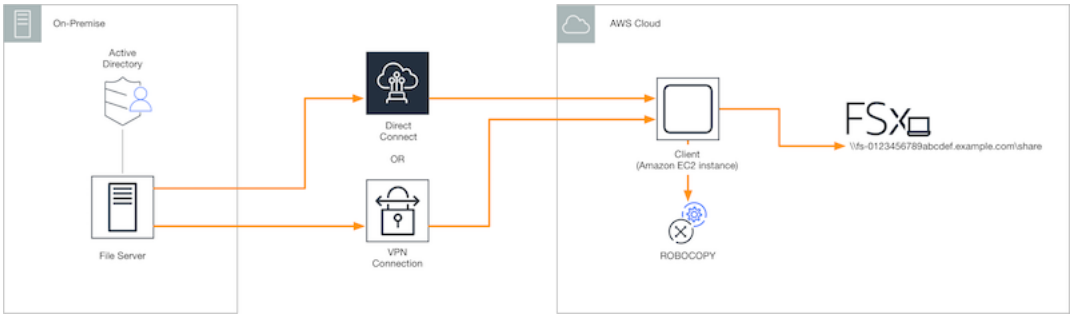
- Estabeleça conectividade de rede (usando AWS Direct Connect nossa VPN) entre seu Active Directory local e a VPC na qual você deseja criar o sistema de arquivos Amazon FSx.
- Crie uma conta de serviço no Active Directory com permissões delegadas para associar computadores ao domínio. Para obter mais informações, consulte Delegar privilégios à conta de serviço no Guia de administração do AWS Directory Service .

- Crie um sistema de arquivos do Amazon FSx, associado ao seu diretório autogerenciado (on-premises) do Microsoft AD.
- Observe a localização (por exemplo,`\\Source\Share`) do compartilhamento de arquivos (local ou interno AWS) que contém os arquivos existentes que você deseja transferir para o Amazon FSx.
- Observe a localização (por exemplo, `\\Target\Share`) do compartilhamento de arquivos no sistema de arquivos do Amazon FSx para o qual você deseja transferir os arquivos atuais.

A tabela a seguir resume os requisitos de acessibilidade do sistema de arquivos de origem e de destino para três modelos de acesso do usuário da migração.

Modelo de acesso do usuário da migração	Requisitos de acessibilidade do sistema de arquivos de origem	Requisitos de acessibilidade do servidor de arquivos do FSx de destino
Modelo de permissões diretas de leitura/gravação	O usuário precisa ter pelo menos permissões de leitura (ACLs do NTFS) nos arquivos e pastas que estão sendo migrados.	O usuário precisa ter pelo menos permissões de gravação (ACLs do NTFS) nos arquivos e pastas que estão sendo migrados.
Modelo de privilégios de backup/restauração para substituição das permissões de acesso	O usuário precisa ser membro do grupo Operadores de Backup do Active Directory local e usar a sinalização /b com. RoboCopy	O usuário precisa ser membro do grupo de administradores do sistema de arquivos Amazon FSx* e usar a bandeira /b com. RoboCopy
Modelo de privilégio de administrador de domínio (completo) para substituição das permissões de acesso	O usuário precisa ser membro do grupo de Administradores de domínio do Active Directory on-premises.	O usuário precisa ser membro do grupo de administradores do sistema de arquivos Amazon FSx* e usar a bandeira /b com RoboCopy

> **Note**
>
> * Para sistemas de arquivos unidos a um Microsoft AD AWS gerenciado, o grupo de administradores do sistema de arquivos Amazon FSx é Delegated AWS FSx Administrators. No Microsoft AD autogerenciado, o grupo de administradores do sistema de arquivos do Amazon FSx é Administradores de domínio ou o grupo personalizado que você especificou para administração ao criar o sistema de arquivos.



Como migrar arquivos atuais para o Amazon FSx usando o Robocopy

Você pode migrar arquivos atuais para o Amazon FSx usando o procedimento a seguir.

Migrar arquivos atuais para o Amazon FSx

1. Inicie uma instância do Amazon EC2 do Windows Server 2016 na mesma Amazon VPC do sistema de arquivos do Amazon FSx.
2. Conecte-se à sua instância Amazon EC2. Para obter mais informações, consulte Conectar-se à sua instância do Windows no Guia do usuário do Amazon EC2 para instâncias do Windows.
3. Abra o prompt de comando e mapeie o compartilhamento do arquivo de origem em seu servidor de arquivos existente (local ou interno AWS) para uma letra de drive (por exemplo, *Y*:) da seguinte maneira. Como parte disso, você fornece credenciais para um membro do grupo de Administradores de domínio do Active Directory on-premises.

```
C:\>net use Y: \\fileserver1.mydata.com\localdata /user:mydata.com\Administrator
Enter the password for 'fileserver1.mydata.com': _

Drive Y: is now connected to \\fileserver1.mydata.com\localdata.

The command completed successfully.
```

4. Mapeie o compartilhamento de arquivos de destino do sistema de arquivos do Amazon FSx para uma letra de unidade diferente (por exemplo, *Z*:) na instância do Amazon EC2 como mostrado a seguir. Como parte disso, você fornece credenciais para a conta de um usuário que é membro do grupo de administradores de domínio do Active Directory on-premises e do grupo de administradores do sistema de arquivos do Amazon FSx. Para sistemas de arquivos associados a um Microsoft AD AWS gerenciado, esse grupo é **`AWS Delegated FSx Administrators`**. No Microsoft AD autogerenciado, esse grupo é **`Domain Admins`** ou o grupo personalizado que você especificou para a administração quando criou o sistema de arquivos.

   Para obter mais informações, consulte a tabela de requisitos de acessibilidade do sistema de arquivos de origem e destino nos Pré-requisitos.

   ```
   C:\>net use Z: \\amznfsxabcdef1.mydata.com\share /user:mydata.com\Administrator
   Enter the password for 'amznfsxabcdef1.mydata.com': _

   Drive Z: is now connected to \\amznfsxabcdef1.mydata.com\share.

   The command completed successfully.
   ```

5. Escolha Executar como administrador no menu de contexto. Abra o prompt de comando ou o Windows PowerShell como administrador e execute o seguinte comando do Robocopy para copiar os arquivos do compartilhamento de origem para o compartilhamento de destino.

   O comando ROBOCOPY é um utilitário flexível de transferência de arquivos com várias opções para controlar o processo de transferência de dados. Por causa desse processo de comando do ROBOCOPY, todos os arquivos e diretórios do compartilhamento de origem são copiados para o compartilhamento de destino do Amazon FSx. A cópia preserva ACLs do NTFS de arquivos e pastas, atributos, carimbos de data e hora, informações do proprietário e informações de auditoria.

   ```
   robocopy Y:\ Z:\ /copy:DATSOU /secfix /e /b /MT:8
   ```

   O comando de exemplo anterior usa os seguintes elementos e opções:

   - Y: refere-se ao compartilhamento de origem localizado na floresta mydata.com do Active Directory on-premises.
   - Z: refere-se ao compartilhamento de destino\\amznfsxabcdef1.mydata.com\share no Amazon FSx.

- /copy: especifica as seguintes propriedades do arquivo a serem copiadas:
  - D: dados
  - A: atributos
  - T: carimbos de data e hora
  - S: ACLs do NTFS
  - O: informações do proprietário
  - U: informações de auditoria.
- /secfix: corrige a segurança de todos os arquivos, mesmo dos ignorados.
- /e: copia subdiretórios, inclusive os vazios.
- /b: usa o privilégio de backup e restauração no Windows para copiar arquivos mesmo que suas ACLs do NTFS neguem permissões ao usuário atual.
- /MT:8: especifica quantos threads devem ser usados para a execução de cópias com vários threads.

> **Note**
>
> Se você estiver copiando arquivos grandes em uma conexão lenta ou não confiável, poderá habilitar o modo reiniciável usando a opção /zb com a opção robocopy no lugar da opção /b. Com o modo reiniciável, se a transferência de um arquivo grande for interrompida, uma operação subsequente do Robocopy poderá prosseguir no meio da transferência em vez de ser necessário copiar novamente o arquivo inteiro desde o início. A ação de habilitar o modo reiniciável pode reduzir a velocidade de transferência de dados.

Como migrar configurações de compartilhamento de arquivos para o Amazon FSx

Você pode migrar uma configuração de compartilhamento de arquivos atual para o Amazon FSx usando o procedimento a seguir. Nesse procedimento, o servidor de arquivos de origem é o servidor de arquivos cuja configuração de compartilhamento de arquivos você deseja migrar para o Amazon FSx.

> **Note**
>
> Primeiro, migre os arquivos para o Amazon FSx antes de migrar a configuração de compartilhamento de arquivos. Para ter mais informações, consulte Como migrar o armazenamento de arquivos atual para o FSx para Windows File Server.

Migrar compartilhamentos de arquivos atuais para o FSx for Windows File Server

1. No servidor de arquivos de origem, escolha Executar como administrador no menu de contexto. Abra o Windows PowerShell como administrador.
2. Exporte os compartilhamentos de arquivos do servidor de arquivos de origem para um arquivo chamado `SmbShares.xml` executando os seguintes comandos no PowerShell. Substitua F: neste exemplo pela letra da unidade do servidor de arquivos do qual você está exportando compartilhamentos de arquivos.

   ```
   $shareFolder = Get-SmbShare -Special $false | ? { $_.Path -like “F:\*” }
   $shareFolder | Export-Clixml -Path F:\SmbShares.xml
   ```

3. Edite o arquivo `SmbShares.xml`, substituindo todas as referências a F: (a letra da sua unidade) por D:\share, pois os sistemas de arquivos do Amazon FSx residem em D:\share.
4. Importe a configuração de compartilhamento de arquivos atual para o FSx para Windows File Server. Em um cliente que tenha acesso ao sistema de arquivos do Amazon FSx de destino e ao servidor de arquivos de origem, copie a configuração de compartilhamento de arquivos salva. Em seguida, importe-a para uma variável usando o comando a seguir.

   ```
   $shares = Import-Clixml -Path F:\SmbShares.xml
   ```

5. Prepare o objeto de credencial necessário para criar os compartilhamentos de arquivos no servidor de arquivos do FSx para Windows File Server usando uma das opções a seguir.

   Para gerar o objeto de credencial de forma interativa, use o comando a seguir.

   ```
   $credential = Get-Credential
   ```

   Para gerar o objeto de credencial usando um AWS Secrets Manager recurso, use o comando a seguir.

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

6. Migre a configuração de compartilhamento de arquivos para o servidor de arquivos do Amazon FSx usando o script a seguir.

```
$FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",
 "ConcurrentUserLimit", "CATimeout", "FolderEnumerationMode", "CachingMode",
 "FullAccess", "ChangeAccess", "ReadAccess", "NoAccess", "SecurityDescriptor",
 "Path", "Name", "EncryptData")
ForEach ($item in $shares) {
    $param = @{};
    Foreach ($property in $item.psObject.properties) {
        if ($property.Name -In $FSxAcceptedParameters) {
            $param[$property.Name] = $property.Value
        }
    }
    Invoke-Command -ConfigurationName FSxRemoteAdmin -ComputerName
 amznfsxxxxxxxxx.corp.com -ErrorVariable errmsg -ScriptBlock { New-FSxSmbShare -
Credential $Using:credential @Using:param }
}
```

Como migrar a configuração de DNS para usar o Amazon FSx

O FSx para Windows File Server fornece um nome de Sistema de Nomes de Domínio (DNS) padrão para cada sistema de arquivos que você pode usar para acessar os dados no sistema de arquivos. Você também pode acessar os sistemas de arquivos usando qualquer nome DNS de sua escolha ao configurar o nome DNS alternativo como um alias de DNS para o sistema de arquivos do Amazon FSx.

Com aliases de DNS, você pode continuar usando os nomes DNS atuais para acessar dados armazenados no Amazon FSx ao migrar o armazenamento do sistema de arquivos on-premises para o Amazon FSx. Isso ajuda a eliminar a necessidade de atualizar quaisquer ferramentas ou aplicações que usem seus nomes DNS na migração para o Amazon FSx. Você pode associar aliases de DNS aos sistemas de arquivos do FSx para Windows File Server atuais quando criar novos sistemas de arquivos e quando criar um novo sistema de arquivos com base em um backup.

Você pode associar até 50 aliases de DNS a um sistema de arquivos a qualquer momento. Para ter mais informações, consulte Como gerenciar aliases de DNS.

Um nome de alias de DNS deve atender aos seguintes requisitos:

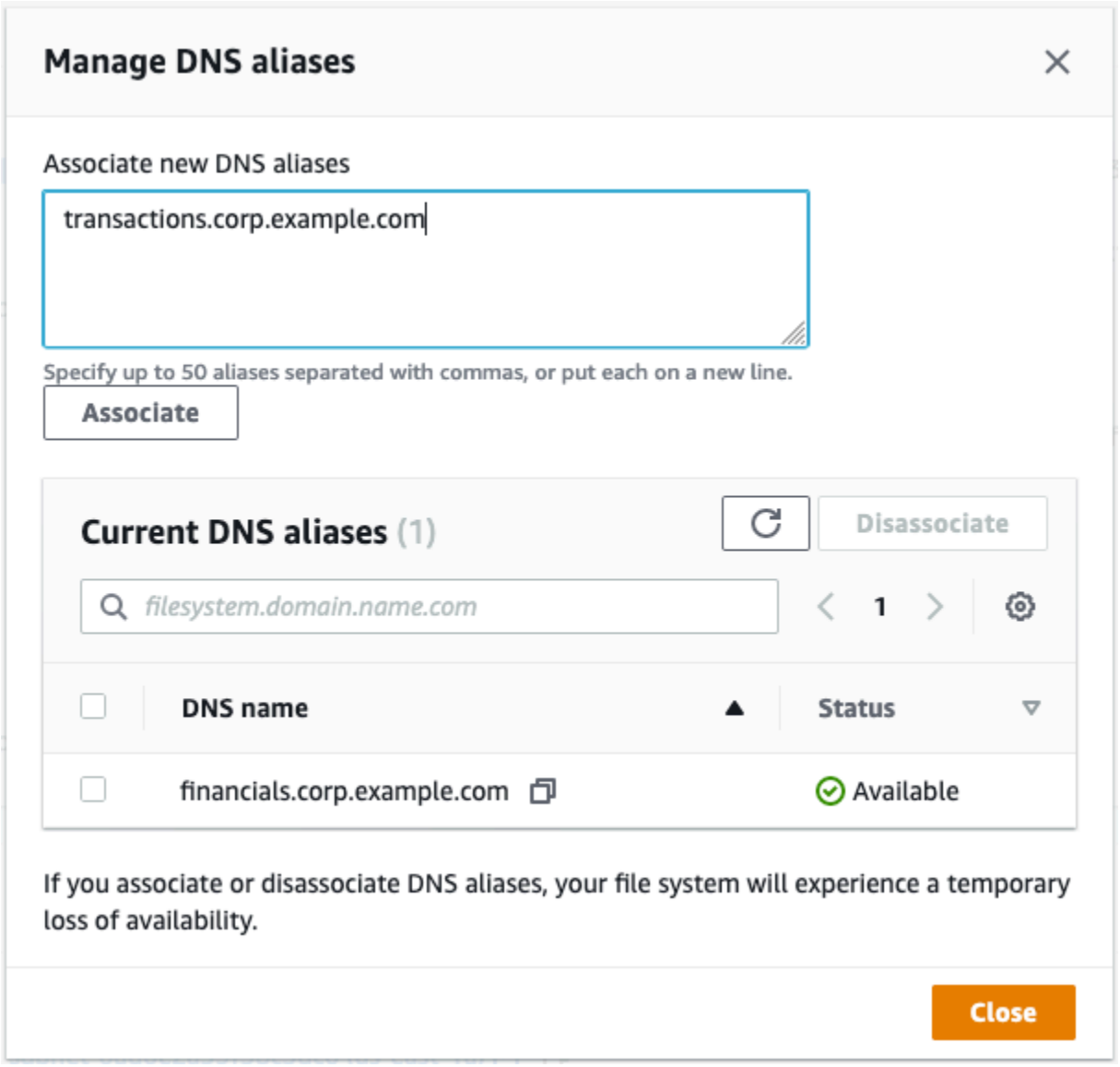
- Deve ser formatado como um fully qualified domain name (FQDN - nome de domínio totalmente qualificado), por exemplo, `accounting.example.com`.
- Pode conter caracteres alfanuméricos e o hífen (-).
- Não pode começar ou terminar com um hífen (-).
- Pode começar com um caractere numérico.

Para nomes de alias DNS, o Amazon FSx armazena caracteres alfabéticos como letras minúsculas (a-z), independentemente de como elas são especificadas: como letras maiúsculas, letras minúsculas ou as letras correspondentes em códigos de escape.

Os procedimentos a seguir descrevem como associar aliases de DNS aos sistemas de arquivos atuais do FSx para Windows File Server usando o console do Amazon FSx, a CLI e a API. Para obter mais informações sobre a associação de aliases de DNS na criação de sistemas de arquivos, incluindo sistemas de arquivos com base em um backup, consulte Associando aliases de DNS a sistemas de arquivos.

Associar aliases de DNS a um sistema de arquivos atual (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 Windows ao qual você deseja associar os aliases de DNS.
3. Na guia Rede e segurança, escolha Gerenciar em Aliases de DNS para abrir a caixa de diálogo Gerenciar aliases de DNS.



4. Na caixa Associar novos aliases, insira os aliases de DNS que você deseja associar.
5. Escolha Associar para adicionar os aliases ao sistema de arquivos.

   Você pode monitorar o status dos aliases que você acabou de associar na lista de aliases atuais. Quando o status indica Disponível, o alias é associado ao sistema de arquivos (um processo que pode levar até 2,5 minutos).

Associar aliases de DNS a um sistema de arquivos atual (CLI)

- Use o comando `associate-file-system-aliases` CLI ou a operação da AssociateFileSystemAliasesAPI para associar aliases de DNS a um sistema de arquivos existente.

A solicitação da CLI a seguir associa dois aliases ao sistema de arquivos especificado.

```
aws fsx associate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com transfers.corp.example.com
```

A resposta mostra o status dos aliases que o Amazon FSx está associando ao sistema de arquivos.

```
{
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": CREATING
          },
          {
              "Name": "transfers.corp.example.com",
              "Lifecycle": CREATING
          }
      ]
  }
```

Para monitorar o status dos aliases que você está associando, use o comando `describe-file-system-aliases` CLI (DescribeFileSystemAliasesé a operação de API equivalente). Quando o `Lifecycle` de alias tem um valor de DISPONÍVEL, você pode usá-lo para acessar o sistema de arquivos (um processo que pode levar até 2,5 minutos).

Substituição para o Amazon FSx

Para mudar para o sistema de arquivos do FSx para Windows File Server, execute as seguintes etapas:

- Preparar para a mudança.
  - Desconecte temporariamente os clientes SMB do sistema de arquivos original.
  - Execute uma sincronização final da configuração de arquivos e do compartilhamento de arquivos.

- Configure nomes de entidades principais de serviço (SPNs) para o sistema de arquivos do Amazon FSx.
- Atualize os registros CNAME do DNS para que apontem para o sistema de arquivos do Amazon FSx.

Os procedimentos para a execução de cada uma dessas etapas são fornecidos nas seções a seguir.

Tópicos

Preparar a substituição para o Amazon FSx

Para preparar a substituição para o sistema de arquivos do Amazon FSx, você deve fazer o seguinte:

- Desconecte todos os clientes que gravam no sistema de arquivos original.
- Execute uma sincronização final de arquivos usando o AWS DataSync Robocopy. Para ter mais informações, consulte Como migrar o armazenamento de arquivos atual para o FSx para Windows File Server.
- Execute uma sincronização final da configuração do compartilhamento de arquivos. Para ter mais informações, consulte Como migrar configurações de compartilhamento de arquivos para o Amazon FSx.

Configurar SPNs para autenticação Kerberos

Recomendamos que você use autenticação e criptografia baseadas no Kerberos em trânsito com o Amazon FSx. O Kerberos oferece a autenticação mais segura para clientes que acessam o sistema de arquivos. Para habilitar a autenticação Kerberos para clientes que acessam o Amazon FSx usando um alias de DNS, você deve adicionar nomes de entidades principais de serviço (SPNs) que correspondam ao alias de DNS no objeto de computador do Active Directory do sistema de arquivos do Amazon FSx.

Existem dois SPNs necessários para autenticação Kerberos.

```
HOST/alias
```

```
HOST/alias.domain
```

Por exemplo, se o alias é `finance.domain.com`, os dois SPNs necessários são os seguintes.

```
HOST/finance
HOST/finance.domain.com
```

Um SPN só pode ser associado a um único objeto de computador do Active Directory de cada vez. Se houver SPNs para o nome DNS configurado para o objeto de computador do Active Directory do sistema de arquivos original, você deverá excluí-los antes de criar SPNs para o sistema de arquivos do Amazon FSx.

Os procedimentos a seguir descrevem como encontrar quaisquer SPNs atuais, excluí-los e criar SPNs para o objeto de computador do Active Directory do sistema de arquivos do Amazon FSx.

Para instalar o módulo necessário do PowerShell Active Directory

1. Faça logon em uma instância do Windows associada ao Active Directory à qual o sistema de arquivos do Amazon FSx está associado.
2. Abra PowerShell como administrador.
3. Instale o módulo do PowerShell Active Directory usando o comando a seguir.

   ```
   Install-WindowsFeature RSAT-AD-PowerShell
   ```

Encontrar e excluir SPNs de alias de DNS atuais no objeto de computador do Active Directory do sistema de arquivos original

1. Encontre todos os SPNs atuais usando os comandos a seguir. Substitua *alias_fqdn* pelo alias de DNS que você associou ao sistema de arquivos em Como migrar a configuração de DNS para usar o Amazon FSx.

   ```
   ## Find SPNs for original file system's AD computer object
   $ALIAS = "alias_fqdn"
   SetSPN /Q ("HOST/" + $ALIAS)
   SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
   ```

2. Exclua os SPNs HOST atuais retornados na etapa anterior usando o exemplo de script a seguir.

- Substitua *alias_fqdn* pelo alias de DNS completo que você associou ao sistema de arquivos em Como migrar a configuração de DNS para usar o Amazon FSx.
- Substitua *file_system_DNS_name* pelo nome DNS do sistema de arquivos original.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. Repita essas etapas para cada alias de DNS que você associou ao sistema de arquivos em Como migrar a configuração de DNS para usar o Amazon FSx.

Definir SPNs no objeto de computador do Active Directory do sistema de arquivos do Amazon FSx

1. Defina novos SPNs para o sistema de arquivos do Amazon FSx executando os comandos a seguir.

   - Substitua *file_system_DNS_name* pelo nome DNS que o Amazon FSx atribuiu ao sistema de arquivos.

     Para encontrar o nome DNS do sistema de arquivos no console do Amazon FSx, escolha Sistemas de arquivos e escolha o sistema de arquivos. Escolha o painel Rede e segurança da página de detalhes do sistema de arquivos. Você também pode obter o nome DNS na resposta da operação da API de DescribeFilesistemas.
   - Substitua *alias_fqdn* pelo alias de DNS completo que você associou ao sistema de arquivos em Como migrar a configuração de DNS para usar o Amazon FSx.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
```

```
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> A configuração de um SPN para o sistema de arquivos do Amazon FSx apresentará falha se existir um SPN para o alias de DNS no AD do objeto de computador do sistema de arquivos original. Para obter informações sobre como encontrar e excluir SPNs atuais, consulte Encontrar e excluir SPNs de alias de DNS atuais no objeto de computador do Active Directory do sistema de arquivos original.

2. Verifique se os novos SPNs estão configurados para o alias de DNS usando o exemplo de script a seguir. Certifique-se de que a resposta inclua dois SPNs HOST, `HOST/`*`alias`* e `HOST/`*`alias_fqdn`*.

   Substitua *`file_system_DNS_name`* pelo nome DNS que o Amazon FSx atribuiu ao sistema de arquivos. Para encontrar o nome DNS do sistema de arquivos no console do Amazon FSx, escolha Sistemas de arquivos, escolha o sistema de arquivos e, em seguida, escolha o painel Rede e segurança na página de detalhes do sistema de arquivos.

   Você também pode obter o nome DNS na resposta da operação da API de DescribeFilesistemas.

   ```
   ## Verify SPNs on FSx file system AD computer object
   $FileSystemDnsName = "file_system_dns_name"
   $FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
   [0].Name.Split(".")[0]
   $FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
   SetSpn /L ${FSxAdComputer}.Name
   ```

3. Repita as etapas anteriores para cada alias de DNS que você associou ao sistema de arquivos em Como migrar a configuração de DNS para usar o Amazon FSx.

> **Note**
>
> Você pode aplicar a autenticação e a criptografia Kerberos em trânsito com clientes que se conectam ao sistema de arquivos usando aliases de DNS ao definir os seguintes Group Policy Objects (GPOs - Objetos de política de grupo) no Active Directory:
>
> - Restringir NTLM: tráfego NTLM de saída para servidores remotos
> - Restringir NTLM: adicionar exceções de servidor remoto para autenticação NTLM
>
> Para obter mais informações, consulte Como reforçar a autenticação do Kerberos usando GPOs em Passo a passo 5: usar aliases de DNS para acessar o sistema de arquivos.

Atualizar os registros CNAME do DNS para o sistema de arquivos do Amazon FSx

Depois de configurar adequadamente os SPNs do sistema de arquivos, mude para o Amazon FSx substituindo cada registro DNS resolvido no sistema de arquivos original por um registro DNS resolvido com o nome DNS padrão do sistema de arquivos do Amazon FSx.

Para instalar os PowerShell cmdlets necessários

1. Faça login em uma instância do Windows associada ao Active Directory à qual seu sistema de arquivos Amazon FSx está associado como um usuário que é membro de um grupo que tem permissões de administração de DNS (administradores de sistema de nomes de domínio AWS delegados no Microsoft Active Directory AWS gerenciado e administradores de domínio ou outro grupo ao qual você delegou permissões de administração de DNS em seu Active Directory autogerenciado)

   Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
2. Abra PowerShell como administrador.
3. O módulo do servidor PowerShell DNS é necessário para executar as instruções neste procedimento. Instale-o usando o comando a seguir.

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

Atualizar um registro CNAME do DNS atual

1. O script a seguir atualiza todos os registros CNAME do DNS atuais do *alias_fqdn* para o objeto de computador do sistema de arquivos do Amazon FSx. Se nenhum for encontrado, ele cria um novo registro CNAME do DNS para o alias de DNS *alias_fqdn* que é resolvido para o nome DNS padrão do sistema de arquivos do Amazon FSx.

   Para executar o script:

   - Substitua *alias_fqdn* pelo alias de DNS que você associou ao sistema de arquivos.
   - Substitua *file_system_DNS_name* pelo nome DNS padrão que o Amazon FSx atribuiu ao sistema de arquivos.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name)[0]

Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

2. Repita a etapa anterior para cada alias de DNS que você associou ao sistema de arquivos em Como migrar a configuração de DNS para usar o Amazon FSx.

Como usar o FSx para Windows File Server com o Microsoft SQL Server

O Microsoft SQL Server de alta disponibilidade (HA) é normalmente implantado em vários nós de banco de dados em um cluster de failover do Windows Server (WSFC), com cada nó tendo acesso ao armazenamento de arquivos compartilhado. Você pode usar o FSx para Windows File Server como armazenamento compartilhado para implantações de alta disponibilidade (HA) do Microsoft SQL Server de duas maneiras: como armazenamento para arquivos de dados ativos e como testemunha de compartilhamento de arquivos SMB.

> **Note**
>
> Atualmente, o Amazon FSx não é compatível com o recurso IFI (Inicialização Instantânea de Arquivo) do Microsoft SQL Server.

O armazenamento SSD é recomendado para o SQL Server. O armazenamento SSD foi projetado para as workloads de mais alta performance e mais sensíveis à latência, incluindo bancos de dados.

Para obter informações sobre como usar o Amazon FSx para reduzir a complexidade e os custos de suas implantações de alta disponibilidade do SQL Server, consulte as seguintes postagens no AWS Storage Blog:

- Simplify your Microsoft SQL Server high availability deployments using Amazon FSx para Windows File Server
- Optimizing cost for your high availability SQL Server deployments on AWS
- Simplify SQL Server Always On deployments with AWS Launch Wizard and Amazon FSx

Como usar o Amazon FSx para arquivos de dados ativos do SQL Server

O Microsoft SQL Server pode ser implantado com um compartilhamento de arquivos SMB como opção de armazenamento para arquivos de dados ativos. O Amazon FSx é otimizado para fornecer armazenamento compartilhado para bancos de dados do SQL Server, e é compatível com compartilhamentos de arquivos continuamente disponíveis (CA). Esses compartilhamentos

de arquivos são projetados para aplicações como o SQL Server, que exigem acesso ininterrupto a dados de arquivos compartilhados. Embora você possa criar compartilhamentos CA em sistemas de arquivos single-AZ 2, é necessário usar compartilhamentos CA em sistemas de arquivos multi-AZ para todas as implantações do SQL Server, sejam elas HA ou não.

Criar um compartilhamento continuamente disponível

Você pode criar compartilhamentos CA usando a CLI do Amazon FSx para gerenciamento remoto no PowerShell. Para especificar que o compartilhamento é um compartilhamento continuamente disponível, use a opção `New-FSxSmbShare` com a opção `-ContinuouslyAvailable` definida como `$True`. Para saber mais sobre como criar um novo compartilhamento CA, consulte Criação de compartilhamento continuamente disponível (CA).

Configurar as definições de tempo limite do SMB

Conforme descrito em Processo de failover para o FSx para Windows File Server, o failover e o failback para multi-AZ podem resultar em pausas de E/S que normalmente são concluídas em menos de 30 segundos. A aplicação do SQL Server pode ter uma sensibilidade diferente às configurações de tempo limite, dependendo de como ela esteja configurada.

Você pode ajustar o tempo limite da sessão de configuração do cliente SMB para garantir que sua aplicação seja resistente a falhas no sistema de arquivos multi-AZ. Você pode testar o comportamento da sua aplicação durante os failovers atualizando a capacidade de throughput do seu sistema de arquivos, o que inicia um failover e um failback automáticos.

Como usar o Amazon FSx como testemunha de compartilhamento de arquivos SMB

As implantações de cluster de failover do Windows Server normalmente implantam uma testemunha de compartilhamento de arquivos SMB para manter o quórum dos recursos do cluster. Os compartilhamentos de arquivos de testemunhas requerem apenas uma pequena quantidade de armazenamento para informações de quórum. Os sistemas de arquivos do Amazon FSx podem ser usados como testemunha de compartilhamento de arquivos SMB para implantações do cluster de failover do Windows Server.

Como usar o FSx para Windows File Server com o Amazon Kendra

O Amazon Kendra é um serviço de pesquisa altamente preciso e inteligente. Os sistemas de arquivos do FSx para Windows File Server podem ser usados como fontes de dados para o Amazon Kendra, permitindo que você indexe e pesquise de forma inteligente as informações contidas nos documentos armazenados no sistema de arquivos.

- Para obter mais informações sobre o Amazon Kendra, consulte O que é Amazon Kendra no Guia do desenvolvedor do Amazon Kendra.
- Para obter mais informações sobre como adicionar o sistema de arquivos como uma fonte de dados do Amazon Kendra, consulte Introdução a uma fonte de dados do Amazon FSx (console) no Guia do desenvolvedor do Amazon Kendra.
- Para obter informações da visão geral sobre o Amazon Kendra, consulte o site do Amazon Kendra.
- Para ter uma demonstração sobre como pesquisar o sistema de arquivos usando o Amazon Kendra, consulte Pesquisar com segurança dados não estruturados em sistemas de arquivos Windows com o conector do Amazon Kendra para Amazon FSx para Windows File Server no Blog sobre machine learning da AWS.

Performance do sistema de arquivos

Quando você adiciona um sistema de arquivos do FSx para Windows File Server como fonte de dados, o Amazon Kendra rastreia os arquivos e pastas no sistema de arquivos em uma frequência de sincronização regular para criar e manter seu índice de pesquisa. (Você pode selecionar a frequência de sincronização quando estabelecer a integração.) Essa atividade de acesso a arquivos do Amazon Kendra consumirá recursos do sistema de arquivos, semelhante à atividade das próprias workloads que acessam o sistema de arquivos.

Certifique-se de que o sistema de arquivos esteja configurado com recursos suficientes para que a performance da workload não seja afetada. Especificamente, se você planeja indexar um grande número de arquivos, recomendamos o uso de um sistema de arquivos com o tipo de armazenamento SSD, que oferece throughput máximo e níveis de IOPS para solicitações que precisem acessar os volumes de armazenamento.

Para obter mais informações sobre o modelo de performance do Amazon FSx, consulte Performance do FSx para Windows File Server.

Como proteger seus dados com backups, cópias de sombra e replicação programada

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.
- AWS Backup os backups de seus sistemas de arquivos Amazon FSx fazem parte de uma solução de backup centralizada e automatizada em todos AWS os serviços na nuvem e no local.
- As cópias de sombra do Windows permitem que seus usuários desfaçam facilmente as alterações nos arquivos e comparem as versões dos arquivos, restaurando-os para versões anteriores.
- AWS DataSync a replicação programada do seu sistema de arquivos Amazon FSx para um segundo sistema de arquivos fornece proteção e recuperação de dados.

Tópicos

Trabalhar com backups

Com o Amazon FSx, os backups são file-system-consistent altamente duráveis e incrementais. Cada backup contém todas as informações necessárias para criar um novo sistema de arquivos, restaurando efetivamente um point-in-time instantâneo do sistema de arquivos. Para garantir a consistência do sistema de arquivos, o Amazon FSx usa o Volume Shadow Copy Service (VSS) no Microsoft Windows. Para garantir uma alta durabilidade, o Amazon FSx armazena backups no Amazon Simple Storage Service (Amazon S3).

Os backups do Amazon FSx são incrementais, sejam eles gerados usando o backup diário automático, sejam eles o recurso de backup iniciado pelo usuário. Isso significa que somente os dados do sistema de arquivos que foram alterados após o backup mais recente são salvos. Isso

minimiza o tempo necessário para criar o backup e economiza custos de armazenamento ao não duplicar os dados.

Em algum momento durante o processo de backup, a E/S do armazenamento pode ser suspensa brevemente, normalmente por alguns segundos. Como o serviço VSS precisa liberar todas as gravações em cache para o disco antes de retomar a E/S, a duração da pausa poderá ser maior se a workload tiver uma grande quantidade de operações de gravação por segundo (`DataWriteOperations`). A maioria dos usuários finais e aplicações perceberá essa suspensão de E/S como uma breve pausa de E/S. Suas aplicações podem ter sensibilidade diferente às configurações de tempo limite, dependendo de como estão configuradas.

Criar backups regulares para seu sistema de arquivos é uma prática recomendada que complementa a replicação que o Amazon FSx para Windows File Server realiza para seu sistema de arquivos. Os backups do Amazon FSx ajudam a atender às suas necessidades de retenção e conformidade de backup. Trabalhar com backups do Amazon FSx é fácil, seja para criar backups, copiar um backup, seja para restaurar um sistema de arquivos de um backup ou excluir um backup. Observe que, para visualizar o uso de um único backup do sistema de arquivos, você precisará ativar as tags para esse backup específico e ativar o relatório de faturamento baseado em tags.

Tópicos

Como trabalhar com backups diários automáticos

Por padrão, o Amazon FSx faz um backup diário automático do seu sistema de arquivos. Esses backups diários automáticos ocorrem durante a janela de backup diário estabelecida quando você criou o sistema de arquivos. Ao escolher sua janela de backup diário, recomendamos que seja uma hora do dia conveniente. O ideal é que esse horário esteja fora do horário normal de funcionamento das aplicações que usam o sistema de arquivos.

Os backups diários automáticos são mantidos por um determinado período, conhecido como período de retenção. Ao criar um sistema de arquivos no console do Amazon FSx, o período padrão de retenção de backup diário automático é de 30 dias. O período padrão de retenção é diferente na API e na CLI do Amazon FSx. Você pode definir o período de retenção entre zero e noventa dias. Definir o período de retenção como zero dia desativa os backups diários automáticos. Os backups diários automáticos são excluídos quando o sistema de arquivos é excluído.

> **Note**
>
> Definir o período de retenção como zero dia significa que o backup do sistema de arquivos nunca é realizado automaticamente. É altamente recomendável que você use backups diários automáticos para sistemas de arquivos que tenham qualquer nível de funcionalidade crítica associada a eles.

Você pode usar o AWS CLI ou um dos AWS SDKs para alterar a janela de backup e o período de retenção de backup de seus sistemas de arquivos. Use a operação`UpdateFileSystem` da API ou o comando `update-file-system` da CLI. Para ter mais informações, consulte Passo a passo 3: atualizar um sistema de arquivos existente.

Como trabalhar com backups iniciados pelo usuário

Com o Amazon FSx, você pode fazer backups manuais dos seus sistemas de arquivos a qualquer momento. Você pode fazer isso usando o console Amazon FSx, a API ou o AWS Command Line Interface ()AWS CLI. Os backups iniciados pelo usuário dos sistemas de arquivos do Amazon FSx nunca expiram e ficam disponíveis pelo tempo que você quiser mantê-los. Os backups iniciados pelo usuário são mantidos mesmo depois de você excluir o sistema de arquivos do qual foi feito o backup. Você 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.

Se um backup for iniciado enquanto o sistema de arquivos estiver sendo modificado (como durante uma atualização da capacidade de throughput ou durante a manutenção do sistema de arquivos), a solicitação de backup será colocada na fila e será retomada quando a atividade for concluída.

Como criar backups iniciados pelo usuário

O procedimento a seguir orienta você sobre como criar um backup iniciado pelo usuário no console do Amazon FSx para um sistema de arquivos existente.

Criar um backup do sistema de arquivos iniciado pelo usuário

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel do console, escolha o nome do sistema de arquivos do qual deseja fazer backup.
3. Em Ações, escolha Criar backup.
4. Na caixa de diálogo Criar backup que é aberta, forneça um nome para o backup. Os nomes de backup podem ter no máximo 256 caracteres Unicode, incluindo letras, espaço em branco, números e os caracteres especiais . + - = _ : /
5. Escolha Create backup.

Agora você criou o backup do sistema de arquivos. Você pode encontrar uma tabela de todos os backups no console do Amazon FSx 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.

Usando AWS Backup com o Amazon FSx

AWS Backup é uma forma simples e econômica de proteger seus dados fazendo backup de seus sistemas de arquivos Amazon FSx. AWS Backup é um serviço de backup unificado projetado para simplificar a criação, cópia, 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.
- Copie backups entre AWS regiões e AWS contas.
- Monitore todas as atividades recentes de backup, cópia e restauração.

AWS Backup usa a funcionalidade de backup integrada do Amazon FSx. Os backups feitos do AWS Backup console têm o mesmo nível de consistência e desempenho do sistema de arquivos e

as mesmas opções de restauração dos backups feitos pelo console do Amazon FSx. Os backups obtidos AWS Backup são incrementais em relação a quaisquer outros backups do Amazon FSx que você fizer, sejam eles iniciados pelo usuário ou automáticos.

Se você usa AWS Backup para gerenciar esses backups, obtém funcionalidades adicionais, como opções de retenção ilimitadas e a capacidade de criar backups agendados com a mesma frequência a cada hora. Além disso, AWS Backup mantém seus backups imutáveis mesmo após a exclusão do sistema de arquivos de origem. Isso protege contra exclusões acidentais ou mal-intencionadas.

Os backups feitos pelo Amazon AWS Backup FSx são considerados backups iniciados pelo usuário e contam para a cota de backup iniciada pelo usuário para o Amazon FSx. Você pode ver e restaurar os backups feitos no console, AWS Backup na CLI e na API do Amazon FSx. No entanto, você não pode excluir backups feitos no console, AWS Backup na CLI ou na API do Amazon FSx. Para obter mais informações sobre como usar AWS Backup para fazer backup de seus sistemas de arquivos Amazon FSx, consulte Como trabalhar com sistemas de arquivos Amazon FSx no Guia do desenvolvedor.AWS Backup

Copiar backups

Você pode usar o Amazon FSx para copiar manualmente backups dentro da mesma AWS conta para outra AWS região (cópias entre regiões) ou dentro da mesma região (cópias dentro da AWS região). Você pode fazer cópias entre regiões somente dentro da mesma AWS partição. Você pode criar cópias de backup iniciadas pelo usuário usando o console AWS CLI ou a API do Amazon FSx. Quando você cria uma cópia de backup iniciada pelo usuário, ela é do tipo `USER_INITIATED`.

Você também pode usar AWS Backup para copiar backups entre AWS regiões e AWS contas. AWS Backup é um serviço de gerenciamento de backup totalmente gerenciado que fornece uma interface central para planos de backup baseados em políticas. Com o gerenciamento entre contas, você pode usar automaticamente as políticas de backup para aplicar planos de backup em todas as contas da sua organização.

As cópias de backup entre regiões são particularmente valiosas para a recuperação de desastres entre regiões. Você faz backups e os copia para outra AWS região para que, no caso de um desastre na AWS região principal, você possa restaurar a partir do backup e recuperar rapidamente a disponibilidade na outra AWS região. Você também pode usar cópias de backup para clonar seu conjunto de dados de arquivos em outra AWS região ou dentro da mesma AWS região. Você faz cópias de backup na mesma AWS conta (entre regiões ou dentro da região) usando o console do Amazon FSx ou a API do AWS CLI Amazon FSx. Você também pode usar o AWS Backup para fazer cópias de backup, sob demanda ou com base em políticas.

As cópias de backup entre contas são valiosas para atender aos requisitos de conformidade regulatória para a cópia de backups em uma conta isolada. Eles também fornecem uma camada adicional de proteção de dados para ajudar a evitar a exclusão acidental ou mal-intencionada de backups, a perda de credenciais ou o comprometimento de chaves. AWS KMS Os backups entre contas oferecem suporte a fan-in (cópia de backups de várias contas primárias para uma conta de cópia de backup isolada) e fan-out (cópia de backups de uma conta primária para várias contas de cópia de backup isoladas).

Você pode fazer cópias de backup entre contas usando AWS Backup com AWS Organizations suporte. Os limites da conta para cópias entre contas são definidos pelas AWS Organizations políticas. Para obter mais informações sobre como usar AWS Backup para fazer cópias de backup entre contas, consulte Criação de cópias de backup Contas da AWS no Guia do AWS Backup desenvolvedor.

Limitações de cópias de backup

Veja abaixo algumas limitações quando você copia backups:

- As cópias de backup entre regiões são suportadas somente entre duas AWS regiões comerciais, entre as regiões da China (Pequim) e China (Ningxia) e entre as regiões AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA), mas não entre esses conjuntos de regiões.
- Não há suporte para cópias de backup entre regiões nas regiões de aceitação.
- Você pode fazer cópias de backup na região em qualquer AWS região.
- O backup de origem deve ter o status `AVAILABLE` para que você possa copiá-lo.
- Não será possível excluir um backup de origem se ele estiver sendo copiado. Pode haver um pequeno atraso entre o momento em que o backup de destino fica disponível e o momento em que você tem permissão para excluir o backup de origem. Leve em consideração esse atraso se tentar excluir novamente um backup de origem.
- Você pode ter até cinco solicitações de cópia de backup em andamento em uma única AWS região de destino por conta.

Permissões para cópias de backup entre regiões

Você usa uma declaração de política do IAM para conceder permissões para executar uma operação de cópia de backup. Para se comunicar com a AWS região de origem para solicitar uma cópia de backup entre regiões, o solicitante (função do IAM ou usuário do IAM) deve ter acesso ao backup de origem e à região de origem AWS .

Você usa a política para conceder permissões à ação `CopyBackup` para a operação de cópia de backup. Você especifica a ação no campo `Action` da política e especifica o valor do recurso no campo `Resource` da política, como no exemplo a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111111111111:backup/*"
        }
    ]
}
```

Para obter mais informações sobre as políticas do IAM, consulte Políticas e permissões no IAM no Guia do usuário do IAM.

Cópias completas e incrementais

Quando você copia um backup para uma AWS região de destino ou AWS conta de destino diferente do backup de origem, a primeira cópia é uma cópia de backup completa, mesmo se você usar a mesma chave KMS para criptografar as cópias de origem e de destino do backup.

Depois da primeira cópia de backup, todas as cópias de backup subsequentes para a mesma região de destino na mesma AWS conta são incrementais, desde que você não tenha excluído todos os backups copiados anteriormente nessa região e esteja usando a mesma chave. AWS KMS Se uma das condições não for atendida, a operação de cópia resultará em uma cópia de backup completa (não incremental).

Copiar um backup dentro da mesma conta (entre regiões ou dentro da região) usando o console

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação, selecione Backups.
3. Na tabela Backups, escolha o backup que você deseja copiar e, em seguida, selecione Copiar backup.
4. Na seção Configurações, faça o seguinte:

- Na lista Região de destino, escolha uma AWS região de destino para a qual copiar o backup. O destino pode estar em outra AWS região (cópia entre regiões) ou dentro da mesma AWS região (cópia na região).
- (Opcional) Selecione Copiar tags para copiar tags do backup de origem para o backup de destino. Se você selecionar Copiar tags e também adicionar tags na etapa 6, todas as tags serão mescladas.

5. Em Criptografia, escolha a chave de AWS KMS criptografia para criptografar o backup copiado.
6. Em Tags: opcional, insira uma chave e um valor para adicionar tags ao backup copiado. Se você adicionar tags aqui e também tiver selecionado Copiar tags na etapa 4, todas as tags serão mescladas.
7. Selecione Copy backup (Copiar backup).

Seu backup é copiado na mesma AWS conta para a AWS região selecionada.

Copiar um backup dentro da mesma conta (entre regiões ou dentro da região) usando a CLI

- Use o comando `copy-backup` CLI ou a operação da CopyBackupAPI para copiar um backup na mesma AWS conta, em uma AWS região ou em uma AWS região.

  O comando a seguir copia um backup com um ID de `backup-0abc123456789cba7` da região `us-east-1`.

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  A resposta mostra a descrição do backup copiado.

  Você pode visualizar seus backups no console Amazon FSx ou programaticamente usando o comando `describe-backups` CLI ou a operação da API. DescribeBackups

Como restaurar backups

Você pode usar um backup disponível para criar um novo sistema de arquivos, restaurando efetivamente um point-in-time instantâneo de outro sistema de arquivos. Você pode restaurar um backup usando o console ou um dos AWS SDKs. AWS CLI A restauração de um backup em um

novo sistema de arquivos leva o mesmo tempo que a criação de um novo sistema de arquivos. Os dados restaurados do backup são carregados lentamente no sistema de arquivos, e durante esse tempo você perceberá uma latência um pouco maior.

Para garantir que os usuários possam continuar a acessar o sistema de arquivos restaurado, certifique-se de que o domínio do Active Directory associado ao sistema de arquivos restaurado seja o mesmo do sistema de arquivos original ou que seja confiável para o domínio do AD do sistema de arquivos original. Para obter mais informações sobre o Active Directory, consulte Trabalhar com o Microsoft Active Directory no FSx para Windows File Server.

O procedimento a seguir apresenta instruções sobre como restaurar um backup usando o console para criar um novo sistema de arquivos.

> **Note**
>
> Só é possível restaurar o backup em um sistema de arquivos com o mesmo tipo de implantação e capacidade de armazenamento que o original. Você poderá aumentar a capacidade de armazenamento do sistema de arquivos restaurado depois que ele estiver disponível. Para ter mais informações, consulte Como gerenciar a capacidade de armazenamento.

Restaurar um sistema de arquivos de um backup

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel do console, escolha Backups na navegação do lado esquerdo.
3. Escolha o backup que você deseja restaurar na tabela Backups e, em seguida, selecione Restaurar backup.

   Isso abre o assistente de criação do sistema de arquivos. Esse assistente é idêntico ao assistente de criação de sistema de arquivos padrão, exceto pelo fato de que o Tipo de implantação e a Capacidade de armazenamento já estão definidos e não podem ser alterados. No entanto, você pode alterar a capacidade de throughput, a VPC associada e outras configurações, além do tipo de armazenamento. O tipo de armazenamento é definido como SSD por padrão, mas você pode alterá-lo para HDD nas seguintes condições:

   - O tipo de implantação do sistema de arquivos é multi-AZ ou single-AZ 2.
   - A capacidade de armazenamento é de pelo menos 2 mil GiB.

4. Conclua o assistente da forma como você faz quando cria um novo sistema de arquivos.
5. Selecione Review and create.
6. Revise as configurações que você escolheu para o sistema de arquivos do Amazon FSx e, em seguida, selecione Criar sistema de arquivos.

Você restaurou por meio de um backup e um novo sistema de arquivos agora está sendo criado. Quando seu status mudar para `AVAILABLE`, você poderá usar o sistema de arquivos normalmente.

Excluir backups

A exclusão de um backup é uma ação permanente e irrecuperável. Todos os dados em um backup excluído também são excluídos. Não exclua um backup, a menos que tenha certeza de que não precisará dele novamente no futuro. Você não pode excluir backups feitos por AWS Backup, que tenham o tipo AWS Backup, no console, na CLI ou na API do Amazon FSx.

Para excluir um backup

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 é aberta, confirme se o ID do backup identifica o backup que você deseja excluir.
5. Confirme se a caixa de seleção do backup que deseja excluir está marcada.
6. Escolha Excluir backups.

Seu backup e todos os dados incluídos agora são excluídos de forma permanente e irrecuperável.

Tamanho dos backups

O tamanho dos backups é determinado usando o armazenamento usado no sistema de arquivos, e não a capacidade total de armazenamento provisionada. O tamanho de seus backups dependerá da capacidade de armazenamento usada, bem como da quantidade de dados acumulados em seu sistema de arquivos. Dependendo de como os dados são distribuídos nos volumes de armazenamento do sistema de arquivos e da frequência com que são alterados, o uso total do backup pode ser maior ou menor do que a capacidade de armazenamento utilizada. Ao excluir

um backup, somente os dados exclusivos desse backup serão removidos. Com o Amazon FSx, a economia de eficiência de armazenamento da eliminação de duplicação e da compactação se aplica não apenas ao seu armazenamento primário em SSD/HDD, mas também aos backups.

Para fornecer file-system-consistent backups duráveis e incrementais, o Amazon FSx faz backup dos dados no nível do bloco. Os dados nos volumes de armazenamento do sistema de arquivos podem ser armazenados em vários blocos, dependendo do padrão em que foram gravados ou sobrescritos. Como resultado, o tamanho total do uso do backup pode não corresponder ao tamanho exato dos arquivos e diretórios no sistema de arquivos.

Seu uso e custo gerais de backup podem ser encontrados no AWS Billing Painel ou AWS Cost Management Console. Para calcular o tamanho e o custo de backups individuais do sistema de arquivos, você pode marcar backups individuais e ativar o relatório de faturamento baseado em tags.

Protegendo seus dados com cópias de sombra

Uma cópia de sombra do Microsoft Windows é um snapshot de um sistema de arquivos do Windows em um determinado momento. Com as cópias de sombra ativadas, os usuários podem recuperar rapidamente os arquivos excluídos ou alterados que estão armazenados na rede e comparar as versões dos arquivos. Os administradores de armazenamento podem facilmente programar cópias de sombra para serem feitas periodicamente usando PowerShell os comandos do Windows.

As cópias de sombra são armazenadas junto com os dados do seu sistema de arquivos e consomem a capacidade de armazenamento do sistema de arquivos somente para as partes alteradas dos arquivos. Todas as cópias de sombra armazenadas em seu sistema de arquivos estão incluídas nos backups do sistema de arquivos.

> **Note**
>
> As cópias de sombra não são habilitadas no FSx para Windows File Server por padrão. Para proteger os dados em seu sistema de arquivos usando cópias de sombra, você deve habilitar as cópias de sombra e configurar um agendamento de cópia de sombra em seu sistema de arquivos. Para ter mais informações, consulte Configurando cópias de sombra para usar o armazenamento e a programação padrão.

> **Warning**
>
> As cópias de sombra não substituem os backups. Se você ativar as cópias de sombra, certifique-se de continuar realizando backups regulares.

Tópicos

Práticas recomendadas ao usar cópias de sombra

Você pode habilitar cópias de sombra em seu sistema de arquivos para permitir que os usuários finais visualizem e restaurem arquivos ou pastas individuais de um snapshot anterior no Explorador de Arquivos do Windows. O Amazon FSx usa o recurso de cópias de sombra fornecido pelo Microsoft Windows Server. Use estas práticas recomendadas para cópias de sombra:

- Certifique-se de que seu sistema de arquivos tenha recursos de desempenho suficientes: por padrão, o Microsoft Windows usa um copy-on-write método para registrar as alterações desde o ponto de cópia sombra mais recente, e essa copy-on-write atividade pode resultar em até três operações de E/S para cada operação de gravação de arquivo.

- Usar armazenamento SSD e aumentar a capacidade de throughput: como o Windows exige um alto nível de performance de E/S para manter cópias de sombra, recomendamos usar o armazenamento SSD e aumentar a capacidade de throughput em até três vezes a workload esperada. Isso ajuda a garantir que seu sistema de arquivos tenha recursos suficientes para evitar problemas como a exclusão indesejada de cópias paralelas.
- Manter somente o número de cópias de sombra necessárias: se você tiver um grande número de cópias de sombra, por exemplo, mais de 64 das cópias de sombra mais recentes, ou cópias de sombra que ocupam uma grande quantidade de armazenamento (escala de TB) em um único sistema de arquivos, processos como failover e failback podem levar mais tempo. Isso se deve à necessidade do FSx para Windows executar verificações de consistência no armazenamento de cópias paralelas. Você também pode experimentar uma maior latência das operações de E/S devido à necessidade de o FSx for Windows realizar copy-on-write atividades enquanto mantém as cópias de sombra. Para minimizar a disponibilidade e o impacto na performance das cópias de sombra, exclua manualmente as cópias de sombra não utilizadas ou configure scripts para excluir automaticamente as cópias de sombra antigas do sistema de arquivos.

> **Note**
>
> Durante eventos de failover em sistemas de arquivos multi-AZ, o FSx para Windows executa uma análise de consistência que exige a verificação do armazenamento de cópias de sombra no sistema de arquivos antes que o novo servidor de arquivos ativos fique on-line. A duração da análise de consistência está relacionada ao número de cópias de sombra no sistema de arquivos, bem como ao armazenamento consumido. Para evitar eventos atrasados de failover e failback, recomendamos manter menos de 64 cópias de sombra no sistema de arquivos e seguir as etapas abaixo para monitorar e excluir regularmente as cópias de sombra mais antigas.

Configurando cópias de sombra

Você ativa e programa cópias paralelas periódicas em seu sistema de arquivos usando PowerShell comandos do Windows definidos pelo Amazon FSx. A seguir estão três configurações principais ao configurar cópias de sombra em seu sistema de arquivos FSx for Windows File Server:

- Definindo a quantidade máxima de armazenamento que as cópias de sombra podem consumir em seu sistema de arquivos

- (Opcional) Definir o número máximo de cópias de sombra que podem ser armazenadas em seu sistema de arquivos. O valor padrão é 20.
- (Opcional) Definir um cronograma que defina os horários e os intervalos nos quais fazer cópias paralelas, como diariamente, semanalmente e mensalmente

Você pode armazenar no máximo 500 cópias de sombra por sistema de arquivos a qualquer momento; no entanto, recomendamos manter menos de 64 cópias paralelas a qualquer momento para garantir a disponibilidade e o desempenho. Quando você atingir esse limite, a próxima cópia de sombra que você fizer substituirá a cópia de sombra mais antiga. Da mesma forma, quando a quantidade máxima de armazenamento de cópias de sombra é atingida, uma ou mais das cópias de sombra mais antigas são excluídas para criar espaço de armazenamento suficiente para a próxima cópia de sombra.

Para obter informações sobre como ativar e programar rapidamente cópias de sombra periódicas usando as configurações padrão do Amazon FSx, consulte Configurando cópias de sombra para usar o armazenamento e a programação padrão.

Considerações sobre a alocação do armazenamento de cópias de sombra

Uma cópia de sombra é uma cópia em nível de bloco das alterações de arquivos que foram feitas desde a última cópia de sombra. O arquivo inteiro não é copiado, apenas as alterações. Portanto, as versões anteriores dos arquivos normalmente não ocupam tanto espaço de armazenamento quanto o arquivo atual. A quantidade de espaço de volume usada para alterações pode variar de acordo com sua workload. Quando um arquivo é modificado, o espaço de armazenamento usado pelas cópias de sombra depende de sua workload. Ao determinar a quantidade de espaço de armazenamento a ser alocada para cópias de sombra, você deve levar em conta os padrões de uso do sistema de arquivos da workload.

Ao ativar as cópias de sombra, você pode especificar a quantidade máxima de armazenamento que as cópias de sombra podem consumir no sistema de arquivos. O limite padrão é de 10% do sistema de arquivos. Recomendamos que você aumente o limite se os usuários adicionarem ou modificarem arquivos com frequência. Definir um limite muito pequeno pode fazer com que as cópias de sombra mais antigas sejam excluídas com mais frequência do que os usuários esperam.

Você pode definir o armazenamento de cópias de sombra como ilimitado (`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`). No entanto, uma configuração ilimitada pode resultar em um grande número de cópias de sombra que consomem o armazenamento do sistema de arquivos. Isso pode resultar na falta de capacidade de armazenamento suficiente para suas workloads. Se você definir

um armazenamento ilimitado, certifique-se de escalar sua capacidade de armazenamento à medida que os limites da cópia de sombra forem atingidos. Para obter informações sobre como configurar o armazenamento de cópias de sombra para um tamanho específico ou como ilimitado, consulte Definindo a quantidade máxima de armazenamento de cópia de sombra.

Depois de ativar as cópias de sombra, você pode monitorar a quantidade de espaço de armazenamento consumido pelas cópias de sombra. Para ter mais informações, consulte Como visualizar o armazenamento de cópias de sombra.

Considerações ao definir o número máximo de cópias de sombra

Ao ativar as cópias de sombra, você pode especificar o número máximo de cópias de sombra armazenadas no sistema de arquivos. O limite padrão é 20 e, para minimizar a disponibilidade e o impacto no desempenho das cópias de sombra, a Microsoft recomenda configurar o número máximo de cópias de sombra para menos de 64. Como o Windows exige um alto nível de desempenho de E/S para manter as cópias de sombra, recomendamos usar o armazenamento SSD e aumentar a capacidade de taxa de transferência em até três vezes a carga de trabalho esperada. Isso ajuda a garantir que seu sistema de arquivos tenha recursos suficientes para evitar problemas como a exclusão indesejada de cópias paralelas.

Você pode definir o número máximo de cópias de sombra até 500. No entanto, se você tiver um grande número de cópias de sombra ou cópias de sombra que ocupam uma grande quantidade de armazenamento (escala de TB) em um único sistema de arquivos, processos como failover e failback podem levar mais tempo do que o esperado. Isso ocorre porque o Windows precisa executar verificações de consistência no armazenamento de cópias de sombra. Você também pode experimentar uma maior latência das operações de E/S devido à necessidade de o Windows realizar copy-on-write atividades enquanto mantém as cópias de sombra.

Recomendações do sistema de arquivos para cópias de sombra

Veja a seguir as recomendações do sistema de arquivos para o uso de cópias de sombra.

- Certifique-se de fornecer capacidade de performance suficiente para as necessidades de sua workload em seu sistema de arquivos. O Amazon FSx oferece o recurso de cópias de sombra, conforme fornecido pelo Microsoft Windows Server. Por padrão, o Microsoft Windows usa um copy-on-write método para registrar as alterações desde o ponto de cópia de sombra mais recente, e essa copy-on-write atividade pode resultar em até três operações de E/S para cada operação de gravação de arquivo. Se o Windows não conseguir acompanhar a taxa de entrada das operações de E/S por segundo, isso poderá fazer com que todas as cópias de sombra

sejam excluídas, pois não poderá mais manter as cópias de sombra por meio dela. copy-on-write Portanto, é importante que você forneça capacidade de performance de E/S suficiente para as necessidades da workload no sistema de arquivos (tanto a dimensão da capacidade de throughput que determina a performance de E/S do servidor de arquivos quanto o tipo e a capacidade de armazenamento que determinam a performance de E/S do armazenamento).

- Em geral, recomendamos que você use sistemas de arquivos configurados com armazenamento SSD em vez de armazenamento HDD ao ativar as cópias de sombra, pois o Windows consome uma performance de E/S mais alta para manter as cópias de sombra e o armazenamento HDD oferece uma capacidade de performance mais baixa para operações de E/S.
- Seu sistema de arquivos deve ter pelo menos 320 MB de espaço livre, além da quantidade máxima de armazenamento de cópias de sombra configurada (`MaxSpace`). Por exemplo, se você alocou um `MaxSpace` 5 GB para cópias de sombra, seu sistema de arquivos deve sempre ter pelo menos 320 MB de espaço livre, além do `MaxSpace` do 5 GB.

> **Warning**
>
> Ao configurar a programação da cópia de sombra, certifique-se de não programar cópias de sombra durante a migração de dados ou quando os trabalhos de eliminação de duplicação dos dados estiverem programados para execução. Você deve programar cópias de sombra quando espera que o sistema de arquivos esteja ocioso. Para obter informações sobre como configurar uma programação de cópia de sombra personalizada, consulte Como criar uma programação de cópias de sombra personalizada.

Configurando cópias de sombra para usar o armazenamento e a programação padrão

Você pode configurar rapidamente cópias de sombra em seu sistema de arquivos usando a configuração e o agendamento padrão de armazenamento de cópia de sombra. A configuração padrão de armazenamento de cópias de sombra permite que as cópias de sombra consumam no máximo 10% da capacidade de armazenamento do sistema de arquivos. Se você aumentar a capacidade de armazenamento do seu sistema de arquivos, a quantidade de armazenamento de cópia sombra atualmente alocada não aumentará da mesma forma.

A programação padrão realiza cópias de sombra automaticamente todas as segundas, terças, quartas, quintas e sextas-feiras, às 4h e 9h no horário de Brasília.

Configurar o nível padrão de armazenamento de cópias de sombra

1. Conecte-se a uma instância de computação do Windows que tenha conectividade de rede com seu sistema de arquivos.
2. Faça login na instância de computação do Windows como membro do grupo de administradores do sistema de arquivos. Em AWS Managed Microsoft AD, esse grupo é AWS Delegated FSx Administrators. No Microsoft AD autogerenciado, esse grupo é Administradores de domínio ou o grupo personalizado que você especificou para administração ao criar o sistema de arquivos. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
3. Defina a quantidade padrão de armazenamento de sombra usando o seguinte comando. *FSxFileSystem-Remote-PowerShell-Endpoint*Substitua pelo PowerShell endpoint remoto do Windows do sistema de arquivos que você deseja administrar. Você pode encontrar o PowerShell endpoint remoto do Windows no console do Amazon FSx, na seção Rede e Segurança da tela de detalhes do sistema de arquivos ou na resposta da operação `DescribeFileSystem` da API.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
FsxShadowStorage -Default}
```

A resposta é semelhante à seguinte.

```
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 10737418240                 20
```

Para definir o cronograma padrão de cópia de sombra

1. Conecte-se a uma instância de computação do Windows que tenha conectividade de rede com seu sistema de arquivos.
2. Faça login na instância de computação do Windows como membro do grupo de administradores do sistema de arquivos. Em AWS Managed Microsoft AD, esse grupo é AWS Delegated FSx Administrators. No Microsoft AD autogerenciado, esse grupo é Administradores de domínio ou o grupo personalizado que você especificou para administração ao criar o sistema de arquivos.

Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.

3. Defina o cronograma padrão de cópia de sombra usando o comando a seguir.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-FsxShadowCopySchedule -Default}
```

A resposta exibe a programação padrão que está definida agora.

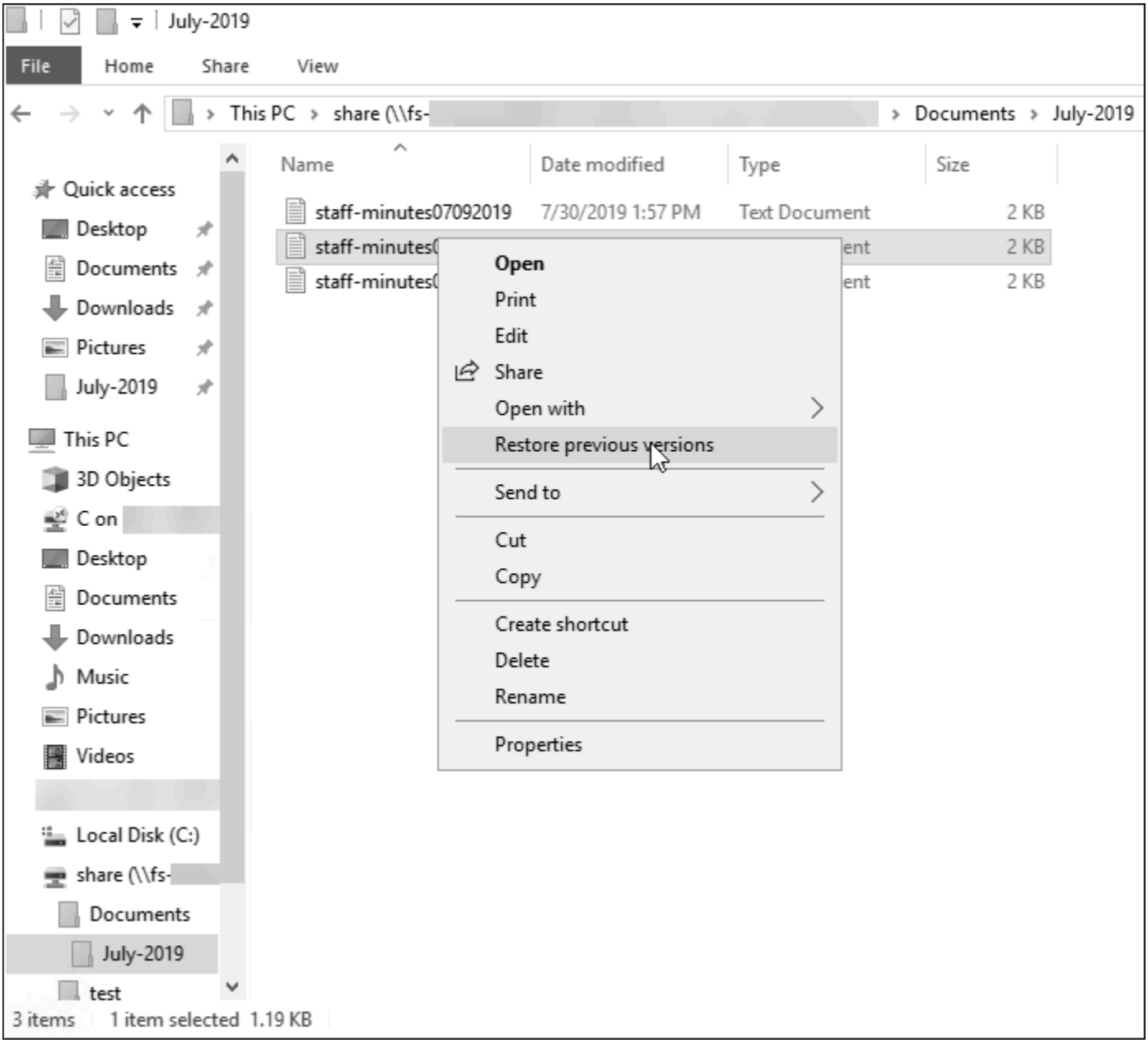
```
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

Para saber mais sobre opções adicionais e como criar uma programação de cópia de sombra personalizada, consulte Como criar uma programação de cópias de sombra personalizada.

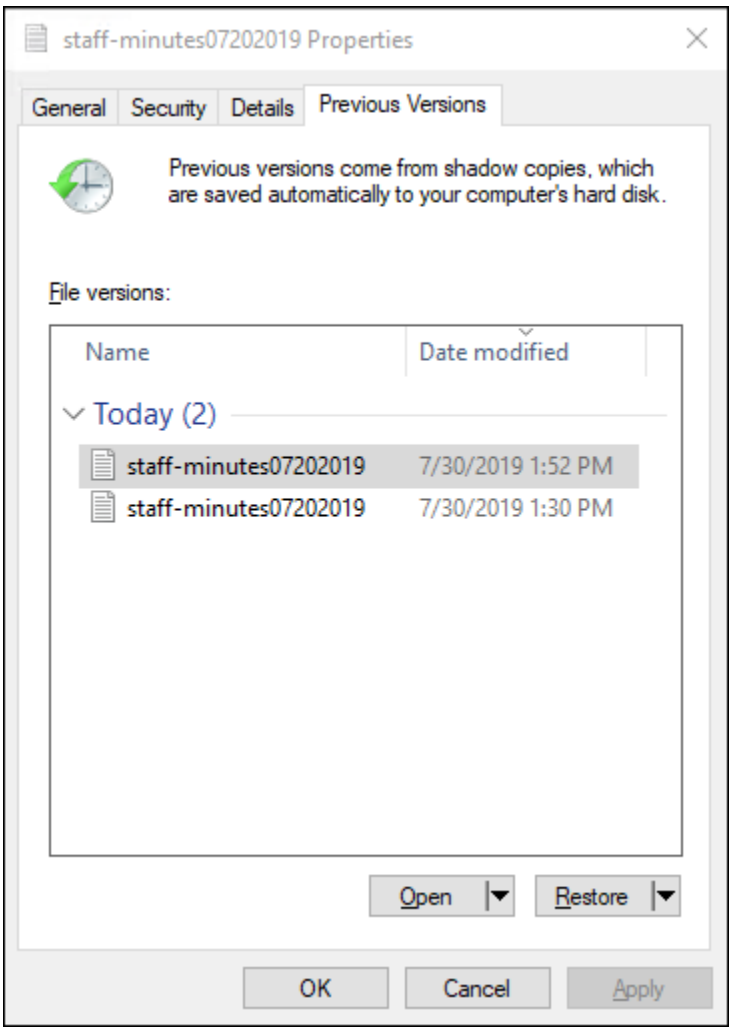
Como restaurar arquivos e pastas individuais

Depois de configurar cópias de sombra em seu sistema de arquivos Amazon FSx, seus usuários podem restaurar rapidamente versões anteriores de arquivos ou pastas individuais e recuperar arquivos excluídos.

Os usuários restauram arquivos para versões anteriores usando a interface familiar do Explorador de Arquivos do Windows. Para restaurar um arquivo, escolha o arquivo a ser restaurado e, em seguida, selecione Restaurar versões anteriores no menu de contexto (clique com o botão direito do mouse).



Os usuários podem então visualizar e restaurar uma versão anterior na lista Versões anteriores.



Definindo a quantidade máxima de armazenamento de cópia de sombra

Você define a quantidade máxima de armazenamento que as cópias de sombra podem consumir em um sistema de arquivos usando o PowerShell comando `Set-FsxShadowStorage` personalizado. Você pode especificar o tamanho máximo para o qual as cópias de sombra podem crescer usando os `-Default` parâmetros `-Maxsize` ou os. Usar `Default` define o máximo para 10% da capacidade de armazenamento do sistema de arquivos. Você não pode especificar os `-Default` parâmetros `-Maxsize` e no mesmo comando.

Caso use `-Maxsize`, você poderá definir o armazenamento de cópias de sombra da seguinte forma:

- Em bytes: `Set-FsxShadowStorage -Maxsize 2500000000`
- Em kilobytes, megabytes, gigabytes ou outras unidades: `Set-FsxShadowStorage -Maxsize (2500MB)` ou `Set-FsxShadowStorage -Maxsize (2.5GB)`
- Como porcentagem do armazenamento geral: `Set-FsxShadowStorage -Maxsize "20%"`

- Como ilimitado: `Set-FsxShadowStorage -Maxsize "UNBOUNDED"`

Use `-Default` para definir o armazenamento de sombra para usar até 10% do sistema de arquivos: `Set-FsxShadowStorage -Default`. Para saber mais sobre como usar a opção padrão, consulte Configurando cópias de sombra para usar o armazenamento e a programação padrão.

Definir a quantidade de armazenamento de cópias de sombra em um sistema de arquivos do FSx para Windows File Server

1. Conecte-se a uma instância de computação que tenha conectividade de rede com o sistema de arquivos como um usuário que seja membro do grupo de administradores do sistema de arquivos. Em AWS Managed Microsoft AD, esse grupo é AWS Delegated FSx Administrators. No Microsoft AD autogerenciado, esse grupo é Administradores de domínio ou o grupo personalizado que você especificou para administração ao criar o sistema de arquivos. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
2. Abra uma PowerShell janela do Windows na instância de computação.
3. Use o comando a seguir para abrir uma PowerShell sessão remota no seu sistema de arquivos Amazon FSx. *`FSxFileSystem-Remote-PowerShell-Endpoint`*Substitua pelo PowerShell endpoint remoto do Windows do sistema de arquivos que você deseja administrar. Você pode encontrar o PowerShell endpoint remoto do Windows no console do Amazon FSx, na seção Rede e Segurança da tela de detalhes do sistema de arquivos ou na resposta da operação `DescribeFileSystem` da API.

   ```
   PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-
   PowerShell-Endpoint -configurationname fsxremoteadmin
   ```

4. Verifique se o armazenamento de cópias de sombra ainda não está configurado no sistema de arquivos usando o comando a seguir.

   ```
   [fs-1234567890abcef12]: PS>Get-FsxShadowStorage
   No Fsx Shadow Storage Configured
   ```

5. Defina a quantidade de armazenamento de sombra para 10 por cento do volume e o número máximo de cópias de sombra para 20 usando a `-Default` opção.

   ```
   [fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
   FSx Shadow Storage Configuration
   ```

```
AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
             0         0 32530536858                  20
```

Você pode limitar o número máximo de cópias de sombra permitidas em seu sistema de arquivos usando o `Set-FSxShadowStorage` comando com o `-MaxShadowCopyNumber` parâmetro e especificando um valor de 1 a 500. Por padrão, o número máximo de cópias de sombra é definido como 20, conforme recomendado pela Microsoft para cargas de trabalho ativas.

Como visualizar o armazenamento de cópias de sombra

Você pode visualizar a quantidade de armazenamento atualmente consumida pelas cópias de sombra em seu sistema de arquivos usando o `Get-FsxShadowStorage` comando em uma PowerShell sessão remota em seu sistema de arquivos. Para obter instruções sobre como iniciar uma PowerShell sessão remota em seu sistema de arquivos, consulteUsando a CLI do Amazon FSx para PowerShell.

```
[fs-1234567890abcef12]: PS>PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
             0         0 10737418240                  20
```

A saída mostra a configuração de armazenamento de sombra, da seguinte forma:

- `AllocatedSpace`— A quantidade de armazenamento no sistema de arquivos em bytes atualmente alocada para cópias de sombra. Inicialmente, esse valor é 0.
- `UsedSpace`— A quantidade de armazenamento, em bytes, usada atualmente pelas cópias de sombra. Inicialmente, esse valor é 0.
- `MaxSpace`— A quantidade máxima de armazenamento, em bytes, até a qual o armazenamento paralelo pode crescer. Esse é o valor que você define para armazenamento de cópias de sombra usando o comando `Set-FsxShadowStorage`.
- `MaxShadowCopyNumber`— O número máximo de cópias de sombra que o sistema de arquivos pode ter, de 1 a 500.

Quando a `UsedSpace` quantidade atinge a quantidade máxima de armazenamento de cópias de sombra configurada (`MaxSpace`) ou o número de cópias de sombra atinge o número máximo de cópias de sombra configurado (`MaxShadowCopyNumber`), a próxima cópia de sombra que você fizer substituirá a cópia de sombra mais antiga. Se você não quiser perder as cópias de sombra mais antigas, monitore o armazenamento de cópias de sombra para garantir que você tenha espaço de armazenamento suficiente para novas cópias de sombra. Se precisar de mais espaço, você poderá excluir as cópias de sombra atuais ou aumentar a quantidade máxima do armazenamento de cópias de sombra.

> **Note**
>
> Quando as cópias de sombra são criadas automática ou manualmente, elas usam a quantidade de armazenamento de cópia de sombra que você configurou como limite de armazenamento. As cópias de sombra aumentam de tamanho com o tempo e utilizam o espaço de armazenamento disponível mostrado pela CloudWatch `FreeStorageCapacity` métrica até a quantidade máxima de armazenamento de cópias de sombra configurada (`MaxSpace`).

Como excluir o armazenamento de cópias de sombra, a programação e todas as cópias de sombra

Você pode excluir a configuração de cópias de sombra, incluindo todas as cópias de sombra atuais e a programação de cópias de sombra. Ao mesmo tempo, você pode liberar o armazenamento de cópias de sombra no sistema de arquivos.

Para fazer isso, digite o `Remove-FsxShadowStorage` comando em uma PowerShell sessão remota no seu sistema de arquivos. Para obter instruções sobre como iniciar uma PowerShell sessão remota em seu sistema de arquivos, consulteUsando a CLI do Amazon FSx para PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowStorage

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowStorage" on target "Removing all Shadow
 Copies, Shadow Copy Schedule, and Shadow Storage".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
FSx Shadow Storage Configuration
Removing Shadow Copy Schedule
```

```
Removing Shadow Copies
All shadow copies removed.
Removing Shadow Storage
Shadow Storage removed successfully.
```

Como criar uma programação de cópias de sombra personalizada

As programações de cópias de sombra usam gatilhos de tarefas programadas no Microsoft Windows para especificar quando as cópias de sombra são automaticamente criadas. Uma programação de cópias de sombra pode ter vários gatilhos, oferecendo muita flexibilidade de programação. Só pode existir uma programação de cópias de sombra de cada vez. Antes de criar uma programação de cópias de sombra, você deve primeiro definir a quantidade de armazenamento de cópias de sombra.

Ao executar o comando `Set-FsxShadowCopySchedule` em um sistema de arquivos, você substitui qualquer programação de cópias de sombra atual. Se o computador cliente estiver no fuso horário UTC, você também poderá especificar o fuso horário de um gatilho usando os fusos horários do Windows e a opção `-TimezoneId`. Para obter uma lista de fusos horários do Windows, consulte a documentação sobre Fuso horário padrão da Microsoft ou execute o seguinte em um prompt de comando do Windows: `tzutil /l`. Para saber mais sobre gatilhos de tarefas do Windows, consulte Gatilhos de tarefa na documentação da Central de Desenvolvedores do Microsoft Windows.

Você também pode usar a opção `-Default` para configurar rapidamente uma programação padrão de cópias de sombra. Para saber mais, consulte Configurando cópias de sombra para usar o armazenamento e a programação padrão.

Criar uma programação de cópias de sombra personalizada

1. Crie um conjunto de gatilhos de tarefas programadas do Windows para definir quando são criadas cópias de sombra na programação de cópias de sombra. Use o `new-scheduledTaskTrigger` comando em a PowerShell em sua máquina local para definir vários gatilhos.

   O exemplo a seguir cria uma programação de cópias de sombra personalizada que cria cópias de sombra de segunda a sexta-feira às 6h e às 18h UTC. Por padrão, os horários estão em UTC, a menos que você especifique um fuso horário nos gatilhos de tarefas programadas do Windows que você criar.

   ```
   PS C:\Users\delegateadmin> $trigger1 = new-scheduledTaskTrigger -weekly -DaysOfWeek
    Monday,Tuesday,Wednesday,Thursday,Friday -at 06:00
   ```

```
PS C:\Users\delegateadmin> $trigger2 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 18:00
```

2. Use `invoke-command` para executar o comando `scriptblock`. Essa ação grava um script que define a programação de cópias de sombra com o valor `new-scheduledTaskTrigger` que você acabou de criar. *`FSxFileSystem-Remote-PowerShell-Endpoint`*Substitua pelo PowerShell endpoint remoto do Windows do sistema de arquivos que você deseja administrar. Você pode encontrar o PowerShell endpoint remoto do Windows no console do Amazon FSx, na seção Rede e Segurança da tela de detalhes do sistema de arquivos ou na resposta da operação `DescribeFileSystem` da API.

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

3. Insira a linha a seguir no prompt >> para definir a programação de cópias de sombra usando o comando `set-fsxshadowcopyschedule`.

```
>> set-fsxshadowcopyschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2
 -Confirm:$false }
```

A resposta exibe a programação de cópias de sombra que você configurou no sistema de arquivos.

```
FSx Shadow Copy Schedule


Start Time:    : 2019-07-16T06:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcde1

Start Time:    : 2019-07-16T18:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcdef
```

Como visualizar a programação de cópias de sombra

Para visualizar a agenda de cópia paralela existente em seu sistema de arquivos, digite o comando a seguir em uma PowerShell sessão remota em seu sistema de arquivos. Para obter instruções sobre como iniciar uma PowerShell sessão remota em seu sistema de arquivos, consulteUsando a CLI do Amazon FSx para PowerShell.

```
[fs-0123456789abcdef1]PS> Get-FsxShadowCopySchedule
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

Como excluir uma programação de cópias de sombra

Para excluir a agenda de cópia paralela existente em seu sistema de arquivos, digite o comando a seguir em uma PowerShell sessão remota em seu sistema de arquivos. Para obter instruções sobre como iniciar uma PowerShell sessão remota em seu sistema de arquivos, consulteUsando a CLI do Amazon FSx para PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopySchedule

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowCopySchedule" on target "Removing FSx Shadow
 Copy Schedule".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y"): Y
[fs-0123456789abcdef1]PS>
```

Como criar uma cópia de sombra

Para criar manualmente uma cópia de sombra, digite o comando a seguir em uma PowerShell sessão remota no seu sistema de arquivos. Para obter instruções sobre como iniciar uma PowerShell sessão remota em seu sistema de arquivos, consulteUsando a CLI do Amazon FSx para PowerShell.

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy
```

```
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

Como visualizar as cópias de sombra atuais

Para visualizar o conjunto de cópias de sombra existentes em seu sistema de arquivos, digite o comando a seguir em uma PowerShell sessão remota em seu sistema de arquivos. Para obter instruções sobre como iniciar uma PowerShell sessão remota em seu sistema de arquivos, consulteUsando a CLI do Amazon FSx para PowerShell.

```
[fs-0123456789abcdef1]PS>Get-FsxShadowCopies
FSx Shadow Copies: 2 total

Shadow Copy ID                          Creation Time
--------------                          -----------------
{ABCDEF12-3456-7890-ABCD-EF1234567890} 6/17/2019 7:11:09 AM
{FEDCBA21-6543-0987-0987-EF3214567892} 6/19/2019 11:24:19 AM
```

Como excluir cópias de sombra

Você pode excluir uma ou mais cópias de sombra existentes no sistema de arquivos usando o `Remove-FsxShadowCopies` comando em uma PowerShell sessão remota no sistema de arquivos. Para obter instruções sobre como iniciar uma PowerShell sessão remota em seu sistema de arquivos, consulteUsando a CLI do Amazon FSx para PowerShell.

Especifique quais cópias de sombra serão excluídas usando uma das seguintes opções obrigatórias:

- `-Oldest` exclui a cópia de sombra mais antiga;
- `-All` exclui todas as cópias de sombra atuais;
- `-ShadowCopyId` exclui uma cópia de sombra específica por ID.

Você só pode usar uma opção com o comando. Ocorrerá um erro se você não especificar qual cópia de sombra será excluída, se especificar vários IDs de cópia de sombra ou se especificar um ID inválido de cópia de sombra.

Para excluir a cópia de sombra mais antiga em seu sistema de arquivos, digite o comando a seguir em uma PowerShell sessão remota em seu sistema de arquivos.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -Oldest
```

```
Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing oldest shadow
 copy".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} deleted
```

Para excluir uma cópia de sombra específica em seu sistema de arquivos, digite o comando a seguir em uma PowerShell sessão remota em seu sistema de arquivos.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -ShadowCopyId "{ABCDEF12-3456-7890-
ABCD-EF1234567890}"
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing shadow copy
 {ABCDEF12-3456-7890-ABCD-EF1234567890}".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y":>Y
Shadow Copy \\AMZNFSXABCDE123\root\cimv2:Wind32_ShadowCopy.ID{ABCDEF12-3456-7890-ABCD-
EF1234567890}".ID deleted.
```

Para excluir um certo número das cópias de sombra mais antigas em seu sistema de arquivos, atualize seu `-MaxShadowCopyNumber` parâmetro para o número desejado de cópias de sombra que você gostaria de ter restantes. No entanto, essa alteração só entrará em vigor após a captura instantânea da próxima cópia de sombra, quando o sistema excluirá automaticamente as cópias de sombra em excesso. Use o comando a seguir em uma PowerShell sessão remota no seu sistema de arquivos.

```
[fs-1234567890abcef12]: PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace MaxSpace    MaxShadowCopyNumber
-------------- --------- ----------- -------------------
     556679168  21659648 10737418240                  50

[fs-1234567890abcef12]: PS>Set-FsxShadowStorage  -MaxShadowCopyNumber 5
Validation
You have 50 shadow copies. Older versions of shadow copies will be deleted, keeping 5
 latest shadow copies on your file system.
Do you want to continue?
[Y] Yes  [N] No  [?] Help (default is "N"): y
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
```

```
-------------- ---------    -------- -------------------
     556679168  21659648 10737418240                   5
```

Replicação programada usando AWS DataSync

Você pode usar AWS DataSync para programar a replicação periódica do seu sistema de arquivos FSx for Windows File Server em um segundo sistema de arquivos. Esse recurso está disponível para implantações na região e entre regiões. Para saber mais, consulte Como migrar arquivos atuais para o FSx para Windows File Server usando o AWS DataSync neste guia Transferência de dados entre serviços AWS de armazenamento no Guia do AWS DataSync usuário.

Como administrar sistemas de arquivos

Este capítulo descreve como acessar a CLI do Amazon FSx para gerenciamento remoto e como realizar as tarefas administrativas disponíveis do sistema de arquivos. PowerShell Você também pode usar a interface gráfica de usuário (GUI) nativa do Microsoft Windows para realizar algumas tarefas administrativas.

Tópicos

Usando a CLI do Amazon FSx para PowerShell

A CLI do Amazon FSx para gerenciamento remoto ativado PowerShell permite a administração do sistema de arquivos para usuários no grupo de administradores do sistema de arquivos. Para iniciar uma PowerShell sessão remota em seu sistema de arquivos FSx for Windows File Server, primeiro você precisa atender aos seguintes pré-requisitos:

- Consiga se conectar a uma instância de computação do Windows que tenha conectividade de rede com seu sistema de arquivos FSx for Windows File Server.

- Esteja conectado à instância de computação do Windows como membro do grupo de administradores do sistema de arquivos. Se você estiver usando AWS Managed Microsoft AD, esse é o grupo AWS Delegated FSx Administrators. Se você estiver usando um Microsoft Active Directory autogerenciado, esse é o grupo Administradores de Domínio ou o grupo personalizado que você especificou para administração ao criar seu sistema de arquivos. Para ter mais informações, consulte Práticas recomendadas de Active Directory autogerenciado.
- As regras de entrada do grupo de segurança VPC do seu sistema de arquivos permitem tráfego na porta 5985.

A CLI do Amazon FSx para gerenciamento remoto PowerShell usa os seguintes recursos de segurança:

- As credenciais do usuário são autenticadas usando a autenticação Kerberos.
- As comunicações da sessão de gerenciamento entre o cliente conectado e o sistema de arquivos são criptografadas usando o Kerberos.

Você tem duas opções para executar comandos CLI de gerenciamento remoto em seu sistema de arquivos Amazon FSx:

- Você pode estabelecer uma PowerShell sessão remota de longa duração e executar os comandos dentro da sessão.
- Você pode usar o `Invoke-Command` para executar um único comando ou um único bloco de comandos sem estabelecer uma PowerShell sessão remota de longa duração.

Se você quiser definir e passar variáveis como parâmetros para o comando de gerenciamento remoto, você precisará usar`Invoke-Command`.

> **Note**
>
> Para sistemas de arquivos Multi-AZ, você só pode usar a CLI do Amazon FSx para gerenciamento remoto enquanto o sistema de arquivos estiver usando seu servidor de arquivos preferido. Para ter mais informações, consulte Disponibilidade e durabilidade: sistemas de arquivos single-AZ e multi-AZ.

Você precisa usar o Windows Remote PowerShell Endpoint do sistema de arquivos ao usar o Remote PowerShell. Usando o AWS Management Console, você pode encontrar o endpoint na guia Rede e segurança, na página de detalhes do sistema de arquivos. Usando o AWS CLI `describe-file-systems` comando, a `RemoteAdministrationEndpoint` propriedade é retornada na resposta. O endpoint de administração remota usa o formato`amznfsxctlyaa1k.`*`ActiveDirectory-DNS-name`*, por exemplo,`amznfsxctlyaa1k.corp.example.com`.

Você pode usar o `Get-Command` cmdlet para obter informações sobre os cmdlets, funções e aliases disponíveis em. PowerShell Para obter mais informações, consulte a documentação Get-Command da Microsoft.

Você também pode executar a CLI do Amazon FSx para gerenciamento remoto da CLI em PowerShell comandos no seu sistema de arquivos usando o `Invoke-Command` cmdlet, usando a seguinte sintaxe.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName
 amznfsxctlyaa1k.corp.example.com -ConfigurationName FSxRemoteAdmin -scriptblock { fsx-
command}
```

Para obter instruções sobre como iniciar uma PowerShell sessão remota de longa duração em seu sistema de arquivos FSx for Windows File Server, consulte Iniciando uma sessão remota do Amazon FSx PowerShell

Iniciando uma sessão remota do Amazon FSx PowerShell

Este tópico fornece instruções para iniciar uma PowerShell sessão remota de longa duração em seu servidor de arquivos FSx for Windows File Server.

Para iniciar uma PowerShell sessão remota em seu sistema de arquivos

1. Conecte-se a uma instância computacional que tenha conectividade de rede com seu sistema de arquivos como um usuário que é membro do Grupo de Administradores FSx delegado que você escolheu ao criar o sistema de arquivos.
2. Abra uma PowerShell janela do Windows na instância de computação.
3. Em PowerShell, digite o comando a seguir para abrir uma sessão remota de longa duração em seu sistema de arquivos Amazon FSx. *`Remote-PowerShell-Endpoint`*Substitua pelo

PowerShell endpoint remoto do Windows do sistema de arquivos que você deseja administrar. Use `FsxRemoteAdmin` como nome da configuração da sessão.

```
PS C:\Users\delegateadmin> enter-pssession -ComputerName Remote-PowerShell-Endpoint
 -ConfigurationName FsxRemoteAdmin
[fs-0123456789abcdef0]: PS>
```

Se sua instância não fizer parte do domínio Amazon FSx Active Directory, você será solicitado a inserir as credenciais do usuário em um pop-up. Insira as credenciais do usuário que é membro do FSx Administrators Group. Se sua instância estiver associada ao domínio, você não precisará fornecer credenciais.

Como gerenciar aliases de DNS

O FSx para Windows File Server fornece um nome de Sistema de Nomes de Domínio (DNS) padrão para cada sistema de arquivos que você pode usar para acessar os dados no sistema de arquivos. Você também pode acessar os sistemas de arquivos usando um alias de DNS de sua escolha. Com aliases de DNS, você pode continuar usando os nomes DNS atuais para acessar dados armazenados no Amazon FSx ao migrar o armazenamento do sistema de arquivos on-premises para o Amazon FSx, sem precisar atualizar qualquer ferramenta ou aplicação. Para ter mais informações, consulte Como migrar o armazenamento de arquivos atual para o Amazon FSx.

> **Note**
>
> O suporte para aliases de DNS está disponível nos sistemas de arquivos do FSx para Windows File Server criados após as 12h ET de 9 de novembro de 2020. Para usar aliases de DNS em um sistema de arquivos criado antes das 12h ET de 9 de novembro de 2020, faça o seguinte:
>
> 1. Faça um backup do sistema de arquivos atual. Para ter mais informações, consulte Como trabalhar com backups iniciados pelo usuário.
> 2. Restaure o backup em um novo sistema de arquivos. Para ter mais informações, consulte Como restaurar backups.
>
> Quando o novo sistema de arquivos estiver disponível, você poderá usar aliases de DNS para acessá-lo, usando as informações fornecidas nesta seção.

> **Note**
>
> As informações apresentadas aqui pressupõem que você esteja trabalhando inteiramente no Active Directory e que não esteja usando provedores de DNS externos. Provedores de DNS de terceiros podem ocasionar comportamento inesperado.
> O Amazon FSx só gravará registros de DNS em um sistema de arquivos se o domínio do AD ao qual você o está associando estiver usando o DNS da Microsoft como DNS padrão. Se você estiver usando um DNS de terceiros, precisará configurar manualmente as entradas de DNS para os sistemas de arquivos do Amazon FSx depois de criar o sistema de arquivos. Para obter mais informações sobre como escolher os endereços IP corretos a serem usados no sistema de arquivos, consulte Como obter os endereços IP corretos do sistema de arquivos para usar no DNS.

Você pode associar aliases de DNS aos sistemas de arquivos do FSx para Windows File Server atuais quando criar novos sistemas de arquivos e quando criar um novo sistema de arquivos com base em um backup. Você pode associar até 50 aliases de DNS a um sistema de arquivos a qualquer momento.

Além de associar aliases de DNS ao sistema de arquivos, para que os clientes se conectem ao sistema de arquivos usando os aliases de DNS, você também deve fazer o seguinte:

- Configure nomes de entidades principais de serviço (SPNs) para autenticação e criptografia Kerberos.
- Configure um registro CNAME do DNS para o alias de DNS que é resolvido para o nome DNS padrão do sistema de arquivos do Amazon FSx.

Para ter mais informações, consulte Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos.

Um nome de alias de DNS para seu sistema de arquivos FSx for Windows File Server precisa atender aos seguintes requisitos:

- Deve ser formatado como um nome de domínio totalmente qualificado (FQDN).
- Pode conter caracteres alfanuméricos e hifens (-).
- Não pode começar ou terminar com um hífen (-).
- Pode começar com um caractere numérico.

Para nomes de alias DNS, o Amazon FSx armazena caracteres alfabéticos como letras minúsculas (a-z), independentemente de como elas são especificadas: como letras maiúsculas, letras minúsculas ou as letras correspondentes em códigos de escape.

Se você tentar associar um alias que já esteja associado ao sistema de arquivos, esta ação não terá efeito. Se você tentar desassociar um alias de um sistema de arquivos que não esteja associado ao sistema de arquivos, o Amazon FSx responderá com um erro de solicitação inválida.

> **Note**
>
> Quando o Amazon FSx adiciona ou remove aliases em um sistema de arquivos, os clientes conectados são temporariamente desconectados e se reconectarão automaticamente ao sistema de arquivos. Todos os arquivos que foram abertos por clientes que mapeiam um compartilhamento non-Continuously-Available (non-CA - não disponível continuamente) no momento da desconexão devem ser reabertos pelo cliente.

Tópicos

Status do alias de DNS

Os aliases de DNS podem ter um dos seguintes valores de status:

- Disponível: o alias de DNS está associado a um sistema de arquivos do Amazon FSx.
- Criando: o Amazon FSx está criando o alias de DNS e associando-o ao sistema de arquivos.
- Excluindo: o Amazon FSx está desassociando o alias DNS do sistema de arquivos e excluindo-o.
- Falha ao criar: o Amazon FSx não conseguiu associar o alias de DNS ao sistema de arquivos.
- Falha ao excluir: o Amazon FSx não conseguiu desassociar o alias de DNS do sistema de arquivos.

Como usar aliases de DNS com autenticação Kerberos

Recomendamos que você use autenticação e criptografia baseadas no Kerberos em trânsito com o Amazon FSx. O Kerberos oferece a autenticação mais segura para clientes que acessam o sistema de arquivos. Para habilitar a autenticação Kerberos para clientes que acessam seu sistema de arquivos Amazon FSx usando um alias de DNS, você deve configurar nomes principais de serviço (SPNs) que correspondam ao alias DNS no objeto de computador do Active Directory do seu sistema de arquivos.

Se você tiver SPNs configurados para o alias de DNS que você atribuiu a outro sistema de arquivos em um objeto de computador no Active Directory, primeiro remova esses SPNs antes de adicionar SPNs ao objeto de computador do sistema de arquivos. Para ter mais informações, consulte Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos.

Visualizando aliases de DNS para sistemas de arquivos e backups

Você pode ver os aliases de DNS atualmente associados a sistemas de arquivos e backups usando o console Amazon FSx, a CLI e a API AWS . Este tópico fornece instruções sobre como visualizar os aliases de DNS para seus sistemas de arquivos e backups.

Para visualizar os aliases de DNS associados aos sistemas de arquivos

- Como usar o console: escolha um sistema de arquivos para visualizar a página de detalhes dos Sistemas de arquivos. Escolha a guia Rede e segurança para visualizar os Aliases de DNS.
- Usando a CLI ou a API — Use o comando da `describe-file-system-aliases` CLI ou a operação da API. DescribeFileSystemAliases

Para ver os aliases de DNS associados aos backups

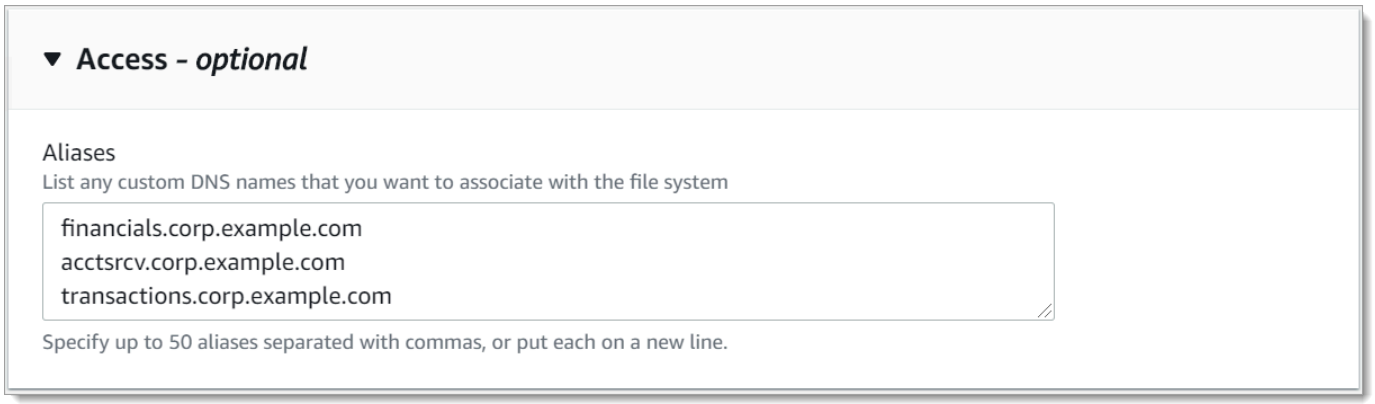
- Como usar o console: no painel de navegação, escolha Backups e, em seguida, escolha o backup que você deseja visualizar. No painel Resumo, visualize o campo Aliases de DNS.
- Usando a CLI ou a API — Use o comando da `describe-backups` CLI ou a operação da API. DescribeBackups

Associando aliases de DNS a sistemas de arquivos

Este tópico descreve como associar aliases de DNS ao criar um novo sistema de arquivos FSx for Windows File Server do zero ou ao criar um sistema de arquivos a partir de um backup, usando AWS Management Console a API AWS CLI, e.

Para associar aliases de DNS ao criar um novo sistema de arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para a criação de um novo sistema de arquivos descrito na Crie seu sistema de arquivos na seção de Conceitos básicos.
3. Na seção Acesso: opcional do assistente Criar sistema de arquivos, insira os aliases de DNS que você deseja associar ao sistema de arquivos.



4. Quando o sistema de arquivos está Disponível, você pode acessá-lo usando o alias de DNS configurando nomes de entidades principais de serviço (SPNs) e atualizando ou criando um registro CNAME do DNS para o alias. Para ter mais informações, consulte Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos.

Associar alias de DNS ao ser criado um sistema de arquivos do Amazon FSx (CLI)

1. Ao criar um novo sistema de arquivos, use a propriedade Alias com a operação da CreateFileSystemAPI para associar aliases de DNS ao novo sistema de arquivos.

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 2000 \
  --storage-type SSD \
  --subnet-ids subnet-123456 \
```

```
  --windows-configuration Aliases=[financials.corp.example.com,accts-
rcv.corp.example.com]
```

2. Quando o sistema de arquivos está Disponível, você pode acessá-lo usando o alias de DNS configurando nomes de entidades principais de serviço (SPNs) e atualizando ou criando um registro CNAME do DNS para o alias. Para ter mais informações, consulte Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos.

Para adicionar ou remover aliases de DNS ao restaurar um backup (CLI)

1. Ao criar um novo sistema de arquivos a partir de um backup de um sistema de arquivos existente, você pode usar a propriedade Aliases com a operação da CreateFileSystemFromBackupAPI da seguinte forma:

   - Por padrão, todos os aliases associados ao backup são associados ao novo sistema de arquivos.
   - Para criar um sistema de arquivos sem preservar quaisquer aliases do backup, use a propriedade `Aliases` com um conjunto vazio.

     Para associar aliases de DNS adicionais, use a propriedade `Aliases` e inclua os aliases originais associados ao backup e os novos aliases que você deseja associar.

   O comando da CLI a seguir associa dois aliases ao sistema de arquivos que o Amazon FSx está criando com base em um backup.

```
aws fsx create-file-system-from-backup \
  --backup-id backup-0123456789abcdef0
  --storage-capacity 2000 \
  --storage-type HDD \
  --subnet-ids subnet-123456 \
  --windows-configuration Aliases=[transactions.corp.example.com,accts-
rcv.corp.example.com]
```

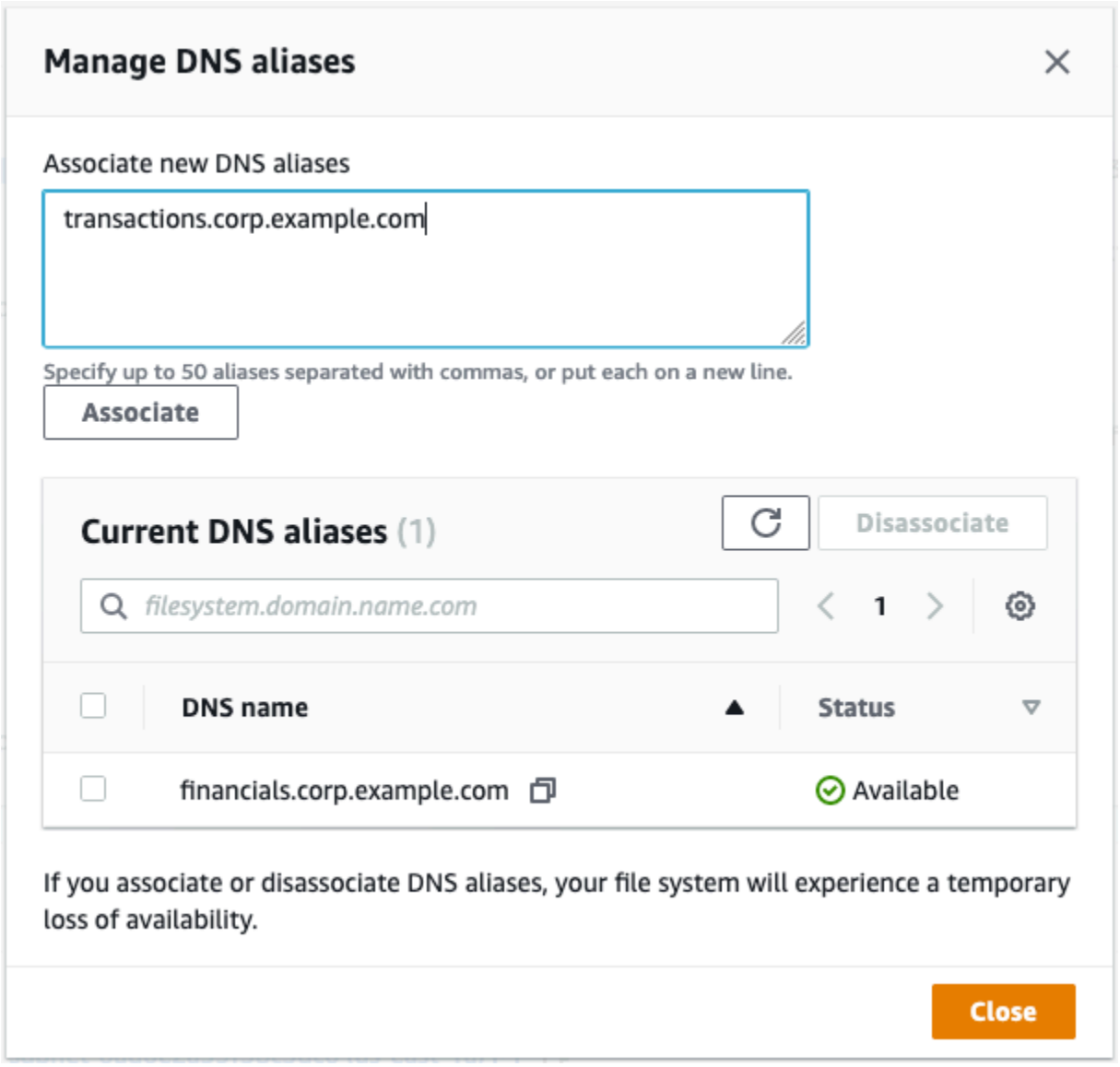
2. Quando o sistema de arquivos está Disponível, você pode acessá-lo usando o alias de DNS configurando nomes de entidades principais de serviço (SPNs) e atualizando ou criando um registro CNAME do DNS para o alias. Para ter mais informações, consulte Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos.

Como gerenciar aliases de DNS em sistemas de arquivos atuais

Este tópico descreve como você usa AWS Management Console e AWS CLI para adicionar e remover aliases em sistemas de arquivos existentes.

Para gerenciar aliases de DNS do 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 Windows para o qual você deseja gerenciar aliases de DNS.
3. Na guia Rede e segurança, escolha Gerenciar para que os Aliases de DNS exibam a caixa de diálogo Gerenciar aliases de DNS.



- Para associar aliases de DNS: na caixa Associar novos aliases, insira os aliases de DNS que você deseja associar. Selecione Associar.
- Para dissociar aliases de DNS: na lista Aliases atuais, escolha os aliases que você deseja desassociar. Escolha Desassociar.

Você pode monitorar o status dos aliases que você gerenciou na lista Aliases atuais. Atualize a lista para atualizar o status. São necessários até 2,5 minutos para que um alias seja associado ou desassociado de um sistema de arquivos.

4. Quando o alias estiver Disponível, você poderá acessar o sistema de arquivos usando o alias de DNS configurando nomes de entidades principais de serviço (SPNs) e atualizando ou criando um registro CNAME do DNS para o alias. Para ter mais informações, consulte Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos.

Para associar aliases de DNS a sistemas de arquivos (CLI) existentes

1. Use o comando `associate-file-system-aliases` CLI ou a operação da AssociateFileSystemAliasesAPI para associar aliases de DNS a um sistema de arquivos existente.

   A solicitação da CLI a seguir associa dois aliases ao sistema de arquivos especificado.

   ```
   aws fsx associate-file-system-aliases \
     --file-system-id fs-0123456789abcdef0 \
     --aliases financials.corp.example.com transfers.corp.example.com
   ```

   A resposta mostra o status dos aliases que o Amazon FSx está associando ao sistema de arquivos.

   ```
   {
       "Aliases": [
           {
               "Name": "financials.corp.example.com",
               "Lifecycle": CREATING
           },
           {
               "Name": "transfers.corp.example.com",
               "Lifecycle": CREATING
   ```

```
        }
    ]
}
```

2. Use o comando `describe-file-system-aliases` CLI (DescribeFileSystemAliasesé a operação de API equivalente) para monitorar o status dos aliases que você está associando.
3. Quando o `Lifecycle` estiver no valor DISPONÍVEL (um processo que leva até 2,5 minutos), você poderá acessar o sistema de arquivos usando o alias de DNS configurando nomes de entidades principais de serviço (SPNs) e atualizando ou criando um registro CNAME do DNS para o alias. Para ter mais informações, consulte Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos.

Para dissociar aliases de DNS dos sistemas de arquivos (CLI)

- Use o comando `disassociate-file-system-aliases` CLI ou a operação da DisassociateFileSystemAliasesAPI para dissociar aliases de DNS de um sistema de arquivos existente.

  O comando a seguir desassocia um alias de um sistema de arquivos.

  ```
  aws fsx disassociate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com
  ```

  A resposta mostra o status dos aliases que o Amazon FSx está desassociando do sistema de arquivos.

  ```
  {
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": DELETING
          }
      ]
  }
  ```

  Use o comando `describe-file-system-aliases` CLI (DescribeFileSystemAliasesé a operação equivalente da API) para monitorar o status dos aliases. Leva até 2,5 minutos para que o alias seja excluído.

Gerenciando compartilhamentos de arquivos em sistemas de arquivos FSx for Windows File Server

Este tópico descreve como você pode gerenciar compartilhamentos de arquivos executando as seguintes tarefas.

- Criar um compartilhamento de arquivos
- Modificar um compartilhamento de arquivos existente
- Remover um compartilhamento de arquivos existente

Você pode usar a GUI de pastas compartilhadas nativa do Windows e a CLI do Amazon FSx para gerenciamento remoto para gerenciar compartilhamentos de arquivos em seu PowerShell sistema de arquivos FSx for Windows File Server. Você pode enfrentar atrasos ao usar a GUI da pasta compartilhada (fsmgmt.msc) ao abrir pela primeira vez o menu de contexto para compartilhamentos localizados em um sistema de arquivos diferente. Para evitar esses atrasos, use PowerShell para gerenciar compartilhamentos de arquivos localizados em vários sistemas de arquivos.

Existem regras e limitações necessárias para todos os sistemas de arquivos compatíveis com o Windows nos nomes de arquivos e diretórios". Para garantir que você possa criar e acessar seus dados com êxito, você deve nomear seus arquivos e diretórios de acordo com essas diretrizes do Windows. Para obter mais informações, consulte Convenções de nomenclatura.

> ⚠ Warning
>
> O Amazon FSx exige que o usuário SYSTEM tenha permissões de ACL do NTFS de Controle total em cada pasta na qual você cria um compartilhamento de arquivos SMB. Não altere as permissões de ACL do NTFS para esse usuário nas pastas, pois isso pode tornar seus compartilhamentos de arquivos inacessíveis.

Gerenciando compartilhamentos de arquivos com a GUI de Pastas Compartilhadas

Para gerenciar compartilhamentos de arquivos no sistema de arquivos do Amazon FSx, você pode usar a GUI de pastas compartilhadas. A GUI de pastas compartilhadas fornece um local central para

o gerenciamento de todas as pastas compartilhadas em um servidor Windows. Os procedimentos a seguir descrevem como gerenciar compartilhamentos de arquivos.

Conectar pastas compartilhadas ao sistema de arquivos do FSx para Windows File Server

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. No Microsoft Active Directory AWS gerenciado, esse grupo é chamado de Administradores FSx AWS Delegados. No Microsoft Active Directory autogerenciado, esse grupo é chamado de Administradores de domínio ou o nome personalizado do grupo de administradores que você forneceu durante a criação. Para obter mais informações, consulte Conectar-se à sua instância do Windows no Guia do usuário do Amazon Elastic Compute Cloud (Amazon EC2) para instâncias do Windows.
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 do Sistema de Nomes de Domínio (DNS) do sistema de arquivos do Amazon FSx, por exemplo, **`amznfsxabcd0123.corp.example.com`**.

   Para encontrar o nome DNS do sistema de arquivos no console do Amazon FSx, escolha Sistemas de arquivos, escolha o sistema de arquivos e, em seguida, marque a seção Rede e segurança na página de detalhes do sistema de arquivos. Você também pode obter o nome DNS na resposta da operação da API de DescribeFilesistemas.
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 sistema de arquivos do Amazon FSx, você pode gerenciar os compartilhamentos de arquivos do Windows no sistema de arquivos. O compartilhamento padrão é denominado `\share`. Para isso, siga as seguintes ações:

- 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. 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: clique em “Procurar” quando especificar um caminho de pasta local e clique em “Criar pasta” para criar a pasta local.
- Como usar a linha de comando:

```
New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share
\MyNewShare
```

- 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**
>
> Para sistemas de arquivos single-AZ 2 e multi-AZ, a remoção ou a modificação de compartilhamentos de arquivos (incluindo a atualização de permissões, limites de usuário e outras propriedades) usando a ferramenta GUI de pastas compartilhadas só é possível se você se conectar a fsmgmt.msc usando o nome DNS do sistema de arquivos do Amazon FSx. A ferramenta GUI de Pastas Compartilhadas não oferece suporte a essas ações se você se conectar usando o endereço IP ou o nome de alias de DNS do sistema de arquivos.

> **Note**
>
> Se você estiver usando a ferramenta GUI de pastas compartilhadas fsmgmt.msc para acessar compartilhamentos localizados em vários sistemas de arquivos do FSx, poderá haver atrasos quando for aberto pela primeira vez o menu de contexto de um compartilhamento de arquivos localizado em um sistema de arquivos diferente. Para evitar

esses atrasos, você pode gerenciar compartilhamentos de arquivos usando PowerShell conforme descrito abaixo.

Gerenciando compartilhamentos de arquivos com PowerShell

Você pode gerenciar compartilhamentos de arquivos usando comandos personalizados de gerenciamento remoto para. PowerShell Esses comandos podem ajudar você a automatizar mais facilmente as seguintes tarefas:

- Migração de compartilhamentos de arquivos em servidores de arquivos atuais para o Amazon FSx
- Sincronização de compartilhamentos de arquivos entre AWS regiões para recuperação de desastres
- Gerenciamento programático de compartilhamentos de arquivos para fluxos de trabalho contínuos, como provisionamento de compartilhamento de arquivos em equipe

Para saber como usar a CLI do Amazon FSx para gerenciamento remoto em, consulte. PowerShell Usando a CLI do Amazon FSx para PowerShell

A tabela a seguir lista os PowerShell comandos de gerenciamento remoto da CLI do Amazon FSx que você pode usar para gerenciar compartilhamentos de arquivos nos sistemas de arquivos FSx for Windows File Server.

Comando de gerenciamento de compartilhamento	Descrição
New-FSxSmbShare	Cria um compartilhamento de arquivos.
Remove-FSxSmbShare	Remove um compartilhamento de arquivos.
Get-FSxSmbShare	Recupera compartilhamentos de arquivos atuais.
Set-FSxSmbShare	Define as propriedades de um compartilhamento.
Get-FSxSmbShareAccess	Recupera a lista de controle de acesso (ACL) de um compartil hamento.

Comando de gerenciamento de compartilhamento	Descrição
Grant-FSxSmbShareAccess	Adiciona uma access control entry (ACE - entrada de controle de acesso) de permissão para um administrador ao descritor de segurança de um compartilhamento.
Revoke-FSxSmbShareAccess	Remove todas as ACEs de permissão para um administrador do descritor de segurança de um compartilhamento.
Block-FSxSmbShareAccess	Adiciona uma ACE de negação para um administrador ao descritor de segurança de um compartilhamento.
Unblock-FSxSmbShareAccess	Remove todas as ACEs de negação para um administrador do descritor de segurança de um compartilhamento.

A ajuda on-line de cada comando fornece uma referência de todas as opções de comando. Para acessar essa ajuda, execute o comando com um `-?`, por exemplo `New-FSxSmbShare -?`.

Passando credenciais para o SxSmb New-F Share

Você pode passar as credenciais para o New-F SxSmbShare para poder executá-las em um loop para criar centenas ou milhares de compartilhamentos sem precisar inserir as credenciais novamente a cada vez.

Prepare o objeto de credencial necessário para criar os compartilhamentos de arquivos no servidor de arquivos do FSx para Windows File Server usando uma das opções a seguir.

- Para gerar o objeto de credencial de forma interativa, use o comando a seguir.

```
$credential = Get-Credential
```

- Para gerar o objeto de credencial usando um AWS Secrets Manager recurso, use o comando a seguir.

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

Criação de compartilhamento continuamente disponível (CA)

Você pode criar compartilhamentos continuamente disponíveis (CA) usando a CLI do Amazon FSx para gerenciamento remoto ativado. PowerShell Os compartilhamentos CA criados em um sistema de arquivos multi-AZ do FSx para Windows File Server são altamente duráveis e altamente disponíveis. Um sistema de arquivos single-AZ do Amazon FSx AZ é criado em um cluster de nó individual. Como resultado, os compartilhamentos CA criados em um sistema de arquivos single-AZ são altamente duráveis, mas não são altamente disponíveis. Use o comando `New-FSxSmbShare` com a opção `-ContinuouslyAvailable` definida como `$True` para especificar que o compartilhamento é um compartilhamento continuamente disponível. Veja a seguir um exemplo de comando para criar um compartilhamento CA.

```
New-FSxSmbShare -Name "New CA Share" -Path "D:\share\new-share" -Description "CA share"
 -ContinuouslyAvailable $True
```

Você pode modificar a opção `-ContinuouslyAvailable` em um compartilhamento de arquivos atual usando o comando `Set-FSxSmbShare`.

Determine se um compartilhamento de arquivos existente está continuamente disponível

Use o comando a seguir para visualizar o valor da propriedade Continuely Available para um compartilhamento de arquivos existente.

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { get-fsxsmbshare -name share_name }
```

Se a CA estiver habilitada, a saída incluirá a seguinte linha:

```
[...]
ContinuouslyAvailable : True
[...]
```

Se a CA não estiver habilitada, a saída incluirá a seguinte linha:

```
[...]
ContinuouslyAvailable : False
[...]
```

Para ativar a Disponibilidade Contínua em um compartilhamento de arquivos existente, use o seguinte comando:

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { set-fsxsmbshare -name share_name -ContinuouslyAvailable $True}
```

Auditoria de acesso a arquivos

O Amazon FSx for Windows File Server oferece suporte à auditoria do acesso do usuário final a arquivos, pastas e compartilhamentos de arquivos. Você pode optar por enviar os registros de eventos de auditoria de um sistema de arquivos para outros AWS serviços que oferecem um rico conjunto de recursos. Isso inclui permitir a consulta, o processamento, o armazenamento e o arquivamento de registros, a emissão de notificações e o acionamento de ações para promover ainda mais suas metas de segurança e conformidade.

Para obter mais informações sobre o uso da auditoria de acesso a arquivos para obter insights sobre padrões de acesso e implementar notificações de segurança para a atividade do usuário final, consulte File storage access patterns insights e Implementing security notifications for end user activity.

A auditoria de acesso a arquivos permite que você registre os acessos de usuários finais a arquivos, pastas e compartilhamentos de arquivos individuais com base nos controles de auditoria definidos. Os controles de auditoria também são conhecidos como listas de controle de acesso do sistema NTFS (SACLs). Caso já tenha controles de auditoria configurados em seus dados de arquivos existentes, você pode tirar proveito da auditoria de acesso a arquivos criando um novo sistema de arquivos do Amazon FSx para Windows File Server e migrando seus dados.

O Amazon FSx oferece suporte aos seguintes eventos de auditoria do Windows para acessos a arquivos, pastas e compartilhamentos de arquivos:

- Para acessos a arquivos, ele é compatível com: Tudo, Ir para pasta/Executar arquivo, Listar pasta/Ler dados, Ler atributos, Criar arquivos/Gravar dados, Criar pastas/Anexar dados, Gravar recursos, Excluir subpastas e arquivos, Excluir, Ler permissões, Alterar permissões e Assumir propriedade.
- Para acessos ao compartilhamento de arquivos, ele é compatível com: Conectar com um compartilhamento de arquivos.

Em todos os acessos a arquivos, pastas e compartilhamentos de arquivos, o Amazon FSx é compatível com o registro em log de tentativas com êxito (como um usuário com permissões

suficientes acessando com êxito um arquivo ou compartilhamento de arquivos), tentativas malsucedidas ou ambas.

Você pode configurar se deseja auditoria de acesso somente em arquivos e pastas, somente em compartilhamentos de arquivos ou em ambos. Você também pode configurar quais tipos de acesso devem ser registrados em log (somente tentativas com êxito, somente tentativas malsucedidas ou ambas). Você também pode desativar a auditoria de acesso a arquivos a qualquer momento.

> **Note**
>
> A auditoria de acesso a arquivos registra os dados de acesso do usuário final somente a partir do momento em que é ativada. Ou seja, a auditoria de acesso a arquivos não gera logs de eventos de auditoria de atividades de acesso a arquivos, pastas e compartilhamentos de arquivos do usuário final que ocorreram antes da habilitação da auditoria de acesso a arquivos.

A taxa máxima de eventos de auditoria de acesso compatível é de cinco mil eventos por segundo. Os eventos de auditoria de acesso não são gerados para cada operação de leitura e gravação de arquivo, mas são gerados uma vez por operação de metadados de arquivo, como quando um usuário cria, abre ou exclui um arquivo.

Tópicos

Destinos dos logs de eventos de auditoria

Ao habilitar a auditoria de acesso a arquivos, você deve configurar um AWS serviço para o qual o Amazon FSx envia os registros de eventos de auditoria. Você pode enviar registros de eventos de auditoria para um stream de CloudWatch logs do Amazon Logs em um grupo de CloudWatch logs do Logs ou para um stream de entrega do Amazon Data Firehose. Você escolhe o destino dos logs de eventos de auditoria ao criar seu sistema de arquivos Amazon FSx for Windows File Server

ou a qualquer momento ao atualizar um sistema de arquivos existente. Para ter mais informações, consulte Como gerenciar a auditoria de acesso a arquivos.

Veja abaixo algumas recomendações que podem ajudar você a decidir qual destino dos logs de eventos de auditoria escolher:

- Escolha CloudWatch Logs se quiser armazenar, visualizar e pesquisar registros de eventos de auditoria no CloudWatch console da Amazon, executar consultas nos CloudWatch registros usando o Logs Insights e acionar CloudWatch alarmes ou funções Lambda.
- Escolha Firehose se quiser transmitir eventos continuamente para armazenamento no Amazon S3, para um banco de dados no Amazon Redshift, para o OpenSearch Amazon Service ou para soluções de parceiros (como Splunk ou Datadog) AWS para análise posterior.

Por padrão, o Amazon FSx criará e usará um grupo padrão de registros de CloudWatch registros em sua conta como destino do registro de eventos de auditoria. Se você quiser usar um grupo de registros de CloudWatch registros personalizado ou usar o Firehose como destino do registro de eventos de auditoria, aqui estão os requisitos para os nomes e locais do destino do registro de eventos de auditoria:

- O nome do grupo de CloudWatch registros de registros deve começar com o `/aws/fsx/` prefixo. Se você não tiver um grupo de CloudWatch registros de registros existente ao criar ou atualizar um sistema de arquivos no console, o Amazon FSx pode criar e usar um fluxo de registros padrão no grupo de registros de CloudWatch `/aws/fsx/windows` registros. Se você não quiser usar o grupo de registros padrão, a interface de configuração permite criar um grupo de CloudWatch registros de registros ao criar ou atualizar seu sistema de arquivos no console.
- O nome do stream de entrega do Firehose deve começar com o `aws-fsx-` prefixo. Se você não tiver um stream de entrega do Firehose existente, poderá criar um ao criar ou atualizar seu sistema de arquivos no console.
- O stream de entrega do Firehose deve ser configurado para ser usado `Direct PUT` como fonte. Você não pode usar um fluxo de dados existente do Kinesis como fonte de dados para seu fluxo de entrega.
- O destino (grupo de CloudWatch registros de registros de registros ou stream de entrega do Firehose) deve estar na mesma AWS partição e Conta da AWS em seu sistema de arquivos Amazon FSx. Região da AWS

Você pode alterar o destino do registro de eventos de auditoria a qualquer momento (por exemplo, de CloudWatch Logs para Firehose). Ao fazer isso, os novos logs de eventos de auditoria serão enviados somente para o novo destino.

Entrega de máximo esforço de logs de eventos de auditoria

Normalmente, os registros do registro de eventos de auditoria são entregues ao destino em minutos, mas às vezes podem levar mais tempo. Em ocasiões muito raras, os registros de logs de eventos de auditoria podem ser perdidos. Se seu caso de uso exigir uma semântica específica (por exemplo, garantir que nenhum evento de auditoria seja perdido), recomendamos que você contabilize os eventos perdidos ao criar seus fluxos de trabalho. Você pode auditar eventos perdidos verificando a estrutura de arquivos e pastas em seu sistema de arquivos.

Como migrar seus controles de auditoria

Se você tiver controles de auditoria (SACLs) já configurados em seus dados de arquivos existentes, você pode criar um sistema de arquivos do Amazon FSx e migrar seus dados para o novo sistema de arquivos. Recomendamos usar AWS DataSync para transferir dados e os SACLs associados para seu sistema de arquivos Amazon FSx. Como solução alternativa, você pode usar o Robocopy (Robust File Copy). Para ter mais informações, consulte Como migrar o armazenamento de arquivos atual para o Amazon FSx.

Como visualizar logs de eventos

Você pode visualizar os logs de eventos de auditoria depois que o Amazon FSx começar a emiti-los. Onde e como você visualiza os logs, depende do destino dos logs de eventos de auditoria:

- Você pode ver CloudWatch os registros de registros acessando o CloudWatch console e escolhendo o grupo de registros e o stream de registros para os quais seus registros de eventos de auditoria são enviados. Para obter mais informações, consulte Exibir dados de log enviados para CloudWatch Logs no Guia do usuário do Amazon CloudWatch Logs.

  Você pode usar o CloudWatch Logs Insights para pesquisar e analisar interativamente seus dados de registro. Para obter mais informações, consulte Análise de dados de log com o CloudWatch Logs Insights, no Guia do usuário do Amazon CloudWatch Logs.

  Você também pode exportar logs de eventos de auditoria para o Amazon S3. Para obter mais informações, consulte Exportação de dados de log para o Amazon S3, também no Guia do usuário do CloudWatch Amazon Logs.

- Você não pode ver os registros de eventos de auditoria no Firehose. No entanto, você pode configurar o Firehose para encaminhar os registros para um destino que você possa ler. Os destinos incluem Amazon S3, Amazon Redshift, OpenSearch Amazon Service e soluções de parceiros, como Splunk e Datadog. Para obter mais informações, consulte Escolha o destino no Guia do desenvolvedor do Amazon Data Firehose.

Campos de eventos de auditoria

Esta seção fornece descrições das informações nos logs de eventos de auditoria e exemplos de eventos de auditoria.

A seguir, estão as descrições dos campos relevantes em um evento de auditoria do Windows.

- EventID refere-se à ID de evento do log de eventos do Windows definida pela Microsoft. Consulte a documentação da Microsoft para obter informações sobre eventos do sistema de arquivos e eventos de compartilhamento de arquivos.
- SubjectUserNamerefere-se ao usuário que está realizando o acesso.
- ObjectNamerefere-se ao arquivo, pasta ou compartilhamento de arquivos de destino que foi acessado.
- ShareNameestá disponível para eventos gerados para acesso ao compartilhamento de arquivos. Por exemplo, o `EventID 5140` será gerado quando um objeto de compartilhamento de rede for acessado.
- IpAddressrefere-se ao cliente que iniciou o evento para eventos de compartilhamento de arquivos.
- As palavras-chave, quando disponíveis, referem-se a se o acesso ao arquivo foi bem-sucedido ou falhou. Para acessos bem-sucedidos, o valor é `0x8020000000000000`. Para acessos malsucedidos, o valor é `0x8010000000000000`.
- TimeCreated SystemTimerefere-se à hora em que o evento foi gerado no sistema e exibido no <YYYY-MM-DDThh:mm:ss.s>formato Z.
- Computador se refere ao nome DNS do sistema de arquivos Windows Remote PowerShell Endpoint e pode ser usado para identificar o sistema de arquivos.
- AccessMask, quando disponível, refere-se ao tipo de acesso ao arquivo realizado (por exemplo, ReadData, WriteData).
- AccessListrefere-se ao acesso solicitado ou concedido a um objeto. Para obter detalhes, consulte a tabela abaixo e a documentação da Microsoft (conforme no Evento 4556).

Tipo de acesso	Máscara de acesso	Valor
Ler dados ou listar diretório	0x1	%%4416
Gravar dados ou adicionar arquivo	0x2	%%4417
Anexar dados ou adicionar subdiretório	0x4	%%4418
Ler atributos estendidos	0x8	%%4419
Gravar atributos estendidos	0x10	%%4420
Executar ou percorrer	0x20	%%4421
Excluir filho	0x40	%%4422
Ler atributos	0x80	%%4423
Atributos de gravação	0x100	%%4424
Delete	0x10000	%%1537
Ler a ACL	0x20000	%%1538
Gravar a ACL	0x40000	%%1539
Gravar o proprietário	0x80000	%%1540
Sincronizar	0x100000	%%1541
Acessar a ACL de segurança	0x1000000	%%1542

Veja abaixo alguns eventos importantes com exemplos. Observe que o XML é formatado para facilitar a leitura.

O ID de evento 4660 será registrado quando um objeto for excluído.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
```

```
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4660</EventID><Version>0</Version><Level>0</Level>
<Task>12800</Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-05-18T04:51:56.916563800Z'/>
<EventRecordID>315452</EventRecordID><Correlation/>
<Execution ProcessID='4' ThreadID='5636'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x50932f71</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='HandleId'>0x12e0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data></EventData></
Event>
```

O ID de evento 4659 será registrado em uma solicitação para excluir um arquivo.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4659</EventID><Version>0</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-0603T19:18:09.951551200Z'/>
<EventRecordID>308888</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5540'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\shar
\event.txt</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1537
    %%4423
    </Data><Data Name='AccessMask'>0x10080</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='ProcessId'>0x4</Data></EventData></Event>
```

O ID de evento 4663 será registrado quando uma operação específica for executada no objeto. O exemplo a seguir mostra a leitura de dados de um arquivo, que podem ser interpretados na `AccessList %%4416`.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663< /EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:10:13.887145400Z'/>
<EventRecordID>308831</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='6916'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData>< Data
 Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113< /Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0x101c</Data><Data Name='AccessList'>%%4416
    </Data>
<Data Name='AccessMask'>0x1</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data>
</EventData></Event>
```

O exemplo a seguir mostra como gravar ou acrescentar dados de um arquivo, que podem ser interpretados na `AccessList %%4417`.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:12:16.813827100Z'/>
<EventRecordID>308838</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5828'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
```

```
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0xa38</Data><Data Name='AccessList'>%%4417
    </Data><Data Name='AccessMask'>0x2</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data></
EventData></Event>
```

O ID de evento 4656 indica que um acesso específico foi solicitado para um objeto. No exemplo a seguir, a solicitação de leitura foi iniciada para ObjectName “permtest” e foi uma tentativa malsucedida, conforme visto no valor de palavras-chave de`0x8010000000000000`.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4656</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:22:55.113783500Z'/>
<EventRecordID>308919</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='4924'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1541
    %%4416
    %%4423
    </Data><Data Name='AccessReason'>%%1541: %%1805
    %%4416: %%1805
    %%4423: %%1811 D:(A;OICI;0x1301bf;;;AU)
    </Data><Data Name='AccessMask'>0x100081</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='RestrictedSidCount'>0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
```

```
<Data Name='ResourceAttributes'>-</Data></EventData></Event>
```

O ID de evento 4670 é registrado quando as permissões de um objeto são alteradas. O exemplo a seguir mostra que o usuário “admin” modificou a permissão em “permtest” para adicionar permissões ao SID ObjectName “S-1-5-21-658495921-4185342820-3824891517-1113". Consulte a documentação da Microsoft para obter mais informações sobre como interpretar as permissões.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4670</EventID><Version>0</Version><Level>0</Level>
<Task>13570</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='2021-06-03T19:39:47.537129500Z'/><EventRecordID>308992</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='2776'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0xcc8</Data>
<Data Name='OldSd'>D:PAI(A;OICI;FA;;;SY)
(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-2622)</Data>
<Data Name='NewSd'>D:PARAI(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-1113)
(A;OICI;FA;;;SY)(A;OICI;FA;;;
S-1-5-21-658495921-4185342820-3824891517-2622)</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data></EventData></Event>
```

O ID de evento 5140 é registrado sempre que um compartilhamento de arquivo é acessado.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5140</EventID><Version>1</Version><Level>0</Level><Task>12808</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:32:07.535208200Z'/>
<EventRecordID>308947</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='3120'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
```

```
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-2620</
Data>
<Data Name='SubjectUserName'>EC2AMAZ-1GP4HMN$</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2d4ca529</Data><Data Name='ObjectType'>File</Data><Data
 Name='IpAddress'>172.45.6.789</Data>
<Data Name='IpPort'>49730</Data><Data Name='ShareName'>\\AMZNFSXCYDKLDZZ\share</Data>
<Data Name='ShareLocalPath'>\??\D:\share</Data><Data Name='AccessMask'>0x1</Data><Data
 Name='AccessList'>%%4416
    </Data></EventData></Event>
```

O ID de evento 5145 é registrado quando o acesso é negado no nível do compartilhamento de arquivos. O exemplo a seguir mostra que o acesso a ShareName “demoshare01" foi negado.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5145</EventID><Version>0</Version><Level>0</Level>
<Task>12811</Task><Opcode>0</Opcode><Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime='2021-05-19T22:30:40.485188700Z'/><EventRecordID>282939</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='344'/><Channel>Security</Channel>
<Computer>amznfsxtmn9autz.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-
1113</Data><Data Name='SubjectUserName'>Admin</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x95b3fb7</Data><Data Name='ObjectType'>File</Data>
<Data Name='IpAddress'>172.31.7.112</Data><Data Name='IpPort'>59979</Data>
<Data Name='ShareName'>\\AMZNFSXDPNTE0DC\demoshare01</Data><Data Name='ShareLocalPath'>
\??\D:\demoshare01</Data>
<Data Name='RelativeTargetName'>Desktop.ini</Data><Data Name='AccessMask'>0x120089</
Data>
<Data Name='AccessList'>%%1538 %%1541 %%4416 %%4419 %%4423 </Data><Data
 Name='AccessReason'>%%1538:
%%1804 %%1541: %%1805 %%4416: %%1805 %%4419: %%1805 %%4423: %%1805 </Data></
EventData></Event>
```

Se você usar o CloudWatch Logs Insights para pesquisar seus dados de registro, poderá executar consultas nos campos de eventos, conforme mostrado nos exemplos a seguir:

- Para consultar um ID de evento específico:

```
fields @message
   | filter @message like /4660/
```

- Para consultar todos os eventos que correspondem a um nome de arquivo específico:

```
fields @message
   | filter @message like /event.txt/
```

Para obter mais informações sobre a linguagem de consulta do CloudWatch Logs Insights, consulte Análise de dados de log com o CloudWatch Logs Insights, no Guia do usuário do Amazon CloudWatch Logs.

Configurando controles de auditoria de arquivos e pastas

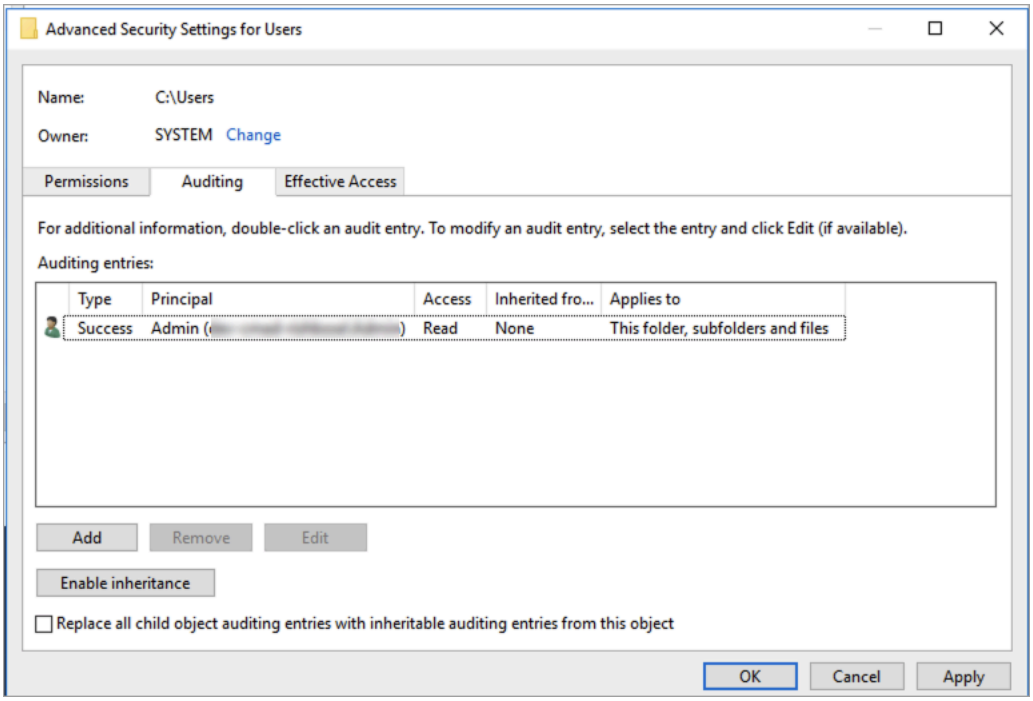
Você precisa definir controles de auditoria nos arquivos e pastas que você deseja auditar quanto a tentativas de acesso do usuário. Os controles de auditoria também são conhecidos como listas de controle de acesso do sistema NTFS (SACLs).

Você configura os controles de auditoria usando a interface GUI nativa do Windows ou programaticamente usando comandos do Windows. PowerShell Se a herança estiver habilitada, você normalmente precisará definir controles de auditoria somente nas pastas de nível superior nas quais deseja registrar os acessos.

Como usar a GUI do Windows para definir o acesso de auditoria

Para usar uma GUI para definir controles de auditoria em seus arquivos e pastas, use o Explorador de Arquivos do Windows. Em um determinado arquivo ou pasta, abra o Explorador de Arquivos do Windows e selecione a guia Propriedades > Segurança > Avançado > Auditoria.

O exemplo de controle de auditoria a seguir audita eventos com êxito de uma pasta. Uma entrada de logs de eventos do Windows será emitida sempre que esse identificador for aberto para leitura com êxito pelo usuário administrador.



O campo Tipo indica quais ações você deseja auditar. Defina esse campo como Com êxito para tentativas de auditoria com êxito, como Falha para tentativas de auditoria com falha ou Tudo para tentativas de auditoria com êxito e com falha.

Para obter mais informações sobre os campos de entrada de auditoria, consulte Apply a basic audit policy on a file or folder na documentação da Microsoft.

Usando PowerShell comandos para definir o acesso de auditoria

Você pode usar o comando `Set-Acl` do Microsoft Windows para definir a SACL de auditoria em qualquer arquivo ou pasta. Para obter informações sobre esse comando, consulte a documentação do Set-Acl da Microsoft.

Veja a seguir um exemplo do uso de uma série de PowerShell comandos e variáveis para definir o acesso de auditoria para tentativas bem-sucedidas. Você pode adaptar esses comandos de exemplo para atender às necessidades do seu sistema de arquivos.

```
$path = "C:\Users\TestUser\Desktop\DemoTest\"

$ACL = Get-Acl $path

$ACL | Format-List

$AuditUser = "TESTDOMAIN\TestUser"
```

```
$AuditRules = "FullControl"

$InheritType = "ContainerInherit,ObjectInherit"

$AuditType = "Success"

$AccessRule = New-Object System.Security.AccessControl.FileSystemAuditRule($AuditUser,
$AuditRules,$InheritType,"None",$AuditType)

$ACL.SetAuditRule($AccessRule)

$ACL | Set-Acl $path

Get-Acl $path -Audit | Format-List
```

Como gerenciar a auditoria de acesso a arquivos

Você pode habilitar a auditoria de acesso a arquivos ao criar um novo sistema de arquivos do Amazon FSx para Windows File Server. A auditoria de acesso a arquivos é desativada por padrão quando você cria um sistema de arquivos no console do Amazon FSx.

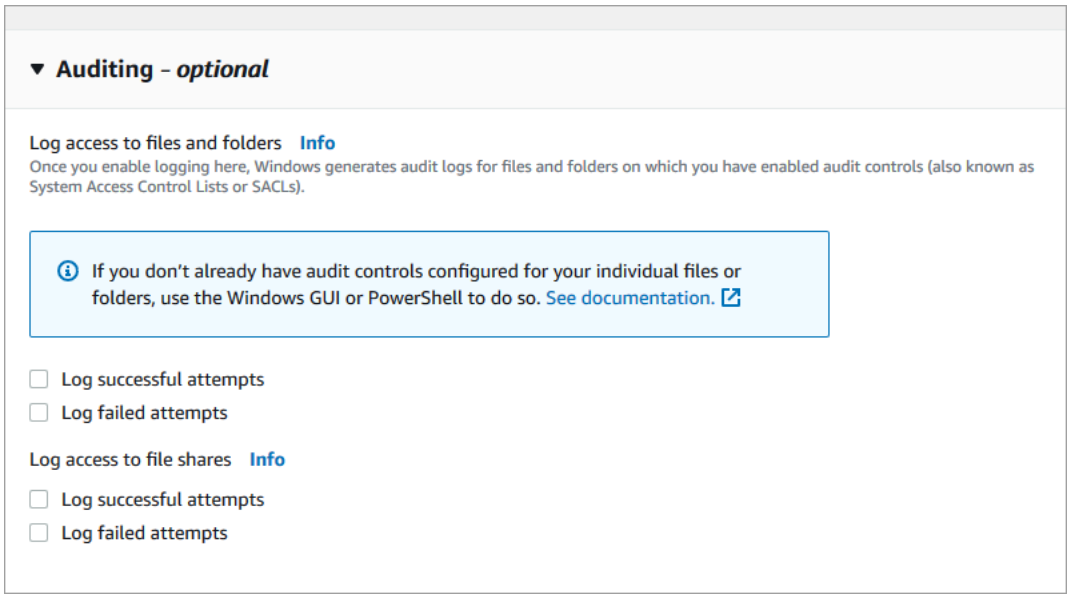
Em sistemas de arquivos existentes que têm a auditoria de acesso a arquivos habilitada, você pode alterar as configurações de auditoria de acesso a arquivos, incluindo a alteração dos tipos de tentativa de acesso para acessos a arquivos e compartilhamentos de arquivos e o destino dos logs de eventos de auditoria. Você pode realizar essas tarefas usando o console ou a API do Amazon FSx. AWS CLI

> **Note**
>
> A auditoria de acesso a arquivos é compatível somente nos sistemas de arquivos do Amazon FSx para Windows File Server com uma capacidade de throughput de 32 MB/s ou maior. Você não pode criar ou atualizar um sistema de arquivos com uma capacidade de throughput inferior a 32 MB/s se a auditoria de acesso a arquivos estiver habilitada. Você pode modificar a capacidade de throughput a qualquer momento depois de criar o sistema de arquivos. Para ter mais informações, consulte Como gerenciar a capacidade de throughput.

Habilitar a auditoria de acesso a arquivos ao criar um sistema de arquivos (console)

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

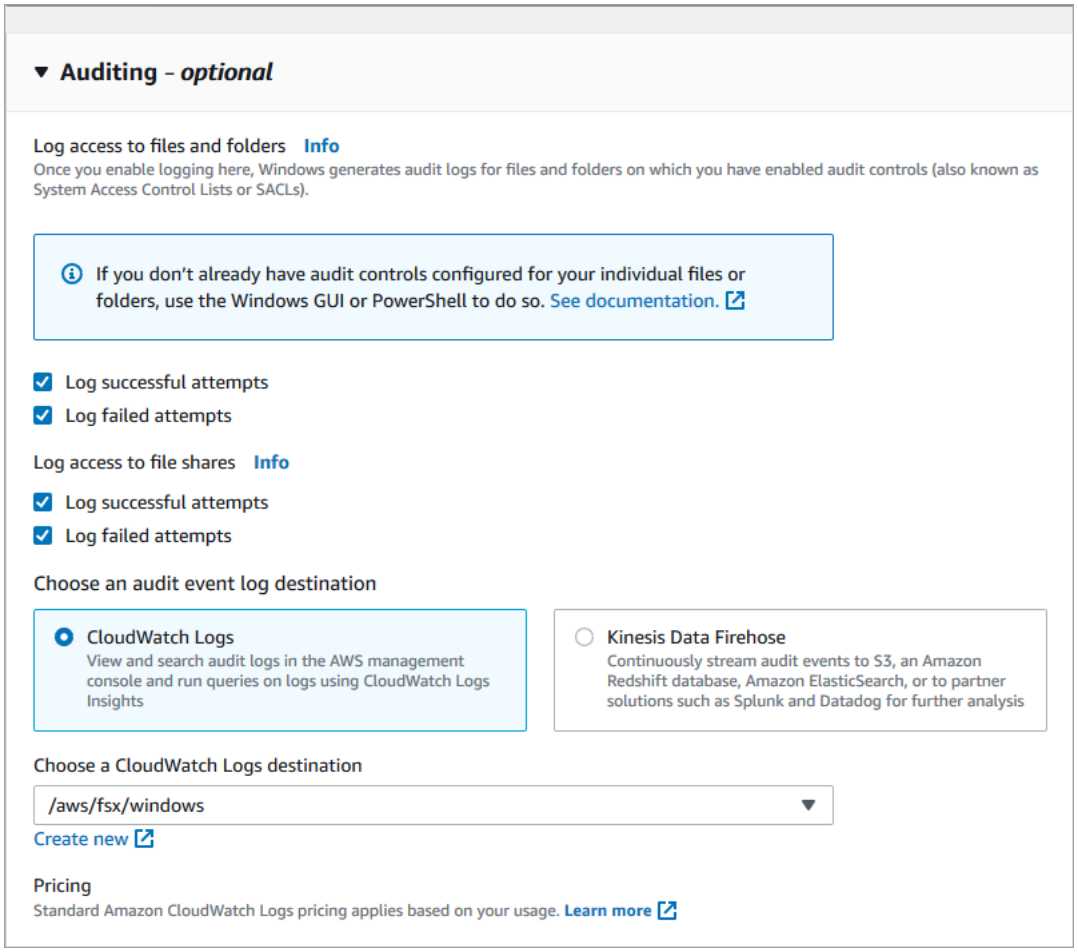
2. Siga o procedimento para a criação de um novo sistema de arquivos descrito na Crie seu sistema de arquivos na seção de Conceitos básicos.
3. Abra a seção Auditoria: opcional. A auditoria de acesso a arquivos é desabilitada por padrão.



4. Para habilitar e configurar a auditoria de acesso a arquivos, siga o procedimento a seguir.

   - Em Registrar acesso a arquivos e pastas, selecione o registro em log de tentativas com êxito e/ou malsucedidas. O registro em log estará desabilitado para arquivos e pastas caso você não selecione.
   - Em Registrar acesso aos compartilhamentos de arquivos, selecione o registro em log de tentativas com êxito e/ou malsucedidas. O registro em log estará desabilitado para compartilhamentos de arquivos, caso você não faça uma seleção.
   - Em Escolher um destino de registro de eventos de auditoria, escolha CloudWatch Logs ou Firehose. Em seguida, escolha um fluxo de logs ou fluxo de entrega existente ou crie um. Para CloudWatch registros, o Amazon FSx pode criar e usar um fluxo de registros padrão no grupo de CloudWatch registros de `/aws/fsx/windows` registros.

   Veja a seguir um exemplo de uma configuração de auditoria de acesso a arquivos que auditará tentativas de acesso com êxito e malsucedidas de usuários finais a arquivos, pastas e compartilhamentos de arquivos. Os registros de eventos de auditoria serão enviados para o destino padrão do grupo de CloudWatch `/aws/fsx/windows` registros de registros.



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

Quando o sistema de arquivos está Disponível, o recurso de auditoria de acesso a arquivos está habilitado.

Habilitar a auditoria de acesso a arquivos ao criar um sistema de arquivos (CLI)

1. Ao criar um novo sistema de arquivos, use a `AuditLogConfiguration` propriedade com a operação da CreateFileSystemAPI para habilitar a auditoria de acesso a arquivos para o novo sistema de arquivos.

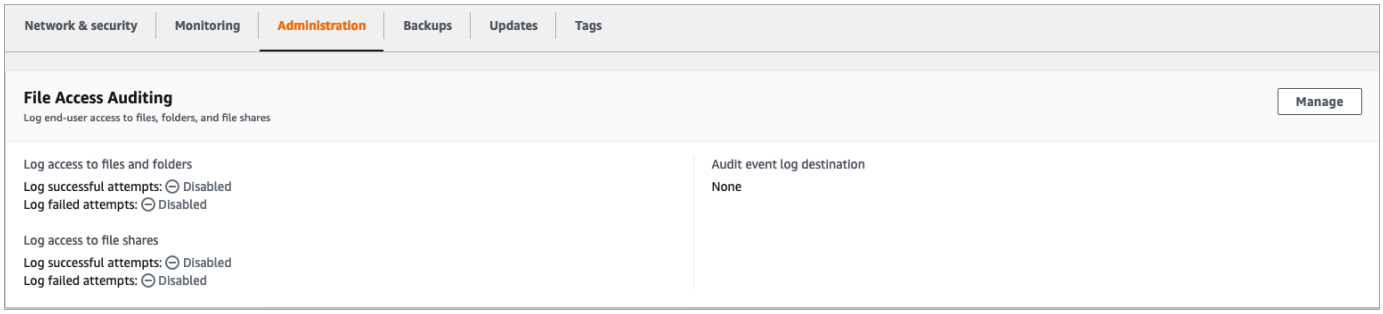
```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
```

```
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

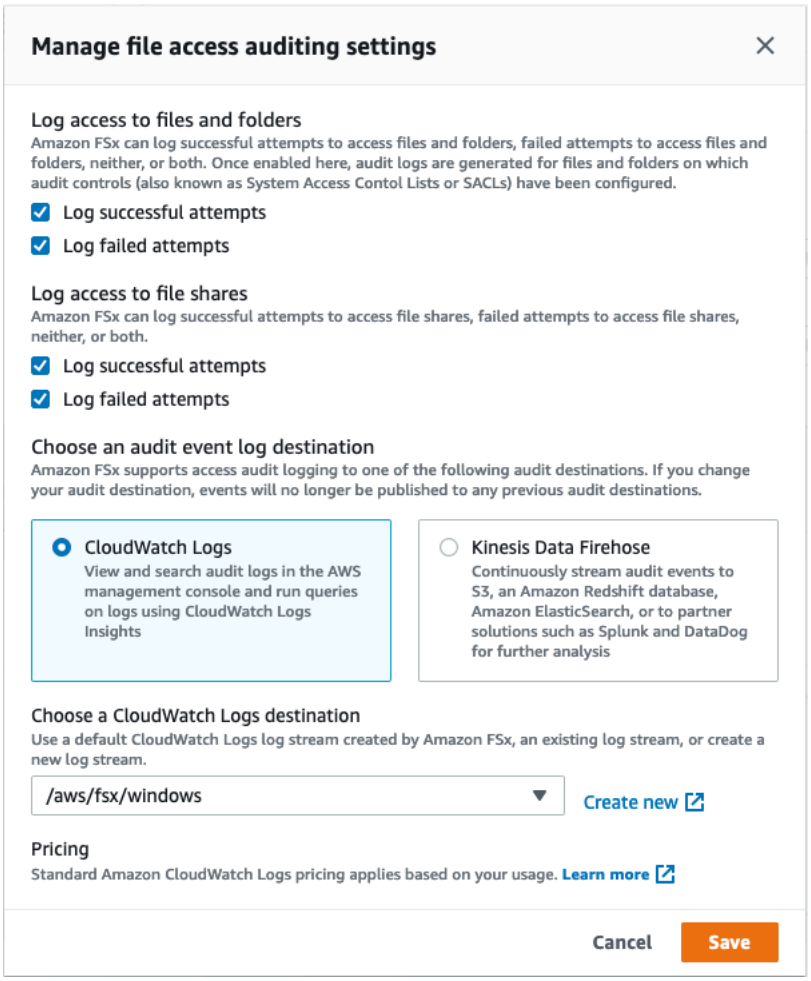
2. Quando o sistema de arquivos está Disponível, o recurso de auditoria de acesso a arquivos está habilitado.

Alterar a configuração de auditoria de acesso a 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 Windows para o qual você deseja gerenciar a auditoria de acesso a arquivos.
3. Escolha a guia Administração.
4. No painel Auditoria de acesso a arquivos, escolha Gerenciar.



5. Na caixa de diálogo Gerenciar configurações de auditoria de acesso a arquivos, altere as configurações desejadas.



- Em Registrar acesso a arquivos e pastas, selecione o registro em log de tentativas com êxito e/ou malsucedidas. O registro em log estará desabilitado para arquivos e pastas caso você não selecione.
- Em Registrar acesso aos compartilhamentos de arquivos, selecione o registro em log de tentativas com êxito e/ou malsucedidas. O registro em log estará desabilitado para compartilhamentos de arquivos, caso você não faça uma seleção.
- Em Escolher um destino de registro de eventos de auditoria, escolha CloudWatch Logs ou Firehose. Em seguida, escolha um fluxo de logs ou fluxo de entrega existente ou crie um.

6. Escolha Salvar.

Alterar a configuração de auditoria de acesso a arquivos (CLI)

- Use o comando `update-file-system` da CLI ou a operação de API `UpdateFileSystem` equivalente.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_ONLY", \
    FileShareAccessAuditLogLevel="FAILURE_ONLY", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

Sessões de usuário e arquivos abertos

Você pode monitorar as sessões de usuários conectados e abrir arquivos no sistema de arquivos do FSx para Windows File Server usando a ferramenta Pastas compartilhadas. A ferramenta Pastas compartilhadas fornece um local central para monitorar quem está conectado ao sistema de arquivos, além de quais arquivos estão abertos e por quem. Você pode usar essa ferramenta para fazer o seguinte:

- Restaurar o acesso aos arquivos bloqueados.
- Desconectar uma sessão de usuário, que fecha todos os arquivos abertos por esse usuário.

Você pode usar a ferramenta GUI de pastas compartilhadas nativa do Windows e a CLI do Amazon FSx para gerenciamento remoto para gerenciar sessões de usuários e abrir arquivos em seu PowerShell sistema de arquivos FSx for Windows File Server.

Como usar a GUI para gerenciar usuários e sessões

Os procedimentos a seguir detalham como você pode gerenciar sessões de usuário e abrir arquivos em seu sistema de arquivos Amazon FSx usando a ferramenta de pastas compartilhadas do Microsoft Windows.

Iniciar a ferramenta de pastas compartilhadas

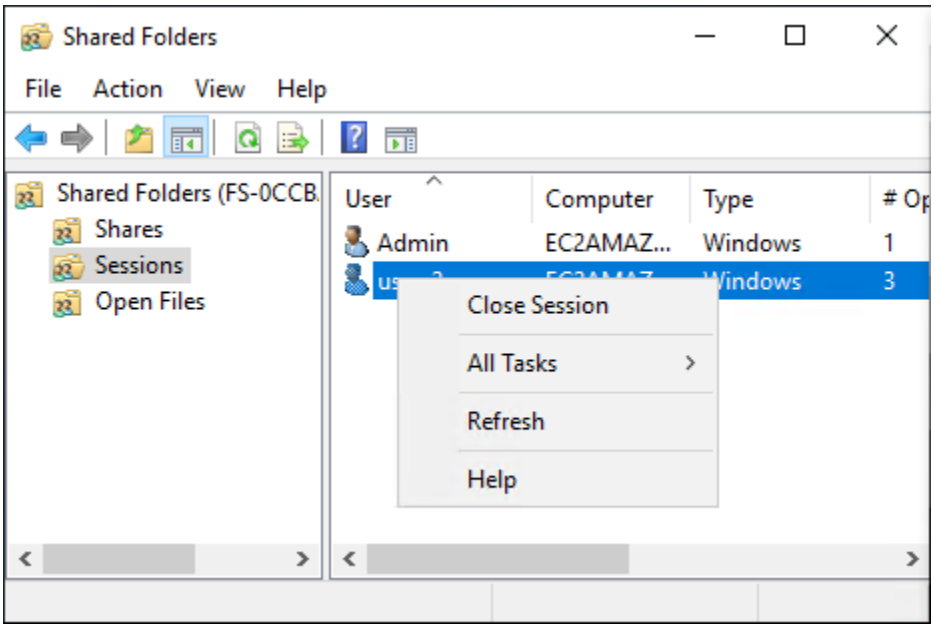
1. Inicie a instância do Amazon EC2 e conecte-a ao Microsoft Active Directory ao qual o sistema de arquivos do Amazon FSx está associado. Para fazer isso, escolha um dos seguintes procedimentos no Guia de administração do AWS Directory Service :

   - Associe continuamente uma instância do EC2 do Windows
   - Associar manualmente uma instância do Windows

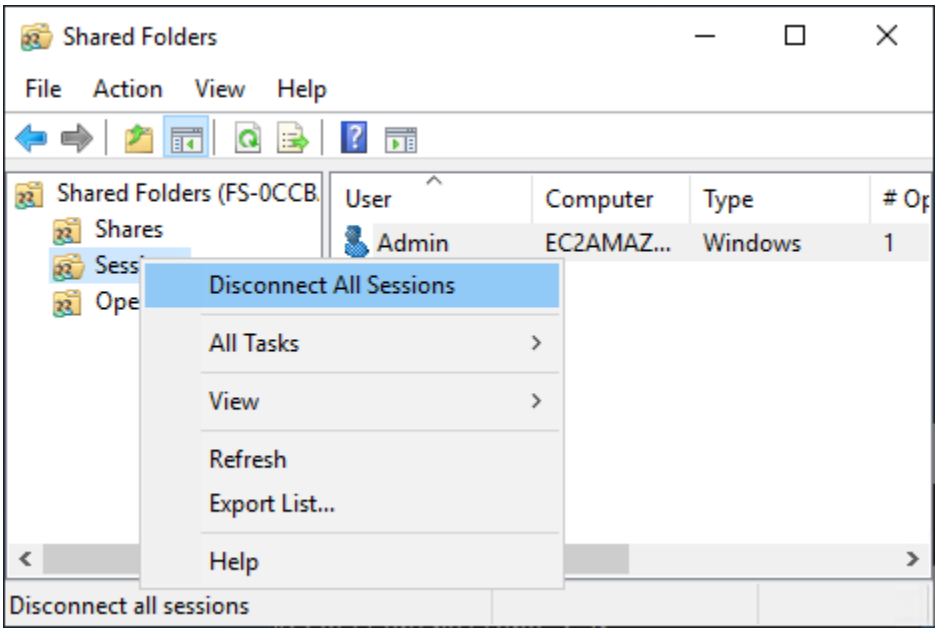
2. Conecte-se a uma instância como usuário membro do grupo de administradores do sistema de arquivos. No Microsoft Active Directory AWS gerenciado, esse grupo é chamado de Administradores FSx AWS Delegados. No Microsoft Active Directory autogerenciado, esse grupo é chamado de Administradores de domínio ou o nome personalizado do grupo de administradores que você forneceu durante a criação. 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 `Run As Administrator`. Essa ação abre a ferramenta de pastas compartilhadas da GUI.
4. Em Ação, escolha Conectar a outro computador.
5. Para Outro computador, insira o nome do DNS do sistema de arquivos do Amazon FSx, por exemplo `fs-`*`012345678901234567`*`.`*`ad-domain`*`.com`.
6. Escolha OK. Uma entrada para seu sistema de arquivos do Amazon FSx então é exibida na lista da ferramenta Pastas compartilhadas.

Para gerenciar sessões de usuário (GUI)

Na ferramenta Pastas compartilhadas, escolha Sessões para visualizar todas as sessões do usuário conectadas ao seu sistema de arquivos do FSx para Windows File Server. Se um usuário ou aplicação estiver acessando um compartilhamento de arquivos no seu sistema de arquivos do Amazon FSx, esse snap-in mostrará sua sessão. Você pode desconectar as sessões abrindo o menu de contexto (clique com o botão direito) de uma sessão e escolhendo Fechar sessão.

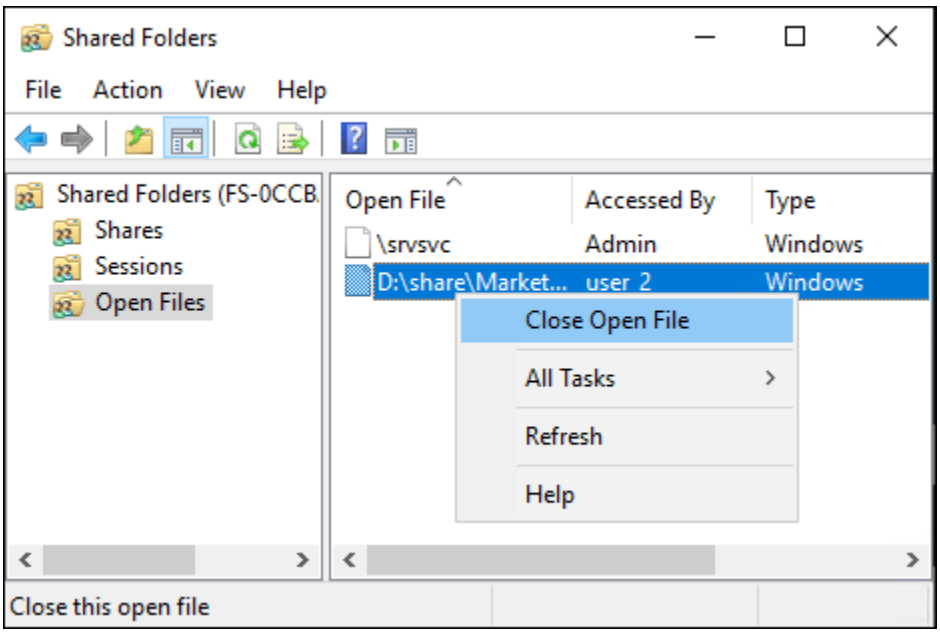


Para desconectar todas as sessões abertas, abra o menu de contexto (clique com o botão direito) de Sessões, escolha Desconectar todas as sessões e confirme a ação.

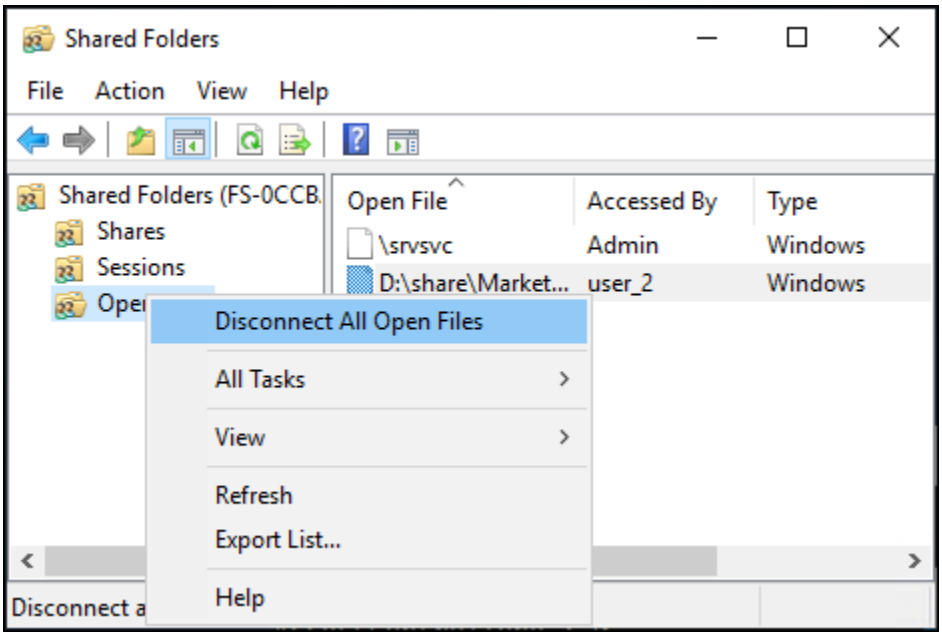


Para gerenciar arquivos abertos (GUI)

Na ferramenta Pastas compartilhadas, escolha Abrir arquivos para visualizar todos os arquivos no sistema que estão abertos no momento. A visualização também mostra quais usuários têm os arquivos ou pastas abertos. Essas informações podem ser úteis para descobrir por que outros usuários não conseguem abrir determinados arquivos. Você pode fechar qualquer arquivo que qualquer usuário tenha aberto simplesmente abrindo o menu de contexto (clique com o botão direito do mouse) da entrada do arquivo na lista e escolhendo Fechar arquivo aberto.



Para desconectar todos os arquivos abertos no sistema de arquivos, acesse o menu de contexto (clique com o botão direito) para Abrir arquivos, escolha Desconectar todos os arquivos abertos e confirme aa ação.



Usando PowerShell para gerenciar sessões de usuários e abrir arquivos

Você pode gerenciar sessões de usuário ativas e abrir arquivos em seu sistema de arquivos usando a CLI do Amazon FSx para gerenciamento remoto ativado. PowerShell Para saber como usar essa CLI, consulte Usando a CLI do Amazon FSx para PowerShell.

A seguir estão os comandos que você pode usar para a sessão do usuário e para o gerenciamento de arquivos abertos.

Command	Descrição
Get-FSxSmbSession	Recupera informações sobre as sessões do Server Message Block (SMB) atualmente estabelecidas entre o sistema de arquivos e os clientes associados.
Close-FSxSmbSession	Encerra uma sessão SMB.
Get-FSxSmbOpenFile	Recupera informações sobre arquivos que estão abertos para os clientes conectados ao sistema de arquivos.
Close-FSxSmbOpenFile	Fecha um arquivo que está aberto para um dos clientes do servidor SMB.

A ajuda on-line de cada comando fornece uma referência de todas as opções de comando. Para acessar essa ajuda, execute o comando com um -?, por exemplo Get-FSxSmbSession -?.

Eliminação de duplicação de dados

O FSx suporta o uso da Eliminação de duplicação de dados para identificar e eliminar dados redundantes. Grandes conjuntos de dados geralmente têm dados redundantes, o que aumenta os custos de armazenamento de dados. Por exemplo, com compartilhamentos de arquivos do usuário, vários usuários podem armazenar várias cópias ou versões do mesmo arquivo. Com compartilhamentos de desenvolvimento de software, muitos binários permanecem inalterados de compilação para compilação.

Você pode reduzir seus custos de armazenamento de dados ativando a eliminação de duplicação de dados no sistema de arquivos. A eliminação de duplicação de dados reduz ou elimina dados redundantes ao armazenar partes duplicadas do conjunto de dados somente uma vez. A compactação de dados é habilitada por padrão quando você usa a eliminação de duplicação de dados, reduzindo ainda mais a quantidade de armazenamento de dados ao compactar os dados após a eliminação de duplicação. A eliminação de duplicação de dados é executada como um processo em segundo plano que verifica e otimiza seu sistema de arquivos de forma contínua e automática, além de ser transparente para seus usuários e clientes conectados.

A economia de armazenamento que você pode obter com a eliminação de duplicação de dados depende da natureza do seu conjunto de dados, incluindo a quantidade de duplicação existente nos arquivos. A economia típica é em média de 50 a 60% para compartilhamentos de arquivos de uso geral. Em compartilhamentos, as economias variam de 30 a 50% para documentos do usuário a 70 a 80% para conjuntos de dados de desenvolvimento de software. Você pode medir a economia potencial de eliminação de duplicação usando o comando `Measure-FSxDedupFileMetadata` descrito abaixo.

Você também pode personalizar a eliminação de duplicação de dados para atender às suas necessidades específicas de armazenamento. Por exemplo, você pode configurar a eliminação de duplicação para ser executada somente em determinados tipos de arquivo ou criar uma programação de trabalho personalizada. Como as tarefas de eliminação de duplicação podem consumir recursos do servidor de arquivos, recomendamos monitorar o status das tarefas de eliminação de duplicação usando o comando `Get-FSxDedupStatus` descrito abaixo.

Para obter mais informações sobre a eliminação de duplicação de dados, consulte a documentação da Microsoft Noções básicas da eliminação de duplicação de dados.

> **Note**
>
> Consulte nossas práticas recomendadas para Práticas recomendadas ao usar a desduplicação de dados. Se você encontrar problemas com a execução bem-sucedida dos trabalhos de eliminação de duplicação de dados, consulte Solução de problemas da eliminação de duplicação dos dados.

> **Warning**
>
> Não é recomendável executar determinados comandos do Robocopy com eliminação de duplicação de dados, pois esses comandos podem afetar a integridade dos dados do armazenamento em blocos. Para obter mais informações, consulte a documentação Data Deduplication Interoperability da Microsoft.

Práticas recomendadas ao usar a desduplicação de dados

Veja a seguir algumas práticas recomendadas para usar a eliminação de duplicação de dados:

- Programar trabalhos de eliminação de duplicação de dados para serem executados quando o sistema de arquivos estiver inativo: a programação padrão inclui um trabalho `GarbageCollection` semanal às 2h45 UTC, aos sábados. Pode levar várias horas para ser concluído, se você tiver uma grande quantidade de rotatividade de dados em seu sistema de arquivos. Se esse horário não for ideal para sua workload, agende essa tarefa para ser executada em um momento em que você espera pouco tráfego em seu sistema de arquivos.
- Configurar capacidade de throughput suficiente para que a eliminação de duplicação de dados seja concluída: capacidades de throughput mais altas fornecem níveis mais altos de memória. A Microsoft recomenda ter 1 GB de memória por 1 TB de dados lógicos para executar a eliminação de duplicação de dados. Use a tabela de performance do Amazon FSx para determinar a memória associada à capacidade de throughput do seu sistema de arquivos e garantir que os recursos de memória sejam suficientes para o tamanho dos seus dados.
- Personalizar as configurações de eliminação de duplicação de dados para atender às suas necessidades específicas de armazenamento e reduzir os requisitos de performance: você pode restringir a otimização para execução em tipos de arquivos ou pastas específicos ou definir um tamanho mínimo de arquivo e uma idade para otimização. Para saber mais, consulte Eliminação de duplicação de dados.

Como gerenciar a eliminação de duplicação de dados

Você pode gerenciar a desduplicação de dados em seu sistema de arquivos usando a CLI do Amazon FSx para gerenciamento remoto ativado. PowerShell Para saber como usar essa CLI, consulte Usando a CLI do Amazon FSx para PowerShell.

A seguir estão os comandos que você pode usar para eliminação de duplicação de dados.

Comando de eliminação de duplicação de dados	Descrição
Enable-FSxDedup	Permite a eliminação de duplicação de dados no compartil hamento de arquivos. A compactação de dados, após a eliminação de duplicação de dados, é habilitada por padrão quando você habilita a eliminação de duplicação de dados.
Disable-FSxDedup	Desativa a eliminação de duplicação de dados no compartil hamento de arquivos.

Comando de eliminação de duplicação de dados	Descrição
Get-FSxDedupConfiguration	Recupera informações de configuração de eliminação de duplicação de dados, incluindo tamanho mínimo do arquivo e idade para otimização, configurações de compactação e tipos de arquivos e pastas excluídos.
Set-FSxDedupConfiguration	Altera as configurações de eliminação de duplicação, incluindo tamanho e idade mínimos do arquivo para otimização, configurações de compactação e tipos de arquivos e pastas excluídos.
Get-FSxDedupStatus	Recupera o status da eliminação de duplicação e inclui propriedades somente para leitura que descrevem a economia e o status da otimização no sistema de arquivos, os horários e o status de conclusão dos últimos trabalhos no sistema de arquivos.
Get-FSxDedupMetadata	Recupera metadados de otimização de eliminação de duplicação.
Update-FSxDedupStatus	Calcula e recupera informações atualizadas sobre economia de eliminação de duplicação de dados.
Measure-FSxDedupFileMetadata	Mede e recupera o espaço de armazenamento potencial que você pode recuperar em seu sistema de arquivos, se excluir um grupo de pastas. Os arquivos geralmente têm partes que são compartilhadas em outras pastas, e o mecanismo de eliminação de duplicação calcula quais partes são exclusivas e que seriam excluídas.
Get-FSxDedupSchedule	Recupera as programações de eliminação de duplicação que estão definidas atualmente.
New-FSxDedupSchedule	Cria e personaliza uma programação de eliminação de duplicação de dados.
Set-FSxDedupSchedule	Altera as configurações das programações de eliminação de duplicação de dados existentes.

Comando de eliminação de duplicação de dados	Descrição
Remove-FSxDedupSchedule	Exclui uma programação de eliminação de duplicação.
Get-FSxDedupJob	Obtém o status e as informações de todos os trabalhos de eliminação de duplicação atualmente em execução ou em fila.
Stop-FSxDedupJob	Cancele um ou mais trabalhos de eliminação de duplicação de dados especificados.

A ajuda on-line de cada comando fornece uma referência de todas as opções de comando. Para acessar essa ajuda, execute o comando com -?, por exemplo Enable-FSxDedup -?.

Como habilitar a eliminação de duplicação de dados

Você habilita a eliminação de duplicação de dados em um compartilhamento de arquivos do Amazon FSx para Windows File Server usando o comando `Enable-FSxDedup`, conforme a seguir.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {Enable-FsxDedup }
```

Quando você habilita a eliminação de duplicação de dados, uma programação e uma configuração padrão são criadas. Você pode criar, modificar e remover programações e configurações usando os comandos abaixo.

Você pode usar o comando `Disable-FSxDedup` para desativar totalmente a eliminação de duplicação de dados em seu sistema de arquivos.

Como criar uma programação de eliminação de duplicação de dados

Embora a programação padrão funcione bem na maioria dos casos, você pode criar um nova programação de eliminação de duplicação usando o comando `New-FsxDedupSchedule`, mostrado a seguir. As programações de eliminação de duplicação de dados usam o horário UTC.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
New-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Wed,Sat -
Start 08:00 -DurationHours 7
```

```
}
```

Esse comando cria uma programação chamada `CustomOptimization` que é executada na segunda, quarta e sábado, iniciando o trabalho às 8h (UTC) todos os dias, com uma duração máxima de sete horas, após as quais o trabalho é interrompido, se ainda estiver em execução.

Observe que a criação de novas programações de trabalho de eliminação de duplicação personalizadas não substitui nem remove a programação padrão existente. Antes de criar um trabalho de eliminação de duplicação personalizado, talvez você queira desativar o trabalho padrão se não precisar dele.

Você pode desativar a programação de eliminação de duplicação padrão usando o comando `Set-FsxDedupSchedule`, mostrado a seguir.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com
 -ConfigurationName FSxRemoteAdmin -ScriptBlock {Set-FSxDedupSchedule -Name
 “BackgroundOptimization” -Enabled $false}
```

Você pode remover uma programação de eliminação de duplicação usando o comando `Remove-FSxDedupSchedule -Name "ScheduleName"`. Observe que a programação padrão de eliminação de duplicação `BackgroundOptimization` não pode ser modificada ou removida e, em vez disso, precisará ser desabilitada.

Como modificar uma programação de eliminação de duplicação de dados

Você pode modificar uma programação de eliminação de duplicação existente usando o comando `Set-FsxDedupSchedule`, mostrado a seguir.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
Set-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days
 Mon,Tues,Wed,Sat -Start 09:00 -DurationHours 9
}
```

Esse comando modifica a programação `CustomOptimization` existente para ser executada de segunda a quarta e sábado, iniciando a tarefa às 9h (UTC) todos os dias, com uma duração máxima de nove horas, após a qual a tarefa será interrompida, se ainda estiver em execução.

Para modificar a idade mínima do arquivo antes de otimizar a configuração, use o comando `Set-FSxDedupConfiguration`.

Como visualizar a quantidade de espaço economizado

Para visualizar a quantidade de espaço em disco que você está economizando ao executar a eliminação de duplicação de dados, use o comando `Get-FSxDedupStatus` como a seguir.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FsxRemoteAdmin -ScriptBlock {
Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate

OptimizedFilesCount OptimizedFilesSize SavedSpace OptimizedFilesSavingsRate
------------------- ------------------ ---------- -------------------------
              12587           31163594   25944826                        83
```

> **Note**
>
> Os valores mostrados na resposta do comando para os seguintes parâmetros não são confiáveis e você não deve usar esses valores: Capacidade FreeSpace UsedSpace, UnoptimizedSize,, SavingsRate e.

Solução de problemas da eliminação de duplicação dos dados

Há várias causas possíveis para problemas de eliminação de duplicação dos dados, conforme descrito na seção a seguir.

Tópicos

- A eliminação de duplicação dos dados não está funcionando
- Os valores de eliminação de duplicação são inesperadamente definidos como 0
- O espaço não é liberado no sistema de arquivos após a exclusão de arquivos

A eliminação de duplicação dos dados não está funcionando

Seguindo as instruções da nossa documentação sobre eliminação de duplicação dos dados, execute o comando `Get-FSxDedupStatus` para visualizar o status de conclusão dos trabalhos de eliminação de duplicação mais recentes. Se um ou mais trabalhos estiverem falhando, talvez você não veja um aumento na capacidade de armazenamento livre no seu sistema de arquivos.

O motivo mais comum de falha nos trabalhos de eliminação de duplicação é a falta de memória.

- A Microsoft recomenda ter, idealmente, 1 GB de memória por 1 TB de dados lógicos (ou, no mínimo, 300 MB + 50 MB por 1 TB de dados lógicos). Use a tabela de performance do Amazon FSx para determinar a memória associada à capacidade de throughput do seu sistema de arquivos e garantir que os recursos de memória sejam suficientes para o tamanho dos seus dados.
- Os trabalhos de eliminação de duplicação são configurados com o padrão recomendado pelo Windows de 25% de alocação de memória, o que significa que, para um sistema de arquivos com 32 GB de memória, 8 GB estarão disponíveis para eliminação de duplicação. A alocação de memória é configurável (usando o comando `Set-FSxDedupSchedule` com o parâmetro `-Memory`), mas o consumo de memória adicional pode afetar a performance do sistema de arquivos.
- É possível modificar a configuração dos trabalhos de eliminação de duplicação para reduzir ainda mais os requisitos de memória. Por exemplo, você pode restringir a otimização a ser executada em tipos de arquivos ou pastas específicos ou definir um tamanho e uma idade mínimos para a otimização. Também recomendamos configurar os trabalhos de eliminação de duplicação para serem executados durante períodos ociosos, quando há carga mínima no sistema de arquivos.

Você também poderá visualizar erros se os trabalhos de eliminação de duplicação não tiverem tempo suficiente para serem concluídos. Talvez você precise alterar a duração máxima dos trabalhos, conforme descrito em Como modificar uma programação de eliminação de duplicação de dados.

Se os trabalhos de eliminação de duplicação estiverem falhando por um longo período e houver alterações nos dados do sistema de arquivos durante esse período, os trabalhos de eliminação de duplicação subsequentes poderão exigir mais recursos para serem concluídos com êxito pela primeira vez.

Os valores de eliminação de duplicação são inesperadamente definidos como 0

Os valores para `SavedSpace` e `OptimizedFilesSavingsRate` são inesperadamente definidos como 0 para um sistema de arquivos no qual você configurou a eliminação de duplicação dos dados.

Isso pode ocorrer durante o processo de otimização do armazenamento quando você aumenta a capacidade de armazenamento do sistema de arquivos. Quando você aumenta a capacidade de armazenamento de um sistema de arquivos, o Amazon FSx cancela os trabalhos de eliminação de duplicação dos dados existentes durante o processo de otimização do armazenamento, que

migra os dados dos discos antigos para os discos novos e maiores. O Amazon FSx retoma a eliminação de duplicação dos dados no sistema de arquivos assim que o trabalho de otimização do armazenamento é concluído. Para obter mais informações sobre o aumento da capacidade de armazenamento e a otimização do armazenamento, consulte Como gerenciar a capacidade de armazenamento.

O espaço não é liberado no sistema de arquivos após a exclusão de arquivos

O comportamento esperado da eliminação de duplicação dos dados é que, se os dados que foram excluídos eram dados para os quais a eliminação de duplicação havia economizado espaço, o espaço não será realmente liberado no sistema de arquivos até que o trabalho de coleta de resíduos seja executado.

Uma prática que pode ser útil é definir uma programação para a execução do trabalho de coleta de resíduos logo após a exclusão de um grande número de arquivos. Após a conclusão do trabalho de coleta de resíduos, você pode definir o cronograma de coleta de resíduos de volta às configurações originais. Isso garante que você possa visualizar rapidamente o espaço resultante de suas exclusões.

Use o procedimento a seguir para definir o trabalho de coleta de resíduos para ser executado em 5 minutos.

1. Para verificar se a eliminação de duplicação dos dados está habilitada, use o comando `Get-FSxDedupStatus`. Para obter mais informações sobre o comando e sua saída esperada, consulte Como visualizar a quantidade de espaço economizado.
2. Use o procedimento a seguir para definir a programação de execução do trabalho de coleta de resíduos para daqui a cinco minutos.

   ```
   $FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
   $DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
   $Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

   Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
   ScriptBlock {
       Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
   Start $Using:Time -DurationHours 9
   }
   ```
3. Depois que o trabalho de coleta de resíduos tiver sido executado e o espaço tiver sido liberado, defina a programação de volta para suas configurações originais.

Cotas de armazenamento

Você pode configurar cotas de armazenamento do usuário em seus sistemas de arquivos para limitar a quantidade de armazenamento de dados que os usuários podem consumir. Depois de definir cotas, você pode acompanhar o status da cota para monitorar o uso e ver quando os usuários ultrapassam suas cotas.

Você também pode impor cotas impedindo que os usuários que atingem suas cotas gravem no espaço de armazenamento. Quando você impõe cotas, um usuário que excede sua cota recebe uma mensagem de erro de “espaço insuficiente no disco”.

Você pode definir esses limites para as configurações de cota:

- Aviso: usado para rastrear se um usuário ou grupo está se aproximando do limite de cota, relevante somente para rastreamento.
- Limite: o limite da cota de armazenamento para um usuário ou grupo.

Você pode configurar cotas padrão que são aplicadas a novos usuários que acessam um sistema de arquivos e cotas que se aplicam a usuários ou grupos específicos. Você também pode ver um relatório do volume de armazenamento que cada usuário ou grupo está consumindo e se eles estão superando suas cotas.

O consumo de armazenamento no nível do usuário é monitorado com base na propriedade do arquivo. O consumo de armazenamento é calculado usando o tamanho lógico do arquivo, não o espaço real de armazenamento físico que os arquivos ocupam. As cotas de armazenamento do usuário são monitoradas no momento em que os dados são gravados em um arquivo.

A atualização de cotas para vários usuários exige executar o comando de atualização uma vez para cada usuário ou organizar os usuários em um grupo e atualizar a cota desse grupo.

Como gerenciar cotas de armazenamento do usuário

Você pode gerenciar cotas de armazenamento de usuários em seu sistema de arquivos usando a CLI do Amazon FSx para gerenciamento remoto ativado. PowerShell Para saber como usar essa CLI, consulte Usando a CLI do Amazon FSx para PowerShell.

A seguir estão os comandos que podem ser usados para gerenciar cotas de armazenamento do usuário.

Comando de cotas de armazenamento do usuário	Descrição
Enable-FSxUserQuotas	Começa a rastrear ou impor as cotas de armazenamento do usuário, ou executar as duas ações.
Disable-FSxUserQuotas	Interrompe o rastreamento e a imposição das cotas de armazenamento do usuário.
Get-FSxUserQuotaSettings	Recupera as configurações atuais de cota de armazenamento do usuário para o sistema de arquivos.
Get-FSxUserQuotaEntries	Recupera as entradas atuais da cota de armazenamento do usuário para usuários e grupos individuais no sistema de arquivos.
Set-FSxUserQuotas	Defina a cota de armazenamento do usuário para um usuário ou grupo individual. Os valores de cota são especificados em bytes.

A ajuda on-line de cada comando fornece uma referência de todas as opções de comando. Para acessar essa ajuda, execute o comando com -?, por exemplo Enable-FSxUserQuotas -?.

Como gerenciar criptografia em trânsito

Você pode usar um conjunto de PowerShell comandos personalizados para controlar a criptografia dos dados em trânsito entre o sistema de arquivos FSx for Windows File Server e os clientes. Você pode limitar o acesso ao sistema de arquivos somente a clientes que oferecem suporte à criptografia SMB, para que ela data-in-transit seja sempre criptografada. Quando a imposição é ativada para criptografia de data-in-transit, os usuários que acessam o sistema de arquivos de clientes que não oferecem suporte à criptografia SMB 3.0 não poderão acessar compartilhamentos de arquivos para os quais a criptografia está ativada.

Você também pode controlar a criptografia data-in-transit no nível do compartilhamento de arquivos em vez do nível do servidor de arquivos. Você pode usar controles de criptografia em nível de compartilhamento de arquivos para ter uma combinação de compartilhamentos de arquivos criptografados e não criptografados no mesmo sistema de arquivos, se quiser impor a criptografia

em trânsito para alguns compartilhamentos de arquivos que tenham dados confidenciais e permitir que todos os usuários acessem outros compartilhamentos de arquivos. A criptografia do servidor tem precedência sobre a criptografia em nível de compartilhamento. Se a criptografia global estiver habilitada, você não poderá desabilitar seletivamente a criptografia para determinados compartilhamentos.

Você pode gerenciar a criptografia de usuários em trânsito em seu sistema de arquivos usando a CLI do Amazon FSx para gerenciamento remoto ativado. PowerShell Para saber como usar essa CLI, consulte Usando a CLI do Amazon FSx para PowerShell.

A seguir estão os comandos que você pode usar para gerenciar a criptografia em trânsito do usuário em seu sistema de arquivos.

Comando de criptografia em trânsito	Descrição
Get-FSxSmbServerConfiguration	Recupera a configuração do servidor Server Message Block (SMB).
Set-FSxSmbServerConfiguration	Esse comando tem duas opções para configurar a criptografia em trânsito: • `-EncryptData $True\|$False` — Defina esse parâmetro `True` para ativar a criptografia de dados em trânsito. Defina esse parâmetro `False` para desativar a criptografia de dados em trânsito. • `-RejectUnencryptedAccess $True\|$False` — Defina esse parâmetro `True` para impedir que clientes que não oferecem suporte à criptografia acessem o sistema de arquivos. Defina esse parâmetro `False` para permitir que clientes que não oferecem suporte à criptografia acessem o sistema de arquivos.

A ajuda on-line de cada comando fornece uma referência de todas as opções de comando. Para acessar essa ajuda, execute o comando com -?, por exemplo Get-FSxSmbServerConfiguration -?.

Como gerenciar a configuração do armazenamento

A configuração de armazenamento do sistema de arquivos inclui capacidade de armazenamento, tipo de armazenamento e IOPS SSD. Você pode configurar esses recursos junto com a capacidade de throughput para atingir o nível de performance desejado para sua workload, durante e depois da criação do sistema de arquivos. Para obter mais informações, consulte os tópicos a seguir.

Tópicos

Como gerenciar a capacidade de armazenamento

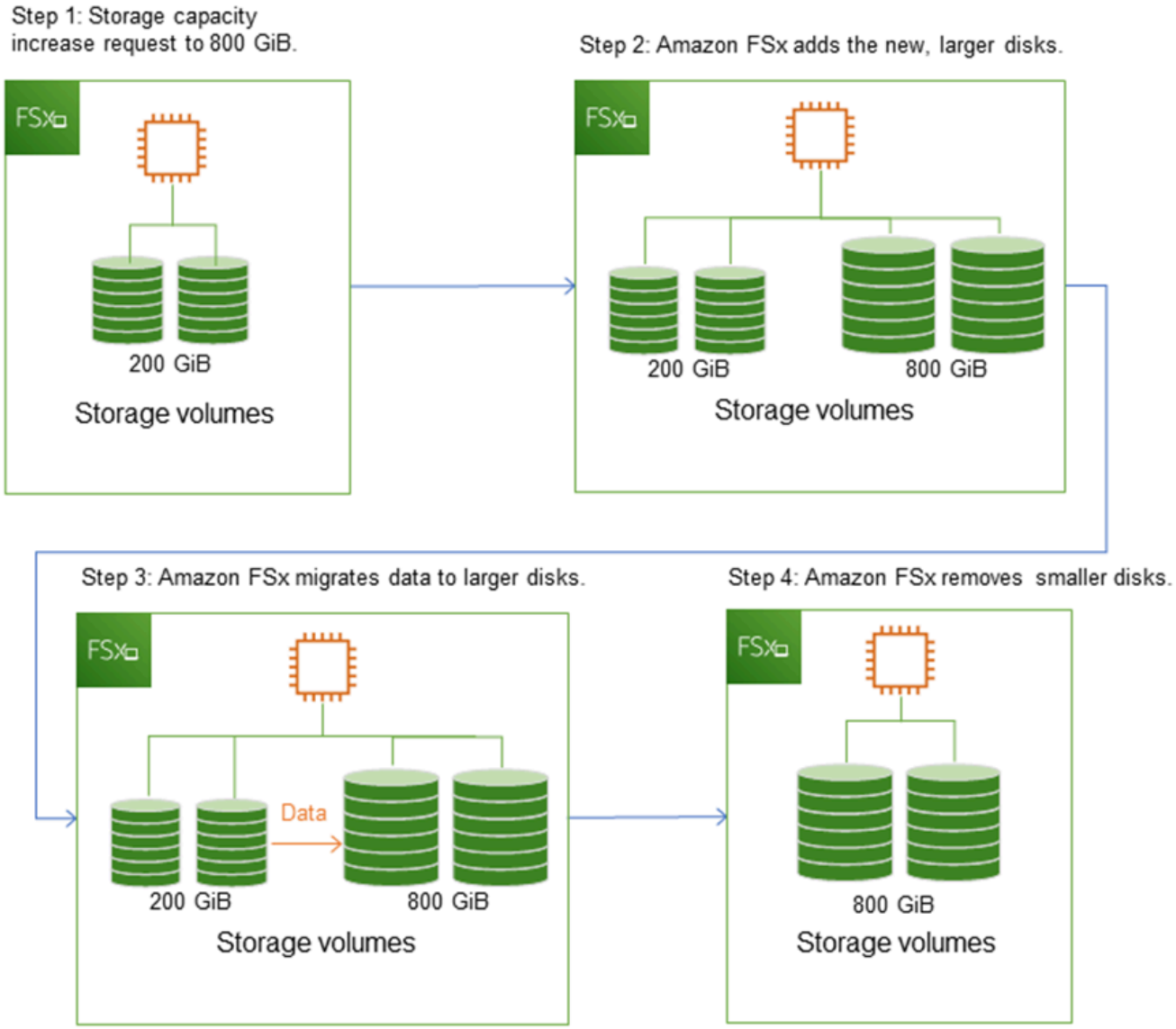
Você pode aumentar a capacidade de armazenamento configurada em um sistema de arquivos do FSx para Windows File Server conforme necessário. Para fazê-lo, você pode usar o console do Amazon FSx, a API do Amazon FSx ou a AWS Command Line Interface (AWS CLI). Você só pode aumentar a capacidade de armazenamento de um sistema de arquivos, não pode diminuí-la.

> **Note**
>
> Você não pode aumentar a capacidade de armazenamento de sistemas de arquivos criados antes de 23 de junho de 2019 ou de sistemas de arquivos restaurados com base em um backup pertencente a um sistema de arquivos criado antes de 23 de junho de 2019.

Quando você aumenta a capacidade de armazenamento de um sistema de arquivos do Amazon FSx, o Amazon FSx adiciona automaticamente um conjunto de discos novo e maior ao sistema de arquivos. Em seguida, o Amazon FSx executa um processo de otimização de armazenamento em segundo plano para migrar de forma transparente os dados dos discos antigos para os novos discos. A otimização do armazenamento pode levar de algumas horas a alguns dias, com um impacto mínimo perceptível na performance da workload. Durante essa otimização, o uso do backup é temporariamente maior, porque os volumes de armazenamento antigos e novos estão incluídos nos backups no nível de sistema de arquivos. Ambos os conjuntos de volumes de armazenamento são incluídos para garantir que o Amazon FSx possa obter e restaurar backups com êxito, mesmo durante a atividade de escalabilidade de armazenamento. O uso do backup faz a reversão ao nível básico anterior depois que os volumes de armazenamento antigos não estão mais incluídos no

histórico de backup. Quando a nova capacidade de armazenamento estiver disponível, você será cobrado somente pela nova capacidade de armazenamento.

A ilustração a seguir mostra as quatro etapas principais do processo que o Amazon FSx usa quando aumenta a capacidade de armazenamento de um sistema de arquivos.



Você pode acompanhar o andamento da otimização do armazenamento, dos aumentos da capacidade de armazenamento SSD ou das atualizações do IOPS SSD a qualquer momento usando

o console do Amazon FSx, a CLI ou a API. Para obter mais informações, consulte Como monitorar os aumentos da capacidade de armazenamento.

Tópicos

Pontos importantes a conhecer no aumento da capacidade de armazenamento

Aqui estão alguns itens importantes a serem considerados ao aumentar a capacidade de armazenamento:

- Apenas aumentar: você só pode aumentar a capacidade de armazenamento de um sistema de arquivos, não pode diminuí-la.
- Aumento mínimo: cada aumento na capacidade de armazenamento deve ser, no mínimo, de 10% da capacidade de armazenamento atual do sistema de arquivos, até o valor máximo permitido de 65.536 GiB.
- Capacidade de throughput mínima: para aumentar a capacidade de armazenamento, o sistema de arquivos deve ter uma capacidade de throughput mínima de 16 MB/s. Isso ocorre porque a etapa de otimização do armazenamento é um processo que exige throughput elevado.
- Tempo entre os aumentos: não é possível fazer mais aumentos de capacidade de armazenamento em um sistema de arquivos até seis horas após a solicitação do último aumento ou até que o processo de otimização de armazenamento seja concluído, o que for mais longo. A otimização do armazenamento pode levar de algumas horas a alguns dias para ser concluída. Para minimizar o tempo necessário para a conclusão da otimização do armazenamento, recomendamos o aumento da capacidade de throughput do sistema de arquivos antes do aumento da capacidade de armazenamento (a capacidade de throughput pode ser reduzida novamente após a conclusão da escalabilidade do armazenamento) e o aumento da capacidade de armazenamento quando houver tráfego mínimo no sistema de arquivos.

> **Note**
>
> Certos eventos do sistema de arquivos podem consumir recursos de performance de E/S de disco. Por exemplo:
> A fase de otimização da escalabilidade da capacidade de armazenamento pode gerar maior throughput de disco e causar avisos de performance. Para obter mais informações, consulte Avisos e recomendações de performance.

Quando aumentar a capacidade de armazenamento

Aumente a capacidade de armazenamento do sistema de arquivos quando ele estiver com pouca capacidade de armazenamento livre. Use a métrica `FreeStorageCapacity` do CloudWatch para monitorar a quantidade de armazenamento livre disponível no sistema de arquivos. Você pode criar um alarme do Amazon CloudWatch nessa métrica e receber notificações quando ela se tornar inferior a um limite específico. Para obter mais informações, consulte Monitoramento de métricas com a Amazon CloudWatch.

Recomendamos manter pelo menos 10% da capacidade de armazenamento livre em todos os momentos em seu sistema de arquivos. O uso de toda a capacidade de armazenamento pode afetar negativamente a performance e introduzir inconsistências de dados.

Você poderá aumentar automaticamente a capacidade de armazenamento do sistema de arquivos quando a capacidade de armazenamento livre cair abaixo de um limite definido que você especificar. Use o modelo personalizado do AWS CloudFormation desenvolvido pela AWS para implantar todos os componentes necessários para a implementação da solução automatizada. Para obter mais informações, consulte Como aumentar a capacidade de armazenamento de forma dinâmica.

Aumentos da capacidade de armazenamento e performance do sistema de arquivos

A maioria das workloads sofre um impacto mínimo na performance enquanto o Amazon FSx executa o processo de otimização de armazenamento em segundo plano após a disponibilidade da nova capacidade de armazenamento. Aplicações com uso pesado de gravação e grandes conjuntos de dados ativos podem temporariamente sofrer uma redução de até a metade na performance de gravação. Nesses casos, você pode primeiro aumentar a capacidade de throughput do sistema de arquivos antes de aumentar a capacidade de armazenamento. Isso permite que você continue a fornecer o mesmo nível de throughput para atender às necessidades de performance da aplicação. Para obter mais informações, consulte Como gerenciar a capacidade de throughput.

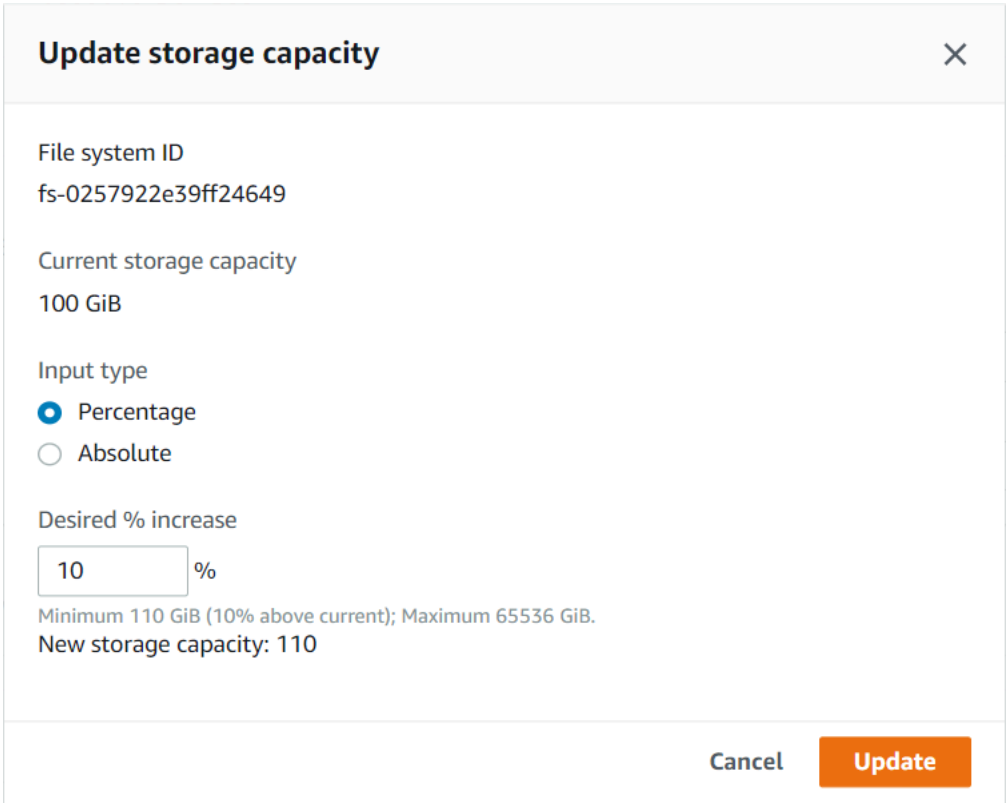
Como aumentar a capacidade de armazenamento

Você pode aumentar a capacidade de armazenamento de um sistema de arquivos usando o console do Amazon FSx, a AWS CLI ou a API do Amazon FSx.

Aumentar a capacidade de armazenamento de um sistema de arquivos (console)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do Windows para o qual você deseja aumentar a capacidade de armazenamento.
3. Em Ações, escolha Atualizar armazenamento. Como alternativa, no painel Resumo, escolha Atualizar ao lado da Capacidade de armazenamento do sistema de arquivos.

   A janela Atualizar capacidade de armazenamento é exibida.



4. Em Tipo de entrada, escolha Porcentagem para inserir a nova capacidade de armazenamento como uma alteração da porcentagem em relação ao valor atual, ou escolha Absoluto para inserir o novo valor em GiB.
5. Insira a Capacidade de armazenamento desejada.

> **Note**
>
> A capacidade desejada deve ser pelo menos 10% maior do que a capacidade atual, até o valor máximo de 65.536 GiB.

6. Escolha Atualizar para iniciar a atualização da capacidade de armazenamento.
7. Você pode monitorar o progresso da atualização na página de detalhes dos Sistemas de arquivos, na guia Atualizações.

Aumentar a capacidade de armazenamento de um sistema de arquivos (CLI)

Para aumentar a capacidade de armazenamento de um sistema de arquivos do FSx para Windows File Server, use o comando update-file-system da AWS CLI. Defina os seguintes parâmetros:

- `--file-system-id` para o ID do sistema de arquivos que você está atualizando.
- `--storage-capacity` para um valor que seja pelo menos 10% maior do que o valor atual.

Você pode monitorar o progresso da atualização usando o comando describe-file-systems da AWS CLI. Procure `administrative-actions` na saída.

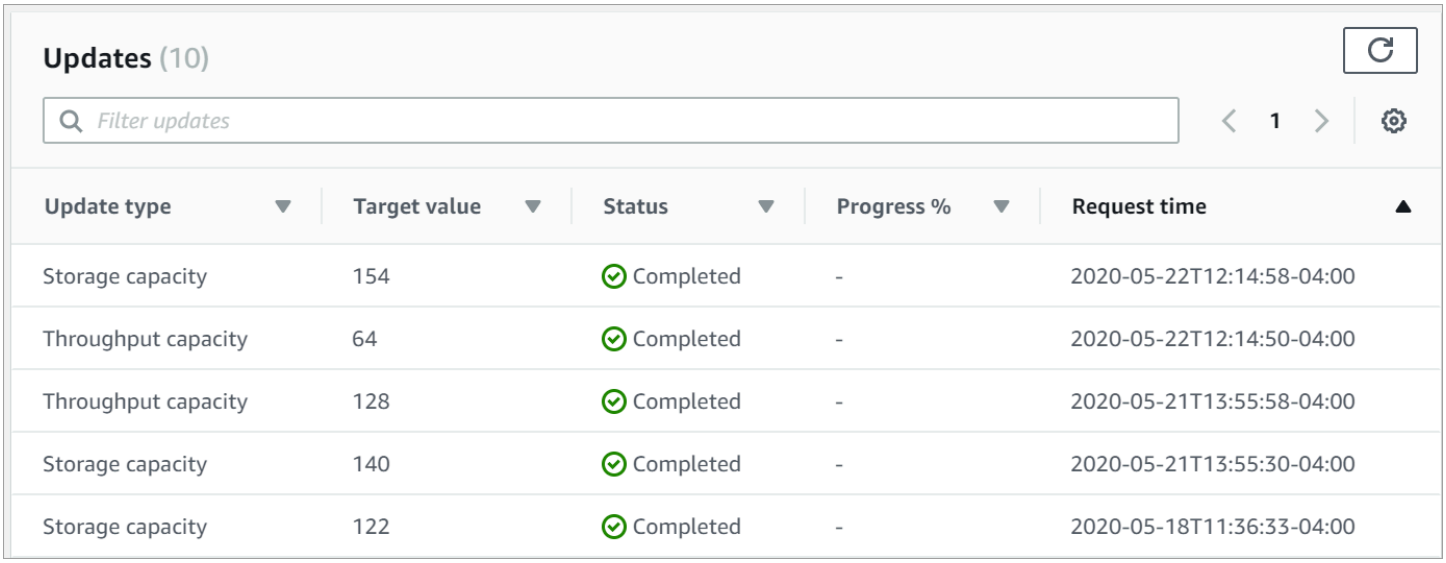
Para obter mais informações, consulte AdministrativeAction.

Como monitorar os aumentos da capacidade de armazenamento

Você pode monitorar o progresso de um aumento na capacidade de armazenamento usando o console do Amazon FSx, a API ou a AWS CLI.

Como monitorar os aumentos no console

Na guia Atualizações na janela Detalhes do sistema de arquivos, você pode ver as dez atualizações mais recentes para cada tipo de atualização.



Para atualizações de capacidade de armazenamento, você pode visualizar as informações a seguir.

Tipo de atualização

Os valores possíveis são Capacidade de armazenamento.

Target value (Valor de destino)

O valor desejado para a atualização da capacidade de armazenamento do sistema de arquivos.

Status

O status atual da atualização. Para atualizações de capacidade de armazenamento, os valores possíveis são:

- Pendente: o Amazon FSx recebeu a solicitação de atualização, mas não começou a processá-la.
- Em andamento: o Amazon FSx está processando a solicitação de atualização.
- Otimização atualizada: o Amazon FSx aumentou a capacidade de armazenamento do sistema de arquivos. O processo de otimização de armazenamento agora está transferindo os dados do sistema de arquivos para os novos discos maiores.
- Concluído: o aumento da capacidade de armazenamento foi concluído com êxito.
- Com falha: o aumento da capacidade de armazenamento falhou. Escolha o ponto de interrogação (?) para ver os detalhes sobre o motivo da falha na atualização do armazenamento.

% de progresso

Exibe o progresso do processo de otimização do armazenamento como a porcentagem concluída.

Horário da solicitação

O horário em que o Amazon FSx recebeu a solicitação de ação de atualização.

Como monitorar os aumentos com a AWS CLI e a API

Você pode visualizar e monitorar as solicitações de aumento de capacidade de armazenamento do sistema de arquivos usando o comando describe-file-systems da AWS CLI e a ação de API DescribeFileSystems. A matriz `AdministrativeActions` lista as dez ações de atualização mais recentes para cada tipo de ação administrativa. Ao aumentar a capacidade de armazenamento de um sistema de arquivos, duas `AdministrativeActions` são geradas: uma ação `FILE_SYSTEM_UPDATE` e uma `STORAGE_OPTIMIZATION`.

O exemplo apresentado a seguir mostra um trecho da resposta de um comando describe-file-systems da CLI. O sistema de arquivos tem uma capacidade de armazenamento de 300 GB e há uma ação administrativa pendente para aumentar a capacidade de armazenamento para 1.000 GB.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 1000
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
```

```
                    "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`. Isso é mostrado no trecho a seguir da resposta de um comando describe-file-systems da CLI.

A propriedade `ProgressPercent` exibe o andamento do processo de otimização do armazenamento. Após a conclusão com êxito do processo de otimização do armazenamento, o status da ação `FILE_SYSTEM_UPDATE` é alterado para `COMPLETED` e a ação `STORAGE_OPTIMIZATION` não aparece mais.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 1000
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

Se o aumento da capacidade de armazenamento falhar, o status da ação `FILE_SYSTEM_UPDATE` será alterado para `FAILED`. A propriedade `FailureDetails` fornece informações sobre a falha, mostradas no exemplo a seguir.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 1000
                }
            ]
```

Para obter informações sobre a solução de problemas de ações com falha, consulte Falha nas atualizações da capacidade de armazenamento ou capacidade de throughput.

Como aumentar dinamicamente a capacidade de armazenamento de um sistema de arquivos do FSx para Windows File Server

Você pode usar a solução a seguir para aumentar dinamicamente a capacidade de armazenamento de um sistema de arquivos do FSx para Windows File Server quando a capacidade de armazenamento livre está abaixo de um limite definido por você. Esse modelo do AWS CloudFormation implanta automaticamente todos os componentes necessários para definir o limite de capacidade de armazenamento livre, o alarme do Amazon CloudWatch baseado neste limite e a função do AWS Lambda que aumenta a capacidade de armazenamento do sistema de arquivos.

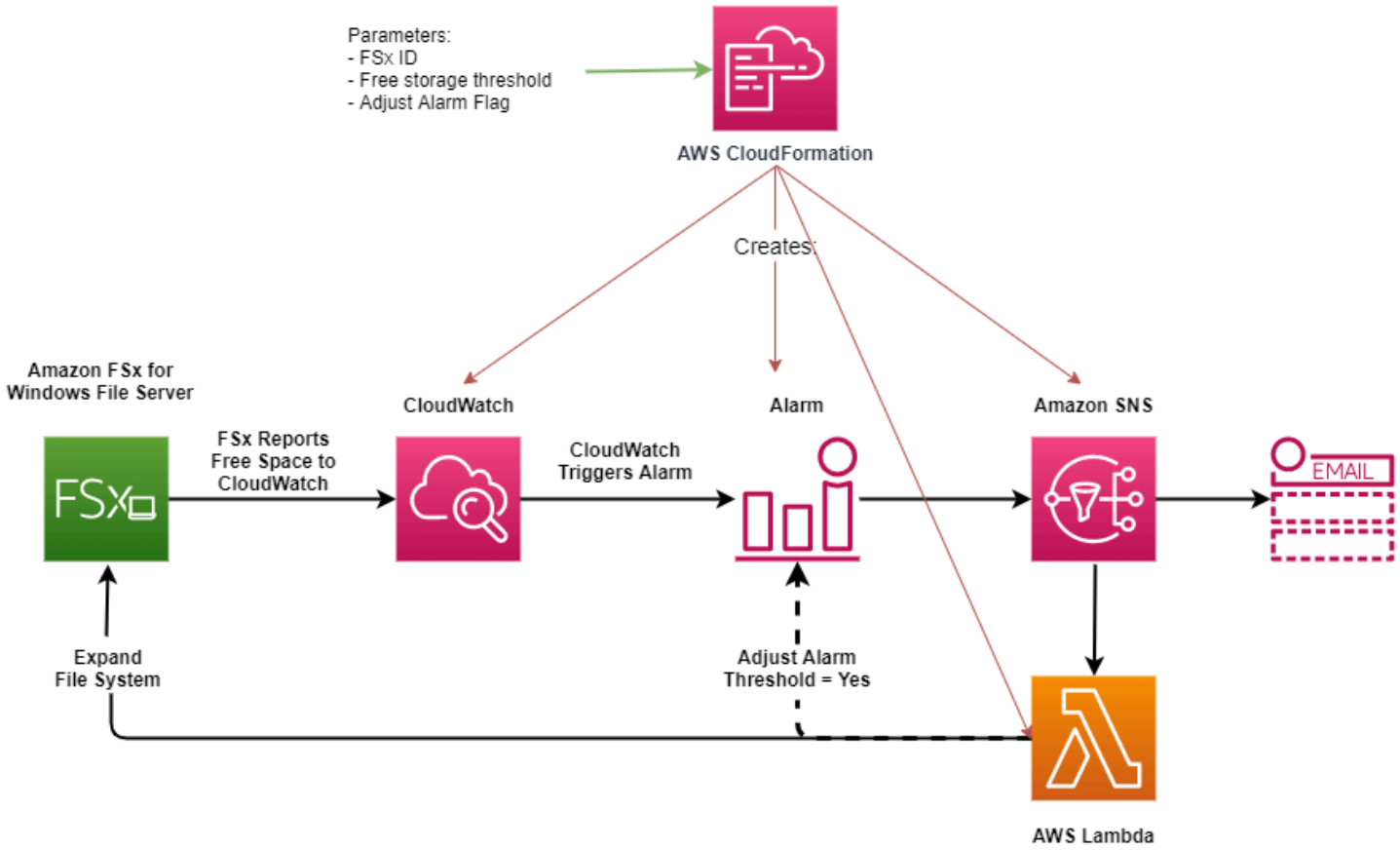
A solução implanta automaticamente todos os componentes necessários e assimila os seguintes parâmetros:

- O ID do sistema de arquivos
- O limite de capacidade de armazenamento livre (valor numérico)
- Unidade de medida (porcentagem [padrão] ou GiB)
- A porcentagem em que a capacidade de armazenamento (%) será aumentada
- O endereço de e-mail da assinatura do SNS
- Ajustar o limite do alarme (Sim/Não)

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 modelo do AWS CloudFormation implanta um alarme do CloudWatch, uma função do AWS Lambda, uma fila do Amazon Simple Notification Service (Amazon SNS) e todos os perfis do AWS Identity and Access Management (IAM) necessários. O perfil do IAM concede à função do Lambda permissão para invocar as operações de API do Amazon FSx.
2. O CloudWatch aciona um alarme quando a capacidade de armazenamento livre do sistema de arquivos cai abaixo do limite especificado e envia uma mensagem à fila do Amazon SNS.
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. A função do Lambda pode, opcionalmente, ajustar o limite de capacidade de armazenamento livre para que ele seja igual a uma porcentagem especificada da nova capacidade de armazenamento do sistema de arquivos.
6. O estado original do alarme do CloudWatch e os resultados das operações da função do Lambda são enviados para a fila do Amazon SNS.

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

Modelo AWS CloudFormation

Essa solução usa o AWS CloudFormation para automatizar a implantação dos componentes que são usados para aumentar automaticamente a capacidade de armazenamento de um sistema de arquivos do FSx para Windows File Server. Para usar essa solução, faça download do modelo IncreaseFSxSize do AWS CloudFormation.

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 inicial da capacidade de armazenamento livre no qual é acionado um alarme e é aumentada automaticamente a capacidade de armazenamento do sistema de arquivos, especificada em GiB ou como uma porcentagem (%) da capacidade de armazenamento atual do sistema de arquivos. Quando expressa como uma porcentagem, o modelo do CloudFormation recalcula em GiB para corresponder às configurações de alarme do CloudWatch.

LowFreeDataStorageCapacityThresholdUnit

O padrão é %. Especifica as unidades do `LowFreeDataStorageCapacityThreshold`, em GiB ou como uma porcentagem da capacidade de armazenamento atual.

AlarmModificationNotification

O padrão é Sim. Se for definido como Sim, o `LowFreeDataStorageCapacityThreshold` inicial será aumentado proporcionalmente para o valor de `PercentIncrease` para limites de alarme subsequentes.

Por exemplo, quando `PercentIncrease` é definido como 20 e AlarmModificationNotification é definido como Sim, o limite de espaço livre disponível (`LowFreeDataStorageCapacityThreshold`) especificado em GiB é aumentado em 20% para eventos subsequentes de aumento da capacidade de armazenamento.

EmailAddress

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

PercentIncrease

Nenhum valor padrão. Especifica a quantidade pela qual aumentar a capacidade de armazenamento, expressa como uma porcentagem da capacidade de armazenamento atual.

Implantação automatizada com o AWS CloudFormation

O procedimento a seguir configura e implanta uma pilha do AWS CloudFormation para aumentar automaticamente a capacidade de armazenamento de um sistema de arquivos do FSx para Windows File Server. A implantação leva cerca de cinco minutos.

> **Note**
>
> A implementação desta solução incorre em cobranças pelos serviços da AWS associados. Para obter mais informações, consulte as páginas de detalhes de preços desses serviços.

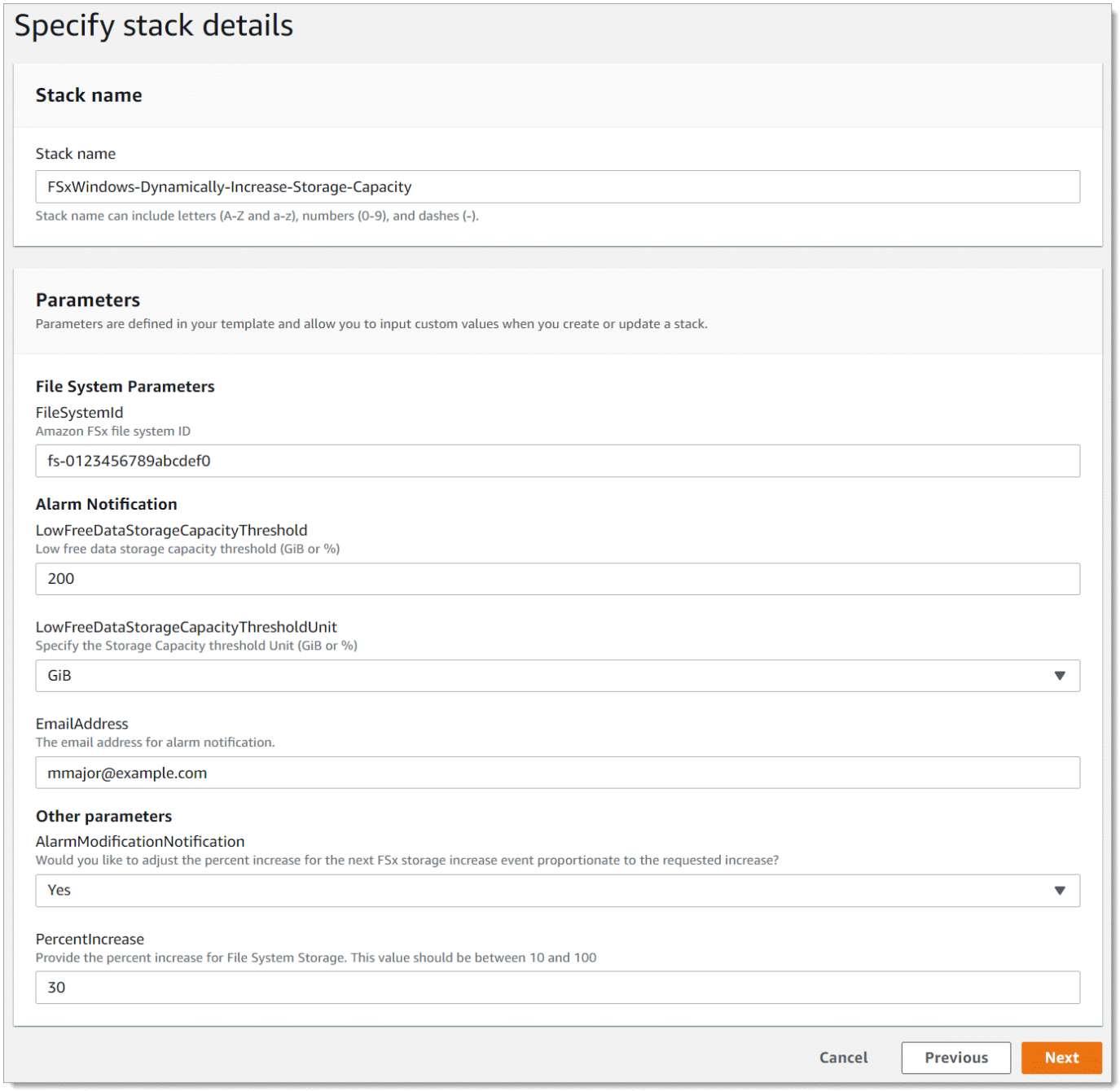
Antes de começar, você deve ter o ID do sistema de arquivos do Amazon FSx em execução em uma Amazon Virtual Private Cloud (Amazon VPC) na sua conta da AWS. Para obter mais informações sobre como criar recursos do Amazon FSx, consulte Introdução ao Amazon FSx para Windows File Server.

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

1. Baixe o modelo IncreaseFSxSize do AWS CloudFormation. Para obter mais informações sobre a criação de uma pilha do CloudFormation, consulte Criar uma pilha no console do AWS CloudFormation no Guia do usuário do AWS CloudFormation.

   > **Note**
   >
   > Atualmente, o Amazon FSx está disponível somente em regiões específicas da AWS. Você deve iniciar essa solução em uma região da AWS na qual o Amazon FSx esteja disponível. Para obter mais informações, consulte Amazon FSx endpoints and quotas na Referência geral da AWS.

2. Em Especificar detalhes da pilha, insira os valores da solução para o aumento automático da capacidade de armazenamento.



3. Insira um Nome da pilha.
4. Em Parâmetros, analise os parâmetros para o modelo e modifique-os de acordo com as necessidades do seu sistema de arquivos. Em seguida, escolha Next (Próximo).
5. Insira as configurações de Opções desejadas para a solução personalizada e escolha Avançar.
6. Em Analisar, revise e confirme as configurações da solução. Você deve selecionar a caixa de seleção confirmando que o modelo cria recursos do IAM.
7. Selecione Criar para implantar a stack.

Você pode visualizar o status da pilha no console do AWS CloudFormation, na coluna Status. Você deverá ver um status CREATE_COMPLETE em cerca de cinco 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.

Como gerenciar o tipo de armazenamento

O FSx para Windows File Server oferece tipos de armazenamento em unidade de estado sólido (SSD) e em unidade de disco rígido (HDD) magnético. O armazenamento SSD foi projetado para as workloads de mais alta performance e mais sensíveis à latência, incluindo bancos de dados, workloads de processamento de mídia e aplicações de análise de dados. O armazenamento HDD foi projetado para um amplo espectro de workloads, incluindo diretórios iniciais, compartilhamentos de arquivos de usuários e departamentos e sistemas de gerenciamento de conteúdo.

Você pode alterar o tipo de armazenamento do sistema de arquivos de HDD para SSD usando o console do Amazon FSx ou a API do Amazon FSx. Você não pode alterar o tipo de armazenamento do sistema de arquivos de SSD para HDD. Lembre-se de que você não pode atualizar a configuração do sistema de arquivos novamente até seis horas após a solicitação do último aumento ou até que o processo de otimização do armazenamento seja concluído, o que for mais longo. A otimização do armazenamento pode levar de algumas horas a alguns dias para ser concluída. Para minimizar esse tempo, recomendamos atualizar o tipo de armazenamento quando houver tráfego mínimo no sistema de arquivos.

Você também pode alterar o tipo de armazenamento do sistema de arquivos de HDD para SSD restaurando um backup disponível para criar um novo sistema de arquivos e selecionando um novo tipo de armazenamento. Para obter mais informações, consulte Como restaurar backups.

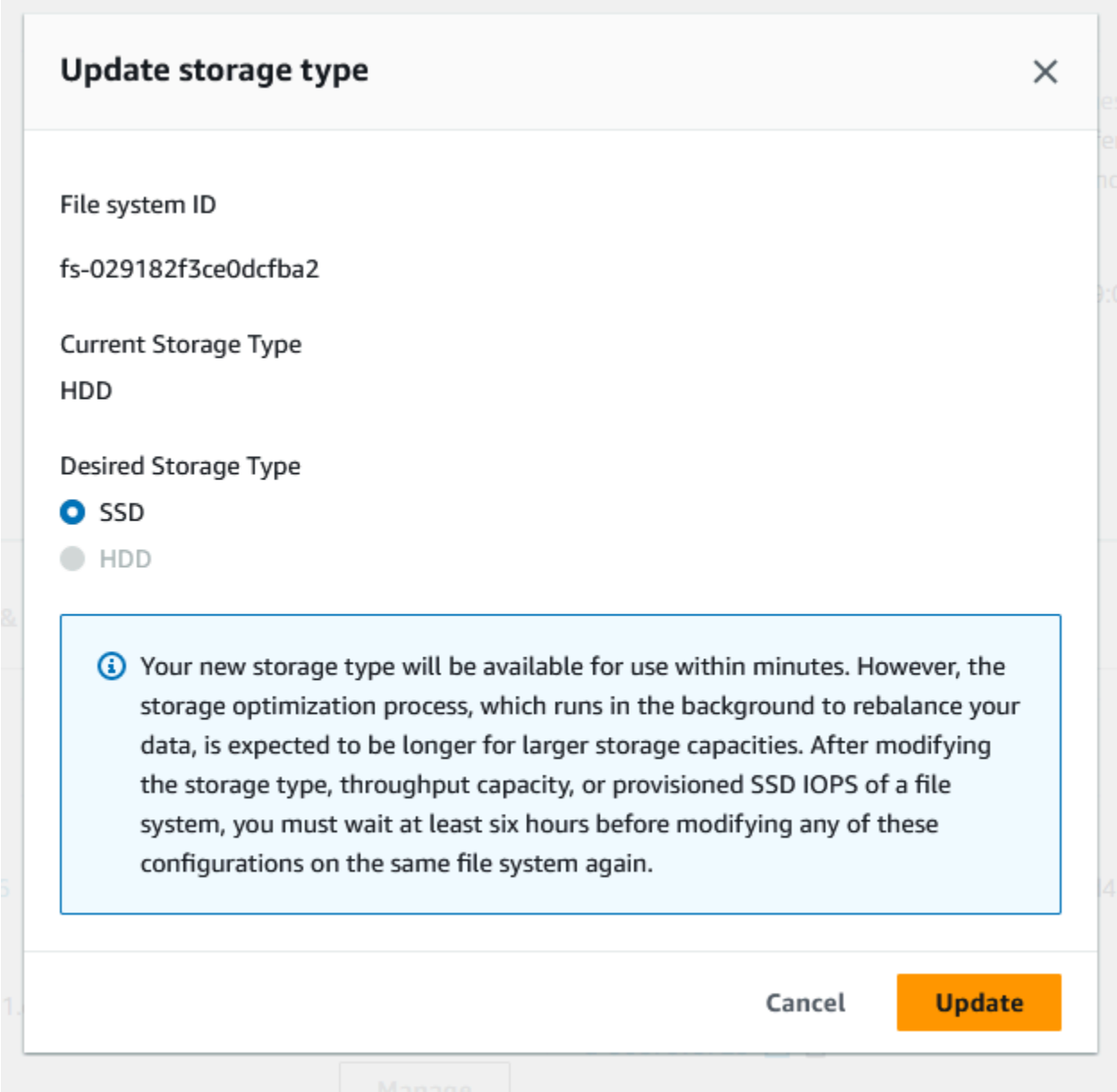
Como atualizar o tipo de armazenamento

É possível atualizar o tipo de armazenamento de um sistema de arquivos usando o console do Amazon FSx, a AWS CLI ou a API do Amazon FSx.

Atualizar o tipo de armazenamento de um sistema de arquivos (console)

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

2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do Windows para o qual você deseja atualizar o tipo de armazenamento.
3. Em Ações, escolha Atualizar tipo de armazenamento. Alternativamente, no painel Resumo, selecione o botão Atualizar ao lado de HDD. A janela Atualizar tipo de armazenamento é exibida.



4. Em Tipo de armazenamento desejado, escolha SSD. Escolha Atualizar para iniciar a atualização do tipo de armazenamento.
5. Você pode monitorar o progresso da atualização na página de detalhes dos Sistemas de arquivos, na guia Atualizações.

Atualizar o tipo de armazenamento de um sistema de arquivos (CLI)

Para atualizar o tipo de armazenamento de um sistema de arquivos do FSx para Windows File Server, use o comando update-file-system da AWS CLI. Defina os seguintes parâmetros:

- `--file-system-id` para o ID do sistema de arquivos que você deseja atualizar.
- `--storage-type` para SSD. Você não pode mudar do tipo de armazenamento SSD para o tipo de armazenamento HDD.

Você pode monitorar o progresso da atualização usando o comando describe-file-systems da AWS CLI. Procure `administrative-actions` na saída.

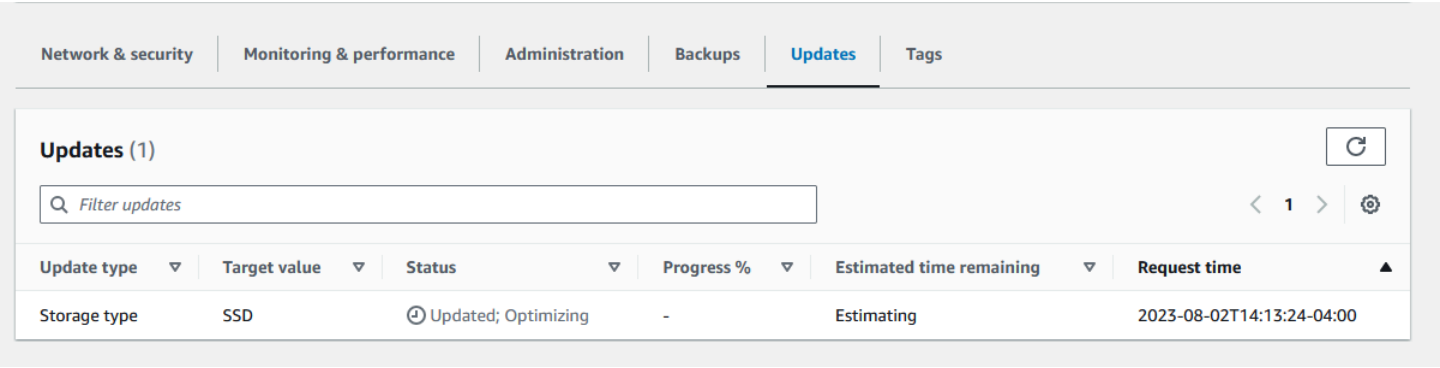
Para obter mais informações, consulte AdministrativeAction.

Como monitorar as atualizações de tipo de armazenamento

Você pode monitorar o andamento de uma atualização do tipo de armazenamento usando o console do Amazon FSx, a API ou a AWS CLI.

Como monitorar as atualizações no console

Na guia Atualizações na janela Detalhes do sistema de arquivos, você pode ver as dez atualizações mais recentes para cada tipo de atualização.



Para atualizações de tipo de armazenamento, você pode visualizar as informações a seguir.

Tipo de atualização

O valor possível é Tipo de armazenamento.

Target value (Valor de destino)

SSD

Status

O status atual da atualização. Para atualizações de tipo de armazenamento, os valores possíveis são:

- Pendente: o Amazon FSx recebeu a solicitação de atualização, mas não começou a processá-la.
- Em andamento: o Amazon FSx está processando a solicitação de atualização.
- Otimização atualizada: a performance do armazenamento SSD está disponível para as operações de gravação da workload. Sua atualização entrará em um Estado de otimização atualizada, que normalmente durará algumas horas, durante o qual as operações de leitura da workload terão níveis de performance entre HDD e SSD. Quando a ação de atualização estiver concluída, a performance do novo SSD estará disponível para leituras e gravações.
- Concluída: a atualização do tipo de armazenamento foi concluída com êxito.
- Com falha: a atualização do tipo de armazenamento apresentou falha. Escolha o ponto de interrogação (?) para ver os detalhes.

% de progresso

Exibe o andamento do processo de otimização do armazenamento pela porcentagem que está concluída.

Horário da solicitação

O horário em que o Amazon FSx recebeu a solicitação de ação de atualização.

Monitorar as atualizações com a AWS CLI e a API

Você pode visualizar e monitorar as solicitações de atualização do tipo de armazenamento do sistema de arquivos usando o comando describe-file-systems da AWS CLI e a ação de API DescribeFileSystems. A matriz `AdministrativeActions` lista as dez ações de atualização mais recentes para cada tipo de ação administrativa. Quando você aumenta o IOPS SSD de um sistema de arquivos, duas `AdministrativeActions` são geradas: uma ação `FILE_SYSTEM_UPDATE` e uma `STORAGE_TYPE_OPTIMIZATION`.

Como gerenciar IOPS de SSD

Para volumes de armazenamento SSD, você pode selecionar e escalar IOPS independentemente da capacidade de armazenamento. O máximo de IOPS de SSD que você pode provisionar depende da capacidade de armazenamento e da capacidade de throughput que você seleciona para o sistema

de arquivos. Se você tentar aumentar a IOPS de SSD acima do limite compatível com a capacidade de throughput, talvez seja necessário aumentar a capacidade de throughput para suportar o nível de IOPS de SSD solicitado. Para obter mais informações, consulte Como gerenciar a capacidade de throughput e Performance do FSx para Windows File Server.

Tópicos

Pontos importantes que você deve conhecer quando atualizar IOPS de SSD

Veja alguns itens importantes a serem considerados quando atualizar a IOPS de SSD:

- Para especificar a quantidade de IOPS de SSD provisionada para o sistema de arquivos, você deve escolher um dos dois modos de IOPS:
  - Automático — O Amazon FSx escala automaticamente seu SSD IOPS para manter 3 SSD IOPS por GiB de capacidade de armazenamento, até 400.000 SSD IOPS por sistema de arquivos.
  - Provisionado pelo usuário — você especifica o número de SSD IOPS no intervalo de 96 a 400.000. Especifique um número entre 3 e 50 IOPS por GiB de capacidade de armazenamento em todas as Regiões da AWS nas quais o Amazon FSx está disponível ou entre 3 e 500 IOPS por GiB de capacidade de armazenamento nas regiões Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Leste dos EUA (Ohio), Europa (Irlanda), Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Singapura). Se a quantidade de IOPS de SSD não for pelo menos 3 IOPS por GiB, a solicitação apresentará falha. Para níveis mais altos de IOPS de SSD provisionada, você paga pela média de IOPS acima de 3 IOPS por GiB por sistema de arquivos.
- Atualizações da capacidade de armazenamento: se você aumentar a capacidade de armazenamento e a nova capacidade exigir um nível mais alto de IOPS de SSD do que o nível provisionado pelo usuário, o Amazon FSx alternará automaticamente o sistema de arquivos para o modo Automático.
- Atualizações da capacidade de throughput: se você aumentar a capacidade de throughput e a IOPS de SSD compatível com a nova capacidade de throughput for superior ao nível de IOPS de SSD provisionado pelo usuário, o Amazon FSx alternará automaticamente o sistema de arquivos para o modo Automático.
- Tempo entre aumentos: não é possível fazer mais aumentos da IOPS de SSD, aumentos da capacidade de throughput ou atualizações no tipo de armazenamento em um sistema de arquivos

até seis horas após a solicitação do último aumento ou até que o processo de otimização de armazenamento tenha sido concluído, o que for mais longo. A otimização do armazenamento pode levar de algumas horas a alguns dias para ser concluída. Para minimizar o tempo necessário para a conclusão da otimização do armazenamento, recomendamos escalar a IOPS de SSD quando houver tráfego mínimo no sistema de arquivos.

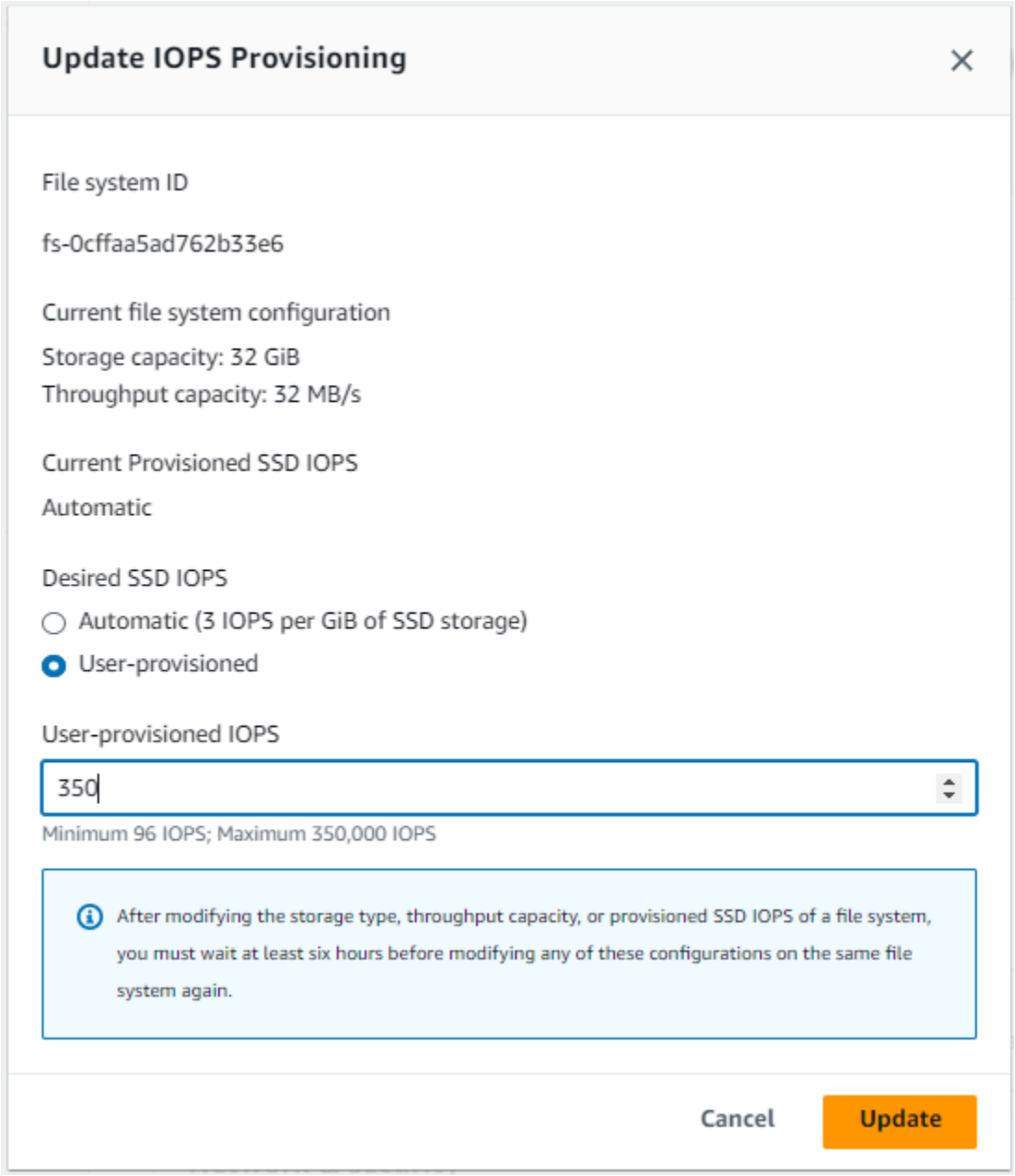
> **Note**
>
> Observe que níveis de capacidade de throughput de 4.608 MBps ou mais são compatíveis apenas nas seguintes Regiões da AWS: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Leste dos EUA (Ohio), Europa (Irlanda), Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Singapura).

Como atualizar a IOPS de SSD

Você pode atualizar a IOPS de SSD de um sistema de arquivos usando o console do Amazon FSx, a AWS CLI ou a API do Amazon FSx.

Atualizar a IOPS de SSD para 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 Windows para o qual você deseja atualizar a IOPS de SSD.
3. Em Ações, escolha Atualizar IOPS de SSD. Alternativamente, no painel Resumo, selecione o botão Atualizar ao lado de IOPS de SSD provisionada. A janela Atualizar provisionamento de IOPS é aberta.



4. Em Modo, escolha Automático ou Provisionado pelo usuário. Se você escolher Automático, o Amazon FSx provisionará automaticamente 3 IOPS de SSD por GiB de capacidade de armazenamento para o sistema de arquivos. Se você escolher Provisionado pelo usuário, insira qualquer número inteiro no intervalo de 96 a 400.000.
5. Escolha Atualizar para iniciar a atualização da IOPS de SSD provisionada.
6. Você pode monitorar o progresso da atualização na página de detalhes dos Sistemas de arquivos, na guia Atualizações.

Atualizar a IOPS de SSD para um sistema de arquivos (CLI)

Para atualizar a IOPS de SSD de um sistema de arquivos do FSx para Windows File Server, use a propriedade `--windows-configuration DiskIopsConfiguration`. Essa propriedade tem dois parâmetros, `Iops` e `Mode`:

- Se você quiser especificar o número de SSD IOPS`Iops=`*`number_of_IOPS`*, use até um máximo de 400.000 nas regiões suportadas e. AWS `Mode=USER_PROVISIONED`
- Se você quiser que o Amazon FSx aumente automaticamente a IOPS de SSD, use `Mode=AUTOMATIC` e não use o parâmetro `Iops`. O Amazon FSx mantém automaticamente 3 SSD IOPS por GiB de capacidade de armazenamento em seu sistema de arquivos, até um máximo de 400.000 nas regiões suportadas. AWS

Você pode monitorar o progresso da atualização usando o AWS CLI comando describe-file-systems. Procure `administrative-actions` na saída.

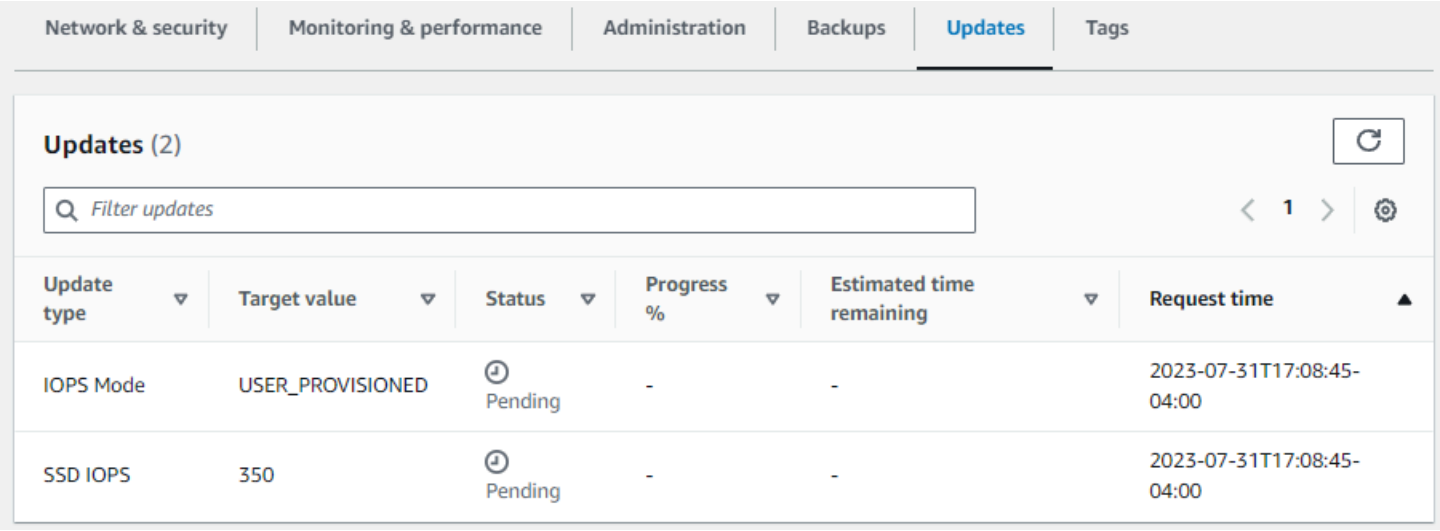
Para obter mais informações, consulte AdministrativeAction.

Monitorar atualizações de IOPS de SSD provisionadas

Você pode monitorar o andamento de uma atualização de IOPS de SSD provisionada usando o console do Amazon FSx, a API ou a AWS CLI.

Como monitorar as atualizações no console

Na guia Atualizações na janela Detalhes do sistema de arquivos, você pode ver as dez atualizações mais recentes para cada tipo de atualização.



Para atualizações de IOPS de SSD provisionadas, você pode visualizar as informações a seguir.

Tipo de atualização

Os valores possíveis são Modo IOPS e IOPS de SSD.

Target value (Valor de destino)

O valor desejado para atualização do modo IOPS e a IOPS de SSD do sistema de arquivos.

Status

O status atual da atualização. Para atualizações de IOPS de SSD, os valores possíveis são os seguintes:

- 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.
- Otimização atualizada: o novo nível de IOPS está disponível para as operações de gravação da workload. A atualização entrará em um estado de Otimização atualizada, que normalmente durará algumas horas, durante o qual as operações de leitura da workload terão níveis de performance de IOPS entre o nível anterior e o novo nível. Depois que a ação de atualização for concluída, o novo nível de IOPS estará disponível para leituras e gravações.
- Concluída: a atualização de IOPS de SSD foi concluída com êxito.
- Com falha: a atualização de IOPS SSD apresentou falha. Escolha o ponto de interrogação (?) para ver os detalhes sobre o motivo da falha na atualização do armazenamento.

% de progresso

Exibe o progresso do processo de otimização do armazenamento como a porcentagem concluída.

Horário da solicitação

O horário em que o Amazon FSx recebeu a solicitação de ação de atualização.

Monitorar as atualizações com a AWS CLI e a API

Você pode visualizar e monitorar solicitações de atualização de SSD IOPS do sistema de arquivos usando o describe-file-systemsAWS CLIcomando e a ação da DescribeFileSystemsAPI. A matriz `AdministrativeActions` lista as dez ações de atualização mais recentes para cada tipo de ação administrativa. Quando você aumenta a IOPS de SSD de um sistema de arquivos,

duas `AdministrativeActions` são geradas: uma ação `FILE_SYSTEM_UPDATE` e uma ação `IOPS_OPTIMIZATION`.

Como gerenciar a capacidade de throughput

Cada sistema de arquivos do FSx para Windows File Server tem uma capacidade de throughput configurada quando o sistema de arquivos é criado. Você pode modificar a capacidade de throughput do sistema de arquivos a qualquer momento, conforme necessário. A capacidade de throughput é um fator que determina a velocidade com que o servidor de arquivos que hospeda o sistema de arquivos pode disponibilizar os dados de arquivos. Níveis mais elevados de capacidade de throughput também apresentam níveis mais elevados de operações de E/S por segundo (IOPS) e mais memória para armazenamento em cache de dados no servidor de arquivos. Para obter mais informações, consulte Performance do FSx para Windows File Server.

Quando você modifica a capacidade de throughput do sistema de arquivos, o Amazon FSx automaticamente desativa o servidor de arquivos do sistema de arquivos. Para sistemas de arquivos multi-AZ, isso resulta em failover e failback automáticos, enquanto o Amazon FSx substitui os servidores de arquivos preferenciais e secundários. Para sistemas single-AZ, o sistema de arquivos ficará indisponível por alguns minutos durante o ajuste de escala da capacidade de throughput. Você será cobrado pela nova capacidade de throughput quando ela estiver disponível para o sistema de arquivos.

> **Note**
>
> Durante uma operação de manutenção no back-end, as modificações do sistema (como uma modificação na capacidade de throughput) podem ser atrasadas. A manutenção pode fazer com que essas alterações fiquem na fila até estarem prestes a ser processadas.

Tópicos

Quando modificar a capacidade de throughput

O Amazon FSx se integra ao Amazon CloudWatch, possibilitando que você monitore os níveis contínuos de uso do throughput do sistema de arquivos. A performance (throughput e IOPS) que você pode gerar usando o sistema de arquivos depende das características específicas da workload, além da capacidade de throughput, da capacidade de armazenamento e do tipo de armazenamento do sistema de arquivos. Você pode usar as métricas do CloudWatch para determinar quais dessas dimensões devem ser alteradas para melhorar a performance. Para obter mais informações, consulte Monitoramento de métricas com a Amazon CloudWatch.

Para sistemas de arquivos multi-AZ, o ajuste de escala da capacidade de throughput resulta em failover e failback automáticos, enquanto o Amazon FSx substitui os servidores de arquivos preferenciais e secundários. Durante as substituições do servidor de arquivos, que ocorrem durante o ajuste de escala da capacidade de throughput, e também durante a manutenção do sistema de arquivos e a interrupção não planejada do serviço, qualquer tráfego contínuo para o sistema de arquivos será disponibilizado pelo servidor de arquivos restante. Quando o servidor de arquivos substituído estiver on-line novamente, o FSx para Windows executará um trabalho de ressincronização para garantir que os dados sejam ressincronizados com o servidor de arquivos recém-substituído.

O FSx para Windows foi projetado para minimizar o impacto dessa atividade de ressincronização na aplicação e nos usuários. No entanto, o processo de ressincronização envolve a sincronização de dados em grandes blocos. Isso significa que um grande bloco de dados pode precisar de sincronização mesmo que apenas uma pequena parte seja atualizada. Consequentemente, o volume de ressincronização depende não apenas do nível da rotatividade de dados, mas também da natureza da rotatividade de dados no sistema de arquivos. Se a workload tiver um uso pesado de gravação e de IOPS, o processo de sincronização de dados poderá levar mais tempo e exigir recursos adicionais de performance.

O sistema de arquivos permanecerá disponível durante esse período. Porém, para reduzir a duração da sincronização de dados, é recomendável modificar a capacidade de throughput durante períodos ociosos quando houver uma carga mínima no sistema de arquivos. Também é recomendável garantir que o sistema de arquivos tenha capacidade de throughput suficiente para executar o trabalho de sincronização além da workload, para reduzir a duração da sincronização de dados. Por fim, recomendamos testar o impacto dos failovers enquanto o sistema de arquivos tiver uma carga mais leve.

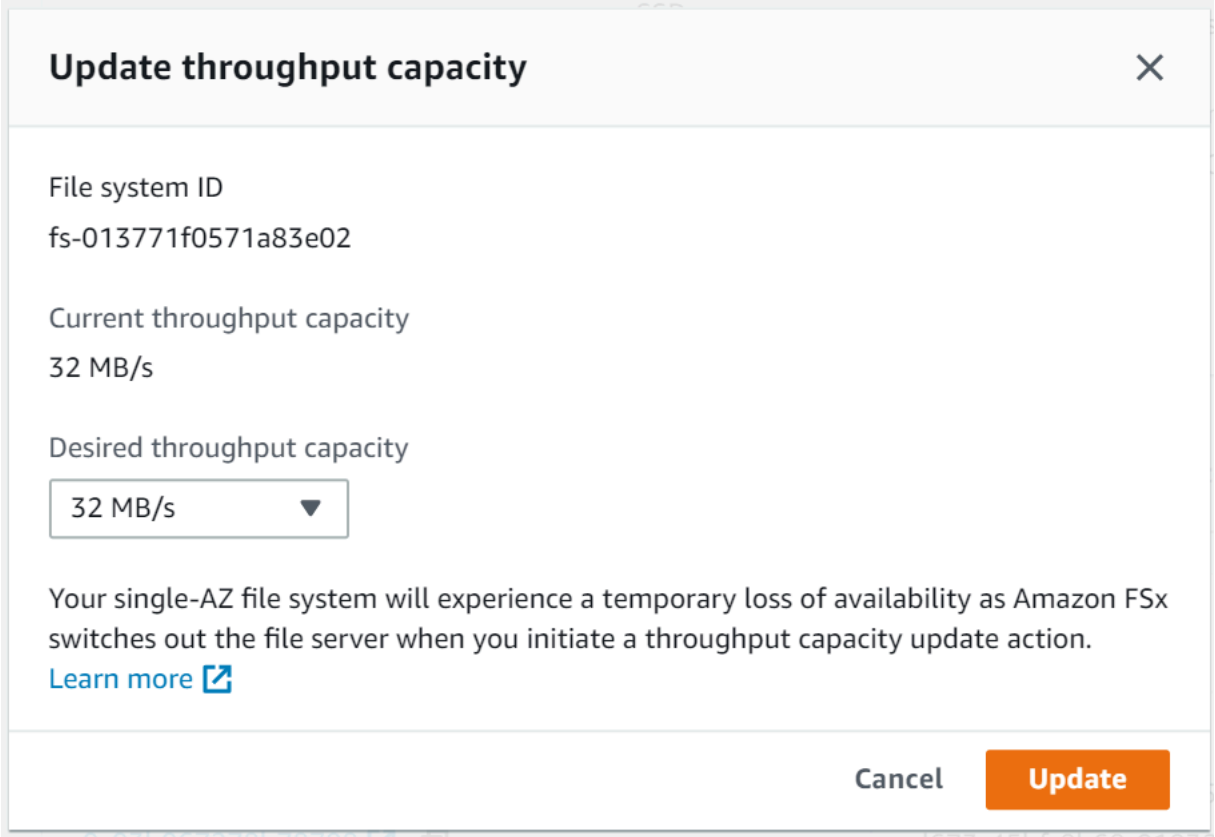
Como modificar a capacidade de throughput

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 Windows para o qual você deseja aumentar a capacidade de throughput.
3. Em Ações, escolha Atualizar throughput. Como alternativa, no painel Resumo, escolha Atualizar ao lado da Capacidade de throughput do sistema de arquivos.

   A janela Atualizar capacidade de throughput é exibida.
4. Escolha o novo valor para Capacidade de throughput na lista.



5. Escolha Atualizar para iniciar a atualização da capacidade de throughput.

> **Note**
>
> Os sistemas de arquivos multi-AZ apresentam failover e failback durante a atualização do ajuste de escala de throughput e permanecem totalmente disponíveis. Os sistemas de arquivos single-AZ passam por um breve período de indisponibilidade durante a atualização.

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 throughput de um sistema de arquivos, use o comando update-file-system da AWS CLI. 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.

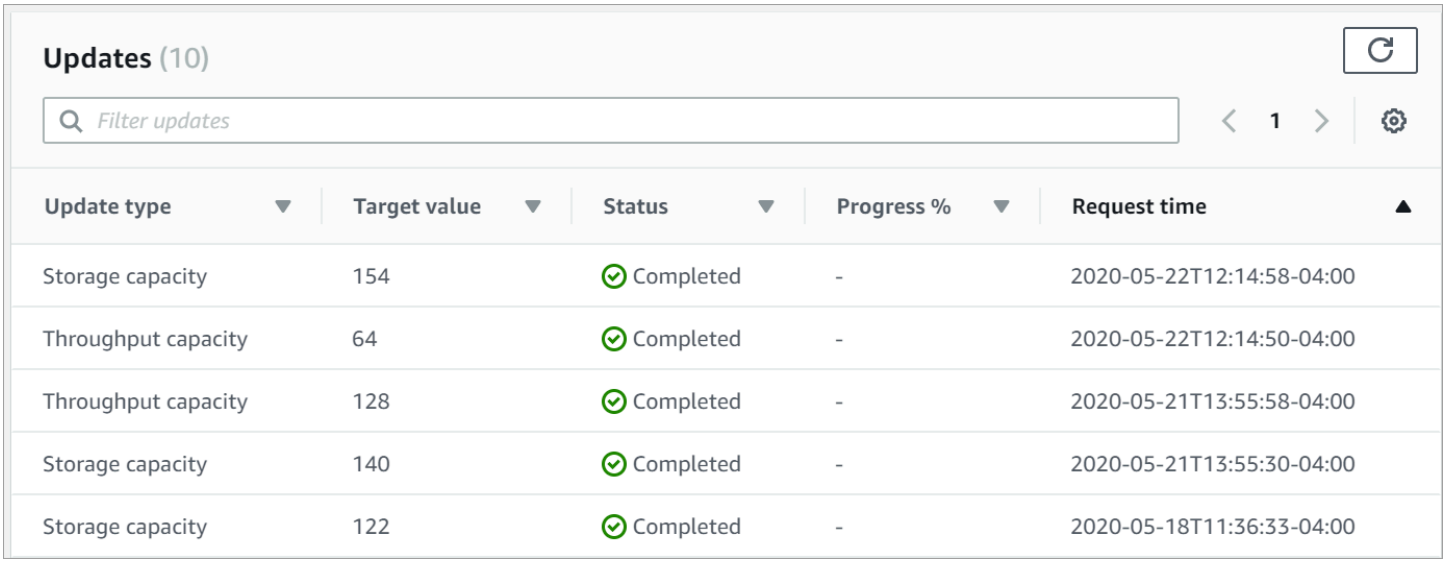
Você pode monitorar o progresso da atualização usando o console do Amazon FSx, a AWS CLI e a API. Para obter mais informações, consulte Como monitorar as alterações na capacidade de throughput.

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 ver as dez ações de atualização mais recentes para cada tipo de ação de atualização.



Nas ações de atualização da capacidade de throughput, é possível visualizar as informações apresentadas a seguir.

Tipo de atualização

O valor possível é Capacidade de throughput.

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.
- Otimização atualizada: o Amazon FSx atualizou os recursos de E/S da rede, CPU e memória do sistema de arquivos. O novo nível de performance de E/S de disco está disponível para operações de gravação. As operações de leitura terão uma performance de E/S de disco entre o nível anterior e o novo nível até que o sistema de arquivos não esteja mais neste estado.
- Concluído: a atualização da capacidade de throughput foi concluída com êxito.
- Com falha: a atualização da capacidade de throughput falhou. Escolha o ponto de interrogação (?) para ver os detalhes sobre o motivo da falha na atualização do throughput.

Horário da solicitação

O horário em que o Amazon FSx recebeu a solicitação de atualização.

Como monitorar as alterações com a AWS CLI e a API

Você pode visualizar e monitorar as solicitações de modificação da capacidade de throughput do sistema de arquivos usando o comando describe-file-systems da CLI e a ação de API DescribeFileSystems. 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 8 MB/s e a capacidade de throughput de destino de 256 MB/s.

```
.
.
.
    "ThroughputCapacity": 8,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Quando o Amazon FSx conclui o processamento da ação com êxito, o status muda 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": {
          "WindowsConfiguration": {
            "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. Para obter informações sobre a solução de problemas de ações com falha, consulte Falha nas atualizações da capacidade de armazenamento ou capacidade de throughput.

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. As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Isso é útil quando você tem muitos recursos do mesmo tipo. É possível identificar rapidamente um recurso específico baseado nas tags que você atribuiu a ele. Este tópico descreve tags e mostra a você como criá-los.

Tópicos

Conceitos básicos de tags

Uma etiqueta é um rótulo atribuído a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional, ambos definidos por você.

As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Por exemplo, é possível definir um conjunto de tags para os sistemas de arquivos do Amazon FSx 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, consulte o whitepaper da AWS, Tagging Best Practices (Práticas recomendadas de marcação).

As tags não têm nenhum significado semântico para o Amazon FSx e são interpretadas estritamente como uma sequência de caracteres. Além disso, as tags não são automaticamente atribuídas aos seus recursos. É possível editar chaves de tags e valores, e é possível remover as tags de um recurso a qualquer momento. É possível definir o valor de uma tag a uma string vazia, mas não pode configurar o valor de um tag como nula. Se você adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo. Se você excluir um recurso, todas as tags do recurso também serão excluídas.

Caso esteja usando a API do Amazon FSx, a AWS CLI, ou um AWS SDK, você poderá usar a ação `TagResource` da API para aplicar tags aos recursos existentes. Além disso, algumas ações de criação de recursos permitem que você especifique tags para um recurso quando ele é criado. Se as tags não puderem ser aplicadas durante a criação dos recursos, nós reverteremos o processo de criação de recursos. Isso garante que os recursos sejam criados com tags ou, então, não criados, e que nenhum recurso seja deixado sem tags. Ao marcar com tags os recursos no momento da criação, você elimina a necessidade de executar scripts personalizados de uso de tags após a criação do recurso. Para obter mais informações sobre como permitir que os usuários marquem os recursos durante a criação, consulte Conceder permissão para marcar recursos durante a criação.

Marcar recursos da

É possível 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. O console pode organizar os recursos de acordo com a tag Nome, mas ela não tem nenhum significado semântico para o serviço do Amazon FSx.

Você pode 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 para implementar controle granular sobre os usuários e grupos que podem marcar recursos na criação. Seus recursos estão devidamente protegidos contra criação. As tags aplicadas imediatamente aos recursos; portanto, todas as permissões em nível de recurso baseadas em tags que controlam o uso de recursos entram imediatamente em vigor. Seus recursos podem ser rastreados e relatados com mais precisão. É possível obrigar o uso de marcação com tags nos novos recursos e controlar quais chaves e valores de tag são definidos nos seus recursos.

Você também pode aplicar permissões no nível de recurso às ações de API `TagResource` e `UntagResource` do Amazon FSx nas suas políticas do IAM para controlar quais chaves e valores de tags serão definidos nos recursos existentes.

Para obter mais informações sobre a aplicação de tags nos seus recursos para faturamento, consulte Uso de tags de alocação de custos no Guia do usuário do AWS Billing.

Restrições de tags

As restrições básicas a seguir se aplicam às tags:

- Número máximo de tags por recurso: 50
- Em todos os recursos, cada chave de etiqueta deve ser exclusiva e pode ter apenas um valor.
- Comprimento máximo da chave: 128 caracteres Unicode em UTF-8
- Comprimento máximo do valor: 256 caracteres Unicode em UTF-8
- Os caracteres permitidos para tags do Amazon FSx são: letras, números e espaços representáveis em UTF-8 e os seguintes caracteres: + - = . _ : / @.
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.
- O prefixo `aws:` é reservado para uso da AWS. Não é possível editar nem excluir a chave ou o valor de uma tag quando ela tem uma chave de tag com esse prefixo. As tags com o prefixo `aws:` não contam para as tags por limite de recurso.

Você não pode excluir um recurso unicamente com base em suas tags, portanto, você deve especificar o identificador de recursos. Por exemplo, para excluir um sistema de arquivos marcado com uma chave de tag denominada `DeleteMe`, você deve usar a ação `DeleteFileSystem` com o identificador de recursos do sistema de arquivos, como fs-1234567890abcdef0.

Ao marcar recursos públicos ou compartilhados, as tags atribuídas tornam-se disponíveis somente para sua Conta da AWS. Nenhuma outra Conta da AWS terá acesso a essas tags. Para obter um controle de acesso baseado em tags para os recursos compartilhados, cada Conta da AWS deve atribuir seu próprio conjunto de tags para controlar o acesso ao recurso.

Permissões e tag

Para obter mais informações sobre as permissões necessárias para marcar os recursos do Amazon FSx no momento da criação, consulte Conceder permissão para marcar recursos durante a criação. Para obter mais informações sobre 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.

Trabalhar com janelas de manutenção do Amazon FSx

O Amazon FSx para Windows File Server executa correções de software de rotina para o software do Microsoft Windows Server que ele gerencia. A janela de manutenção permite controlar o dia e a hora da semana em que a aplicação de patches de software ocorrerá. Você escolhe a janela de manutenção durante a criação do sistema de arquivos. Se você não tiver preferência de horário, será atribuída uma janela padrão de 30 minutos.

O FSx para Windows File Server permite o ajuste da janela de manutenção para acomodar a workload e os requisitos operacionais. É possível mover a janela de manutenção com a frequência necessária, desde que uma janela de manutenção seja programada, no mínimo, uma vez a cada 14 dias. Se um patch for lançado e você não tiver programado uma janela de manutenção no prazo de 14 dias, o FSx para Windows File Server executará a manutenção no sistema de arquivos para garantir a segurança e confiabilidade.

Enquanto a aplicação de patches estiver em andamento, conte com uma indisponibilidade dos sistemas de arquivos single-AZ, que normalmente dura menos de 20 minutos. Os sistemas de arquivos multi-AZ permanecem disponíveis e automaticamente apresentam failover e failback entre o servidor de arquivos preferencial e o servidor de arquivos em espera. Para obter mais informações, consulte Processo de failover para o FSx para Windows File Server. Como a aplicação de patches em sistemas de arquivos multi-AZ envolve failover e failback, qualquer tráfego para o sistema de arquivos durante esse período deve ser sincronizado entre o servidor de arquivos preferencial e o servidor de arquivos em espera. Para reduzir o tempo de aplicação de patches, recomendamos programar a janela de manutenção durante períodos ociosos quando houver uma carga mínima no sistema de arquivos.

> **Note**
>
> Para garantir a integridade dos dados durante a atividade de manutenção, o Amazon FSx para Windows File Server conclui todas as operações de gravação pendentes nos volumes de armazenamento subjacentes que hospedam o sistema de arquivos antes do início da manutenção.

Você pode usar o console de gerenciamento do Amazon FSx, a AWS CLI, a API da AWS ou um dos AWS SDKs para alterar a janela de manutenção dos seus sistemas de arquivos.

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 você deseja alterar a janela de manutenção semanal. A página de detalhes 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 Save (Salvar) para salvar as alterações. A nova hora de início da manutenção é exibida no painel Configurações de administração.

Para alterar a janela de manutenção semanal usando o comando update-file-system da CLI, consulte Passo a passo 3: atualizar um sistema de arquivos existente.

Práticas recomendadas para administração de sistemas de arquivos do Amazon FSx

O Amazon FSx fornece vários recursos que podem ajudar você a implementar as práticas recomendadas para administrar seus sistemas de arquivos, incluindo:

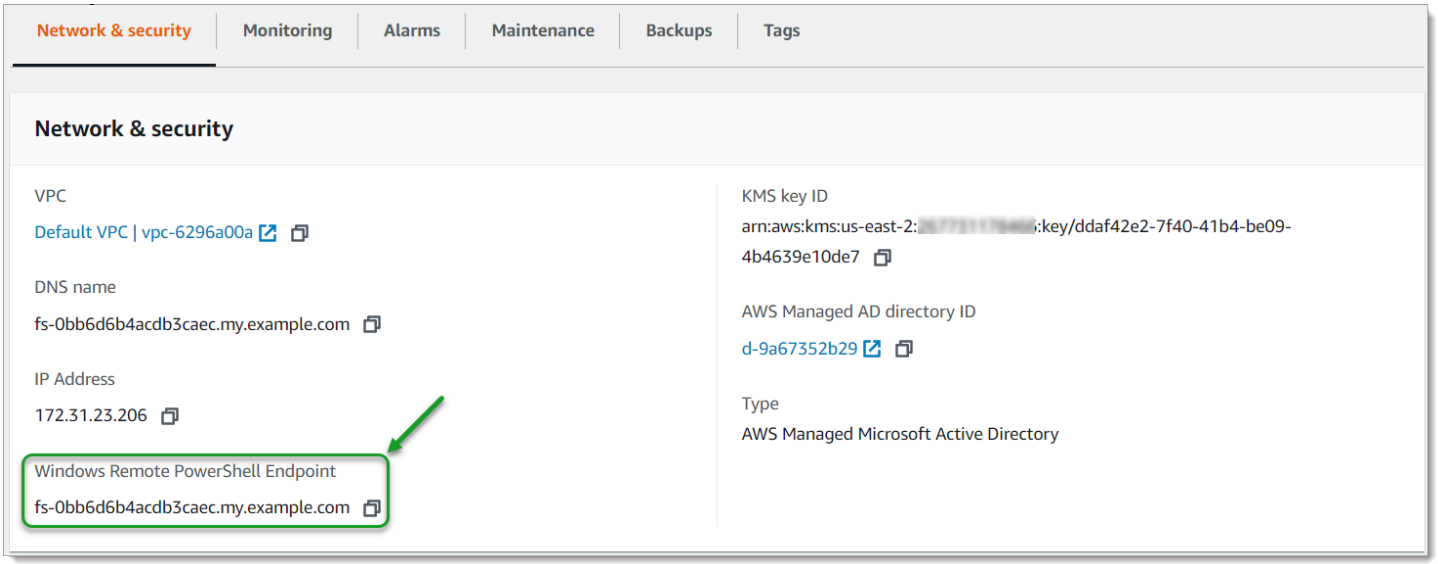
- otimizar o consumo do armazenamento;
- permitir que os usuários finais recuperem arquivos e pastas para versões anteriores;

- aplicar a criptografia para todos os clientes conectados

Use a seguinte CLI do Amazon FSx para gerenciamento remoto em PowerShell comandos para implementar rapidamente essas melhores práticas em seus sistemas de arquivos.

Para executar esses comandos, você deve conhecer o PowerShellEndpoint Remoto do Windows para seu sistema de arquivos. Para encontrar esse endpoint, siga estas etapas:

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Escolha o sistema de arquivos. Na guia Rede e segurança, localize o PowerShell Endpoint Remoto do Windows, conforme mostrado a seguir.



Para obter mais informações, consulte Como administrar sistemas de arquivos e Usando a CLI do Amazon FSx para PowerShell.

Tópicos

- Tarefas únicas de configuração administrativa
- Tarefas administrativas contínuas para monitorar o sistema de arquivos

Tarefas únicas de configuração administrativa

A seguir, estão as tarefas que você pode configurar rapidamente, uma vez, para o sistema de arquivos.

Como gerenciar o consumo do armazenamento

Use os comandos a seguir para gerenciar o consumo de armazenamento do sistema de arquivos.

- Para ativar a eliminação de duplicação de dados com a programação padrão, execute o comando a seguir.

  ```
  Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
   FSxRemoteAdmin -ScriptBlock { Enable-FsxDedup }
  ```

  Há a opção de usar o comando a seguir para que a eliminação de duplicação de dados opere em seus arquivos logo após a criação de um arquivo, sem exigir a idade mínima do arquivo.

  ```
  Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
   FSxRemoteAdmin -ScriptBlock { Set-FSxDedupConfiguration -MinimumFileAgeDays 0 }
  ```

  Para ter mais informações, consulte Eliminação de duplicação de dados.

- Use o comando a seguir para ativar as cotas de armazenamento do usuário no modo “Rastrear”, que serve apenas para fins de emissão de relatórios e não para imposição.

  ```
  $QuotaLimit = Quota limit in bytes
  $QuotaWarningLimit = Quota warning threshold in bytes
  Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
   FSxRemoteAdmin -ScriptBlock { Enable-FSxUserQuotas -Track -DefaultLimit
   $Using:QuotaLimit -DefaultWarningLimit $Using:QuotaWarningLimit }
  ```

  Para ter mais informações, consulte Cotas de armazenamento.

Ativar cópias de sombra para permitir que os usuários finais recuperem arquivos e pastas das versões anteriores

Ative as cópias de sombra com a programação padrão (dias úteis, 7h e 12h), conforme a seguir.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowStorage -Default }
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowCopySchedule -Default -Confirm:$False}
```

Para ter mais informações, consulte Configurando cópias de sombra para usar o armazenamento e a programação padrão.

Aplicar a criptografia em trânsito

O comando a seguir aplica a criptografia para clientes que se conectam ao seu sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxSmbServerConfiguration -EncryptData $True -
RejectUnencryptedAccess $True -Confirm:$False}
```

Você pode fechar todas as sessões abertas e forçar os clientes atualmente conectados a se reconectarem usando criptografia.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbSession -Confirm:$False}
```

Para obter mais informações, consulte Como gerenciar criptografia em trânsito e Sessões de usuário e arquivos abertos.

Tarefas administrativas contínuas para monitorar o sistema de arquivos

As tarefas contínuas a seguir ajudam você a monitorar o uso do disco, as cotas de usuários e os arquivos abertos do sistema de arquivos.

Como monitorar o status da eliminação de duplicação

Monitore o status da eliminação de duplicação, incluindo a taxa de economia alcançada em seu sistema de arquivos, como a seguir.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FsxRemoteAdmin -ScriptBlock { Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate
```

Como monitorar o consumo de armazenamento no nível de usuário

Obtenha um relatório das entradas atuais da cota de armazenamento do usuário, incluindo quanto espaço eles estão consumindo e se estão violando o limite e o limite de aviso.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxUserQuotaEntries }
```

Como monitorar e fechar arquivos abertos

Gerencie arquivos abertos procurando os arquivos que ficaram abertos e fechando-os. Use o comando a seguir para verificar se há arquivos abertos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxSmbOpenFile}
```

Use o comando a seguir para fechar os arquivos abertos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbOpenFile -Confirm:$false}
```

Agrupar vários sistemas de arquivos com namespaces do DFS

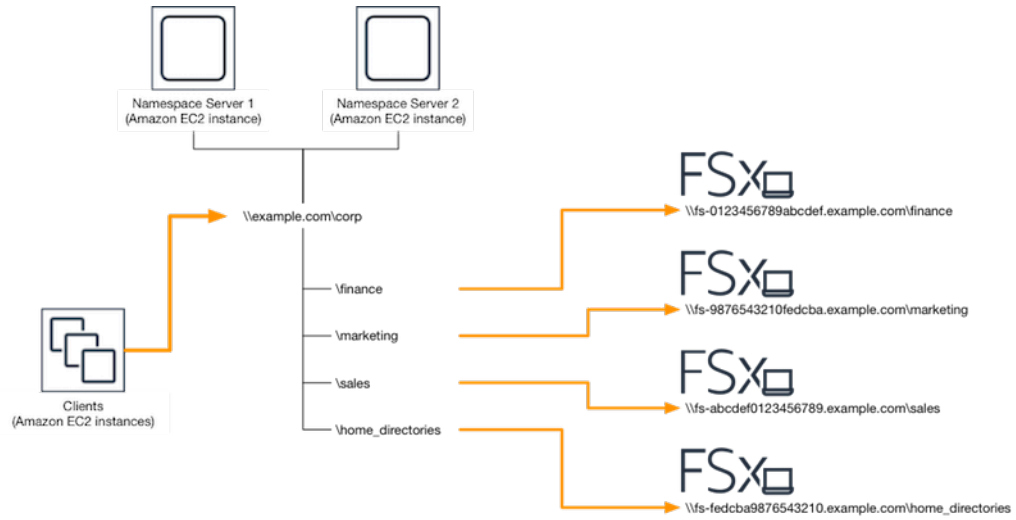
O Amazon FSx para Windows File Server é compatível com o uso des namespaces do Sistema de Arquivos Distribuído (DFS) da Microsoft. Você pode usar namespaces do DFS para agrupar compartilhamentos de arquivos em vários sistemas de arquivos em uma estrutura de pasta comum (um namespace) que você usa para acessar todo o conjunto de dados dos arquivos. Os namespaces do DFS podem ajudar você a organizar e unificar o acesso aos compartilhamentos de arquivos em vários sistemas de arquivos. Os namespaces do DFS também podem ajudar a escalar o armazenamento de dados de arquivos além do que cada sistema de arquivos suporta (64 TB) para grandes conjuntos de dados de arquivos de até centenas de petabytes.

Configurar namespaces do DFS para agrupar vários sistemas de arquivos

Você pode usar namespaces do DFS para agrupar vários sistemas de arquivos em um único namespace. No exemplo a seguir, o namespace baseado em domínio (example.com\corp) é criado em dois servidores de namespace, consolidando compartilhamentos de arquivos armazenados em vários sistemas de arquivos do Amazon FSx (finanças, marketing, vendas, home_directories). Isso permite que os usuários acessem compartilhamentos de arquivos usando um namespace comum. Diante disso, eles não precisam especificar nomes DNS do sistema de arquivos para cada um dos sistemas de arquivos que hospedam os compartilhamentos de arquivos.

> **Note**
>
> O Amazon FSx não pode ser adicionado à raiz do caminho de compartilhamento do DFS.

Essas etapas orientam você na criação de um único namespace (example.com\corp) em dois servidores de namespace. Você também configura quatro compartilhamentos de arquivos no namespace, cada um redirecionando os usuários de forma transparente para compartilhamentos hospedados em sistemas de arquivos do Amazon FSx separados.



Agrupar vários sistemas de arquivos em um namespace comum do DFS

1. Se você ainda não tem servidores de Namespace DFS em execução, você pode iniciar um par de servidores de Namespace DFS altamente disponíveis usando o modelo Setup-DFSN-Servers.template. AWS CloudFormation 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.
2. Conecte-se a um dos servidores de namespace do DFS iniciados na etapa anterior como usuário no grupo de Administradores delegados da AWS . Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
3. Acesse o console de gerenciamento do DFS ao abrir. Abra o menu Iniciar e execute dfsmgmt.msc. Isso abre a ferramenta da GUI de gerenciamento do DFS.
4. Escolha Ação e, em seguida, Novo namespace, digite o nome do computador do primeiro servidor de namespace do DFS que você iniciou em Servidor e selecione Próximo.
5. Em Nome, digite o namespace que você está criando (por exemplo, corp).
6. Escolha Editar configurações e defina as permissões apropriadas com base em seus requisitos. Selecione Next (Próximo).
7. Deixe a opção padrão Namespace baseado em domínio selecionada, deixe a opção Habilitar o modo Windows Server 2008 selecionada e escolha Próximo.

> **Note**
>
> O modo Windows Server 2008 é a opção mais recente disponível para namespaces.

8. Analise as configurações do namespace e escolha Criar.
9. Com o namespace recém-criado selecionado em Namespaces na barra de navegação, escolha Ação e, em seguida, Adicionar servidor do namespace.
10. Digite o nome do computador do segundo servidor do namespace do DFS que você iniciou para o Servidor do namespace.
11. Escolha Editar configurações, defina as permissões apropriadas com base em seus requisitos e escolha OK.
12. Abra o menu de contexto (clique com o botão direito do mouse) do namespace que você acabou de criar, selecione Nova pasta, digite o nome da pasta (por exemplo, `finance` em Nome) e selecione Adicionar.
13. Digite o nome DNS do compartilhamento de arquivos para o qual você deseja que a pasta Namespace do DFS aponte no formato UNC (por exemplo, `\\fs-0123456789abcdef0.example.com\finance`) em Caminho para o destino da pasta e escolha OK.
14. Se o compartilhamento não existir:
    a. Escolha Sim para criá-lo.
    b. Na caixa de diálogo Criar compartilhamento, escolha Procurar.
    c. Escolha uma pasta atual ou crie uma pasta em D$ e escolha OK.
    d. Defina as permissões de compartilhamento apropriadas e escolha OK.
15. Na caixa de diálogo Nova pasta, escolha OK. A nova pasta será criada no namespace.
16. Repita as últimas quatro etapas para outras pastas que você deseja compartilhar no mesmo namespace.

Como monitorar o FSx para Windows File Server

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon FSx e de suas AWS soluções. Você deve coletar dados de monitoramento de todas as partes da sua AWS solução para poder depurar com mais facilidade uma falha multiponto, caso ocorra. Entretanto, antes de começar a monitorar o Amazon FSx, você deve criar um plano de monitoramento que inclua respostas às seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

Para obter mais informações sobre o registro e o monitoramento no FSx para Windows File Server, consulte os tópicos a seguir.

Tópicos

Ferramentas de monitoramento

AWS fornece várias ferramentas que você pode usar para monitorar o Amazon FSx. Você pode configurar algumas dessas ferramentas para fazer o monitoramento para você, enquanto outras ferramentas exigem intervenção manual. Recomendamos que as tarefas de monitoramento sejam automatizadas ao máximo possível.

Ferramentas de monitoramento automatizadas

Você pode usar as seguintes ferramentas de monitoramento automatizado para observar o Amazon FSx e gerar relatórios quando algo estiver errado:

- Amazon CloudWatch Alarms — Observe uma única métrica durante um período de tempo especificado por você e execute uma ou mais ações com base no valor da métrica em relação a um determinado limite em vários períodos. A ação é uma notificação enviada para um tópico do Amazon Simple Notification Service (Amazon SNS) ou para uma política do Amazon EC2 Auto Scaling. CloudWatch os alarmes não invocam ações simplesmente porque estão em um determinado estado; o estado deve ter sido alterado e mantido por um determinado número de períodos. Para ter mais informações, consulte Monitoramento de métricas com a Amazon CloudWatch.
- Amazon CloudWatch Logs — Monitore, armazene e acesse seus arquivos de log de AWS CloudTrail ou de outras fontes. Para obter mais informações, consulte O que é o Amazon CloudWatch Logs? no Guia do usuário do Amazon CloudWatch Logs.
- AWS CloudTrail Monitoramento de log — Compartilhe arquivos de log entre contas, monitore arquivos de CloudTrail log em tempo real enviando-os para o CloudWatch Logs, grave aplicativos de processamento de log em Java e valide se seus arquivos de log não foram alterados após a entrega. CloudTrail Para obter mais informações, consulte Trabalhando com arquivos de CloudTrail log no Guia AWS CloudTrail do usuário.

Ferramentas de monitoramento manual

Outra parte importante do monitoramento do Amazon FSx envolve o monitoramento manual dos itens que os CloudWatch alarmes da Amazon não cobrem. O Amazon FSx, CloudWatch, e outros painéis de AWS console fornecem uma at-a-glance visão do estado do seu ambiente. AWS

Os painéis de Monitoramento e performance do console do Amazon FSx mostram:

- Avisos CloudWatch e alarmes atuais do FSx for Windows File Server
- Gráficos que mostram um resumo da atividade do sistema de arquivos
- Gráficos de capacidade e utilização de armazenamento do sistema de arquivos
- Gráficos de performance do servidor de arquivos e do volume de armazenamento
- CloudWatch alarmes

A página CloudWatch inicial mostra:

- Alertas e status atual
- Gráficos de alertas e recursos

- Estado de integridade do serviço

Além disso, você pode usar CloudWatch para fazer o seguinte:

- Crie Painéis personalizados para monitorar os serviços que você usa.
- Colocar em gráfico dados de métrica para solucionar problemas e descobrir tendências.
- Pesquise e navegue por todas as suas métricas AWS de recursos.
- Criar e editar alertas para ser notificado sobre problemas.

Para obter mais informações sobre o painel de Monitoramento e performance do Amazon FSx, consulte Como usar as métricas do FSx para Windows File Server.

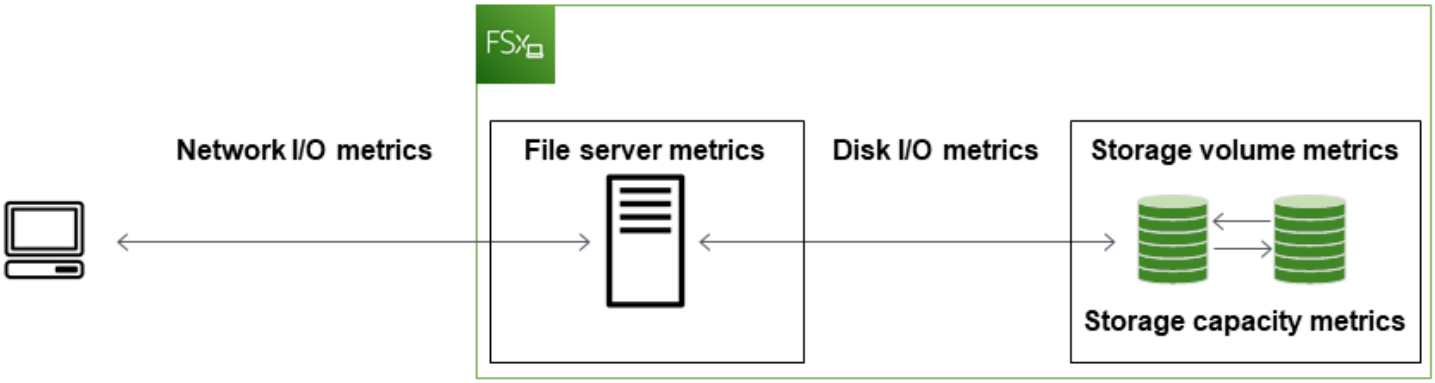
Monitoramento de métricas com a Amazon CloudWatch

Você pode monitorar os sistemas de arquivos FSx for Windows File Server usando a CloudWatch Amazon, que coleta e processa dados brutos do FSx for Windows File Server em métricas legíveis e quase em tempo real. Essas estatísticas são retidas por um período de 15 meses, para que você possa acessar informações históricas e obter perspectivas sobre a performance da sua aplicação Web ou do seu sistema de arquivos.

O FSx for Windows File Server CloudWatch publica métricas nos seguintes domínios:

- As métricas de E/S de rede medem a atividade entre os clientes que acessam o sistema de arquivos e o servidor de arquivos.
- As métricas do servidor de arquivos medem a utilização do throughput da rede, a CPU e a memória do servidor de arquivos, o throughput do disco do servidor de arquivos e a utilização de IOPS.
- As métricas de E/S de disco medem a atividade entre o servidor de arquivos e os volumes de armazenamento.
- As métricas de volume de armazenamento medem a utilização do throughput de disco para volumes de armazenamento HDD e a utilização de IOPS para volumes de armazenamento SSD.
- As métricas de capacidade de armazenamento medem o uso do armazenamento, incluindo a economia de armazenamento devido à eliminação de duplicação dos dados.

O diagrama a seguir ilustra um sistema de arquivos do FSx para Windows File Server, seus componentes e os domínios de métrica.



Por padrão, o Amazon FSx for Windows File Server envia dados métricos CloudWatch para períodos de 1 minuto, com as seguintes exceções que são emitidas em intervalos de 5 minutos:

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

Para obter mais informações sobre CloudWatch, consulte O que é a Amazon CloudWatch? no Guia do CloudWatch usuário da Amazon.

As métricas podem não ser publicadas para sistemas de arquivos single-AZ durante a manutenção do sistema de arquivos ou a substituição de componentes da infraestrutura e para sistemas de arquivos multi-AZ durante o failover e o failback entre os servidores de arquivos primário e secundário.

Algumas CloudWatch métricas do Amazon FSx são relatadas como bytes brutos. Os bytes não são arredondados para um múltiplo decimal ou binário da unidade.

Tópicos

Métricas e dimensões

O FSx for Windows File Server publica as seguintes métricas no namespace `AWS/FSx` na CloudWatch Amazon para todos os sistemas de arquivos:

- `DataReadBytes`
- `DataWriteBytes`
- `DataReadOperations`
- `DataWriteOperations`
- `MetadataOperations`
- `FreeStorageCapacity`

O FSx for Windows File Server publica as métricas descritas a seguir no namespace `AWS/FSx` na CloudWatch Amazon para sistemas de arquivos configurados com uma capacidade de transferência de pelo menos 32 MBps.

Tópicos

Métricas de E/S de rede do FSx para Windows

O namespace do `AWS/FSx` inclui as seguintes métricas de E/S de rede.

Métrica	Descrição
`DataReadBytes`	O número de bytes para operações de leitura para clientes que acessam o sistema de arquivos. Unidades: bytes

Métrica	Descrição
	Estatística válida: `Sum`
`DataWriteBytes`	O número de bytes para operações de gravação para clientes que acessam o sistema de arquivos. Unidades: bytes Estatística válida: `Sum`
`DataReadOperations`	O número de operações de leitura para clientes que acessam o sistema de arquivos. Unidades: contagem Estatística válida: `Sum`
`DataWriteOperations`	O número de operações de gravação para clientes que acessam o sistema de arquivos. Unidades: contagem Estatística válida: `Sum`
`MetadataOperations`	O número de operações de metadados para clientes que acessam o sistema de arquivos. Unidades: contagem Estatística válida: `Sum`
`ClientConnections`	O número de conexões ativas entre clientes e o servidor de arquivos. Unidades: contagem

Métricas do FSx para Windows File Server

O namespace do `AWS/FSx` inclui as seguintes métricas de servidor de arquivos.

Métrica	Descrição
`NetworkThroughputUtilization`	O throughput da rede para clientes que acessam o sistema de arquivos, como uma porcentagem do limite provisionado. Unidades: percentual
`CPUUtilization`	A porcentagem de utilização dos recursos de CPU do seu servidor de arquivos. Unidades: percentual
`MemoryUtilization`	A porcentagem de utilização dos recursos de memória do seu servidor de arquivos. Unidades: percentual
`FileServerDiskThroughputUtilization`	O throughput de disco entre o servidor de arquivos e seus volumes de armazenamento, como uma porcentagem do limite provisionado determinado pela capacidade de throughput. Unidades: percentual
`FileServerDiskThroughputBalance`	A porcentagem de créditos de intermitência disponíveis para o throughput de disco entre o servidor de arquivos e seus volumes de armazenamento. Válido para sistemas de arquivos provisionados com capacidade de throughput de 256 MBps ou menos. Unidades: percentual
`FileServerDiskIopsUtilization`	A IOPS de disco entre o servidor de arquivos e os volumes de armazenamento, como uma porcentagem do limite provisionado determinado pela capacidade de throughput. Unidades: percentual

Métrica	Descrição
`FileServerDiskIopsBalance`	A porcentagem de créditos de intermitência disponíveis para a IOPS de disco entre o servidor de arquivos e seus volumes de armazenamento. Válido para sistemas de arquivos provisionados com capacidade de throughput de 256 MBps ou menos. Unidades: percentual

Métricas de E/S de disco do FSx para Windows

O namespace do `AWS/FSx` inclui as seguintes métricas de E/S de disco:

Métrica	Descrição
`DiskReadBytes`	O número de bytes para operações de leitura que acessam volumes de armazenamento. Unidades: bytes Estatística válida: soma
`DiskWriteBytes`	O número de bytes para operações de gravação que acessam volumes de armazenamento. Unidades: bytes Estatística válida: soma
`DiskReadOperations`	O número de operações de leitura do servidor de arquivos que acessa os volumes de armazenamento. Unidades: contagem Estatística válida: `Sum`
`DiskWriteOperations`	O número de operações de gravação do servidor de arquivos que acessa os volumes de armazenamento.

Métrica	Descrição
	Unidades: contagem Estatística válida: `Sum`

Métricas de volume de armazenamento do FSx para Windows

O namespace do `AWS/FSx` inclui as seguintes métricas de volume de armazenamento.

Métrica	Descrição
`DiskThroughputUtilization`	(Somente HDD) O throughput de disco entre o servidor de arquivos e seus volumes de armazenamento, como uma porcentagem do limite provisionado determinado pelos volumes de armazenamento. Unidades: percentual
`DiskThroughputBalance`	(Somente HDD) A porcentagem de créditos de intermitência disponíveis para o throughput de disco para os volumes de armazenamento. Unidades: percentual
`DiskIopsUtilization`	(Somente SSD) A IOPS de disco entre o servidor de arquivos e os volumes de armazenamento, como uma porcentagem do limite de IOPS provisionadas determinado pelos volumes de armazenamento. Unidades: percentual

Métricas de capacidade de armazenamento do FSx para Windows

O namespace `AWS/FSx` inclui as seguintes métricas de capacidade de armazenamento.

Métrica	Descrição
`FreeStorageCapacity`	A quantidade de capacidade de armazenamento disponível. Unidades: bytes Estatística válida: `Average`, `Minimum`
`StorageCapacityUtilization`	Capacidade de armazenamento físico usada como porcentagem da capacidade total de armazenamento. Unidades: percentual
`DeduplicationSavedStorage`	A quantidade de espaço de armazenamento economizada pela eliminação de duplicação dos dados, se ela estiver desabilitada. Unidades: bytes

Dimensões do FSx para Windows

As métricas do FSx para Windows File Server usam o namespace do `FSx` e fornecem métricas para uma única dimensão, `FileSystemId`. Você pode encontrar o ID de um sistema de arquivos usando o describe-file-systems AWS CLI comando ou o comando DescribeFileSystemsda API. O ID do sistema de arquivos possui o formato de *`fs-0123456789abcdef0`*.

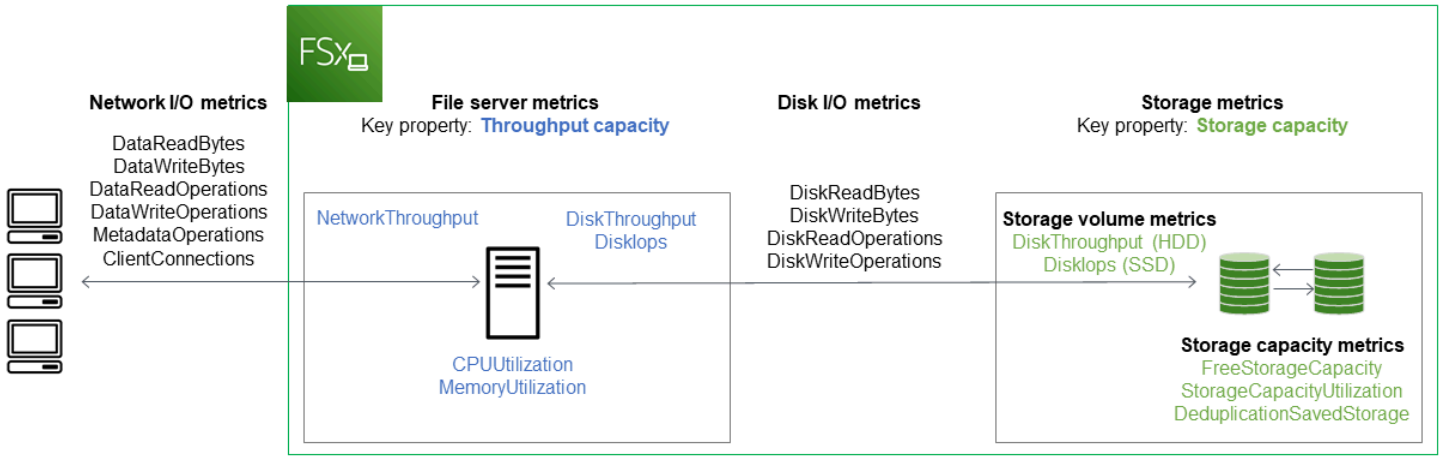
Como usar as métricas do FSx para Windows File Server

Há dois componentes arquitetônicos principais de cada sistema de arquivos do Amazon FSx:

- O servidor de arquivos que fornece dados aos clientes que acessam o sistema de arquivos.
- Os volumes de armazenamento que hospedam os dados em seu sistema de arquivos.

O FSx for Windows File Server relata métricas CloudWatch que rastreiam o desempenho e a utilização de recursos do servidor de arquivos e dos volumes de armazenamento do seu sistema de arquivos. O diagrama a seguir ilustra um sistema de arquivos Amazon FSx com seus componentes arquitetônicos e as métricas de desempenho e CloudWatch recursos disponíveis para

monitoramento. A propriedade principal mostrada para um conjunto de métricas é a propriedade do sistema de arquivos que determina a capacidade para essas métricas. O ajuste dessa propriedade modifica a performance do sistema de arquivos para esse conjunto de métricas.



Use o painel Monitoramento e desempenho no console do Amazon FSx para visualizar as métricas do FSx for Windows File CloudWatch Server descritas na tabela a seguir.

Painel de monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
Resumo	...determinar o total de IOPS do meu sistema de arquivos?	Total de IOPS	SOMA(`DataReadOperations + DataWriteOperations + MetadataOperations`)/Período (em segundos)
	...determinar o throughput total do meu sistema de arquivos?	Throughput total	SOMA(`DataReadBytes + DataWriteBytes`)/ Período (em segundos)
	...determinar a quantidade da capacidade de armazenamento disponível no meu sistema de arquivos?	Capacidade de armazenamento	`FreeStorageCapacity`

Painel de monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
		disponível	
	…determinar o número de conexões estabelecidas entre os clientes e o servidor de arquivos?	Conexões de cliente	`ClientConnections`
	...determinar a quantidade de espaço físico em disco usado como uma porcentagem da capacidade total de armazenamento do sistema de arquivos?	Utilização da capacidade de armazenamento	`StorageCapacityUtilization`
Armazenamento	...determinar a quantidade de espaço físico em disco economizado pela eliminação de duplicação dos dados?	Armazenamento economizado com a eliminação de duplicação dos dados	`DeduplicationSavedStorage`
Performance: servidor de arquivos	...determinar o throughput da rede para clientes que acessam o sistema de arquivos, como uma porcentagem do throughput provisionado do sistema de arquivos?	Utilização do throughput da rede	`NetworkThroughputUtilization`

Painel de monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
	…determinar o throughput do disco entre o servidor de arquivos e seus volumes de armazenamento, como uma porcentagem do limite provisionado determinado pela capacidade de throughput?	Utilização do throughput do disco	`FileServerDiskThroughputUtilization`
	…determinar a porcentagem de créditos de intermitência disponíveis para o throughput do disco entre o servidor de arquivos e seus volumes de armazenamento?	Equilíbrio de intermitência do throughput do disco	`FileServerDiskThroughputBalance`
	…determinar a quantidade de IOPS do disco entre o servidor de arquivos e os volumes de armazenamento, como uma porcentagem do limite provisionado determinado pela capacidade de throughput?	Utilização de IOPS do disco	`FileServerDiskIopsUtilization`
	…determinar a porcentagem de créditos de intermitência disponíveis para a IOPS do disco entre o servidor de arquivos e os volumes de armazenamento?	Equilíbrio de intermitência de IOPS do disco	`FileServerDiskIopsBalance`
	...determinar a porcentagem de utilização da CPU do servidor de arquivos?	Utilização da CPU	`CPUUtilization`

Painel de monitoramento e performance	Como faço para...	Gráfico	Métricas relevantes
	…determinar a porcentagem de utilização de memória do servidor de arquivos?	Utilização da memória	`MemoryUtilization`
Performance: volumes de armazenamento	...determinar o throughput para operações que acessam volumes de armazenamento, como uma porcentagem do limite provisionado determinado pela capacidade de armazenamento do HDD?	Utilização do throughput do disco (HDD)	`DiskThroughputUtilization`
	...determinar a porcentagem de créditos de intermitência disponíveis para o throughput de operações que acessam volumes de armazenamento em HDD?	Equilíbrio de intermitência do throughput do disco (HDD)	`DiskThroughputBalance`
	…determinar a IOPS para operações que acessam volumes de armazenamento, como uma porcentagem do limite provisionado determinado pela capacidade de armazenamento em SSD?	Utilização de IOPS do disco (SSD)	`DiskIopsUtilization`

> **Note**
>
> Recomendamos que você mantenha uma utilização média da capacidade de throughput abaixo de 50% para garantir que tenha capacidade de throughput sobressalente suficiente para picos inesperados em sua workload, bem como para quaisquer operações de

armazenamento do Windows em segundo plano (como sincronização de armazenamento, eliminação de duplicação ou cópias de sombra).

Avisos e recomendações de performance

O FSx para Windows fornece avisos de performance para sistemas de arquivos configurados com uma capacidade de throughput de pelo menos 32 MBps. O Amazon FSx exibe um aviso para um conjunto de 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 em que 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 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.

Se houver um aviso para essa métrica	Faça o seguinte
Throughput da rede: utilização	Aumentar a capacidade de throughput
Servidor de arquivos > IOPS de disco: utilização	
Servidor de arquivos > Throughput de disco: utilização	

Se houver um aviso para essa métrica	Faça o seguinte
Servidor de arquivos > IOPS de disco - equilíbrio de intermitência	
Servidor de arquivos > Throughput de disco: equilíbrio de intermitência	
Utilização da capacidade de armazenamento	Aumentar a capacidade de armazenamento
Volume de armazenamento > Throughput de disco: utilização (HDD)	Aumentar a capacidade de armazenamento ou mudar para o tipo de armazenamento SDD
Volume de armazenamento > Throughput de disco: equilíbrio de intermitência (HDD)	
Volume de armazenamento > IOPS de disco: utilização (SSD)	Aumentar a IOPS do SSD

Note

Certos eventos do sistema de arquivos podem consumir recursos de performance de E/S de disco e potencialmente acionar avisos de performance. Por exemplo: .

- A fase de otimização do dimensionamento da capacidade de armazenamento pode gerar maior throughput de disco, conforme descrito em Aumentos da capacidade de armazenamento e performance do sistema de arquivos
- Para sistemas de arquivos multi-AZ, eventos como o escalonamento da capacidade de throughput, a substituição de hardware ou a interrupção da zona de disponibilidade resultam em eventos automáticos de failover e failback. Todas as alterações de dados que ocorrerem durante esse período precisam ser sincronizadas entre os servidores de arquivos primário e secundário, e o Windows Server executa um trabalho de sincronização de dados que pode consumir recursos de E/S do disco. Para ter mais informações, consulte Como gerenciar a capacidade de throughput.

Para obter mais informações sobre a performance do sistema de arquivos, consulte Performance do FSx para Windows File Server.

Como acessar as métricas do FSx para Windows File Server

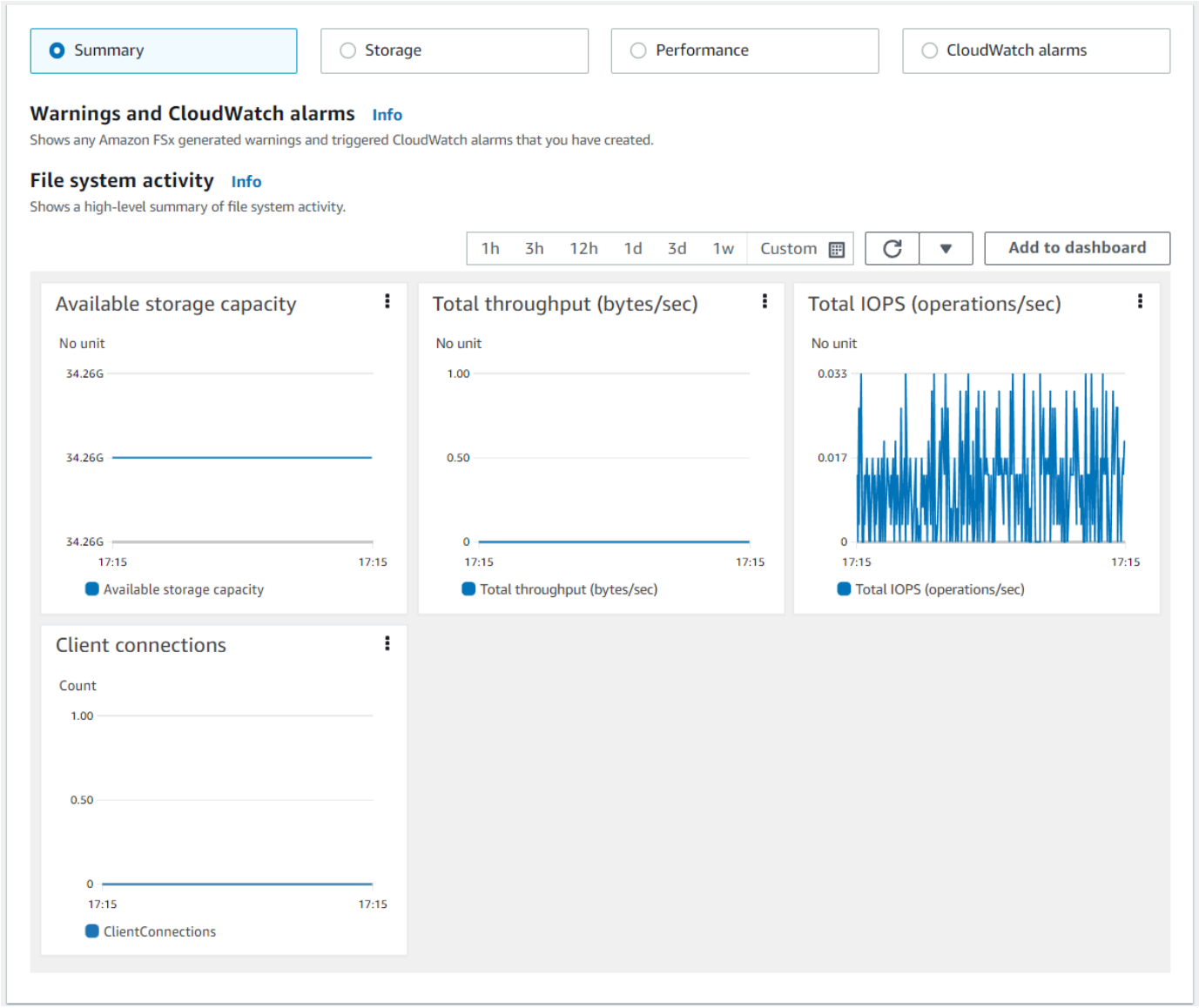
Você pode ver as métricas do Amazon FSx das seguintes formas. CloudWatch

- O console do Amazon FSx.
- O CloudWatch console.
- A CloudWatch CLI (interface de linha de comando).
- A CloudWatch API.

Os procedimentos a seguir descrevem como acessar as métricas do seu sistema de arquivos usando essas várias ferramentas.

Visualizar as métricas do sistema de arquivos usando o console do Amazon FSx

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, selecione Sistemas de arquivos no painel de navegação.
3. Escolha o sistema de arquivos cujas métricas você deseja visualizar.
4. Para exibir gráficos das métricas do sistema de arquivos, escolha Monitoramento e performance no segundo painel.

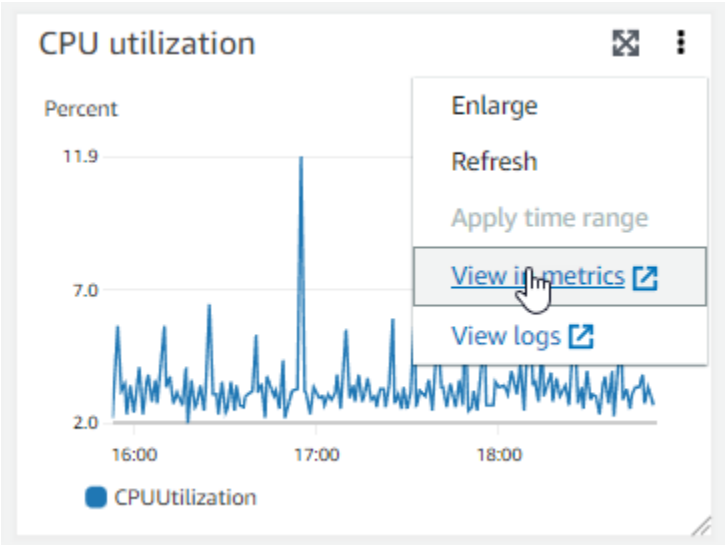


- As métricas de resumo são exibidas por padrão, mostrando todos os avisos e CloudWatch alarmes ativos junto com as métricas de atividade do sistema de arquivos.
- Escolha Armazenamento para visualizar a capacidade de armazenamento e as métricas de utilização.
- Selecione Performance para visualizar as métricas de performance do servidor de arquivos e do armazenamento.
- Escolha CloudWatch alarmes para ver gráficos de todos os alarmes configurados para o sistema de arquivos.

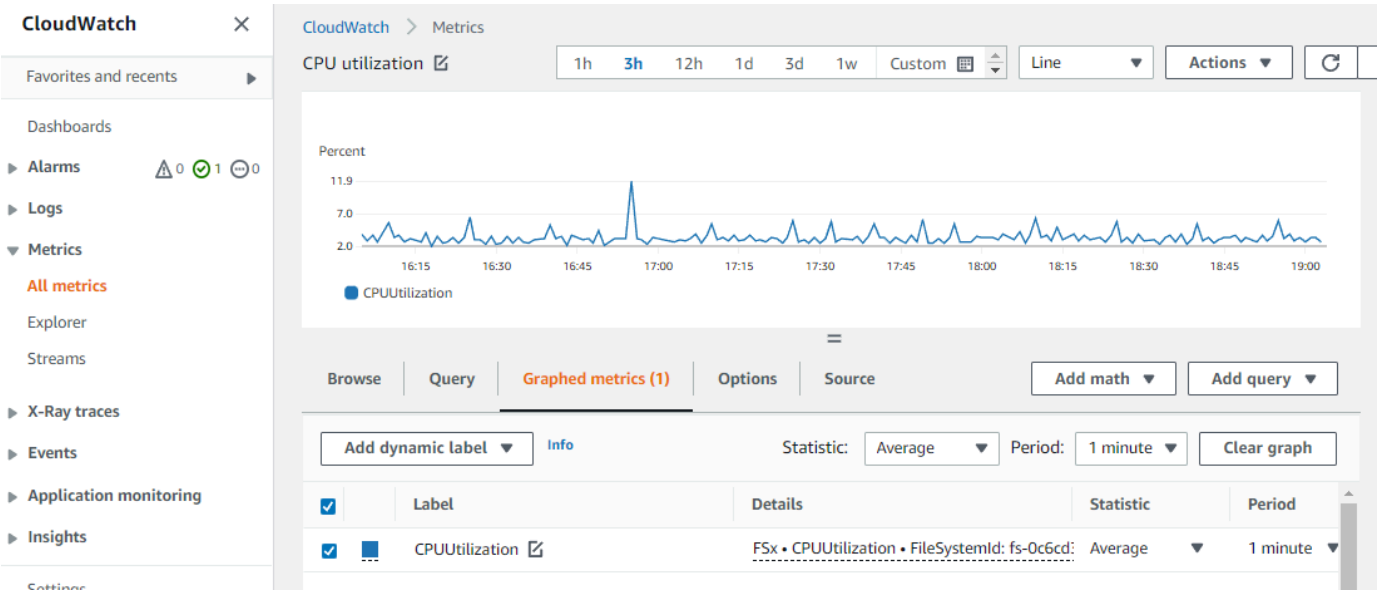
Para mais informações, consulte Como usar as métricas do FSx para Windows File Server.

Para visualizar métricas no CloudWatch console

1. Para visualizar uma métrica do sistema de arquivos na página Métricas do CloudWatch console Amazon, navegue até a métrica no painel Monitoramento e desempenho do console Amazon FSx.
2. Selecione Visualizar em métricas no menu de ações no canto superior direito do gráfico de métricas, conforme mostrado na imagem a seguir.



Isso abre a página Métricas no CloudWatch console, mostrando o gráfico métrico, conforme mostrado na imagem a seguir.



Para adicionar métricas a um CloudWatch painel

1. Para adicionar um conjunto de métricas do sistema de arquivos FSx for Windows a um painel no CloudWatch console, escolha o conjunto de métricas (resumo, armazenamento ou desempenho) no painel Monitoramento e desempenho do console Amazon FSx.
2. Escolha Adicionar ao painel no canto superior direito do painel, isso abrirá o CloudWatch console.
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.

Para acessar as métricas do AWS CLI

- Use o comando `list-metrics` com o namespace `--namespace "AWS/FSx"`. Para obter mais informações, consulte Referência de comandos da AWS CLI.

Usando a CloudWatch API

Para acessar métricas da CloudWatch API

- Chame `GetMetricStatistics`. Para obter mais informações, consulte Amazon CloudWatch API Reference.

Criação de CloudWatch alarmes para monitorar o Amazon FSx

Você pode criar um CloudWatch alarme que envia uma mensagem do Amazon SNS quando o alarme muda de estado. Um alarme observa uma única métrica ao longo de um período especificado por você e realiza uma ou mais ações com base no valor da métrica relativo a um determinado limite ao longo de vários períodos. A ação é uma notificação enviada para um tópico do Amazon SNS ou uma política de Auto Scaling.

Os alarmes invocam ações somente para mudanças de estado sustentadas. CloudWatch os alarmes não invocam ações simplesmente 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 do Amazon FSx ou no CloudWatch console.

Os procedimentos a seguir descrevem como criar alarmes para o Amazon FSx usando o console, a 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, selecione Sistemas de arquivos e, em seguida, selecione o sistema de arquivos para o qual você deseja criar o alarme.
3. Selecione o menu Ações e selecione Visualizar detalhes.
4. Na página Resumo, selecione Monitoramento e performance.
5. Escolha CloudWatch alarmes.
6. Escolha Criar CloudWatch alarme. O sistema redireciona você para o console do CloudWatch.
7. Selecione Selecionar métricas e, em seguida, Próximo.
8. Na seção Métricas, escolha FSx.
9. Selecione Métricas do sistema de arquivos, selecione a métrica para a qual deseja definir o alarme e, em seguida, escolha Selecionar métrica.
10. Na seção Condições, escolha as condições desejadas para o alarme e clique em Próximo.

> **Note**
>
> As métricas não podem ser publicadas durante a manutenção do sistema de arquivos para sistemas de arquivos single-AZ, ou durante o failover e o failback de ou para os servidores primários ou secundários para sistemas de arquivos multi-AZ. 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 uma notificação por e-mail ou SNS quando o estado do alarme acionar a ação, escolha um estado de alarme para Sempre que esse estado de alarme estiver.

    Para selecionar um tópico do SNS, escolha um tópico existente do SNS. Se você selecionar Create topic, poderá definir o nome e o endereço de e-mail para uma nova lista de assinatura de e-mail. Essa lista é salva e aparece no campo para alarmes futuros. Escolha 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 apenas quando o alarme entra em um status de alarme. Se essa alteração no status de alarme ocorrer antes dos endereços de e-mail serem verificados, eles não receberão notificação.

12. Preencha os valores Nome, Descrição e Sempre para a métrica e selecione Próximo.
13. Na página Pré-visualizar e criar, revise o alarme que você está prestes a criar e, em seguida, selecione Criar alarme.

Para definir alarmes usando o console CloudWatch

1. Faça login no AWS Management Console e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Escolha Criar alarme para iniciar o Assistente de criação de alarmes.
3. Selecione Métricas do FSx e percorra as métricas do Amazon FSx para localizar a métrica na qual você deseja colocar um alarme. Para exibir apenas as métricas do Amazon FSx nessa caixa de diálogo, pesquise o ID do sistema de arquivos do seu sistema de arquivos. Selecione a métrica para criar um alarme e selecione Próximo.
4. Preencha os valores de Name, Description e Whenever para a métrica.
5. Se você quiser CloudWatch enviar um e-mail quando o estado do alarme for atingido, em Sempre que este alarme for atingido, escolha Estado é ALARME. Em Enviar notificação para, escolha um tópico do SNS existente. Se você selecionar Create topic, poderá definir o nome e o endereço de e-mail para uma nova lista de assinatura de e-mail. Essa lista é salva e aparece no campo para alarmes futuros.

> **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 apenas quando o alarme entra em um status de alarme. Se essa alteração no status de alarme ocorrer antes dos endereços de e-mail serem verificados, eles não receberão notificação.

6. Neste ponto, a área de Visualização do alarme oferece a chance de visualizar o alarme que será criado. Escolha Create Alarm.

Para definir um alarme usando o AWS CLI

- Chame `put-metric-alarm`. Para obter mais informações, consulte Referência de comandos da AWS CLI.

Para definir um alarme usando a CloudWatch API

- Chame `PutMetricAlarm`. Para obter mais informações, consulte Amazon CloudWatch API Reference.

Registrar em log as chamadas de API do Amazon FSx para Windows File Server usando o AWS CloudTrail

O Amazon FSx para Windows File Server está integrado ao AWS CloudTrail, um serviço que fornece um registro das ações executadas por um usuário, um perfil ou um serviço da AWS no Amazon FSx. O CloudTrail captura todas as chamadas de API do Amazon FSx como eventos. As chamadas capturadas incluem as chamadas do console do Amazon FSx e as chamadas de código para as operações de 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). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita ao Amazon FSx, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e outros detalhes.

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 no Amazon FSx, esta atividade 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 de eventos em andamento na sua 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 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:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as ações do Amazon FSx são registradas em log pelo CloudTrail e documentadas na Amazon FSx API Reference. Por exemplo, as chamadas para as ações `CreateFileSystem`, `CreateBackup` 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 Elemento userIdentity do 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 fonte 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"
}
```

Performance do FSx para Windows File Server

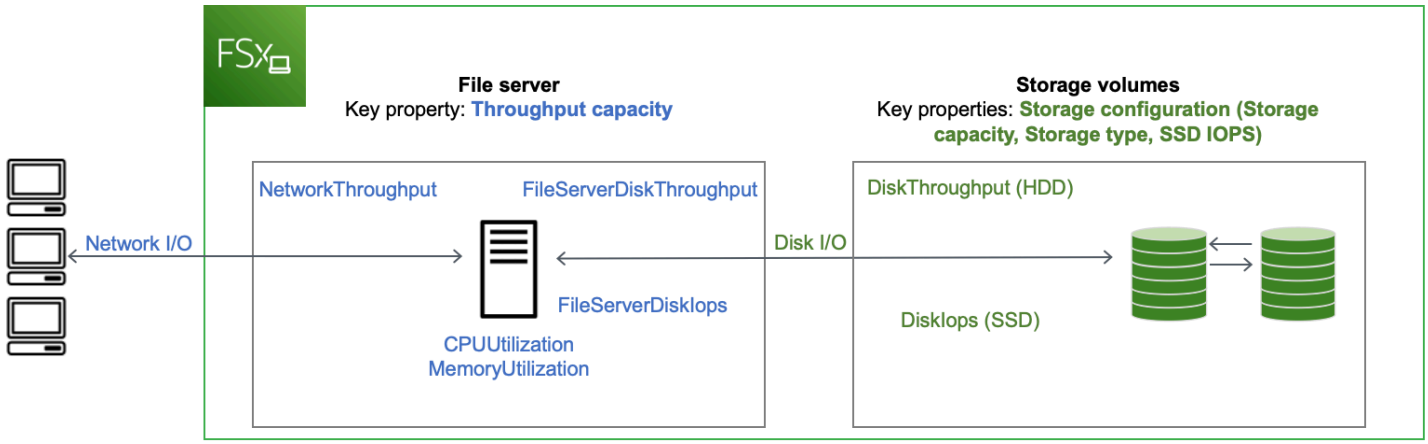
O FSx para Windows File Server oferece opções de configuração do sistema de arquivos para atender a uma variedade de necessidades de performance. Veja a seguir uma visão geral da performance do sistema de arquivos do Amazon FSx, com uma discussão sobre as opções de configuração de performance disponíveis e dicas úteis de performance.

Tópicos

Performance do sistema de arquivos

Cada sistema de arquivos do FSx para Windows File Server consiste em um servidor de arquivos do Windows com o qual os clientes se comunicam e um conjunto de volumes de armazenamento, ou discos, conectados ao servidor de arquivos. Cada servidor de arquivos emprega um cache na memória rápido para aprimorar a performance dos dados acessados com mais frequência.

O diagrama a seguir ilustra como os dados são acessados em um sistema de arquivos do FSx para Windows File Server.



Quando um cliente acessa dados armazenados no cache na memória, os dados são enviados diretamente ao cliente solicitante como E/S de rede. O servidor de arquivos não precisa lê-lo ou gravá-lo no disco. A performance desse acesso aos dados é determinada pelos limites de E/S da rede e pelo tamanho do cache na memória.

Quando um cliente acessa dados que não estão em cache, o servidor de arquivos os lê ou grava no disco como E/S de disco. Os dados são então atendidos no servidor de arquivos para o cliente como E/S de rede. A performance desse acesso aos dados é determinada pelos limites de E/S da rede, bem como pelos limites de E/S do disco.

A performance de E/S da rede e o cache na memória do servidor de arquivos são determinados pela capacidade de throughput do sistema de arquivos. A performance E/S de disco é determinada por uma combinação de capacidade de throughput e configuração de armazenamento. A performance máxima de E/S de disco, que consiste em níveis em throughput e IOPS de disco, que seu sistema de arquivos pode alcançar é o menor dos seguintes:

- O nível de performance de E/S de disco fornecido pelo servidor de arquivos, com base na capacidade de throughput selecionada para o sistema de arquivos.
- O nível de performance de E/S de disco fornecido pela sua configuração de armazenamento (a capacidade de armazenamento, o tipo de armazenamento e o nível de IOPS de SSD que você seleciona para seu sistema de arquivos).

Considerações adicionais sobre performance

Normalmente, a performance do sistema de arquivos é medida por sua latência, throughput e operações de E/S por segundo (IOPS).

Latência

Os servidores de arquivos do FSx para Windows File Server usam um cache rápido na memória para obter latências consistentes de menos de um milissegundo para dados acessados ativamente. Para dados que não estão no cache na memória, ou seja, para operações de arquivos que precisam ser atendidas executando E/S nos volumes de armazenamento subjacentes, o Amazon FSx fornece latências de operação de arquivos abaixo de um milissegundo com armazenamento em unidade de estado sólido (SSD) e latências de um dígito em milissegundos com armazenamento em disco rígido (HDD).

Throughput e IOPS

Os sistemas de arquivos Amazon FSx fornecem até 2 Gb/s e 80.000 IOPS em todos os lugares onde o Regiões da AWS Amazon FSx está disponível, além de 12 Gb/s de taxa de transferência e 400.000 IOPS no Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Leste dos EUA (Ohio), Europa (Irlanda), Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Cingapura). A quantidade específica de throughput e IOPS que sua workload pode gerar em seu sistema de arquivos depende da capacidade de throughput, capacidade de armazenamento e tipo de armazenamento de seu sistema de arquivos, juntamente com a natureza de sua workload, incluindo o tamanho do conjunto de trabalho ativo.

Performance de um único cliente

Com o Amazon FSx, você pode obter até os níveis completos de throughput e IOPS do seu sistema de arquivos de um único cliente acessando-o. O Amazon FSx é compatível com SMB multicanal. Esse recurso permite que ele forneça um throughput de até vários GB/s e centenas de milhares de IOPS para um único cliente acessando seu sistema de arquivos. 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. Embora haja um limite teórico para o número de conexões SMB suportadas pelo Windows, esse limite está na casa dos milhões e, praticamente, você pode ter um número ilimitado de conexões SMB.

Performance de expansão

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 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.

Impacto da capacidade de throughput na performance

A capacidade de throughput determina a performance do sistema de arquivos nas seguintes categorias:

- E/S de rede: a velocidade com que o servidor de arquivos pode fornecer dados de arquivos aos clientes que os acessam.
- CPU e memória do servidor de arquivos: recursos que estão disponíveis para servir dados de arquivos e realizar atividades em segundo plano, como eliminação de duplicação de dados e cópias paralelas.
- E/S de disco: a velocidade na qual o servidor de arquivos pode suportar E/S entre o servidor de arquivos e os volumes de armazenamento.

As tabelas a seguir fornecem detalhes sobre os níveis máximos de E/S de rede (throughput e IOPS) e E/S de disco (throughput e IOPS) que você pode conduzir com cada configuração de capacidade de throughput provisionada e a quantidade de memória disponível para armazenamento em cache e suporte a atividades em segundo plano, como eliminação de duplicação de dados e cópias paralelas. Embora você possa selecionar níveis de capacidade de transferência abaixo de 32 megabytes por segundo (MBps) ao usar a API ou a CLI do Amazon FSx, lembre-se de que esses níveis se destinam a cargas de trabalho de teste e desenvolvimento, não a cargas de trabalho de produção.

> **Note**
>
> Observe que níveis de capacidade de throughput de 4.608 MBps ou mais são compatíveis apenas nas regiões a seguir: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Leste dos EUA (Ohio), Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Singapura).

Memória e E/S de rede

Capacidade de taxa de transferência do FSx (megabytes por segundo)	Taxa de transferência da rede (megabytes por segundo)		IOPS de rede	Memória (GB)
	Linha de base	Expansão (por alguns minutos por dia)		
32	32	600	Milhares	4
64	64	600	Dezenas de milhares	8
128	150	1.250		8
256	300	1.250	Centenas de milhares	16
512	600	1.250		32
1,024	1.500	–		72
2.048	3.125	–		144
4.608	9.375	–	Milhões	192
6,144	12.500	–		256
9,216	18.750	–		384
12,288	21.250	–		512

E/S de disco

Capacidade de taxa de transferência do FSx (megabytes por segundo)	Taxa de transferência de disco (megabytes por segundo)		IOPS de disco	
	Linha de base	Expansão (por 30 minutos por dia)	Linha de base	Expansão (por 30 minutos por dia)
32	32	260	2K	12K
64	64	350	4K	16K
128	128	600	6K	20K
256	256	600	10 mil	20K
512	512	–	20K	–
1,024	1,024	–	40K	–
2.048	2.048	–	80K	–
4.608	4.608	–	150K	–
6,144	6,144	–	200 mil	–
9,216	9.216 [1]	–	300K [1]	–
12,288	12.288 [1]	–	400K [1]	–

Note

[1] Se você tiver um sistema de arquivos Multi-AZ com uma capacidade de taxa de transferência de 9.216 ou 12.288 MBps, o desempenho será limitado a 9.000 MBps e 262.500 IOPS somente para tráfego de gravação. Caso contrário, para tráfego de leitura em todos os sistemas de arquivos multi-AZ, tráfego de leitura e gravação em todos os sistemas

de arquivos single-AZ e todos os outros níveis de capacidade de throughput, seu sistema de arquivos terá suporte para os limites de performance mostrados na tabela.

Escolher o nível certo de capacidade de throughput

Quando você cria um sistema de arquivos usando o Amazon Web Services Management Console, o Amazon FSx seleciona automaticamente o nível de capacidade de throughput recomendado para seu sistema de arquivos com base na quantidade de capacidade de armazenamento que você configura. Embora a capacidade de throughput recomendada deva ser suficiente para a maioria das workloads, você tem a opção de ignorar a recomendação e selecionar uma quantidade específica de capacidade de throughput para atender às necessidades da sua aplicação. Por exemplo, se sua workload exigir o direcionamento de 1 GBps de tráfego para seu sistema de arquivos, você deve selecionar uma capacidade de throughput de pelo menos 1.024 MBps.

Você também deve considerar os recursos que planeja habilitar em seu sistema de arquivos ao decidir o nível de throughput a ser configurado. Por exemplo, habilitar Cópias de sombra pode exigir que você aumente sua capacidade de throughput para um nível de até três vezes a workload esperada para garantir que o servidor de arquivos possa manter as cópias de sombra com a capacidade de performance de E/S disponível. Se estiver habilitando a eliminação de duplicação de dados, você deverá determinar a quantidade de memória associada à capacidade de throughput do sistema de arquivos e garantir que essa quantidade de memória seja suficiente para o tamanho dos seus dados.

Você pode ajustar a quantidade de capacidade de throughput para cima ou para baixo a qualquer momento depois de criá-la. Para ter mais informações, consulte Como gerenciar a capacidade de throughput.

Você pode monitorar a utilização da workload dos recursos de performance do servidor de arquivos e obter recomendações sobre qual capacidade de throughput selecionar visualizando a guia Monitoramento e performance > Performance do console do Amazon FSx. Recomendamos testar em um ambiente de pré-produção para garantir que a configuração selecionada atenda aos requisitos de performance da workload. Para sistemas de arquivos multi-AZ, também recomendamos testar o impacto do processo de failover que ocorre durante a manutenção do sistema de arquivos, as alterações na capacidade de throughput e a interrupção não planejada do serviço em sua workload, além de garantir que você tenha provisionado capacidade de throughput suficiente para evitar impacto na performance durante esses eventos. Para ter mais informações, consulte Como acessar as métricas do FSx para Windows File Server.

Impacto da configuração de armazenamento na performance

A capacidade de armazenamento, o tipo de armazenamento e o nível de IOPS de SSD do seu sistema de arquivos afetam a performance de E/S de disco do seu sistema de arquivos. Você pode configurar esses recursos para fornecer os níveis de performance desejados para sua workload.

Você pode aumentar a capacidade de armazenamento e escalar IOPS de SSD a qualquer momento. Para obter mais informações, consulte Como gerenciar a capacidade de armazenamento e Como gerenciar IOPS de SSD. Você também pode atualizar seu sistema de arquivos do tipo de armazenamento HDD para o tipo de armazenamento SSD. Para ter mais informações, consulte Como gerenciar o tipo de armazenamento.

Seu sistema de arquivos fornece os seguintes níveis padrão de throughput de disco e IOPS:

Tipo de armazenamento	Taxa de transferência de disco (MBps por TiB de armazenamento)	IOPS de disco (IOPS por TiB de armazenamento)
SSD	750	3 mil*
HDD	Linha de base de 12; expansão de 80 (até um máximo de 1 GB/s por sistema de arquivos)	Linha de base de 12; expansão de 80

> **Note**
>
> *Para sistemas de arquivos com tipo de armazenamento SSD, você pode provisionar IOPS adicionais até uma taxa máxima de 500 IOPS por GiB de armazenamento e 400.000 IOPS por sistema de arquivos.

Performance de expansão do HDD

Para volumes de armazenamento HDD, o Amazon FSx usa um modelo de bucket de expansão para performance. O tamanho do volume determina a throughput da linha de base do seu volume, que é a taxa na qual o volume acumula créditos de throughput. O tamanho do volume também determina

a throughput de expansão do seu volume, que é a taxa em que é possível gastar créditos quando estiverem disponíveis. Os volumes maiores têm throughput basal e de expansão mais altos. Quanto mais créditos seu volume tiver, ele será capaz de acionar E/S da unidade em nível de expansão por mais tempo.

O throughput disponível de um volume de armazenamento HDD é expresso pela seguinte fórmula:

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

Para um volume de HDD de 1 TiB, o throughput de expansão está limitado a 80 MiB/s, o bucket é preenchido com créditos a 12 MiB/s e pode suportar até 1 TiB equivalente em créditos.

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 configurado com 2 TiB de capacidade de armazenamento em HDD e 32 MBps de capacidade de throughput tem os seguintes níveis de throughput:

- Throughput da rede: linha de base de 32 MBps e expansão de 600 MBps (consulte a tabela de capacidade de throughput)
- Throughput de disco: 24 MBps de linha de base e expansão de 160 MBps, que é a menor de:
  - os níveis de throughput de disco de 32 MBps (linha de base) e 260 MBps (expansão) compatíveis com o servidor de arquivos, com base na capacidade de throughput do sistema de arquivos
  - os níveis de throughput de disco da linha de base de 24 MBps (12 MBps por TB * 2 TiB) e de intermitência de 160 MBps (80 MBps por TiB * 2 TiB) compatíveis com os volumes de armazenamento, com base no tipo e na capacidade de armazenamento

Portanto, sua workload que acessa o sistema de arquivos será capaz de gerar até 32 MBps de linha de base e 600 MBps de throughtput de expansão para operações de arquivo executadas em dados acessados ativamente armazenados em cache no cache na memória do servidor de arquivos, e até 24 MBps de linha de base e 160 MBps de throughput de expansão para operações de arquivo que precisam ir até o disco, por exemplo, devido a falhas de cache.

Medindo o desempenho usando CloudWatch métricas

Você pode usar CloudWatch a Amazon para medir e monitorar a taxa de transferência e o IOPS do seu sistema de arquivos. Para ter mais informações, consulte Monitoramento de métricas com a Amazon CloudWatch.

Solução de problemas de performance

Para obter ajuda na solução de problemas comuns de performance, consulte Solução de problemas de performance do sistema de arquivos.

Instruções de uso do Amazon FSx

A seguir, você encontrará uma série de instruções orientadas por tarefas que servirão de guia em vários processos.

Tópicos

Passo a passo 1: pré-requisitos para começar

Antes de concluir o exercício de primeiros passos, você já deve ter uma instância do Amazon EC2 baseada no Microsoft Windows associada ao seu diretório do AWS Directory Service. Você também deve se conectar à instância por meio do protocolo de área de trabalho remota do Windows como o usuário administrador do seu diretório. O passo a passo a seguir mostra como executar essas ações de pré-requisito necessárias.

Tópicos

Etapa 1: configurar o Active Directory

Com o Amazon FSx, você pode operar o armazenamento de arquivos totalmente gerenciado para workloads baseadas no Windows. Da mesma forma, o AWS Directory Service fornece diretórios totalmente gerenciados para uso na implantação de sua workload. Se você tiver um domínio

corporativo do AD em execução na AWS em uma nuvem privada virtual (VPC) usando instâncias do EC2, você poderá ativar a autenticação baseada em usuário e o controle de acesso. Isso é feito estabelecendo uma relação de confiança entre o AWS Managed Microsoft AD e o domínio corporativo. Para a autenticação do Windows no Amazon FSx, você só precisa de uma relação de confiança de floresta unidirecional, na qual a floresta gerenciada da AWS confia na floresta de domínio corporativo.

Seu domínio corporativo assume o papel de domínio confiável, e o domínio gerenciado pelo AWS Directory Service assume o papel de domínio confiável. As solicitações de autenticação validadas percorrem os domínios em apenas uma direção, permitindo que as contas em seu domínio corporativo se autentiquem em relação aos recursos compartilhados no domínio gerenciado. Nesse caso, o Amazon FSx interage somente com o domínio gerenciado. O domínio gerenciado então passa as solicitações de autenticação para seu domínio corporativo.

> **Note**
>
> Você também pode usar um tipo de confiança externa com o Amazon FSx para domínios confiáveis.

Seu grupo de segurança do Active Directory deve permitir o acesso de entrada do grupo de segurança do sistema de arquivos do Amazon FSx.

Criar um AWS Directory Services para o Microsoft AD

- Se você ainda não tiver um, use o AWS Directory Service para criar seu diretório do AWS Managed Microsoft AD. Para obter mais informações, consulte Criar seu diretório do AWS Managed Microsoft AD no Guia de administração do AWS Directory Service.

  > **Important**
  >
  > Lembre-se da senha que você atribuiu ao seu usuário Admin. Você precisará dela mais tarde neste exercício de primeiros passos. Se você esquecer a senha, será preciso repetir as etapas deste exercício com o novo diretório do AWS Directory Service e o usuário Admin.

- Se você tiver um AD existente, crie uma relação de confiança entre seu AWS Managed Microsoft AD e seu AD existente. Para obter mais informações, consulte Quando criar uma relação de confiança no Guia de administração do AWS Directory Service.

Etapa 2: executar uma instância do Windows no console do Amazon EC2

Você pode iniciar uma instância do Windows usando o AWS Management Console, conforme descrito no procedimento a seguir. O objetivo é ajudar você a executar sua primeira instância rapidamente, portanto, ele não abrange todas as opções possíveis. Para obter mais informações sobre as opções avançadas, consulte Execução de uma instância.

Como iniciar uma instância

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel do console, selecione Launch Instance.
3. Na página Choose an Amazon Machine Image (AMI), há uma lista de configurações básicas, chamadas Amazon Machine Images (AMIs), que funcionam como modelos para sua instância. Selecione a AMI para Windows Server 2016 Base ou Windows Server 2012 R2 Base. Observe que essas AMIs estão marcadas como "Elegíveis para nível gratuito".
4. Na página Choose an Instance Type, é possível selecionar a configuração de hardware de sua instância. Selecione o tipo `t2.micro`, que é selecionado por padrão. Observe que este tipo de instância está qualificado para o nível gratuito.
5. Escolha Review and Launch para permitir que o assistente conclua outras definições de configuração para você.
6. Na página Revisar inicialização da instância, em Grupos de segurança, será exibido um grupo de segurança que o assistente criou e selecionou para você. Você pode usar esse grupo de segurança ou pode escolher o grupo de segurança que criou ao fazer a configuração usando as etapas a seguir.

   a. Escolha Edit security groups (Editar grupos de segurança).

   b. Na página Configure Security Group (Configurar grupo de segurança), garanta que Select an existing security group (Selecionar um grupo de segurança existente) esteja selecionado.

   c. Selecione o grupo de segurança na lista de grupos de segurança existentes e escolha Review and Launch (Revisar e iniciar).
7. Na página Review Instance Launch, escolha Launch.
8. Se um par de chaves for solicitado, selecione Choose an existing key pair e selecione o par de chaves que você criou ao obter a configuração.

   Como alternativa, você pode criar um novo par de chaves. Selecione Create a new key pair, insira um nome para o par de chaves e, em seguida, escolha Download Key Pair. Esta é a única

chance de você salvar o arquivo de chave privada, logo, não deixe de fazer download dele. Salve o arquivo de chave privada em um lugar seguro. Você precisará fornecer o nome do par de chaves ao iniciar uma instância e a chave privada correspondente sempre que se conectar à instância.

> **Warning**
>
> Não selecione a opção Proceed without a key pair. Se você executar sua instância sem um par de chaves, você não poderá conectá-la.

Quando estiver pronto, selecione a caixa de confirmação e, então, escolha Launch Instances.

9. Uma página de confirmação informa que sua instância está sendo executada. Selecione Visualizar instâncias para fechar a página de confirmação e voltar ao console.
10. Na tela Instances, é possível visualizar o status da execução. Demora um pouco para executar uma instância. Ao executar uma instância, seu estado inicial é `pending`. Após a inicialização da instância, seu estado muda para `running` e ela recebe um nome DNS público. (Se a coluna Public DNS (IPv4) estiver oculta, escolha Mostrar/ocultar colunas (o ícone de engrenagem) no canto superior direito da página e selecione Public DNS (IPv4).)
11. Pode levar alguns minutos até que a instância esteja pronta para que você possa se conectar a ela. Certifique-se de que sua instância tenha sido aprovada nas verificações de status. É possível visualizar essas informações na coluna Status Checks.

> **Important**
>
> Anote a ID do grupo de segurança que foi criado quando você executou essa instância. Você precisará dela quando criar seu sistema de arquivos do Amazon FSx.

Agora que sua instância foi iniciada, você pode se conectar a ela.

Etapa 3: conectar-se à sua instância

Para se conectar a uma instância Windows, você deve recuperar a senha do administrador e especificar essa senha ao se conectar à sua instância usando a Área de Trabalho Remota.

O nome da conta de administrador depende do idioma do sistema operacional. Por exemplo, em inglês é Administrator, em francês é Administrateur e em português é Administrador. Para obter mais informações, consulte Localized Names for Administrator Account in Windows (Nomes localizados da conta de administrador no Windows) no Microsoft TechNet Wiki.

Se você associou sua instância a um domínio, você pode se conectar a ela usando as credenciais de domínio definidas no AWS Directory Service. Na tela de login da Área de trabalho remota, não use o nome do computador local e a senha gerada. Em vez disso, use o nome de usuário totalmente qualificado para o administrador e a senha para essa conta. Um exemplo é **`corp.example.com\Admin`**.

A licença do sistema operacional (SO) Windows Server permite duas conexões remotas simultâneas para fins administrativos. A licença para Windows Server está incluída no preço da sua instância do Windows. Se você precisar de mais de duas conexões remotas simultâneas, deverá adquirir uma licença do Remote Desktop Services (RDS). Se você tentar uma terceira conexão, ocorrerá um erro. Para obter mais informações, consulte Configurar o número de conexões remotas simultâneas permitidas para uma conexão.

Para se conectar à sua instância do Windows usando um cliente RDP

1. No console do Amazon EC2, selecione a instância e, em seguida, escolha Connect (Conectar-se).
2. Na caixa de diálogo Conectar à sua instância, selecione Obter senha (leva alguns minutos após a inicialização da instância até que a senha esteja disponível).
3. Escolha Browse e navegue até o arquivo de chave privada que você criou quando lançou a instância. Selecione o arquivo e escolha Open para copiar todo o conteúdo do arquivo para o campo Contents.
4. Escolha Decrypt Password. O console exibe a senha padrão de administrador da instância na caixa de diálogo Conectar à sua instância, substituindo o link para Obter senha mostrado anteriormente pela senha real.
5. Registre a senha de administrador padrão ou copie-para a área de transferência. Você precisará dessa senha para se conectar à instância.
6. Escolha Download Remote Desktop File. O navegador pergunta se você quer abrir ou salvar o arquivo .rdp. Qualquer uma das opções é aceitável. Quando tiver terminado, você pode selecionar Fechar para descartar a caixa de diálogo Conectar à sua instância.

    - Se tiver aberto o arquivo .rdp, você verá a caixa de diálogo Remote Desktop Connection.

- Se você tiver salvado o arquivo .rdp, navegue até o diretório de downloads e abra o arquivo .rdp para exibir a caixa de diálogo.

7. Talvez você receba um aviso de que o publicador da conexão remota é desconhecido. É possível continuar se conectando à instância.
8. Quando solicitado, faça login na instância usando a conta do administrador do sistema operacional e a senha registrada ou copiada por você anteriormente. Caso sua Remote Desktop Connection (Conexão de Desktop Remoto) já tenha uma conta de administrador configurada, talvez seja necessário escolher a opção Use another account (Usar outra conta) e digitar o nome de usuário e senha manualmente.

   > **Note**
   >
   > Às vezes, quando se copia e cola conteúdo, os dados podem ser corrompidos. Se você encontrar o erro "Password Failed" ao fazer login, experimente digitar a senha manualmente.

9. Devido à natureza dos certificados autoassinados, talvez você receba um aviso indicando que o certificado de segurança não pôde ser autenticado. Use as seguintes etapas para confirmar a identidade do computador remoto ou apenas escolha Yes ou Continue para continuar, caso confie no certificado.

   a. Se estiver usando a Conexão de Desktop Remoto em um PC Windows, escolha View certificate. Se estiver usando o Microsoft Remote Desktop em um Mac, escolha Show Certificate.

   b. Escolha a guia Details (Detalhes) e role a tela para baixo até a entrada Thumbprint (Impressão digital) em um PC com o Windows ou a entrada SHA1 Fingerprints (Impressões digitais com SHA1) em um Mac. Esse é o identificador exclusivo do certificado de segurança do computador remoto.

   c. No console do Amazon EC2, selecione a instância, escolha Actions (Ações) e, em seguida, escolha Get System Log (Obter log do sistema).

   d. Na saída do log do sistema, procure uma entrada rotulada `RDPCERTIFICATE-THUMBPRINT`. Se esse valor corresponder à impressão digital do certificado, você terá verificado a identidade do computador remoto.

   e. Se estiver usando a Conexão de Desktop Remoto em um PC Windows, volte à caixa de diálogo Certificate e escolha OK. Se estiver usando o Microsoft Remote Desktop em um Mac, volte para Verify Certificate e escolha Continue.

f. [Windows] Escolha Yes (Sim) na janela Remote Desktop Connection (Conexão de Desktop Remoto) para se conectar à instância.

Agora que você estabeleceu conexão com a instância, é possível associá-la ao seu diretório do AWS Directory Service.

Etapa 4: associar sua instância ao seu diretório do AWS Directory Service

O procedimento a seguir mostra como associar manualmente uma instância existente do Amazon EC2 do Windows ao seu diretório do AWS Directory Service.

Associar uma instância do Windows ao seu diretório do AWS Directory Service

1. Conecte-se à instância usando qualquer cliente Remote Desktop Protocol.
2. Abra a caixa de diálogo de propriedades TCP/IPv4 na instância.

   a. Abra Conexões de rede.

   > **Tip**
   >
   > Você pode abrir Conexões de rede de maneira direta executando o seguinte comando a partir de um prompt de comando na instância.
   >
   > ```
   > %SystemRoot%\system32\control.exe ncpa.cpl
   > ```

   b. Abra o menu de contexto (clique com o botão direito do mouse) para qualquer conexão de rede habilitada e escolha Propriedades.

   c. Na caixa de diálogo de propriedades da conexão, abra (clique duas vezes) Protocolo de Internet versão 4.
3. (Opcional) Selecione Usar os seguintes endereços de servidor DNS, altere os endereços do Servidor DNS preferencial e do Servidor DNS alternativo para os endereços IP dos servidores DNS fornecidos pelo AWS Directory Service e selecione OK.
4. Abra a caixa de diálogo Propriedades do sistema da instância, selecione a guia Nome do computador e selecione Alterar.

> **Tip**
>
> Você pode abrir a caixa de diálogo Propriedades do sistema de maneira direta executando o seguinte comando a partir de um prompt de comando na instância.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. Na caixa Membro de, selecione Domínio, insira o nome totalmente qualificado de seu diretório do AWS Directory Service e selecione OK.
6. Quando forem solicitados o nome e a senha do administrador do domínio, insira o nome de usuário e a senha da conta Admin.

> **Note**
>
> Você pode inserir o nome totalmente qualificado do seu domínio ou o nome NetBios, seguido de uma barra invertida (\) e, em seguida, o nome do usuário, neste caso, Admin. Por exemplo, corp.example.com\Admin ou corp\Admin.

7. Depois que você receber a mensagem de boas-vindas ao domínio, reinicie a instância para que as alterações entrem em vigor.
8. Reconecte-se à sua instância via RDP e faça login na instância usando o nome de usuário e a senha do usuário Admin do seu diretório do AWS Directory Service.

Agora que sua instância foi associada ao domínio, você pode criar seu sistema de arquivos do Amazon FSx. Em seguida, você pode concluir as outras tarefas do exercício de primeiros passos. Para obter mais informações, consulte Introdução ao Amazon FSx para Windows File Server.

Passo a passo 2: criar um sistema de arquivos de um backup

Com o Amazon FSx, você pode criar um sistema de arquivos de um backup. Ao fazer isso, você pode alterar qualquer um dos seguintes elementos para se adequar melhor ao caso de uso que você tem para o sistema de arquivos recém-criado:

- Tipo de armazenamento
- Capacidade de throughput

- VPC
- zona de disponibilidade
- Sub-rede
- Grupos de segurança da VPC
- Configuração do Active Directory
- Chave de criptografia do AWS KMS
- Hora de início do backup automático diário
- Janela de manutenção semanal

O procedimento a seguir orienta você no processo de criação de um novo sistema de arquivos de um backup. Antes de criar esse sistema de arquivos, você deve ter um backup existente. Para obter mais informações, consulte Trabalhar com backups.

Criar um sistema de arquivos a partir de um backup existente

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Na lista de navegação à direita, selecione Backups.
3. Na tabela do painel, escolha o backup que você deseja usar para criar um novo sistema de arquivos.

   > **Note**
   >
   > Você só pode restaurar seu backup em um sistema de arquivos com a mesma capacidade de armazenamento do original. Você poderá aumentar a capacidade de armazenamento do sistema de arquivos restaurado depois que ele estiver disponível. Para obter mais informações, consulte Como gerenciar a capacidade de armazenamento.

4. Escolha Restore backup (Restaurar backup). Esse procedimento iniciará o assistente de criação de sistema de arquivos.
5. Escolha as configurações que você gostaria de alterar para esse novo sistema de arquivos. O tipo de armazenamento é definido como SSD por padrão, mas você pode alterá-lo para HDD nas seguintes condições:

   - O tipo de implantação do sistema de arquivos é multi-AZ ou single-AZ 2.

- A capacidade de armazenamento é de pelo menos 2 mil GiB.

6. Selecione Revisar resumo para revisar suas configurações antes de criar o sistema de arquivos.
7. Escolha Create file system (Criar sistema de arquivos).

Agora você criou com sucesso o novo sistema de arquivos de um backup existente.

Passo a passo 3: atualizar um sistema de arquivos existente

Há três elementos que você pode atualizar com os procedimentos deste passo a passo. Todos os outros elementos do seu sistema de arquivos que podem ser atualizados podem ser feitos no console. Esses procedimentos pressupõem que você tenha instalado e configurado a AWS CLI em seu computador local. Para obter mais informações, consulte Instalar e Configurar no Guia do usuário da AWS Command Line Interface.

- AutomaticBackupRetentionDays: o número de dias que você deseja reter os backups automáticos do seu sistema de arquivos.
- DailyAutomaticBackupStartTime: 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.
- WeeklyMaintenanceStartTime: a hora da semana em que você deseja que a janela de manutenção comece. 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.

Os procedimentos a seguir descrevem como atualizar seu sistema de arquivos com a AWS CLI.

Atualizar por quanto tempo os backups automáticos são retidos em seu sistema de arquivos

1. Abra um prompt de comando ou terminal em seu computador.
2. Execute o comando a seguir, substituindo o ID do sistema de arquivos pelo ID do seu sistema de arquivos e o número de dias pelo qual você deseja reter os backups automáticos.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration AutomaticBackupRetentionDays=30
```

Atualizar a janela de backup diário de seu sistema de arquivos

1. Abra um prompt de comando ou terminal em seu computador.
2. Execute o comando a seguir, substituindo o ID do sistema de arquivos pelo ID do seu sistema de arquivos e a hora pela hora em que você deseja iniciar a janela.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration DailyAutomaticBackupStartTime=01:00
```

Atualizar a janela de manutenção semanal do seu sistema de arquivos

1. Abra um prompt de comando ou terminal em seu computador.
2. Execute o comando a seguir, substituindo o ID do sistema de arquivos pelo ID do seu sistema de arquivos e a data e o horário em que você deseja iniciar a janela.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

Passo a passo 4: usar o Amazon FSx com o Amazon AppStream 2.0

Ao ser compatível com o protocolo Server Message Block (SMB), o Amazon FSx para Windows File Server é compatível com o acesso ao seu sistema de arquivos nas instâncias do Amazon EC2, VMware Cloud na AWS, Amazon WorkSpaces e Amazon AppStream 2.0. O AppStream 2.0 é um serviço de streaming de aplicações totalmente gerenciado. Você gerencia centralmente suas aplicações de desktop no AppStream 2.0 e as fornece com segurança a um navegador em qualquer computador. Para obter mais informações sobre o AppStream 2.0, consulte o Guia de administração do Amazon AppStream 2.0. Para obter instruções sobre como simplificar o gerenciamento de suas imagens e frotas do Amazon AppStream 2.0, consulte a postagem do blog da AWS Automatically create customized AppStream 2.0 Windows images.

Use este passo a passo como um guia sobre como usar o Amazon FSx com o AppStream 2.0 para dois casos de uso: fornecer armazenamento pessoal persistente para cada usuário e fornecer uma pasta compartilhada entre usuários para acessar arquivos comuns.

Como fornecer armazenamento pessoal persistente para cada usuário

Você pode usar o Amazon FSx para fornecer a cada usuário da sua organização uma unidade de armazenamento exclusiva nas sessões de streaming do AppStream 2.0. Um usuário terá permissões para acessar apenas sua pasta. A unidade é montada automaticamente no início de uma sessão de streaming e os arquivos adicionados ou atualizados na unidade são mantidos automaticamente entre as sessões de streaming.

Há três procedimentos que você precisará executar para concluir essa tarefa.

Criar pastas pessoais para usuários do domínio usando o Amazon FSx

1. Crie um sistema de arquivos do Amazon FSx. Para obter mais informações, consulte Introdução ao Amazon FSx para Windows File Server.
2. Depois que o sistema de arquivos estiver disponível, crie uma pasta para cada usuário do domínio do AppStream 2.0 no sistema de arquivos do Amazon FSx. O exemplo a seguir usa o nome de usuário do domínio do usuário como o nome da pasta correspondente. Isso significa que você pode criar o nome UNC do compartilhamento de arquivos para mapear facilmente usando a variável de ambiente `%username%` do Windows.
3. Compartilhe cada uma dessas pastas como uma pasta compartilhada. Para obter mais informações, consulte Gerenciando compartilhamentos de arquivos em sistemas de arquivos FSx for Windows File Server.

Iniciar um construtor de imagens do AppStream 2.0 associado a um domínio

1. Faça login no console do AppStream 2.0: https://console.aws.amazon.com/appstream2
2. Selecione Configurações do diretório no menu de navegação e crie um objeto de Configuração do diretório. Para obter mais informações, consulte Using Active Directory with AppStream 2.0 no Guia de administração do Amazon AppStream 2.0.
3. Selecione Imagens, Construtor de imagens e inicie um novo construtor de imagens.
4. Escolha o objeto de configuração do diretório criado anteriormente no assistente de inicialização do construtor de imagens para associar o construtor de imagens ao seu domínio do Active Directory.
5. Inicie o construtor de imagens na mesma VPC do seu sistema de arquivos do Amazon FSx. Certifique-se de associar o construtor de imagens ao mesmo diretório do AWS Managed Microsoft AD ao qual o sistema de arquivos do Amazon FSx está associado. Os grupos de

segurança da VPC que você associa ao construtor de imagens devem permitir o acesso ao sistema de arquivos do Amazon FSx.

6. Quando o construtor de imagens estiver disponível, conecte-se ao construtor de imagens e faça login usando sua conta de administrador do domínio.
7. Instale suas aplicações.

Associar os compartilhamentos de arquivos do Amazon FSx ao AppStream 2.0

1. No construtor de imagens, crie um script em lote com o seguinte comando e armazene-o em um local de arquivo conhecido (por exemplo: C:\Scripts\map-fs.bat). O exemplo a seguir usa S: como a letra de drive para mapear a pasta compartilhada em seu sistema de arquivos do Amazon FSx. Use o nome DNS do sistema de arquivos do Amazon FSx ou um alias de DNS associado ao sistema de arquivos nesse script, que pode ser obtido na exibição de detalhes do sistema de arquivos no console do Amazon FSx.

   Se você estiver usando o nome DNS do sistema de arquivos:

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\users\%username%
   ```

   Se você estiver usando um alias de DNS associado ao sistema de arquivos:

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\users\%username%
   ```

2. Abra um prompt do PowerShell e execute `gpedit.msc`.
3. Em Configuração do usuário, selecione Configurações do Windows e, em seguida, Logon.
4. Navegue até o script em lote que você criou na primeira etapa deste procedimento e selecione-o.
5. Em Configuração do computador, selecione Modelos administrativos do Windows, Sistema e, em seguida, Política de grupo.
6. Escolha a política Configurar atraso do script de logon. Habilite a política e reduza o tempo de atraso para `0`. Essa configuração ajuda a garantir que o script de logon do usuário seja executado imediatamente quando o usuário inicia uma sessão de streaming.

7. Crie sua imagem e atribua-a a uma frota do AppStream 2.0. Certifique-se de que você também associe a frota do AppStream 2.0 ao mesmo domínio do Active Directory que você usou para o construtor de imagens. Inicie a frota na mesma VPC usada pelo seu sistema de arquivos do Amazon FSx. Os grupos de segurança da VPC que você associa à frota devem fornecer acesso ao seu sistema de arquivos do Amazon FSx.
8. Inicie uma sessão de streaming usando o SAML SSO. Para se conectar a uma frota que esteja associada ao Active Directory, configure a federação de logon único usando um provedor SAML. Para obter mais informações, consulte Single Sign-on Access to AppStream 2.0 Using SAML 2.0 no Guia de administração do Amazon AppStream 2.0.
9. O compartilhamento de arquivos do Amazon FSx é mapeado para a letra de drive S: na sessão de streaming.

Como fornecer uma pasta compartilhada entre os usuários

Você pode usar o Amazon FSx para fornecer uma pasta compartilhada a usuários na sua organização. Uma pasta compartilhada pode ser usada para manter arquivos comuns (por exemplo, arquivos de demonstração, exemplos de código, manuais de instrução etc.) necessários a todos os usuários.

Há três procedimentos que você precisará executar para concluir essa tarefa.

Criar uma pasta compartilhada usando o Amazon FSx

1. Crie um sistema de arquivos do Amazon FSx. Para obter mais informações, consulte Introdução ao Amazon FSx para Windows File Server.
2. Todo sistema de arquivos do Amazon FSx inclui uma pasta compartilhada por padrão que você pode acessar usando o endereço *file-system-DNS-name*\share, ou *fqdn-DNS-alias*\share se você estiver usando aliases de DNS. Você pode usar o compartilhamento padrão ou criar uma pasta compartilhada diferente. Para obter mais informações, consulte Gerenciando compartilhamentos de arquivos em sistemas de arquivos FSx for Windows File Server.

Iniciar um construtor de imagens do AppStream 2.0

1. No console do AppStream 2.0, inicie um novo construtor de imagens ou conecte-se a um construtor de imagens existente. Inicie o construtor de imagens na mesma VPC usada pelo seu

sistema de arquivos do Amazon FSx. Os grupos de segurança da VPC que você associa ao construtor de imagens devem permitir o acesso ao sistema de arquivos do Amazon FSx.

2. Quando o construtor de imagens estiver disponível, conecte-se ao construtor de imagens como o usuário Administrador.
3. Instale ou atualize suas aplicações como Administrador.

Associar a pasta compartilhada ao AppStream 2.0

1. Crie um script em lote, conforme descrito no procedimento anterior, para montar automaticamente a pasta compartilhada sempre que um usuário iniciar uma sessão de streaming. Para concluir o script, você precisa do nome DNS do sistema de arquivos ou de um alias de DNS associado ao sistema de arquivos (que pode ser obtido na exibição de detalhes do sistema de arquivos no console do Amazon FSx) e das credenciais para acessar a pasta compartilhada.

   Se você estiver usando o nome DNS do sistema de arquivos:

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\share /user:username password
   ```

   Se você estiver usando um alias de DNS associado ao sistema de arquivos:

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\share /user:username password
   ```

2. Crie uma política de grupo para executar esse script em lote a cada logon de usuário. Você pode seguir as mesmas instruções descritas na seção anterior.
3. Crie sua imagem e atribua-a à sua frota.
4. Inicie uma sessão de streaming. Agora você deve visualizar a pasta compartilhada mapeada automaticamente para a letra de drive.

Passo a passo 5: como usar aliases de DNS para acessar seu sistema de arquivos

O FSx para Windows File Server fornece um nome de Sistema de Nomes de Domínio (DNS) padrão para cada sistema de arquivos que você pode usar para acessar os dados no sistema de arquivos. Você também pode acessar os sistemas de arquivos usando um alias de DNS de sua escolha. Com aliases de DNS, você pode continuar usando os nomes DNS atuais para acessar dados armazenados no Amazon FSx ao migrar o armazenamento do sistema de arquivos on-premises para o Amazon FSx, sem precisar atualizar qualquer ferramenta ou aplicação. Você pode associar até 50 aliases de DNS a um sistema de arquivos a qualquer momento.

Acessar seus sistemas de arquivos do Amazon FSx usando aliases de DNS requer a execução das três etapas a seguir.

1. Associe aliases de DNS ao seu sistema de arquivos do Amazon FSx.
2. Configure os nomes das entidades principais de serviço (SPNs) para o objeto de computador do seu sistema de arquivos. (Isso é necessário para obter a autenticação do Kerberos ao acessar o sistema de arquivos usando aliases de DNS).
3. Atualize ou crie um registro CNAME de DNS para o sistema de arquivos e o alias de DNS.

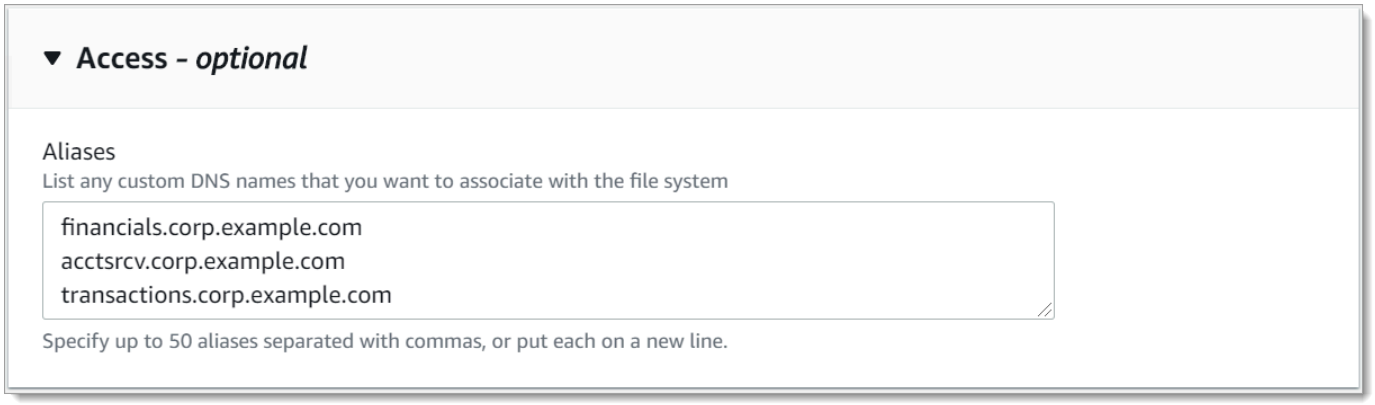
Tópicos

Etapa 1: associe aliases de DNS ao seu sistema de arquivos do Amazon FSx

Você pode associar aliases de DNS a sistemas de arquivos existentes do FSx para Windows File Server, ao criar novos sistemas de arquivos e ao criar um novo sistema de arquivos de um backup usando o console do Amazon FSx, a CLI e a API. Se estiver criando um alias com um nome de domínio diferente, insira o nome completo, incluindo o domínio pai, para associar um alias.

Este procedimento descreve como associar aliases de DNS ao criar um novo sistema de arquivos usando o console do Amazon FSx. Para obter informações sobre a associação de aliases de DNS a sistemas de arquivos existentes e detalhes sobre o uso da CLI e da API, consulte Como gerenciar aliases de DNS.

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. Siga o procedimento para a criação de um novo sistema de arquivos descrito na Crie seu sistema de arquivos da seção de Conceitos básicos.
3. Na seção Acesso: opcional do assistente Criar sistema de arquivos, insira os aliases de DNS que você deseja associar ao sistema de arquivos.



   Use as seguintes diretrizes ao especificar aliases de DNS:

   - Deve ser formatado como um nome de domínio totalmente qualificado (FQDN) *hostname.domain*, por exemplo, `accounting.example.com`.
   - Pode conter caracteres alfanuméricos e hifens (-).
   - Não pode começar ou terminar com um hífen (-).
   - Pode começar com um caractere numérico.

   Para nomes de alias DNS, o Amazon FSx armazena caracteres alfabéticos como letras minúsculas (a-z), independentemente de como elas são especificadas: como letras maiúsculas, letras minúsculas ou as letras correspondentes em códigos de escape.
4. Para as Preferências de manutenção, faça as alterações que você desejar.
5. Na seção Tags - opcional, adicione as tags necessárias e selecione Próximo.
6. Verifique a configuração do sistema de arquivos mostrada na página Criar sistema de arquivos. Selecione Criar sistema de arquivos para criar o sistema de arquivos.

Quando o novo sistema de arquivos estiver disponível, continue com a etapa 2.

Etapa 2: configurar nomes das entidades principais de serviço (SPNs) para o Kerberos

Recomendamos que você use autenticação e criptografia baseadas no Kerberos em trânsito com o Amazon FSx. O Kerberos oferece a autenticação mais segura para clientes que acessam o sistema de arquivos.

Para ativar a autenticação do Kerberos para clientes que acessam o Amazon FSx usando um alias de DNS, você deve adicionar nomes das entidades principais de serviço (SPNs) que correspondam ao alias de DNS no objeto de computador do Active Directory do sistema de arquivos do Amazon FSx. Um SPN só pode ser associado a um único objeto de computador do Active Directory de cada vez. Se você tiver SPNs existentes para o nome DNS configurado para o objeto de computador do Active Directory do sistema de arquivos original, será necessário excluí-los primeiro.

Há dois SPNs necessários para a autenticação do Kerberos:

```
HOST/alias
HOST/alias.domain
```

Se o alias for `finance.domain.com`, os dois SPNs necessários são os seguintes:

```
HOST/finance
HOST/finance.domain.com
```

> **Note**
>
> Você precisará excluir todos os SPNs HOST existentes que correspondam ao alias de DNS no objeto de computador do Active Directory antes de criar novos SPNs HOST para o objeto de computador do Active Directory (AD) do sistema de arquivos do Amazon FSx. As tentativas de definir SPNs para seu sistema de arquivos do Amazon FSx falharão se existir um SPN para o alias de DNS no AD.

Os procedimentos apresentados abaixo descrevem como fazer o seguinte:

- Localize todos os SPNs de alias de DNS existentes no objeto de computador do Active Directory do sistema de arquivos original.
- Exclua os SPNs existentes encontrados, se houver.
- Crie novos SPNs de alias de DNS para o objeto de computador do Active Directory do seu sistema de arquivos do Amazon FSx.

Para instalar o módulo necessário do PowerShell Active Directory

1. Faça logon em uma instância do Windows associada ao Active Directory ao qual seu sistema de arquivos do Amazon FSx está associado.
2. Abra PowerShell como administrador.
3. Instale o módulo do PowerShell Active Directory usando o comando a seguir.

```
Install-WindowsFeature RSAT-AD-PowerShell
```

Encontrar e excluir SPNs de alias de DNS atuais no objeto de computador do Active Directory do sistema de arquivos original

1. Encontre todos os SPNs atuais usando os comandos a seguir. Substitua *alias_fqdn* pelo alias de DNS que você associou ao sistema de arquivos na Etapa 1.

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. Exclua os SPNs HOST atuais retornados na etapa anterior usando o exemplo de script a seguir.
   - Substitua *alias_fqdn* pelo alias de DNS completo que você associou ao sistema de arquivos na Etapa 1.
   - Substitua *file_system_DNS_name* pelo nome DNS do sistema de arquivos original.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
```

```
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. Repita as etapas anteriores para cada alias de DNS que você associou ao sistema de arquivos na Etapa 1.

Definir SPNs no objeto de computador do Active Directory do sistema de arquivos do Amazon FSx

1. Defina novos SPNs para o sistema de arquivos do Amazon FSx executando os comandos a seguir.

   - Substitua *file_system_DNS_name* pelo nome DNS que o Amazon FSx atribuiu ao sistema de arquivos.

     Para encontrar o nome DNS do sistema de arquivos no console do Amazon FSx, escolha Sistemas de arquivos, escolha o sistema de arquivos e, em seguida, escolha o painel Rede e segurança na página de detalhes do sistema de arquivos.

     Você também pode obter o nome DNS na resposta da operação da API de DescribeFilesistemas.

   - Substitua *alias_fqdn* pelo alias de DNS completo que você associou ao sistema de arquivos na Etapa 1.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

##Use one of the following commands, not both:
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
##Or
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> A configuração de um SPN para o sistema de arquivos do Amazon FSx apresentará falha se existir um SPN para o alias de DNS no AD do objeto de computador do sistema de arquivos original. Para obter informações sobre como encontrar e excluir SPNs atuais, consulte Encontrar e excluir SPNs de alias de DNS atuais no objeto de computador do Active Directory do sistema de arquivos original.

2. Verifique se os novos SPNs estão configurados para o alias de DNS usando o exemplo de script a seguir. Certifique-se de que a resposta inclua dois SPNs HOST, `HOST/`*`alias`* e `HOST/`*`alias_fqdn`*, conforme descrito anteriormente neste procedimento.

   Substitua *`file_system_DNS_name`* pelo nome DNS que o Amazon FSx atribuiu ao sistema de arquivos. Para encontrar o nome DNS do sistema de arquivos no console do Amazon FSx, escolha Sistemas de arquivos, escolha o sistema de arquivos e, em seguida, escolha o painel Rede e segurança na página de detalhes do sistema de arquivos.

   Você também pode obter o nome DNS na resposta da operação da API de DescribeFilesistemas.

   ```
   ## Verify SPNs on FSx file system AD computer object
   $FileSystemDnsName = "file_system_dns_name"
   $FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
   [0].Name.Split(".")[0]
   $FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
   SetSpn /L ${FSxAdComputer}.Name
   ```

3. Repita as etapas anteriores para cada alias de DNS que você associou ao sistema de arquivos na Etapa 1.

Para obter informações sobre como impor que os clientes usem a autenticação e a criptografia do Kerberos ao se conectarem ao sistema de arquivos do Amazon FSx, consulte Como reforçar a autenticação do Kerberos usando GPOs.

Etapa 3: atualizar ou criar um registro CNAME do DNS para o sistema de arquivos

Depois de configurar adequadamente os SPNs do sistema de arquivos, mude para o Amazon FSx substituindo cada registro DNS resolvido no sistema de arquivos original por um registro DNS resolvido com o nome DNS padrão do sistema de arquivos do Amazon FSx.

Os módulos do Windows `dnsserver` e `activedirectory` são necessários para executar os comandos apresentados nesta seção.

Para instalar os PowerShell cmdlets necessários

1. Faça login em uma instância do Windows associada ao Active Directory à qual seu sistema de arquivos Amazon FSx está associado como um usuário que é membro de um grupo que tem permissões de administração de DNS (administradores de sistema de nomes de domínio AWSAWS delegados no Active Directory AWS gerenciado e administradores de domínio ou outro grupo ao qual você delegou permissões de administração de DNS em seu Active Directory autogerenciado).

   Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
2. Abra PowerShell como administrador.
3. O módulo Servidor PowerShell DNS é necessário para executar as instruções neste procedimento. Instale-o usando o comando a seguir.

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

Atualizar ou criar um nome DNS personalizado para seu sistema de arquivos do Amazon FSx

1. Conecte-se à sua instância do Amazon EC2 como um usuário que é membro de um grupo que tem permissões de administração de DNS (administradores de sistema de nomes de domínio AWS delegados no Active Directory AWS gerenciado e administradores de domínio ou outro grupo ao qual você delegou permissões de administração de DNS em seu Active Directory autogerenciado).

   Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.

2. No prompt de comando, execute o seguinte script: Esse script migra todos os registros CNAME do DNS existentes para o seu sistema de arquivos do Amazon FSx. Se não for encontrado nenhum, ele cria um novo registro CNAME do DNS para o alias de DNS *alias_fqdn* que resolve para o nome DNS padrão do seu sistema de arquivos do Amazon FSx.

   Para executar o script:

   - Substitua *alias_fqdn* pelo alias de DNS que você associou ao sistema de arquivos.
   - Substitua *file_system_DNS_name* pelo nome DNS que o Amazon FSx atribuiu ao sistema de arquivos.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name) | Select -First 1
foreach ($computer in $DnsServerComputerName)
{
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName $computer -
HostNameAlias $FSxDnsName -ZoneName $ZoneName
}
```

3. Repita a etapa anterior para cada alias de DNS que você associou ao sistema de arquivos na Etapa 1.

Agora você adicionou um valor CNAME do DNS para seu sistema de arquivos do Amazon FSx com o alias de DNS. Agora você pode usar o alias de DNS para acessar seus dados.

> **Note**
>
> Ao atualizar um registro CNAME do DNS para apontar para um sistema de arquivos do Amazon FSx anteriormente apontado para outro sistema de arquivos, os clientes podem não conseguir se conectar ao sistema de arquivos por um breve período de tempo. Quando o cache DNS do cliente for atualizado, ele poderá se conectar usando o alias de DNS. Para ter mais informações, consulte Não é possível acessar o sistema de arquivos usando um alias de DNS.

Como reforçar a autenticação do Kerberos usando GPOs

Você pode reforçar a autenticação do Kerberos ao acessar o sistema de arquivos configurando os seguintes Objetos de Política de Grupo (GPOs) no Active Directory:

- Restringir NTLM: tráfego NTLM de saída para servidores remotos: use essa configuração de política para negar ou auditar o tráfego NTLM de saída de um computador para qualquer servidor remoto que esteja executando o sistema operacional Windows.
- Restringir NTLM: adicionar exceções de servidor remoto para autenticação NTLM: use essa configuração de política para criar uma lista de exceções de servidores remotos para os quais os dispositivos clientes têm permissão de usar a autenticação NTLM se a configuração de política Segurança de rede: restringir NTLM: tráfego NTLM de saída para servidores remotos estiver configurada.

1. Faça logon em uma instância do Windows associada ao Active Directory ao qual seu sistema de arquivos do Amazon FSx está associado como administrador. Se estiver configurando um Active Directory autogerenciado, aplique estas etapas diretamente ao Active Directory.
2. Selecione Iniciar, Ferramentas administrativas e, em seguida, Gerenciamento de política de grupo.
3. Selecione Objetos de Política de Grupo.
4. Se o Objeto de Política de Grupo ainda não existir, crie-o.
5. Localize a política de Segurança de rede existente: restringir NTLM: tráfego NTLM de saída para servidores remotos. (Se não houver uma política existente, crie uma nova política). Na guia Configuração de segurança local, abra o menu de contexto (clique com o botão direito do mouse) e escolha Propriedades.
6. Selecione Negar tudo.
7. Selecione Aplicar para salvar a configuração de segurança.
8. Para definir exceções para conexões NTLM com servidores remotos específicos para o cliente, localize Segurança de rede: restringir NTLM: adicionar exceções de servidor remoto.

   Abra o menu de contexto (clique com o botão direito do mouse) e escolha Propriedades na guia Configuração de segurança local.
9. Insira os nomes dos servidores a serem adicionados à lista de exceções.
10. Selecione Aplicar para salvar a configuração de segurança.

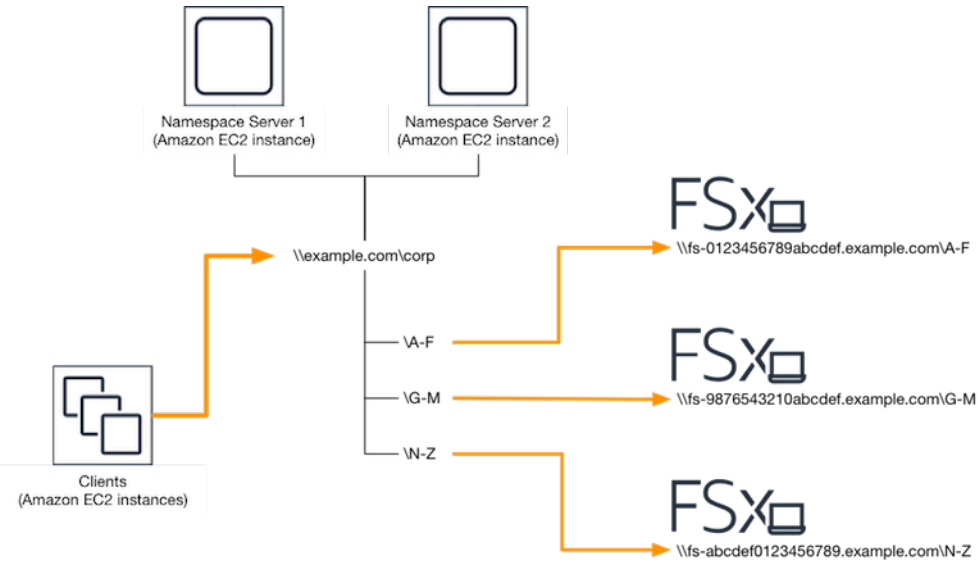
Passo a passo 6: aumentar a escala horizontalmente com fragmentos

O Amazon FSx para Windows File Server é compatível com o uso do Sistema de Arquivos Distribuído (DFS) da Microsoft. Ao usar os namespaces do DFS, você pode aumentar a escala horizontalmente da performance (leitura e gravação) para atender a workloads com uso intensivo de E/S, distribuindo os dados do arquivo em vários sistemas de arquivos do Amazon FSx. Ao mesmo tempo, você ainda pode apresentar às suas aplicações uma visão unificada sob um namespace comum. Essa solução envolve a divisão de seus dados de arquivo em conjuntos de dados menores ou fragmentos e o armazenamento deles em diferentes sistemas de arquivos. As aplicações que acessam seus dados de várias instâncias podem alcançar altos níveis de performance lendo e gravando nesses fragmentos em paralelo.

Você pode usar essa solução quando sua workload exigir acesso de leitura/gravação uniformemente distribuído aos dados do arquivo (por exemplo, se cada subconjunto de instâncias de computação acessar uma parte diferente dos dados do arquivo).

Como configurar os namespaces do DFS para a performance do aumento da escala horizontal

O procedimento a seguir orienta você na criação de uma solução do DFS no Amazon FSx para a performance do aumento da escala horizontal. Neste exemplo, os dados armazenados no namespace `corp` são fragmentados em ordem alfabética. Os arquivos de dados 'A-F', 'G-M' e 'N-Z' estão todos armazenados em diferentes compartilhamentos de arquivos. Com base no tipo de dados, no tamanho de E/S e no padrão de acesso de E/S, você deve decidir qual a melhor forma de fragmentar seus dados em vários compartilhamentos de arquivos. Escolha uma convenção de fragmentação que distribua a E/S uniformemente entre todos os compartilhamentos de arquivos que você planeja usar. Lembre-se de que cada namespace é compatível com até 50 mil compartilhamentos de arquivos e centenas de petabytes de capacidade de armazenamento em conjunto.



Configurar os namespaces do DFS para a performance do aumento da escala horizontal

1. Se você ainda não tem servidores de Namespace DFS em execução, você pode iniciar um par de servidores de Namespace DFS altamente disponíveis usando o modelo Setup-DFSN-Servers.template. AWS CloudFormation 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.
2. Conecte-se a um dos servidores de namespace do DFS iniciados na etapa anterior como usuário no grupo de Administradores delegados da AWS . Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
3. Acesse o console de gerenciamento do DFS. Abra o menu Iniciar e execute dfsmgmt.msc. Isso abre a ferramenta da GUI de gerenciamento do DFS.
4. Escolha Ação e, em seguida, Novo namespace, digite o nome do computador do primeiro servidor de namespace do DFS que você iniciou em Servidor e selecione Próximo.
5. Em Nome, digite o namespace que você está criando (por exemplo, corp).
6. Escolha Editar configurações e defina as permissões apropriadas com base em seus requisitos. Selecione Next (Próximo).
7. Deixe a opção padrão Namespace baseado em domínio selecionada, deixe a opção Habilitar o modo Windows Server 2008 selecionada e escolha Próximo.

> **Note**
>
> O modo Windows Server 2008 é a opção mais recente disponível para namespaces.

8. Analise as configurações do namespace e escolha Criar.
9. Com o namespace recém-criado selecionado em Namespaces na barra de navegação, escolha Ação e, em seguida, Adicionar servidor do namespace.
10. Digite o nome do computador do segundo servidor do namespace do DFS que você iniciou para o Servidor do namespace.
11. Escolha Editar configurações, defina as permissões apropriadas com base em seus requisitos e escolha OK.
12. Abra o menu de contexto (clique com o botão direito do mouse) do namespace que você acabou de criar, selecione Nova pasta, insira o nome da pasta para o primeiro fragmento (por exemplo, `A-F` para Nome) e selecione Adicionar.
13. Insira o nome DNS do compartilhamento de arquivos que hospeda esse fragmento no formato UNC (por exemplo, `\\fs-0123456789abcdef0.example.com\A-F`) para o Caminho para a pasta de destino e selecione OK.
14. Se o compartilhamento não existir:
    a. Escolha Sim para criá-lo.
    b. Na caixa de diálogo Criar compartilhamento, escolha Procurar.
    c. Escolha uma pasta atual ou crie uma pasta em D$ e escolha OK.
    d. Defina as permissões de compartilhamento apropriadas e selecione OK.
15. Com o destino da pasta agora adicionado ao fragmento, selecione OK.
16. Repita as quatro últimas etapas para outros fragmentos que você deseja adicionar ao mesmo namespace.

Passo a passo 7: copiar um backup para outra Região da AWS

Com o Amazon FSx, você pode copiar um backup existente da mesma Conta da AWS para outra Região da AWS (uma cópia de backup entre regiões) ou para a mesma Região da AWS (uma cópia de backup na região).

O procedimento a seguir mostra o processo de criação e armazenamento de uma cópia de um backup usando a mesma Conta da AWS. Antes de criar essa cópia de backup, você deve ter um backup existente. Para obter mais informações, consulte Trabalhar com backups.

Copiar um backup existente da mesma Conta da AWS (entre regiões ou dentro da região)

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel de navegação, selecione Backups.
3. Na tabela Backups, escolha o backup que você deseja copiar.
4. Selecione Copy backup (Copiar backup). Será aberto o assistente de Cópia de backup.
5. Na lista Região de destino, escolha uma Região da AWS de destino para a qual será copiado o backup. O destino pode estar em outro Região da AWS ou dentro da mesma Região da AWS.
6. (Opcional) Selecione Copiar tags para copiar tags do backup de origem para o backup de destino. Se você selecionar Copiar tags e também adicionar tags na etapa 8, todas as tags serão mescladas.
7. Em Criptografia, escolha a chave de criptografia do AWS KMS para criptografar o backup copiado.
8. Em Tags: opcional, insira uma chave e um valor para adicionar tags ao backup copiado. Se você adicionar tags aqui e também tiver selecionado Copiar tags na etapa 6, todas as tags serão mescladas.
9. Selecione Copy backup (Copiar backup).

Agora você copiou com sucesso um backup dentro da mesma Conta da AWS para outra Região da AWS ou dentro da mesma Região da AWS.

Segurança no Amazon FSx

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS serviços na Amazon Web Services Cloud. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programs AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Amazon FSx para Windows File Server, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon FSx para Windows File Server. 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 for Windows File Server.

Tópicos

Criptografia de dados no Amazon FSx

O Amazon FSx para Windows File Server é compatível com duas formas de criptografia para sistemas de arquivos: criptografia de dados em trânsito e criptografia em repouso. A criptografia de dados em trânsito é compatível com compartilhamentos de arquivos mapeados em uma instância de computação que seja compatível com o protocolo SMB 3.0 ou mais recente. A criptografia de dados em repouso é habilitada automaticamente ao criar um sistema de arquivos do Amazon FSx. O Amazon FSx 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.

Quando usar a criptografia

Se sua organização está sujeita a políticas corporativas ou regulatórias que exigem a criptografia de dados e metadados em repouso, recomendamos a criação de um sistema de arquivos criptografado para montar seus sistema usando a criptografia de dados em trânsito.

Para obter mais informações sobre criptografia com o Amazon FSx para Windows File Server, consulte estes tópicos relacionados:

- Criar seu sistema de arquivos do Amazon FSx para Windows File Server
- Ações, recursos e chaves de condição do Amazon FSx no Guia do usuário do IAM

Tópicos

Criptografia em repouso

Todos os sistemas de arquivos do Amazon FSx são criptografados em repouso com chaves gerenciadas usando o 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 um AWS KMS key para criptografar seu 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 gerenciada pela AWS: essa é a chave padrão do KMS e seu uso é gratuito.
- Chave gerenciada pelo cliente: essa é a chave do KMS mais flexível para usar, pois é possível configurar suas políticas de chaves e concessões para diversos usuários ou serviços. Para obter mais informações sobre a criação de chaves gerenciadas pelo cliente, consulte Criação de chaves no Guia do AWS Key Management Service desenvolvedor.

Se você usar uma chave gerenciada pelo cliente como a chave do KMS para descriptografia e criptografia de dados de arquivos, poderá habilitar a rotação de chaves. Ao habilitar a rotação de chaves, o AWS KMS gira sua chave automaticamente uma vez por ano. Além disso, com uma chave gerenciada pelo cliente, você pode escolher quando desativar, reativar, excluir ou revogar o acesso à sua chave do KMS a qualquer momento. Para obter mais informações, consulte Rotação AWS KMS keys no Guia do AWS Key Management Service desenvolvedor.

A criptografia e decriptografia em repouso do sistema de arquivos são gerenciadas de modo transparente. No entanto, Conta da AWS IDs específicos do Amazon FSx aparecem em seus AWS CloudTrail registros relacionados às AWS KMS ações.

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 dados no lado do servidor com uma nova chave KMS, sem expor o texto simples dos dados no lado do cliente. Primeiro os dados são descriptografados e, depois, recriptografados. Essa permissão está incluída na política de chaves padrão.
- kms: 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 Using grants no Guia do desenvolvedor do AWS Key Management Service .. Essa permissão está incluída na política de chaves padrão.
- kms: DescribeKey — (Obrigatório) Fornece informações detalhadas sobre a chave KMS especificada. Essa permissão está incluída na política de chaves padrão.
- kms: ListAliases — (Opcional) Lista todos os aliases de chave na conta. Quando você usa o console para criar um sistema de arquivos criptografado, essa permissão preenche a lista 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 em trânsito

A criptografia de dados em trânsito é compatível com compartilhamentos de arquivos mapeados em uma instância de computação que seja compatível com o protocolo SMB 3.0 ou mais recente. Isso inclui todas as versões do Windows a partir do Windows Server 2012 e do Windows 8, e todos os clientes Linux com o cliente Samba versão 4.2 ou mais recente. O Amazon FSx para Windows File Server criptografa automaticamente os dados em trânsito usando a criptografia SMB à medida que você acessa o sistema de arquivos, sem a necessidade de modificar suas aplicações.

A criptografia SMB usa AES-128-GCM ou AES-128-CCM (com a variante GCM sendo escolhida se o cliente for compatível com SMB 3.1.1) como algoritmo de criptografia e também fornece integridade

de dados com assinatura usando chaves de sessão SMB do Kerberos. O uso do AES-128-GCM leva a uma melhor performance, por exemplo, até 2x mais performance ao copiar arquivos grandes em conexões SMB criptografadas.

Para atender aos requisitos de conformidade para sempre criptografar data-in-transit, você pode limitar o acesso ao sistema de arquivos para permitir o acesso somente a clientes que ofereçam suporte à criptografia SMB. Você também pode ativar ou desativar a criptografia em trânsito por compartilhamento de arquivo ou para todo o sistema de arquivos. Isso permite que você tenha uma combinação de compartilhamentos de arquivos criptografados e não criptografados no mesmo sistema de arquivos. Para saber mais sobre o gerenciamento encryption-in-transit em seu sistema de arquivos, consulteComo gerenciar criptografia em trânsito.

Controle de acesso em nível de arquivo e pasta usando ACLs do Windows

O Amazon FSx para Windows File Server é compatível com a autenticação baseada em identidade no protocolo Server Message Block (SMB) por meio do Microsoft Active Directory. O Active Directory é o serviço de diretório da Microsoft para armazenar informações sobre objetos na rede e facilitar a localização e o uso dessas informações por administradores e usuários. Esses objetos normalmente incluem recursos compartilhados, como servidores de arquivos e contas de usuários e computadores da rede. Para saber mais sobre o suporte do Active Directory no Amazon FSx, consulte Trabalhar com o Microsoft Active Directory no FSx para Windows File Server.

Suas instâncias de computação unidas por domínio podem acessar os compartilhamentos de arquivos do Amazon FSx usando as credenciais do Active Directory. As listas de controle de acesso (ACLs) padrão do Windows são usadas para controle de acesso refinado em nível de arquivo e pasta. Os sistemas de arquivos do Amazon FSx verificam automaticamente as credenciais dos usuários que acessam os dados do sistema de arquivos para aplicar essas ACLs do Windows.

Todo sistema de arquivos do Amazon FSx vem com um compartilhamento de arquivos padrão do Windows chamado `share`. As ACLs do Windows para essa pasta compartilhada estão configuradas para permitir acesso de leitura/gravação aos usuários do domínio. Elas também permitem o controle total do grupo de administradores delegados no Active Directory, que é delegado para executar ações administrativas nos sistemas de arquivos. Se você estiver integrando seu sistema de arquivos com o AWS Managed Microsoft AD, esse grupo é AWS Delegated FSx Administrators. Se você estiver integrando o sistema de arquivos com a configuração do AD autogerenciado da Microsoft, esse grupo pode ser de administradores de domínio. Ou ele pode ser um grupo de administradores

delegados personalizado que você especificou ao criar o sistema de arquivos. Para alterar as ACLs, você pode mapear o compartilhamento como um usuário que seja membro do grupo de administradores delegados.

> **Warning**
>
> O Amazon FSx exige que o usuário SYSTEM tenha permissões de Controle total NTFS ACL em todas as pastas do seu sistema de arquivos. Não altere as permissões de NTFS ACL para esse usuário em suas pastas. Isso pode tornar o compartilhamento de arquivos inacessível e impedir que os backups do sistema de arquivos possam ser usados.

Links relacionados

- O que é AWS Directory Service? no Guia AWS Directory Service de administração.
- Crie seu diretório AWS gerenciado do Microsoft AD no Guia de AWS Directory Service Administração.
- When to Create a Trust Relationship no Guia de administração do AWS Directory Service .
- Passo a passo 1: pré-requisitos para começar.

Controle de acesso ao sistema de arquivos com a Amazon VPC

Você acessa seu sistema de arquivos do Amazon FSx por meio de uma interface de rede elástica. Essa interface de rede reside na nuvem privada virtual (VPC) com base no serviço Amazon Virtual Private Cloud (Amazon VPC) que você associa ao seu sistema de arquivos. Você se conecta ao seu sistema de arquivos do Amazon FSx por meio do nome DNS (Domain Name Service). O nome DNS é mapeado para o endereço IP privado da interface de rede elástica do sistema de arquivos em sua VPC. Somente recursos dentro da VPC associada, recursos conectados à VPC associada por AWS Direct Connect ou VPN ou recursos dentro de VPCs emparelhadas podem acessar a interface de rede do seu sistema de arquivos. Para obter mais informações, consulte O que é a Amazon VPC? no Guia do usuário da Amazon VPC.

> **Warning**
>
> 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.

O FSx for Windows File Server oferece suporte ao compartilhamento de VPC, o que permite visualizar, criar, modificar e excluir recursos em uma sub-rede compartilhada em uma VPC de propriedade de outra conta. AWS Para obter mais informações, consulte Trabalhar com VPCs compartilhadas no Guia do usuário da Amazon VPC.

Grupos de segurança da Amazon VPC

Para controlar ainda mais o tráfego de rede que passa pela(s) interface(s) de rede elástica(s) do seu sistema de arquivos na VPC, use grupos de segurança para limitar o acesso aos sistemas de arquivos. Um grupo de segurança é um firewall com estado que controla o tráfego de e para suas interfaces de rede associadas. Nesse caso, o recurso associado é(são) a(s) interface(s) de rede do seu sistema de arquivos.

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.

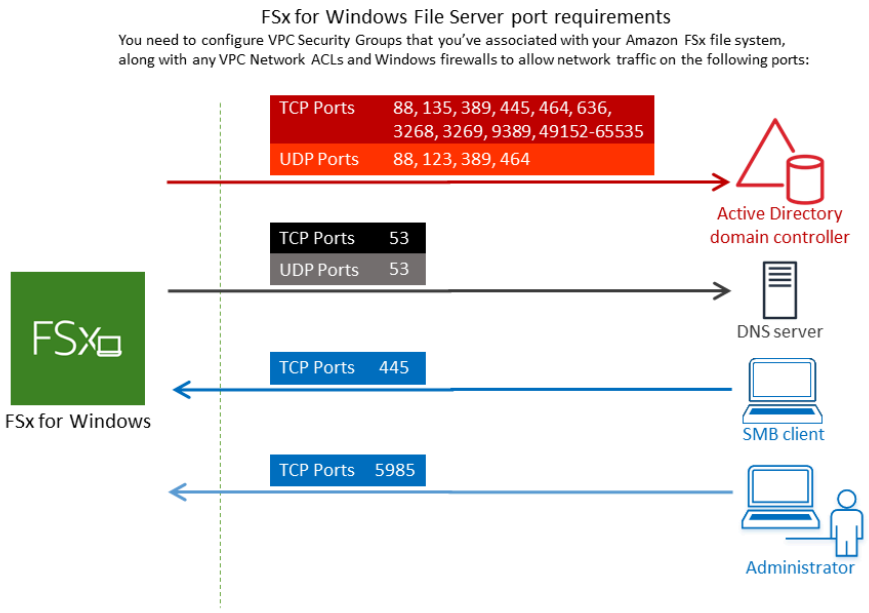
Para obter mais informações sobre regras de grupos de segurança, consulte Regras de grupos de segurança no Guia do usuário do Amazon EC2.

Criar um grupo de segurança 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.

Adicione as seguintes regras para permitir o tráfego de rede de saída nas seguintes portas:

a. Em Grupos de segurança da VPC, o grupo de segurança padrão para a Amazon VPC padrão já está adicionado ao sistema de arquivos no console. Certifique-se de que o grupo de segurança e as ACLs de rede da VPC para as sub-redes nas quais você vai criar seu sistema de arquivos do FSx permite tráfego nas portas e nas direções mostradas no diagrama a seguir.



A tabela a seguir identifica o perfil de cada porta.

Protocolo	Portas	Função
TCP/UDP	53	Domain Name System (DNS)
TCP/UDP	88	Autenticação de Kerberos
TCP/UDP	464	Alterar/definir senha
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)
UDP	123	Network Time Protocol (NTP)

Protocolo	Portas	Função
TCP	135	Distributed Computing Environment/End Point Mapper (DCE/EPMAP)
TCP	445	Compartilhamento de arquivos de SMB para serviços de diretório
TCP	636	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
TCP	3268	Catálogo global da Microsoft
TCP	3269	Catálogo global da Microsoft sobre SSL
TCP	5985	WinRM 2.0 (Gerenciamento Remoto do Microsoft Windows)
TCP	9389	Serviços Web do Microsoft AD DS, PowerShell
TCP	49152 – 65535	Portas efêmeras para RPC

> **Important**
>
> É necessário permitir o tráfego de saída na porta TCP 9389 para implantações de sistemas de arquivos single-AZ 2 e todas as implantações de sistemas de arquivos multi-AZ.

b. Certifique-se de que essas regras de tráfego também sejam espelhadas nos firewalls que se aplicam a cada um dos controladores de domínio do AD, 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.

> **Note**
>
> Se você tiver sites do Active Directory definidos, deverá certificar-se de que a(s) sub-rede(s) na VPC associada ao seu sistema de arquivos do Amazon FSx esteja(m) definida(s) em um site do Active Directory e que não haja conflitos entre a(s) sub-rede(s) na sua VPC e as sub-rede(s) nos outros sites. Você pode exibir e alterar essas configurações usando o snap-in do MMC de Serviços e Sites do Active Directory.

> **Note**
>
> Em alguns casos, você pode ter modificado as regras do grupo de segurança do AWS Managed Microsoft AD com base nas configurações padrão. Nesse caso, certifique-se de que esse grupo de segurança tenha as regras de entrada necessárias para permitir tráfego proveniente do sistema de arquivos do Amazon FSx. Para obter mais informações sobre as regras de entrada necessárias, consulte Pré-requisitos do AWS Managed Microsoft AD no Guia de administração do AWS Directory Service .

Agora que você criou seu grupo de segurança, você pode associá-lo à(s) interface(s) de rede elástica do sistema de arquivos do Amazon FSx.

Associar um grupo de segurança ao seu sistema de arquivos do Amazon FSx

1. Abra o console do Amazon FSx em https://console.aws.amazon.com/fsx/.
2. No painel, escolha seu sistema de arquivos para visualizar seus detalhes.
3. Selecione a guia Rede e segurança e escolha a(s) interface(s) de rede do seu sistema de arquivos; por exemplo, ENI-01234567890123456. Para sistemas de arquivos single-AZ, você verá uma única interface de rede. Para sistemas de arquivos multi-AZ, você verá uma interface de rede na sub-rede preferencial e uma na sub-rede em espera.
4. Para cada interface de rede, escolha a interface de rede e, em Ações, selecione Alterar grupos de segurança.
5. Na caixa de diálogo Alterar grupos de segurança, escolha os grupos de segurança a serem usados e selecione Salvar.

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.

ACLs de rede da Amazon VPC

Outra opção para proteger o acesso ao sistema de arquivos em sua VPC é estabelecer listas de controle de acesso à rede (ACLs da rede). As ACLs da rede são diferentes dos grupos de segurança, mas têm funcionalidade semelhante para adicionar outra camada de segurança aos recursos em sua VPC. Para obter mais informações sobre ACLs da rede, consulte ACLs da rede no Guia do usuário da Amazon VPC.

Gerenciamento de identidade e acesso para o Amazon FSx para Windows File Server

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 ajudá-lo a solicitar as permissões corretas ao seu administrador. Se você não puder acessar um recurso no Amazon FSx, consulte Solução de problemas de identidade e acesso do Amazon FSx para Windows File Server.

Administrador do serviço: se você for o responsável pelos recursos do Amazon FSx em sua empresa, provavelmente terá acesso total ao Amazon FSx. Cabe a você determinar quais funcionalidades e recursos do Amazon FSx os usuários do serviço deverão acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Amazon FSx, consulte Como o Amazon FSx para Windows File Server funciona com o IAM.

Administrador do IAM: se você for administrador do IAM, talvez deseje saber detalhes sobre como criar políticas para gerenciar o acesso ao Amazon FSx. Para ver exemplos de políticas baseadas em identidade do Amazon FSx que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o Amazon FSx para Windows File Server.

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 uma 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 em 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.

Independentemente 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 Guia AWS IAM Identity Center 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 Guia do usuário do AWS IAM Identity Center .

Grupos e usuários 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 as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível 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 grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de 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. Ela é semelhante a um usuário do IAM, mas não está associada 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 o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, 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 Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar 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 Guia do usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em recurso no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal de chamada, usando um perfil de serviço ou um perfil vinculado 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.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

- Função vinculada 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 a função 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 perfis vinculados ao 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 o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do 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 a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação, independentemente 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 um usuário do IAM, grupo de usuários ou função do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de política do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. 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 escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recurso

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos 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 perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

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 atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (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 Organizations e SCPs, consulte Como os SCPs funcionam no Guia do usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como 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 para Windows File Server 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 para Windows File Server

Recurso do IAM	Suporte do FSx
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Sessões de acesso direto	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para ter uma visão de alto nível de como o 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 para o FSx

É compatível 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, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. ‘Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou 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 FSx

Para ver exemplos de políticas baseadas em identidade do Amazon FSx, consulte Exemplos de políticas baseadas em identidade para o Amazon FSx para Windows File Server.

Políticas baseadas em recursos no FSx

Oferece suporte a políticas baseadas em recursos	Não

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico.

Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar um principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a um principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Ações de política para o 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 FSx, consulte Ações definidas pelo Amazon FSx para Windows File Server na Referência de autorização do serviço.

As ações de política no FSx usam o seguinte prefixo antes da ação:

```
fsx
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Para ver exemplos de políticas baseadas em identidade do Amazon FSx, consulte Exemplos de políticas baseadas em identidade para o Amazon FSx para Windows File Server.

Recursos de política para o FSx

Oferece suporte a recursos 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 recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um caractere curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do FSx e seus ARNs, consulte Recursos definidos pelo Amazon FSx para Windows File Server 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 Windows File Server.

Para ver exemplos de políticas baseadas em identidade do Amazon FSx, consulte Exemplos de políticas baseadas em identidade para o Amazon FSx para Windows File Server.

Chaves de condição de política para o FSx

Compatível com chaves de condição de política específicas do serviço	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 `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, 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 para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

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 das chaves de condição do FSx, consulte Chaves de condição do Amazon FSx para Windows File Server na Referência de autorização do serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Amazon FSx para Windows File Server.

Para ver exemplos de políticas baseadas em identidade do Amazon FSx, consulte Exemplos de políticas baseadas em identidade para o Amazon FSx para Windows File Server.

ACLs no FSx

Oferece suporte a ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com o 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 recursos 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 está 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 as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Como usar credenciais temporárias com o 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 perfis, 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 obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para 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 do FSx

Oferece suporte a perfis de serviço	Não

A função de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais

informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.

> **Warning**
>
> A alteração das permissões de um perfil de serviço pode interromper a funcionalidade do FSx. Edite os perfis de serviço somente quando o FSx fornecer orientação para isso.

Perfis vinculados a serviços para o FSx

Oferece suporte a funções vinculadas 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 a função 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 perfis vinculados ao 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 o Amazon FSx para Windows File Server

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 aos usuários permissões para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM 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 recursos definidos pelo FSx, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição do Amazon FSx para Windows File Server na Referência de autorização do serviço.

Tópicos

- Práticas recomendadas de políticas
- Como usar o console do FSx
- Permitir que os usuários visualizem suas próprias permissões

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Amazon FSx em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com 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 Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever 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 Elementos de política JSON do IAM: Condition no Manual do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas

sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.

- Exigir autenticação multifator (MFA) — Se 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 a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Como usar o console do FSx

Para acessar o console do Amazon FSx para Windows File Server, é necessário 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 FSx, anexe também a política `AmazonFSxConsoleReadOnlyAccess` AWS gerenciada do FSx às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou 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": "*"
        }
    ]
}
```

AWS políticas gerenciadas para Amazon FSx

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para obter mais informações, consulte AWS Políticas gerenciadas pela no Guia do usuário do IAM.

Amazon F SxServiceRolePolicy

Permite que o Amazon FSx gerencie AWS recursos em seu nome. Para saber mais, consulte Como usar perfis vinculados a serviço no Amazon FSx.

AWS política gerenciada: AmazonF SxDeleteServiceLinkedRoleAccess

Não é possível anexar `AmazonFSxDeleteServiceLinkedRoleAccess` às entidades do IAM. Essa política está vinculada a um serviço e só é usada com o perfil vinculado a esse serviço. Você não pode anexar, desanexar, modificar ou excluir essa política. Para ter mais informações, consulte Como usar perfis vinculados a serviço no Amazon FSx.

Essa política concede permissões administrativas que permitem que o Amazon FSx exclua o perfil vinculado ao serviço para acesso do Amazon S3, usado somente pelo Amazon FSx para Lustre.

Detalhes da permissão

Essa política inclui permissões 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 SxDeleteServiceLinkedRoleAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonF SxFullAccess

Você pode anexar o AmazonF SxFullAccess às suas entidades do IAM. O Amazon FSx também anexa essa política a um perfil de serviço que permite que o Amazon FSx execute ações em seu nome.

Fornece acesso total ao Amazon FSx e acesso aos serviços relacionados AWS .

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`: permite que as entidades principais tenham acesso total para executar todas as ações do Amazon FSx, exceto `BypassSnaplockEnterpriseRetention`.
- `ds`— Permite que os diretores visualizem informações sobre os AWS Directory Service diretórios.
- `ec2`
  - Permite que os diretores criem tags sob as condições especificadas.
  - Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança que podem ser usados com uma VPC.
- `iam`: permite que as entidades principais criem um perfil vinculado ao serviço do Amazon FSx em nome do usuário. Isso é necessário para que o Amazon FSx possa gerenciar AWS recursos em nome do usuário.
- `logs`: permite que as entidades principais criem grupos de logs, fluxos de logs e gravem eventos nos fluxos de logs. Isso é necessário para que os usuários possam monitorar o acesso ao sistema de arquivos do FSx for Windows File Server enviando registros de acesso de auditoria CloudWatch para o Logs.
- `firehose`— Permite que os diretores gravem registros em um Amazon Data Firehose. Isso é necessário para que os usuários possam monitorar o acesso ao sistema de arquivos FSx for Windows File Server enviando registros de acesso de auditoria para o Firehose.

Para ver as permissões dessa política, consulte a AmazonF SxFullAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonF SxConsoleFullAccess

É possível anexar a política `AmazonFSxConsoleFullAccess` a suas identidades do IAM.

Essa política concede permissões administrativas que permitem acesso total ao Amazon FSx e acesso a AWS serviços relacionados por meio do. AWS Management Console

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`: permite que as entidades principais realizem todas as ações no console de gerenciamento do Amazon FSx, exceto `BypassSnaplockEnterpriseRetention`.
- `cloudwatch`— Permite que os diretores visualizem CloudWatch alarmes e métricas no console de gerenciamento do Amazon FSx.
- `ds`— Permite que os diretores listem informações sobre um AWS Directory Service diretório.
- `ec2`
  - Permite que os diretores criem tags em tabelas de rotas, listem interfaces de rede, tabelas de rotas, grupos de segurança, sub-redes e a VPC associada a um sistema de arquivos Amazon FSx.
  - 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 listem aliases para AWS Key Management Service chaves.
- `s3`: permite que as entidades principais listem alguns ou todos os objetos em um bucket do Amazon S3 (até mil).
- `iam`: concede permissão para criar um perfil vinculado ao serviço que permite que o Amazon FSx execute ações em nome do usuário.

Para ver as permissões dessa política, consulte a AmazonF SxConsoleFullAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonF SxConsoleReadOnlyAccess

É possível anexar a política `AmazonFSxConsoleReadOnlyAccess` a suas identidades do IAM.

Essa política concede permissões somente de leitura ao Amazon FSx e AWS serviços relacionados para que os usuários possam visualizar informações sobre esses serviços no. AWS Management Console

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`: permite que as entidades principais visualizem informações sobre os sistemas de arquivos do Amazon FSx, incluindo todas as tags, no console de gerenciamento do Amazon FSx.
- `cloudwatch`— Permite que os diretores visualizem CloudWatch alarmes e métricas no Amazon FSx Management Console.

- `ds`— Permite que os diretores visualizem informações sobre um AWS Directory Service diretório no Amazon FSx Management Console.
- `ec2`
  - Permite que os diretores visualizem interfaces de rede, grupos de segurança, sub-redes e a VPC associada a um sistema de arquivos Amazon FSx no Amazon FSx Management Console.
  - Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança que podem ser usados com uma VPC.
- `kms`— Permite que os diretores visualizem aliases para AWS Key Management Service chaves no Amazon FSx Management Console.
- `log`— Permite que os diretores descrevam os grupos de log do Amazon CloudWatch Logs associados à conta que fez a solicitação. Isso é necessário para que as entidades principais possam visualizar a configuração de auditoria de acesso a arquivos existente para um sistema de arquivos do FSx para Windows File Server.
- `firehose`— Permite que os diretores descrevam os fluxos de entrega do Amazon Data Firehose associados à conta que fez a solicitação. Isso é necessário para que as entidades principais possam visualizar a configuração de auditoria de acesso a arquivos existente para um sistema de arquivos do FSx para Windows File Server.

Para ver as permissões dessa política, consulte a AmazonF SxConsoleReadOnlyAccess no Guia de referência de políticas AWS gerenciadas.

AWS política gerenciada: AmazonF SxReadOnlyAccess

É possível anexar a política `AmazonFSxReadOnlyAccess` a suas identidades do IAM.

Essa política concede permissões administrativas que permitem acesso somente leitura ao Amazon FSx.

- `fsx`: permite que as entidades principais visualizem informações sobre os sistemas de arquivos do Amazon FSx, incluindo todas as tags, no console de gerenciamento do Amazon FSx.
- `ec2`— Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança que podem ser usados com uma VPC.

Para ver as permissões dessa política, consulte a AmazonF SxReadOnlyAccess no Guia de referência de políticas AWS gerenciadas.

Atualizações do Amazon FSx para AWS políticas gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Amazon FSx desde que esse serviço começou a monitorar essas mudanças. Para receber alertas automáticos sobre alterações nesta página, assine o feed RSS na página Histórico do documento do Amazon FSx.

Alteração	Descrição	Data
AmazonF SxServiceRolePolicy — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	9 de janeiro de 2024
AmazonF SxReadOnlyAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	9 de janeiro de 2024
AmazonF SxConsoleReadOnlyAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	9 de janeiro de 2024

Alteração	Descrição	Data
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão, `ec2:GetSecurityGroupsForVpc` que permite que os diretores forneçam validação aprimorada de grupos de segurança de todos os grupos de segurança que podem ser usados com uma VPC.	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
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação de dados entre regiões e entre contas para sistemas de arquivos FSx for OpenZFS.	20 de dezembro de 2023
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação de dados entre regiões e entre contas para sistemas de arquivos FSx for OpenZFS.	20 de dezembro de 2023

Alteração	Descrição	Data
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação sob demanda de volumes para sistemas de arquivos FSx for OpenZFS.	26 de novembro de 2023
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação sob demanda de volumes para sistemas de arquivos FSx for OpenZFS.	26 de novembro de 2023
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os usuários visualizem, habilitem e desabilitem o suporte compartilhado de VPC para FSx para sistemas de arquivos ONTAP Multi-AZ.	14 de novembro de 2023
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os usuários visualizem, habilitem e desabilitem o suporte compartilhado de VPC para FSx para sistemas de arquivos ONTAP Multi-AZ.	14 de novembro de 2023

Alteração	Descrição	Data
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que ele gerencie as configurações de rede dos sistemas de arquivos do FSx para OpenZFS com várias AZs.	9 de agosto de 2023
AWS política gerenciada: AmazonF SxServiceRolePolicy — Atualização de uma política existente	O Amazon FSx modificou a `cloudwatch:PutMetricData` permissão existente para que o Amazon FSx publique métricas no namespace. CloudWatch `AWS/FSx`	24 de julho de 2023
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx atualizou a política para remover a permissão `fsx:*` e adicionar ações `fsx` específicas.	13 de julho de 2023
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx atualizou a política para remover a permissão `fsx:*` e adicionar ações `fsx` específicas.	13 de julho de 2023
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que ele gerencie as configurações de rede dos sistemas de arquivos do FSx para OpenZFS com várias AZs.	31 de maio de 2023

Alteração	Descrição	Data
AmazonF SxConsole ReadOnlyAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os usuários visualizem métricas de performance aprimoradas e ações recomendadas para sistemas de arquivos do FSx para Windows File Server no console do Amazon FSx.	21 de setembro de 2022
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os usuários visualizem métricas de performance aprimoradas e ações recomendadas para sistemas de arquivos do FSx para Windows File Server no console do Amazon FSx.	21 de setembro de 2022
AmazonF SxReadOnlyAccess — Iniciou a política de rastreamento	Essa política concede acesso somente leitura a todos os recursos do Amazon FSx e a qualquer tag associada a eles.	4 de fevereiro de 2022
AmazonF SxDeleteServiceLinkedRoleAccess — Iniciou a política de rastreamento	Essa política concede permissões administrativas que permitem que o Amazon FSx exclua o perfil vinculado ao serviço para acesso do Amazon S3.	7 de janeiro de 2022

Alteração	Descrição	Data
AmazonF SxServiceRolePolicy — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx gerencie configurações de rede para sistemas de arquivos Amazon FSx for ONTAP. NetApp	2 de setembro de 2021
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx crie tags nas tabelas de rotas do EC2 para chamadas com escopo reduzido.	2 de setembro de 2021
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx crie Amazon FSx para sistemas de arquivos ONTAP Multi-AZ. NetApp	2 de setembro de 2021
AmazonF SxConsole FullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx crie tags nas tabelas de rotas do EC2 para chamadas com escopo reduzido.	2 de setembro de 2021

Alteração	Descrição	Data
AmazonF SxServiceRolePolicy — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx descreva e grave 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 SxServiceRolePolicy — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que o Amazon FSx descreva e grave nos fluxos de entrega do Amazon Data Firehose. Isso é necessário para que os usuários possam visualizar os registros de auditoria de acesso a arquivos de um sistema de arquivos FSx for Windows File Server usando o Amazon Data Firehose.	8 de junho de 2021

Alteração	Descrição	Data
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os diretores descrevam e criem grupos de registros de CloudWatch registros, fluxos de registros e gravem eventos em fluxos de registros. Isso é necessário para que os diretores possam 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
AmazonF SxFullAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os diretores descrevam e gravem registros em um Amazon Data Firehose. Isso é necessário para que os usuários possam visualiza r os registros de auditoria de acesso a arquivos de um sistema de arquivos FSx for Windows File Server usando o Amazon Data Firehose.	8 de junho de 2021

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 Firehose existente ao configurar a auditoria de acesso a arquivos para um sistema de arquivos FSx for Windows File Server.	8 de junho de 2021

Alteração	Descrição	Data
AmazonF SxConsole ReadOnlyAccess — 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
AmazonF SxConsole ReadOnlyAccess — Atualização de uma política existente	O Amazon FSx adicionou novas permissões para permitir que os diretores descrevam os fluxos de entrega do Amazon Data Firehose associados à conta que fez a solicitação. Isso é necessário para que as entidades principais possam visualizar a configuração de auditoria de acesso a arquivos existente para um sistema de arquivos do FSx para Windows File Server.	8 de junho de 2021

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

Solução de problemas de identidade e acesso do Amazon FSx para Windows File Server

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 FSx

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `fsx:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao atributo *`my-example-widget`* usando a ação `fsx:`*`GetWidget`*.

Se 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 a função 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 de FSx

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da organização podem 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 essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Amazon FSx oferece suporte a esses recursos, consulte Como o Amazon FSx para Windows File Server 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.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em 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). Os usuários precisam ter permissão para aplicar tags aos recursos do Amazon FSx durante a criação.

Conceder permissão para marcar recursos durante a criação

Algumas ações da API do Amazon FSx para criação de recursos permitem que você especifique tags ao criar o recurso. É possível usar tags de recursos para implantar o controle de acesso por atributo (ABAC). Para obter mais informações, consulte O que é ABAC para a AWS? no Guia do usuário do IAM.

Para permitir que os usuários marquem recursos na criação, eles devem ter permissões para usar a ação que cria o recurso, como `fsx:CreateFileSystem` ou `fsx:CreateBackup`. Se as tags forem especificadas na ação resource-creating, a Amazon 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 a seguir demonstra uma política que permite aos usuários criar sistemas de arquivos e aplicar tags aos sistemas de arquivos durante a criação em um sistema específico Conta da AWS.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
```

```
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*"
    }
  ]
}
```

Da mesma forma, a política a seguir permite que os usuários criem backups em um sistema de arquivos específico e apliquem qualquer tag ao backup durante a criação do backup.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

A ação `fsx:TagResource` será avaliada somente se as tags forem aplicadas durante a ação resource-creating. Portanto, um usuário que tiver permissões para criar um recurso (pressupondo-se que não existam condições de marcação) não precisa 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 o uso de tags para controlar o acesso aos recursos do 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 aos recursos e ações do Amazon FSx, você pode usar políticas AWS Identity and Access Management (IAM) com base em tags. É possível conceder o controle de duas formas:

1. Controle o acesso aos recursos do Amazon FSx com base nas tags desses recursos.
2. Controlar 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 as ações que um usuário ou perfil pode executar em um recurso do Amazon FSx, você pode 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 política: criar um sistema de arquivos ao fornecer uma tag específica

Essa política permite que o usuário só crie um sistema de arquivos quando marcá-lo com um par de chave/valor de tag específico; neste exemplo, `key=Department, value=Finance`.

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example política: criar backups apenas dos sistemas de arquivos do Amazon FSx com uma tag específica

Essa política permite que os usuários criem backups somente de sistemas de arquivos marcados com o par de chave/valor `key=Department, value=Finance`, e o backup será criado com a tag `Deparment=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example política: criar um sistema de arquivos com uma tag específica de backups com uma tag específica

Essa política permite que os usuários só criem sistemas de arquivos marcados com `Department=Finance` por meio de backups marcados com `Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 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"
                }
            }
        }
    ]
}
```

Como usar perfis vinculados a serviço no Amazon FSx

O Amazon FSx for Windows File Server AWS Identity and Access Management usa funções vinculadas a serviços (IAM). Um perfil vinculado ao serviço é um tipo especial de perfil do IAM vinculado diretamente ao Amazon FSx. As funções vinculadas ao serviço são predefinidas pelo Amazon FSx e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Um perfil vinculado ao serviço facilita a configuração do Amazon FSx porque você não precisa adicionar as permissões necessárias manualmente. O Amazon FSx define as permissões dos perfis vinculados ao serviço e, a não ser que esteja definido de outra forma, somente o Amazon FSx poderá assumir os perfis. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus recursos do Amazon FSx, uma vez que você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham 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 o perfil vinculado ao serviço chamado `AWSServiceRoleForAmazonFSx`, que executa determinadas ações em sua conta, como a criação de interfaces de rede elásticas para seus sistemas de arquivos em sua VPC.

A política de permissões de função permite que o Amazon FSx conclua as seguintes ações em todos os recursos aplicáveis AWS :

Você não pode anexar o AmazonF SxServiceRolePolicy às suas entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite que o FSx gerencie AWS recursos em seu nome. Para ter mais informações, consulte Como usar perfis vinculados a serviço no Amazon FSx.

Para atualizações desta política, consulte Amazon F SxServiceRolePolicy

Essa política concede permissões administrativas que permitem que o FSx gerencie AWS recursos em nome do usuário.

Detalhes da permissão

As permissões de SxServiceRolePolicy função da AmazonF são definidas pela política gerenciada da SxServiceRolePolicy AWS AmazonF. A AmazonF SxServiceRolePolicy tem as seguintes permissões:

> **Note**
>
> O AmazonF SxServiceRolePolicy é usado por todos os tipos de sistema de arquivos Amazon FSx; algumas das permissões listadas podem não ser aplicáveis ao FSx for Windows.

- `ds`— Permite que o FSx visualize, autorize e não autorize aplicativos em seu diretório. AWS Directory Service
- `ec2`: permite que o 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 FSx publique pontos de dados métricos no CloudWatch namespace AWS /FSx.
- `route53`: permite que o FSx associe uma Amazon VPC a uma zona hospedada privada.
- `logs`— Permite que o 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 FSx descreva e grave nos fluxos de entrega do Amazon Data Firehose. Isso é para que os usuários possam publicar os registros de auditoria de acesso a arquivos de um sistema de arquivos FSx for Windows File Server em um stream de distribuição do Amazon Data Firehose.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
```

```
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
```

```
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
```

```
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Todas as atualizações dessa política estão descritas em Atualizações do Amazon FSx para AWS políticas gerenciadas.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado ao serviço. Para obter mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Como criar um perfil vinculado ao serviço para o Amazon FSx

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria um sistema de arquivos na 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 o perfil vinculado ao 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 da função usando o IAM. Para obter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Exclusão de um perfil vinculado ao serviço do Amazon FSx

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve excluir todos os seus sistemas de arquivos e backups para poder excluir manualmente o perfil vinculado ao serviço.

> **Note**
>
> Se o serviço do Amazon FSx estiver usando o perfil quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console, a CLI ou a API do IAM para excluir a função vinculada ao serviço . Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões com suporte para os perfis vinculados a serviço do Amazon FSx

O Amazon FSx fornece suporte ao uso de perfis vinculados ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

Validação de conformidade do Amazon FSx para Windows File Server

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 Windows File Server e endpoints da VPC da interface

Você pode aprimorar a postura de segurança da VPC ao configurar o Amazon FSx para usar um endpoint da VPC de interface. Os endpoints da VPC de interface são desenvolvidos pelo AWS PrivateLink, uma tecnologia que possibilita acessar APIs do Amazon FSx de forma privada sem um gateway da Internet, dispositivo NAT, conexão VPN ou conexão do AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para se comunicar com as APIs do Amazon FSx. O tráfego entre a VPC e o Amazon FSx não é realizado de forma externa à rede da AWS.

Cada endpoint da VPC de interface é representado por uma ou mais interfaces de rede elástica em suas sub-redes. Uma interface de rede fornece um endereço IP privado que serve como um ponto de entrada para o tráfego para a API do Amazon FSx.

Considerações sobre endpoints da VPC de interface do Amazon FSx

Antes de configurar um endpoint da VPC de interface para o Amazon FSx, certifique-se de consultar Interface VPC endpoint properties and limitations no Guia do usuário da Amazon VPC.

É possível chamar qualquer uma das operações de API do Amazon FSx usando sua VPC. Por exemplo, você pode criar um sistema de arquivos do FSx para Windows File Server chamando a API CreateFileSystem de dentro da VPC. Para obter a lista completa de APIs do Amazon FSx, consulte Actions na referência de APIs do Amazon FSx.

Considerações sobre emparelhamento de VPC

Você pode conectar outras VPCs à VPC com endpoints da VPC de interface usando o emparelhamento de VPC. O emparelhamento de VPC é uma conexão de rede entre duas VPCs. É possível estabelecer uma conexão de emparelhamento da VPC entre suas duas VPCs ou com uma VPC em outra Conta da AWS. As VPCs também podem estar em duas Regiões da AWS diferentes.

O tráfego entre VPCs emparelhadas permanece na rede da AWS e não passa pela Internet pública. Depois que as VPCs são emparelhadas, os recursos, como as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em ambas as VPCs, podem acessar a API do Amazon FSx por meio de endpoints da VPC de interface criados em uma das VPCs.

Como criar um endpoint da VPC de interface para a API do Amazon FSx

Você pode criar um endpoint da VPC para a API do Amazon FSx usando o console da Amazon VPC ou a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Creating an interface VPC endpoint no Guia do usuário da Amazon VPC.

Para criar um endpoint da VPC de interface para o Amazon FSx, use um dos seguintes:

- **`com.amazonaws.`*`region`*`.fsx`**: cria um endpoint para as operações de API do Amazon FSx.
- **`com.amazonaws.`*`region`*`.fsx-fips`**: cria um endpoint para a API do Amazon FSx que está em conformidade com o padrão Federal Information Processing Standard (FIPS) 140-2.

Para usar a opção de DNS privado, é necessário definir os recursos `enableDnsHostnames` e `enableDnsSupport` da sua VPC. Para obter mais informações, consulte Viewing and updating DNS support for your VPC no Guia do usuário da Amazon VPC.

Ao excluir as Regiões da AWS na China, se você habilitar o DNS privado para o endpoint, poderá realizar solicitações de API ao Amazon FSx com o endpoint da VPC usando o nome DNS padrão para a Região da AWS, por exemplo, `fsx.us-east-1.amazonaws.com`. Para as Regiões da AWS China (Pequim) e China (Ningxia), você pode realizar solicitações de API com o endpoint da VPC usando `fsx-api.cn-north-1.amazonaws.com.cn` e `fsx-api.cn-northwest-1.amazonaws.com.cn`, respectivamente.

Para obter mais informações, consulte Accessing a service through an interface VPC endpoint no Guia do usuário da Amazon VPC.

Como criar uma política de endpoint da VPC para o Amazon FSx

Para controlar ainda mais o acesso à API do Amazon FSx, como opção, é possível anexar uma política do AWS Identity and Access Management (IAM) ao endpoint da VPC. A política especifica o seguinte:

- A entidade principal que pode executar ações.
- As ações que podem ser executadas.
- Os recursos nos quais as ações podem ser realizadas.

Para obter mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Cotas

A seguir, você poderá entender sobre cotas quando trabalhar com o Amazon FSx para Windows File Server.

Tópicos

Cotas que podem ser aumentadas

Veja a seguir as cotas do Amazon FSx para Windows File Server para cada Conta da AWS e por Região da AWS que você pode aumentar.

Recurso	Padrão	Descrição
Sistemas de arquivos Windows	100	O número máximo de sistemas de arquivos do Amazon FSx para Windows Server que podem ser criados nessa conta.
Capacidade de throughput do Windows	10240	Capacidade de throughput total (em MBps) permitida para todos os sistemas de arquivos do Amazon FSx para Windows nessa conta.
Capacidade de armazenamento HDD do Windows	52428	Capacidade máxima de armazenamento HDD (em GiB) permitida para todos os sistemas de arquivos do

Recurso	Padrão	Descrição
		Amazon FSx para Windows File Server nessa conta.
Capacidade de armazenamento SSD do Windows	52428	Capacidade máxima de armazenamento SSD (em GiB) permitida para todos os sistemas de arquivos do Amazon FSx para Windows File Server nessa conta.
IOPS de SSD total do Windows	500.000	Quantidade total de IOPS de SSD permitida para todos os sistemas de arquivos do Amazon FSx para Windows File Server nessa conta.
Backups do Windows	500	Número máximo de backups iniciados pelo usuário para todos os sistemas de arquivos do Amazon FSx para Windows File Server que você pode ter nessa conta.

Para solicitar um aumento da cota

1. Abra o console do Service Quotas.
2. No painel de navegação, escolha Serviços da AWS.
3. Escolha Amazon FSx.
4. Escolha uma cota.
5. Escolha Solicitar aumento da cota e siga as instruções para solicitar um aumento da cota.
6. Para visualizar o status da solicitação de cota, escolha Histórico de solicitações de cota no painel de navegação do console.

Para obter mais informações, consulte Solicitando um Aumento de Cota no Guia do Usuário do Service Quotas.

Cotas de recursos para cada sistema de arquivos

Veja a seguir as cotas dos recursos do Amazon FSx para Windows File Server para cada sistema de arquivos em uma Região da AWS.

Recurso	Limite por sistema de arquivos
Número máximo de tags	50
Período máximo de retenção para backups automatizados	90 dias
Número máximo de solicitações de cópia de backup em andamento para uma única região de destino por conta.	5
Capacidade mínima de armazenamento, sistemas de arquivos SSD	32 GiB
Capacidade mínima de armazenamento, sistemas de arquivos HDD	2.000 GiB
Capacidade máxima de armazenamento, SSD e HDD	64 TiB
IOPS de SSD mínima	96
IOPS de SSD máxima	400.000
Capacidade de throughput mínima	8 MBps
Capacidade de throughput máxima	12.288 MBps
Número máximo de compartilhamentos de arquivos	100.000

Considerações adicionais

Além disso, observe o seguinte:

- É possível usar cada chave do AWS Key Management Service (AWS KMS) em até 125 sistemas de arquivos do Amazon FSx.
- Para obter uma lista de Regiões da AWS nas quais você pode criar sistemas de arquivos, consulte Amazon FSx Endpoints and Quotas na Referência geral da AWS.
- Mapeie os compartilhamentos de arquivos de instâncias do Amazon EC2 na nuvem privada virtual (VPC) com os nomes Domain Name Service (DNS - Serviço de Nomes de Domínio) deles.

Cotas específicas para o Microsoft Windows

Para obter mais informações, consulte limites de NTFS no Centro de Desenvolvimento do Microsoft Windows.

Solução de problemas do Amazon FSx

Use as seções a seguir como ajuda para solucionar problemas com o Amazon FSx.

Se você encontrar problemas não listados a seguir ao usar o Amazon FSx, tente fazer uma pergunta no fórum do Amazon FSx.

Tópicos

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 usando um cliente on-premises
- O novo sistema de arquivos não está registrado no DNS
- Não é possível acessar o sistema de arquivos usando um alias de DNS
- Não é possível acessar o sistema de arquivos usando um endereço IP

A interface de rede elástica do sistema de arquivos foi modificada ou excluída

Não é permitido modificar nem excluir a interface de rede elástica do sistema de arquivos. A modificação ou a exclusão da interface de rede pode causar uma perda permanente de conexão entre a VPC e o sistema de arquivos. Crie um novo sistema de arquivos e não modifique ou exclua a interface de rede elástica 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, métodos de acesso e ambientes compatíveis com o Amazon FSx para Windows File Server.

O grupo de segurança do sistema de arquivos não possui as regras de entrada ou saída 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 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.

Instância de computação não associada a um Active Directory

Suas instâncias de computação podem não estar associadas corretamente a um dos dois tipos de Active Directory:

- O AWS Managed Microsoft AD diretório ao qual seu sistema de arquivos está associado.
- Um diretório do Microsoft Active Directory que possui uma relação de confiança de floresta unidirecional estabelecida com o diretório AWS Managed Microsoft AD .

Certifique-se de que suas instâncias de computação estejam associadas a um dos dois tipos de diretório. Um tipo é o AWS Managed Microsoft AD diretório ao qual seu sistema de arquivos está associado. O outro tipo é um diretório do Microsoft Active Directory que tem uma relação de confiança de floresta unidirecional estabelecida com o AWS Managed Microsoft AD diretório. Para ter mais informações, consulte Usando o Amazon FSx com AWS Directory Service for Microsoft Active Directory.

O compartilhamento de arquivos não existe

O compartilhamento de arquivos do Microsoft Windows que você está tentando acessar não existe.

Se você estiver usando um compartilhamento de arquivos existente, certifique-se de que o nome DNS do sistema de arquivos e o nome do compartilhamento estejam especificados corretamente. Para gerenciar seus compartilhamentos de arquivos, consulte Gerenciando compartilhamentos de arquivos em sistemas de arquivos FSx for Windows File Server.

O usuário do Active Directory não possui as permissões necessárias

O usuário do Active Directory com o qual você está acessando o compartilhamento de arquivos não possui as permissões de acesso necessárias.

Certifique-se de que as permissões de acesso para o compartilhamento de arquivos e as listas de controle de acesso (ACLs) do Windows para a pasta compartilhada permitam o acesso aos usuários do Active Directory que precisam acessá-la.

Remoção do Permitir controle total de permissões de NTFS ACL

Se você remover Permitir controle total de permissões de NTFS ACL para o usuário SYSTEM em uma pasta compartilhada. Esse compartilhamento poderá se tornar inacessível e qualquer backup do sistema de arquivos feito a partir desse ponto poderá não ser utilizável.

Será necessário recriar o compartilhamento de arquivos afetado. Para ter mais informações, consulte Gerenciando compartilhamentos de arquivos em sistemas de arquivos FSx for Windows File Server. Depois de recriar a pasta ou o compartilhamento, você poderá mapear e usar os compartilhamentos de arquivos do Windows das instâncias de computação.

Não é possível acessar um sistema de arquivos usando um cliente on-premises

Você está usando seu sistema de arquivos Amazon FSx a partir do uso local AWS Direct Connect ou de uma VPN e está usando um intervalo de endereços IP não privado para o cliente local.

O Amazon FSx é compatível apenas com o acesso de clientes on-premises com endereços IP não privados em sistemas de arquivos criados após 17 de dezembro de 2020.

Se você precisar acessar seu sistema de arquivos do FSx para Windows File Server que foi criado antes de 17 de dezembro de 2020 usando um intervalo de endereços IP não privado, você pode criar um novo sistema de arquivos restaurando um backup do sistema de arquivos. Para ter mais informações, consulte Trabalhar com backups.

O novo sistema de arquivos não está registrado no DNS

Para sistemas de arquivos associados a um Active Directory autogerenciado, o Amazon FSx não registrou o DNS do sistema de arquivos quando ele foi criado porque a rede do cliente não usa o Microsoft DNS.

O Amazon FSx não registra sistemas de arquivos no DNS se a sua rede usar um serviço DNS de terceiros ao invés do Microsoft DNS. Você deve configurar manualmente as entradas DNS A para seus sistemas de arquivos do Amazon FSx. Para sistemas de arquivos single-AZ 1, será necessário adicionar uma entrada DNS A; para sistemas de arquivos single-AZ 2 e multi-AZ, será necessário adicionar duas entradas DNS A. Use o procedimento a seguir para obter o endereço ou endereços IP do sistema de arquivos a serem usados ao adicionar manualmente as entradas DNS A.

1. Em https://console.aws.amazon.com/fsx/, escolha o sistema de arquivos do qual você deseja obter o endereço IP para exibir a página de detalhes do sistema de arquivos.
2. Na guia Rede e segurança, siga um destes procedimentos:

   - Para um sistema de arquivos single-AZ 1:
     - No painel Sub-rede, escolha a interface de rede elástica mostrada em Interface de rede para abrir a página Interfaces de rede no Amazon EC2.

    - O endereço IP do sistema de arquivos single-AZ 1 a ser usado é mostrado na coluna IP IPv4 privado primário.
- Para um sistema de arquivos single-AZ 2 ou multi-AZ:
    - No painel Sub-rede preferencial, escolha a interface de rede elástica mostrada em Interface de rede para abrir a página Interfaces de rede no Amazon EC2.
    - O endereço IP da sub-rede preferencial a ser usada é mostrado na coluna IP IPv4 privado secundário.
    - No painel Sub-rede em espera do Amazon FSx, escolha a interface de rede elástica mostrada em Interface de rede para abrir a página Interfaces de rede no console do Amazon EC2.
    - O endereço IP da sub-rede em espera a ser usado é mostrado na coluna IP IPv4 privado secundário.

Não é possível acessar o sistema de arquivos usando um alias de DNS

Se não for possível acessar um sistema de arquivos usando um alias de DNS, use o procedimento a seguir para solucionar o problema.

1. Verifique se o alias está associado ao sistema de arquivos por meio de uma das etapas a seguir.

    a. Como usar o console do Amazon FSx: escolha o sistema de arquivos que você está tentando acessar. Na página Detalhes do sistema de arquivos, os aliases de DNS são mostrados na guia Rede e segurança.

    b. Usando a CLI ou a API — Use o comando `describe-file-system-aliases`CLI ou a operação da DescribeFileSystemAliasesAPI para recuperar os aliases atualmente associados ao sistema de arquivos.
2. Se o alias de DNS não estiver listado, você deverá associá-lo ao sistema de arquivos. Para ter mais informações, consulte Como gerenciar aliases de DNS em sistemas de arquivos atuais.
3. Se o alias de DNS estiver associado ao sistema de arquivos, verifique se você também configurou os seguintes itens necessários:

    - Foram criados nomes das entidades principais de serviço (SPNs) correspondentes ao alias de DNS no objeto de computador do Active Directory do sistema de arquivos do Amazon FSx.

      Para ter mais informações, consulte Etapa 2: configurar nomes das entidades principais de serviço (SPNs) para o Kerberos.

- Foi criado um registro DNS CNAME para o alias de DNS que é resolvido para o nome DNS padrão do sistema de arquivos do Amazon FSx.

  Para ter mais informações, consulte Etapa 3: atualizar ou criar um registro CNAME do DNS para o sistema de arquivos.

4. Se você criou SPNs válidos e um registro DNS CNAME, verifique se o DNS do cliente possui o registro DNS CNAME que é resolvido no sistema de arquivos correto.

   a. Execute `nslookup` para confirmar que o registro existe e que ele é resolvido para o nome DNS padrão do sistema de arquivos.

   b. Se o DNS CNAME for resolvido para outro sistema de arquivos, aguarde a atualização do cache do DNS do cliente e verifique novamente o registro CNAME. Você pode acelerar o processo ao liberar o cache de DNS do cliente usando o seguinte comando:

   ```
   ipconfig /flushdns
   ```

5. Se o registro DNS CNAME for resolvido para o DNS padrão do sistema de arquivos do Amazon FSx e o cliente ainda não conseguir acessar o sistema de arquivos, consulte Não é possível acessar o sistema de arquivos para acessar as etapas adicionais de solução de problemas.

Não é possível acessar o sistema de arquivos usando um endereço IP

Se não for possível acessar o sistema de arquivos usando um endereço IP, tente usar o nome DNS ou o alias de DNS associado.

Você pode encontrar o nome de DNS do sistema de arquivos e quaisquer aliases de DNS associados no console do Amazon FSx, selecionando Windows File Server, Rede e segurança. Ou você pode encontrá-los na resposta da operação CreateFileSystemou da DescribeFileSystemsAPI. Para obter mais informações sobre o uso de aliases de DNS, consulte Como gerenciar aliases de DNS.

- Para um sistema de arquivos Single-AZ associado a um Microsoft Active Directory AWS gerenciado, o nome DNS se parece com o seguinte.

  ```
  fs-0123456789abcdef0.ad-domain.com
  ```

- Para todos os sistemas de arquivos multi-AZ e sistemas de arquivos single-AZ unidos a um Active Directory autogerenciado, o nome DNS é semelhante ao seguinte:

```
amznfsxaa11bb22.ad-domain.com
```

Falha na criação de um novo sistema de arquivos Amazon FSx

Há várias causas possíveis para a falha de uma solicitação de criação de sistema de arquivos, conforme descrito na seção a seguir.

Tópicos

Solução de problemas de sistemas de arquivos associados a um AWS Managed Microsoft Active Directory

Use as seções a seguir para ajudar a solucionar problemas ao tentar criar um sistema de arquivos do FSx para Windows File Server associado ao seu Active Directory autogerenciado.

Grupo de segurança VPC e ACLs de rede mal configurados

Certifique-se de que os grupos de segurança da VPC e as ACLs da rede estejam configurados usando a configuração de grupo de segurança recomendada. Para obter mais informações, consulte Criação de grupos de segurança.

Falha na criação de um sistema de arquivos associado a um Active Directory autogerenciado

Tópicos

- O Amazon FSx não pode acessar a unidade organizacional (OU)
- A conta de serviço não consegue acessar o grupo de administradores
- O Amazon FSx perdeu a conectividade no domínio
- A conta de serviço não tem permissões corretas
- Caracteres Unicode usados nos parâmetros de criação

Nomes de grupos de administradores de sistemas de arquivos duplicados

A criação de um sistema de arquivos associado ao Active Directory autogerenciado apresenta falha com a seguinte mensagem de erro:

```
File system creation failed. Amazon FSx is unable to apply your Microsoft Active
 Directory configuration with the
specified file system administrators group. Please ensure that your Active Directory
 does not contain multiple domain
groups with the name: domain_group.
```

O Amazon FSx não criou o sistema de arquivos porque há vários grupos de administradores no domínio com o mesmo nome.

Se você não especificar um nome de grupo, o Amazon FSx tentará usar o valor padrão “Domain Admins” como grupo de administradores. A solicitação falhará se houver mais de um grupo usando o nome padrão “Administradores de domínio”.

Use as etapas a seguir para resolver o problema.

1. Analise os pré-requisitos para unir seu sistema de arquivos ao Active Directory autogerenciado.
2. Use a ferramenta de validação do Amazon FSx Active Directory para validar sua configuração autogerenciada do Active Directory antes de criar um sistema de arquivos FSx for Windows File Server associado a um Active Directory autogerenciado.
3. Crie um novo sistema de arquivos usando o AWS Management Console ou AWS CLI. Para ter mais informações, consulte Associar um sistema de arquivos do Amazon FSx a um domínio do Microsoft Active Directory autogerenciado.
4. Forneça um nome para o grupo de administradores do sistema de arquivos que seja exclusivo no domínio do seu Active Directory autogerenciado.

Servidores DNS ou controladores de domínio inacessíveis

A criação de um sistema de arquivos associado ao Active Directory autogerenciado apresenta falha com a seguinte mensagem de erro:

```
Amazon FSx can't reach the DNS servers provided or the domain controllers for your
 self-managed directory in Microsoft Active Directory.
File system creation failed. Amazon FSx is unable to communicate with your Microsoft
 Active Directory domain controllers.
This is because Amazon FSx can't reach the DNS servers provided or domain controllers
 for your domain.
To fix this problem, delete your file system and create a new one with valid DNS
 servers and networking configuration that allows
traffic from the file system to the domain controller.
```

Use as etapas a seguir para solucionar o problema.

1. Verifique se você seguiu os pré-requisitos para estabelecer a conectividade de rede e o roteamento entre a sub-rede em que está criando um sistema de arquivos do Amazon FSx e o Active Directory autogerenciado. Para ter mais informações, consulte Pré-requisitos para usar um Microsoft Active Directory autogerenciado.

   Use a Ferramenta de validação do Active Directory do Amazon FSx para testar e verificar essas configurações de rede.

   > **Note**
   >
   > Caso vários sites do Active Directory estejam definidos, certifique-se de que as sub-redes na VPC associadas ao seu sistema de arquivos do Amazon FSx estejam definidas em um site do Active Directory e que não haja conflitos de IP entre as sub-redes da sua VPC e as sub-redes dos outros sites. Você pode exibir e alterar essas configurações usando o snap-in do MMC de Serviços e Sites do Active Directory.

2. Verifique se você configurou os grupos de segurança da VPC que você associou ao seu sistema de arquivos do Amazon FSx, juntamente com quaisquer ACLs da rede da VPC, para permitir o tráfego de rede de saída em todas as portas.

> **Note**
>
> Se você quiser implantar o privilégio mínimo, você poderá permitir o tráfego de saída somente para as portas específicas necessárias para a comunicação com os controladores de domínio do Active Directory. Para obter mais informações, consulte a Documentação do Microsoft Active Directory.

3. Verifique se os valores do servidor de arquivos do Microsoft Windows ou das propriedades administrativas da rede não contêm caracteres non-Latin-1. Por exemplo, a criação do sistema de arquivos falhará se você usar `Domänen-Admins` como o nome do grupo de administradores do sistema de arquivos.
4. Verifique se os servidores DNS e os controladores de domínio do seu domínio do Active Directory estão ativos e podem responder a solicitações para o domínio fornecido.
5. Certifique-se de que o nível funcional de seu domínio do Active Directory seja o Windows Server 2008 R2 ou superior.
6. Certifique-se de que as regras de firewall nos controladores de domínio do seu domínio do Active Directory permitam o tráfego do seu sistema de arquivos do Amazon FSx. Para obter mais informações, consulte a Documentação do Microsoft Active Directory.

Credenciais inválidas da conta de serviço

A criação de um sistema de arquivos associado a um Active Directory autogerenciado falha com a seguinte mensagem de erro:

```
Amazon FSx is unable to establish a connection with your Microsoft Active Directory
 domain controllers
because the service account credentials provided are invalid. To fix this problem,
 delete your file
system and create a new one using a valid service account.
```

Use as etapas a seguir para solucionar o problema.

1. Verifique se você está inserindo apenas o nome de usuário como entrada para o Nome de usuário da conta de serviço, como `ServiceAcct`, na configuração do Active Directory autogerenciado.

> **Important**
>
> NÃO inclua um prefixo de domínio (`corp.com\ServiceAcct`) ou sufixo de domínio (`ServiceAcct@corp.com`) ao inserir o nome de usuário da conta de serviço.
> NÃO use o nome distinto (DN) ao inserir o nome de usuário da conta de serviço (CN=ServiceAcct, OU=exemplo, DC=corp, DC=com).

2. Verifique se a conta de serviço que você forneceu existe em seu domínio do Active Directory.
3. Certifique-se de que você delegou as permissões necessárias à conta de serviço que você forneceu. 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

   Para obter mais informações sobre como criar uma conta de serviço com as permissões corretas, consulte Delegar privilégios à conta de serviço Amazon FSx .

Permissões insuficientes da conta de serviço

A criação de um sistema de arquivos associado ao Active Directory autogerenciado apresenta falha com a seguinte mensagem de erro:

```
Amazon FSx is unable to establish a connection with your
Microsoft Active Directory domain controllers. This is because the service account
 provided does not
have permission to join the file system to the domain with the specified organizational
 unit.
To fix this problem, delete your file system and create a new one using a service
 account with
permission to join the file system to the domain with the specified organizational
 unit.
```

Use o procedimento a seguir para solucionar o problema.

- Certifique-se de que você delegou as permissões necessárias à conta de serviço que você forneceu. 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

  Para obter mais informações sobre como criar uma conta de serviço com as permissões corretas, consulte Delegar privilégios à conta de serviço Amazon FSx .

Capacidade da conta de serviço excedida

A criação de um sistema de arquivos associado ao Active Directory autogerenciado apresenta falha com a seguinte mensagem de erro:

```
Amazon FSx can't establish a connection with your Microsoft Active Directory
domain controllers. This is because the service account provided has reached the
maximum number of computers that it can join to the domain. To fix this problem,
delete your file system and create a new one, supplying a service account that
is able to join new computers to the domain.
```

Para resolver o problema, verifique se a conta de serviço que você forneceu atingiu o número máximo de computadores aos quais ela pode se associar ao domínio. Se ele tiver atingido o limite máximo, crie uma nova conta de serviço com as permissões corretas. Use a nova conta de serviço e crie um novo sistema de arquivos. Para ter mais informações, consulte Delegar privilégios à conta de serviço Amazon FSx .

O Amazon FSx não pode acessar a unidade organizacional (OU)

A criação de um sistema de arquivos associado ao Active Directory autogerenciado apresenta falha com a seguinte mensagem de erro:

```
Amazon FSx can't establish a connection with your Microsoft Active Directory domain
 controller(s).
```

```
This is because the organizational unit you specified either doesn't exist or isn't
 accessible
to the service account provided. To fix this problem, delete your file system and
 create a new one specifying an
organizational unit to which the service account can join the file system.
```

Use as etapas a seguir para solucionar o problema.

1. Verifique se a UO que você forneceu está em seu domínio do Active Directory.
2. Certifique-se de ter delegado as permissões necessárias à conta de serviço que você forneceu. A conta de serviço deve ser capaz de criar e excluir objetos de computador na UO do domínio ao qual você está associando o sistema de arquivos. A conta de serviço também precisa ter, no mínimo, 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
   - Ter controle delegado 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 Delegar privilégios à conta de serviço Amazon FSx .

A conta de serviço não consegue acessar o grupo de administradores

A criação de um sistema de arquivos associado ao Active Directory autogerenciado apresenta falha com a seguinte mensagem de erro:

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. This is
 because the file system
administrators group you provided either doesn't exist or isn't accessible to the
 service account you
provided. To fix this problem, delete your file system and create a new one specifying
 a file
system administrators group in the domain that is accessible to the service account
provided.
```

Use as etapas a seguir para solucionar o problema.

1. Certifique-se de que você está fornecendo apenas o nome do grupo como uma string para o parâmetro de grupo de administradores.

   > **Important**
   >
   > NÃO inclua um prefixo de domínio (`corp.com\FSxAdmins`) ou sufixo de domínio (`FSxAdmins@corp.com`) ao fornecer o parâmetro de nome de grupo.
   > NÃO use o nome distinto (DN) para o grupo. Um exemplo de nome distinto é CN=FSxAdmins, OU=example, DC=corp, DC=com.

2. Certifique-se de que o grupo de administradores fornecido exista no mesmo domínio do Active Directory ao qual você deseja associar o sistema de arquivos.
3. Se você não tiver fornecido um parâmetro de grupo de administradores, o Amazon FSx tentará usar o grupo `Builtin Domain Admins` em seu domínio do Active Directory. Se o nome desse grupo tiver sido alterado ou se você estiver usando um grupo diferente para a administração do domínio, será necessário fornecer esse nome para o grupo.

O Amazon FSx perdeu a conectividade no domínio

A criação de um sistema de arquivos associado ao Active Directory autogerenciado apresenta falha com a seguinte mensagem de erro:

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. To fix
 this problem, delete your file system and create a new one
meeting the pre-requisites described in the Amazon FSx user guide.
```

Ao criar seu sistema de arquivos, o Amazon FSx conseguiu acessar os servidores DNS e os controladores de domínio do seu domínio do Active Directory e associar o sistema de arquivos com êxito ao seu domínio do Active Directory. No entanto, ao concluir a criação do sistema de arquivos, o Amazon FSx perdeu a conectividade ou a associação ao seu domínio. Use as etapas a seguir para solucionar o problema.

1. Certifique-se de que a conectividade de rede continue existindo entre o sistema de arquivos do Amazon FSx e o Active Directory. Além disso, garanta que o tráfego de rede continue a ser permitido entre eles usando regras de roteamento, regras de grupo de segurança da VPC, ACLs da rede da VPC e regras de firewall do controlador de domínio.

2. Certifique-se de que os objetos de computador criados pelo Amazon FSx para os sistemas de arquivos no domínio do Active Directory ainda estejam ativos e não tenham sido excluídos ou manipulados de outra forma.

A conta de serviço não tem permissões corretas

A criação de um sistema de arquivos associado ao Active Directory autogerenciado apresenta falha com a seguinte mensagem de erro:

```
File system creation failed. Amazon FSx is unable to establish a connection with your
 Microsoft Active Directory domain controller(s).
This is because the service account provided does not have permission to join the file
 system to the domain with the specified
organizational unit (OU). To fix this problem, delete your file system and create a new
 one using a service account with permission
to create computer objects and reset passwords within the specified organizational
 unit.
```

Certifique-se de ter delegado as permissões necessárias à conta de serviço que você forneceu. Use as etapas a seguir para solucionar o problema.

A conta de serviço precisa ter, no mínimo, as seguintes permissões:

- Receber a delegação de controle para criar e excluir objetos de computador na UO à qual você está associando o sistema de arquivos
- Tenha as seguintes permissões na UO à qual você está associando o sistema de arquivos:
  - Capacidade de redefinir senhas
  - Capacidade de 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 (pode ser delegada) de criar e excluir objetos de computador
  - Capacidade validada para ler e gravar restrições de conta
  - Capacidade de modificar permissões

  Para obter mais informações sobre como criar uma conta de serviço com as permissões corretas, consulte Delegar privilégios à conta de serviço Amazon FSx.

Caracteres Unicode usados nos parâmetros de criação

A criação de um sistema de arquivos associado ao Active Directory autogerenciado apresenta falha com a seguinte mensagem de erro:

```
File system creation failed. Amazon FSx is unable to create a file system within the
 specified
Microsoft Active Directory. To fix this problem, please delete your file system and
 create a new one
meeting the pre-requisites described in the FSx for ONTAP User Guide.
```

O Amazon FSx não é compatível com caracteres Unicode. Verifique se nenhum dos parâmetros de criação possui caracteres Unicode, como acentos. Isso inclui parâmetros que podem ser deixados em branco, nos quais um valor padrão é preenchido automaticamente. Certifique-se de que os valores padrão correspondentes em seu Active Directory também não contenham caracteres Unicode.

Se você encontrar problemas não listados aqui ao usar o Amazon FSx, faça uma pergunta no Fórum do Amazon FSx ou entre em contato com o Suporte da Amazon Web Services.

O sistema de arquivos está em um estado de configuração incorreta

Um sistema de arquivos do FSx para Windows File Server pode entrar em um estado de Configuração incorreta devido a uma alteração no ambiente do Active Directory. Nesse estado, seu sistema de arquivos está indisponível no momento ou corre o risco de perder a disponibilidade, e os backups podem não ser bem-sucedidos.

O estado de Configuração incorreta inclui uma mensagem de erro e uma ação corretiva recomendada que você pode acessar usando o console do Amazon FSx, a API ou a AWS CLI. Depois de executar a ação corretiva, verifique se o estado do sistema de arquivos acaba mudando para `Available`. Observe que essa mudança pode levar vários minutos para ser concluída.

Seu sistema de arquivos pode entrar em um estado de Configuração incorreta por vários motivos, como os seguintes:

- Os endereços IP do servidor DNS não são mais válidos.
- As credenciais da conta de serviço não são mais válidas ou não têm as permissões necessárias.

- O controlador de domínio do Active Directory não pode ser acessado devido a problemas de conectividade de rede, como a invalidez dos grupos de segurança da VPC, da ACL de rede da VPC, da configuração da tabela de roteamento ou das configurações de firewall do controlador de domínio.

(Para obter a lista completa dos requisitos do Active Directory, consulte Pré-requisitos para usar um Microsoft Active Directory autogerenciado. Você também pode verificar se o seu ambiente do Active Directory está configurado corretamente para atender a esses requisitos ao usar a Ferramenta de validação do Active Directory do Amazon FSx).

Para resolver alguns desses problemas, é necessário atualizar diretamente um ou mais parâmetros na Configuração do Active Directory do seu sistema de arquivos, como alterar os endereços IP do servidor DNS ou alterar o nome de usuário ou a senha da conta de serviço. Nesses casos, sua ação corretiva envolverá necessariamente o uso do console Amazon FSx, da API AWS CLI ou a atualização dos parâmetros de configuração necessários.

Outros problemas podem não exigir a alteração de nenhum parâmetro de configuração do Active Directory, como a alteração das configurações do firewall do controlador de domínio ou dos grupos de segurança da VPC. Nesses casos, no entanto, você precisará tomar outras medidas antes que o sistema de arquivos possa se tornar `Available`. Depois de garantir que seu ambiente do Active Directory esteja configurado corretamente, selecione o botão Tentar recuperação ao lado do status de Configuração incorreta no console do Amazon FSx ou use o comando `StartMisconfiguredStateRecovery` no console do Amazon FSx, API ou AWS CLI.

Tópicos

- Sistema de arquivos com configuração incorreta: o Amazon FSx não consegue acessar os servidores DNS ou os controladores de domínio do seu domínio.
- Sistema de arquivos com configuração incorreta: as credenciais da conta de serviço são inválidas
- Sistema de arquivos com configuração incorreta: a conta de serviço fornecida não tem permissão para associar o sistema de arquivos ao domínio
- Sistema de arquivos com configuração incorreta: a conta de serviço não consegue associar mais computadores ao domínio
- Sistema de arquivos com configuração incorreta: a conta de serviço não tem acesso à UO

Sistema de arquivos com configuração incorreta: o Amazon FSx não consegue acessar os servidores DNS ou os controladores de domínio do seu domínio.

Um sistema de arquivos entrará em um estado de `Misconfigured` quando o Amazon FSx não conseguir se comunicar com seu controlador ou controladores de domínio do Microsoft Active Directory.

Para resolver essa situação, faça o seguinte:

1. Certifique-se de que sua configuração de rede permita o tráfego do sistema de arquivos para o controlador de domínio.
2. Use a Ferramenta de validação do Active Directory do Amazon FSx para testar e verificar as configurações de rede do seu Active Directory autogerenciado. Para ter mais informações, consulte Como usar o Amazon FSx com seu Microsoft Active Directory autogerenciado.
3. Revise a configuração do Active Directory autogerenciado do sistema de arquivos no console do Amazon FSx.
4. Para atualizar a configuração do Active Directory autogerenciado do sistema de arquivos, você pode usar o console do Amazon FSx.

   a. No painel de navegação, escolha Sistemas de arquivos e escolha o sistema de arquivos a ser atualizado; a página Detalhes do sistema de arquivos é exibida.

   b. Na página Detalhes do sistema de arquivos, selecione Atualizar na guia Rede e segurança.

   Você também pode usar o `update-file-system` comando CLI do Amazon FSx ou a operação de API. UpdateFileSystem

Sistema de arquivos com configuração incorreta: as credenciais da conta de serviço são inválidas

O Amazon FSx não consegue estabelecer uma conexão com seu controlador ou controladores de domínio do Microsoft Active Directory. Isso ocorre porque as credenciais da conta de serviço fornecidas são inválidas. Para ter mais informações, consulte Como usar o Amazon FSx com seu Microsoft Active Directory autogerenciado.

Para resolver a configuração incorreta, faça o seguinte:

1. Verifique se você está usando a conta de serviço correta e se está usando as credenciais corretas para essa conta.
2. Em seguida, atualize a configuração do sistema de arquivos com a conta de serviço ou as credenciais de conta corretas usando o console do Amazon FSx.

    a. No painel de navegação, escolha Sistemas de arquivos e escolha o sistema de arquivos com configuração incorreta a ser atualizado.

    b. Na página Detalhes do sistema de arquivos, selecione Atualizar na guia Rede e segurança.

    Também é possível usar a operação da API `update-file-system` do Amazon FSx. Para saber mais, consulte a UpdateFileSystemReferência da API Amazon FSx.

Sistema de arquivos com configuração incorreta: a conta de serviço fornecida não tem permissão para associar o sistema de arquivos ao domínio

O Amazon FSx não consegue estabelecer uma conexão com seus controladores de domínio do Microsoft Active Directory. Isso ocorre porque a conta de serviço fornecida não tem permissão para associar o sistema de arquivos ao domínio com a UO especificada.

Para resolver a configuração incorreta, faça o seguinte:

1. Adicione as permissões necessárias à conta de serviço do Amazon FSx ou crie uma nova conta de serviço com as permissões necessárias. Para obter mais informações sobre como fazer isso, consulte Delegar privilégios à conta de serviço Amazon FSx .
2. Em seguida, atualize a configuração do Active Directory autogerenciado do sistema de arquivos com as credenciais da nova conta de serviço. Para atualizar a configuração, você pode usar o console do Amazon FSx.

    a. No painel de navegação, escolha Sistemas de arquivos e escolha o sistema de arquivos a ser atualizado; a página Detalhes do sistema de arquivos é exibida.

    b. Na página Detalhes do sistema de arquivos, selecione Atualizar na guia Rede e segurança.

    Também é possível usar a operação da API `update-file-system` do Amazon FSx. Para saber mais, consulte a UpdateFileSystemReferência da API Amazon FSx.

Sistema de arquivos com configuração incorreta: a conta de serviço não consegue associar mais computadores ao domínio

O Amazon FSx não consegue estabelecer uma conexão com seus controladores de domínio do Microsoft Active Directory. Nesse caso, isso ocorre porque a conta de serviço fornecida atingiu o número máximo de computadores aos quais ela pode se associar ao domínio.

Para resolver a configuração incorreta, faça o seguinte:

1. Identifique outra conta de serviço ou crie uma nova conta de serviço que possa associar novos computadores ao domínio.
2. Em seguida, atualize a configuração do Active Directory autogerenciado do sistema de arquivos com as credenciais da nova conta de serviço usando o console do Amazon FSx.

    a. No painel de navegação, escolha Sistemas de arquivos e escolha o sistema de arquivos a ser atualizado; a página Detalhes do sistema de arquivos é exibida.

    b. Na página Detalhes do sistema de arquivos, selecione Atualizar na guia Rede e segurança.

    Também é possível usar a operação da API `update-file-system` do Amazon FSx. Para saber mais, consulte a UpdateFileSystemReferência da API Amazon FSx.

Sistema de arquivos com configuração incorreta: a conta de serviço não tem acesso à UO

O Amazon FSx não consegue estabelecer uma conexão com seus controladores de domínio do Microsoft Active Directory porque a conta de serviço fornecida não tem acesso à UO especificada.

Para resolver a configuração incorreta, faça o seguinte:

1. Identifique outra conta de serviço ou crie uma nova conta de serviço que tenha acesso à UO.
2. Em seguida, atualize a configuração do Active Directory autogerenciado do sistema de arquivos com as credenciais da nova conta de serviço.

    a. No painel de navegação, escolha Sistemas de arquivos e escolha o sistema de arquivos a ser atualizado; a página Detalhes do sistema de arquivos é exibida.

    b. Na página Detalhes do sistema de arquivos, selecione Atualizar na guia Rede e segurança.

Também é possível usar a operação da API `update-file-system` do Amazon FSx. Para saber mais, consulte a UpdateFileSystemReferência da API Amazon FSx.

Solução de problemas usando o PowerShell remoto no FSx para Windows File Server

Você pode administrar seus sistemas de arquivos FSx for Windows File Server usando comandos personalizados PowerShell de gerenciamento remoto.

Tópicos

O SxSmbShare comando New-F falha com confiança unidirecional

O Amazon FSx não suporta a execução do `New-FSxSmbShare` PowerShell comando nos casos em que você tem uma relação de confiança unidirecional e o domínio no qual o usuário reside não está configurado para confiar no domínio associado ao sistema de arquivos Amazon FSx.

Você pode resolver essa situação usando uma das seguintes soluções:

- O usuário que executa o comando `New-FSxSmbShare` precisa estar no mesmo domínio que o sistema de arquivos do FSx.
- Você pode usar a GUI fsmgmt.msc para criar compartilhamentos em seu sistema de arquivos. Para ter mais informações, consulte Gerenciando compartilhamentos de arquivos com a GUI de Pastas Compartilhadas.

Você não pode acessar seu sistema de arquivos usando o Remote PowerShell

Há várias causas possíveis para a incapacidade de se conectar ao seu sistema de arquivos usando o Remote PowerShell, cada uma com sua própria resolução, conforme a seguir.

Para primeiro garantir que você possa se conectar com êxito ao PowerShell Endpoint Remoto do Windows, você também pode executar um teste básico de conectividade. Por exemplo, é possível executar o comando `test-netconnection endpoint -port 5985`.

O grupo de segurança do sistema de arquivos não tem as regras de entrada necessárias para permitir uma conexão remota PowerShell

O grupo de segurança do sistema de arquivos deve ter uma regra de entrada que permita o tráfego na porta 5985 para estabelecer uma sessão remota PowerShell . Para ter mais informações, consulte Grupos de segurança da Amazon VPC.

Você tem uma relação de confiança externa configurada entre o Microsoft Active Directory AWS gerenciado e seu Active Directory local.

Para usar o Amazon FSx Remote PowerShell com autenticação Kerberos, você precisa configurar uma política de grupo local no cliente para a ordem de pesquisa na floresta. Para obter mais informações, consulte a documentação da Microsoft Configure Kerberos Forest Search Order (KFSO).

Ocorre um erro de localização de idioma ao tentar iniciar uma sessão remota PowerShell

Você precisa adicionar a seguinte `-SessionOption` ao seu comando: `-SessionOption (New-PSSessionOption -uiCulture "en-US")`

A seguir estão dois exemplos de uso `-SessionOption` ao iniciar uma PowerShell sessão remota em seu sistema de arquivos.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {fsx-command} -SessionOption
 (New-PSSessionOption -uiCulture "en-US")
```

```
PS C:\Users\delegateadmin> Enter-Pssession -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FsxRemoteAdmin -SessionOption (New-PSSessionOption -
uiCulture "en-US")
```

Não é possível configurar o DFS-R em um sistema de arquivos multi-AZ ou single-AZ 2

A Replicação do Sistema de Arquivos Distribuído (DFS-R) da Microsoft não é compatível com os sistemas de arquivos multi-AZ e single-AZ 2.

Os sistemas de arquivos multi-AZ são configurados nativamente para a redundância em várias zonas de acesso. Use o tipo de implantação multi-AZ para obter alta disponibilidade em várias zonas de disponibilidade. Para ter mais informações, consulte Disponibilidade e durabilidade: sistemas de arquivos single-AZ e multi-AZ.

Falha nas atualizações da capacidade de armazenamento ou capacidade de throughput

Há várias causas possíveis de falha nas solicitações de atualização da capacidade de armazenamento e da capacidade de throughput do sistema de arquivos, cada uma com sua própria solução.

O aumento da capacidade de armazenamento falha porque o Amazon FSx não consegue acessar a chave de criptografia do KMS do sistema de arquivos

Uma solicitação de aumento da capacidade de armazenamento falhou porque o Amazon FSx não conseguiu acessar a chave de criptografia do AWS Key Management Service (AWS KMS) do sistema de arquivos.

Você precisa garantir que o Amazon FSx tenha acesso à AWS KMS chave para executar a ação administrativa. Use as informações a seguir para resolver o problema de acesso à chave.

- Se a chave do KMS tiver sido excluída, você deverá criar um novo sistema de arquivos de um backup usando uma nova chave do KMS. Para ter mais informações, consulte Passo a passo 2: criar um sistema de arquivos de um backup. Você pode repetir a solicitação depois que o novo sistema de arquivos estiver disponível.
- Se a chave do KMS estiver desabilitada, habilite-a e tente novamente a solicitação de aumento da capacidade de armazenamento. Para obter mais informações, consulte Como ativar e desativar chaves no Guia do desenvolvedor do AWS Key Management Service .

- Se a chave for inválida devido à sua exclusão pendente, você deverá criar um novo sistema de arquivos de um backup usando uma nova chave do KMS. Você pode repetir a solicitação depois que o novo sistema de arquivos estiver disponível. Para ter mais informações, consulte Passo a passo 2: criar um sistema de arquivos de um backup.
- Se a chave for inválida devido à importação pendente, você deverá aguardar até que a importação seja concluída e, em seguida, tentar novamente a solicitação de aumento de armazenamento.
- Se o limite de concessões da chave tiver sido excedido, você deverá solicitar um aumento no número de concessões para a chave. Para obter mais informações, consulte Cotas de recursos no Guia do desenvolvedor do AWS Key Management Service . Quando o aumento da cota for concedido, tente novamente a solicitação de aumento de armazenamento.

A atualização da capacidade de armazenamento ou da capacidade de throughput falha porque o Active Directory autogerenciado está com a configuração incorreta

A solicitação de atualização da capacidade de armazenamento ou da capacidade de throughput falhou porque o Active Directory autogerenciado do seu sistema de arquivos está em um estado de configuração incorreta.

Para resolver o estado específico de configuração incorreta, consulte O sistema de arquivos está em um estado de configuração incorreta.

O aumento da capacidade de armazenamento falha devido à capacidade de throughput insuficiente

A solicitação de aumento da capacidade de armazenamento falhou porque a capacidade de throughput do sistema de arquivos está definida como 8 MB/s.

Aumente a capacidade de throughput do sistema de arquivos para um mínimo de 16 MB/s e, em seguida, tente novamente a solicitação. Para ter mais informações, consulte Como gerenciar a capacidade de throughput.

Falha na atualização da capacidade de throughput para 8 MB/s

Uma solicitação para modificar a capacidade de throughput de um sistema de arquivos para 8 MB/s falhou.

Isso pode ocorrer quando uma solicitação de aumento da capacidade de armazenamento está pendente ou em andamento. Os aumentos na capacidade de armazenamento exigem um throughput mínimo de 16 MB/s. Aguarde até que a solicitação de aumento da capacidade de armazenamento seja concluída e, em seguida, tente novamente a solicitação de modificação da capacidade de throughput.

Falha ao mudar o tipo de armazenamento para HDD durante a restauração de um backup

A criação de um sistema de arquivos de um backup apresenta falha com a seguinte mensagem de erro:

```
Switching storage type to HDD while creating a file system from backup backup_id is not supported because a storage scaling activity was still under way on the source file system to increase storage capacity from less than 2000 GiB when the backup backup_id was taken, and the minimum storage capacity for HDD storage is 2000 GiB.
```

Esse problema ocorre ao restaurar um backup e quando você alterou o tipo de armazenamento de SSD para HDD. A restauração a partir do backup falha porque o backup que você está restaurando foi feito enquanto um aumento da capacidade de armazenamento ainda estava em andamento no sistema de arquivos original. A capacidade de armazenamento do SSD do sistema de arquivos antes da solicitação de aumento era inferior a 2 mil GiB, a qual é a capacidade mínima de armazenamento necessária para criar um sistema de arquivos em HDD.

Use o procedimento a seguir para resolver esse problema.

1. Aguarde até que a solicitação de aumento da capacidade de armazenamento seja concluída e o sistema de arquivos tenha pelo menos 2 mil GiB de capacidade de armazenamento em SSD. Para ter mais informações, consulte Como monitorar os aumentos da capacidade de armazenamento.
2. Faça um backup do sistema de arquivos iniciado pelo usuário. Para ter mais informações, consulte Como trabalhar com backups iniciados pelo usuário.
3. Restaurar o backup iniciado pelo usuário em um novo sistema de arquivos usando o armazenamento em HDD. Para ter mais informações, consulte Como restaurar backups.

Solução de problemas com cópias de sombra

Há várias causas possíveis quando as cópias de sombra estão ausentes ou inacessíveis, conforme descrito na seção a seguir.

Tópicos

As cópias de sombra mais antigas estão ausentes

As cópias de sombra mais antigas são excluídas em qualquer uma dessas situações:

- Se você tiver 500 cópias de sombra, a próxima cópia de sombra substituirá a cópia de sombra mais antiga, independentemente do espaço restante alocado no volume de armazenamento para cópias de sombra.
- Se a quantidade máxima de armazenamento de cópias de sombra configurada for atingida, a próxima cópia de sombra substituirá uma ou mais das cópias de sombra mais antigas, mesmo que você tenha menos de 500 cópias de sombra.

Ambos os resultados são comportamentos esperados. Caso o armazenamento alocado para cópias de sombra seja insuficiente, considere aumentar o armazenamento alocado.

Todas as minhas cópias de sombra estão ausentes

Se a capacidade de performance de E/S for insuficiente em seu sistema de arquivos (por exemplo, porque você está usando o armazenamento em HDD, porque o armazenamento em HDD ficou sem capacidade de expansão ou porque a capacidade de throughput é insuficiente), todas as cópias de sombra poderão ser excluídas pelo Windows Server, pois ele não conseguirá manter as cópias de sombra com a capacidade de performance de E/S disponível. Considere as seguintes recomendações para ajudar a evitar esse problema:

- Se você estiver usando armazenamento em HDD, use o console Amazon FSx ou a API Amazon FSx para mudar para o uso do armazenamento SSD. Para ter mais informações, consulte Como gerenciar o tipo de armazenamento.

- Aumente a capacidade de throughput do sistema de arquivos para um valor três vezes maior do que a workload esperada.
- Certifique-se de que seu sistema de arquivos tenha pelo menos 320 MB de espaço livre, além da quantidade máxima de armazenamento de cópias de sombra configurada.
- Programe cópias de sombra para quando você esperar que o sistema de arquivos esteja ocioso.

Para ter mais informações, consulte Recomendações do sistema de arquivos para cópias de sombra.

Não é possível criar backups do Amazon FSx ou acessar cópias de sombra em um sistema de arquivos recentemente restaurado ou atualizado

Esse comportamento é esperado. O Amazon FSx reconstrói o estado da cópia de sombra em um sistema de arquivos restaurado recentemente e não permite o acesso a cópias de sombra ou backups durante a reconstrução do estado da cópia de sombra.

Solução de problemas de performance do sistema de arquivos

A performance do sistema de arquivos depende de vários fatores, inclusive do tráfego que você direciona para o sistema de arquivos, de como você provisiona o sistema de arquivos e de quaisquer recursos, como a Eliminação da duplicação dos dados ou Cópias de sombra, que estejam habilitados. Para obter informações sobre como entender a performance do seu sistema de arquivos, consulte Performance do FSx para Windows File Server.

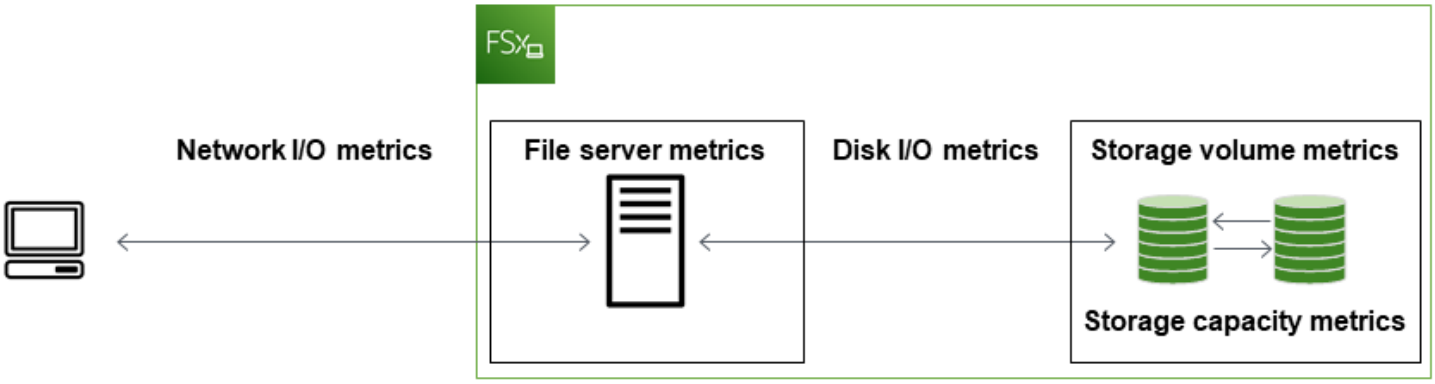
Tópicos

Como posso determinar os limites de throughput e IOPS do meu sistema de arquivos?

Para visualizar os limites de throughput e IOPS de um sistema de arquivos, consulte a tabela que mostra os níveis de performance com base na quantidade de capacidade de throughput provisionada.

Qual é a diferença entre E/S de rede e E/S de disco? Por que a E/S da minha rede é diferente da E/S do meu disco?

Os sistemas de arquivos do Amazon FSx incluem um ou mais servidores de arquivos que fornecem dados pela rede aos clientes que acessam o sistema de arquivos. Essa é a E/S de rede. O servidor de arquivos possui um cache na memória rápido para melhorar a performance dos dados acessados com mais frequência. Os servidores de arquivos também direcionam o tráfego para os volumes de armazenamento que hospedam os dados do sistema de arquivos. Essa é a E/S de disco. O diagrama a seguir ilustra a E/S de rede e de disco para um sistema de arquivos do Amazon FSx.



Para ter mais informações, consulte Monitoramento de métricas com a Amazon CloudWatch.

Por que o uso da CPU ou da memória está alto, mesmo quando a E/S de rede está baixa?

O uso da CPU e da memória do servidor de arquivos depende não apenas do tráfego de rede que você conduz, mas também dos atributos que você ativou no seu sistema de arquivos. A forma como você configura e programa esses atributos pode afetar a utilização da CPU e da memória.

Os trabalhos de eliminação de duplicação dos dados em andamento podem consumir memória. Você pode modificar a configuração dos trabalhos de eliminação de duplicação para reduzir os requisitos de memória. Por exemplo, você pode restringir a otimização a ser executada em

tipos de arquivos ou pastas específicos ou definir um tamanho e uma idade mínimos para a otimização. Também recomendamos configurar os trabalhos de eliminação de duplicação para serem executados durante períodos ociosos, quando há carga mínima no sistema de arquivos. Para ter mais informações, consulte Eliminação de duplicação de dados.

Caso a enumeração baseada em acesso esteja habilitada, você poderá observar uma alta utilização da CPU quando os usuários finais visualizarem ou listarem compartilhamentos de arquivos ou durante a fase de otimização de um trabalho de escalonamento de armazenamento. Para obter mais informações, consulte Ativar enumeração baseada em acesso em um namespace na Documentação de armazenamento da Microsoft.

O que é intermitência? Quanta intermitência meu sistema de arquivos está usando? O que acontece quando os créditos de intermitência se esgotam?

As workloads baseadas em arquivos são normalmente irregulares, caracterizadas por períodos curtos e intensos de alta E/S com tempo ocioso entre as intermitências. Para comportar esses tipos de workloads, além das velocidades de linha de base que um sistema de arquivos pode sustentar, o Amazon FSx oferece a capacidade de atingir velocidades mais altas por períodos de tempo, 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 para alocar o throughput e o IOPS com base na utilização média: os sistemas de arquivos acumulam créditos quando o uso do throughput e da IOPS está abaixo dos limites de linha de base e podem usar esses créditos para expandir acima dos limites de linha de base (até os limites de intermitência) quando necessário. Para obter mais informações sobre os limites e a duração da intermitência de seu sistema de arquivos, consulte Performance do FSx para Windows File Server.

Vejo um aviso na página Monitoramento e performance. Preciso alterar a configuração do meu sistema de arquivos?

A página Monitoramento e performance inclui avisos que indicam quando as demandas recentes de workload se aproximaram ou excederam os limites de recursos determinados pela forma como você configurou o sistema de arquivos. Isso não significa necessariamente que você precise alterar sua configuração, embora seu sistema de arquivos possa estar com provisionamento insuficiente para sua workload se você não executar a ação recomendada.

Se a workload que causou o aviso foi atípica e você não espera que ela continue, pode ser seguro não executar nenhuma ação e monitorar de perto sua utilização no futuro. No entanto, se a workload

que causou o aviso for típica e a expectativa for de que ela continue ou até mesmo se intensifique, recomendamos seguir as ações recomendadas para aumentar a performance do servidor de arquivos (aumentando a capacidade de throughput) ou aumentar a performance do volume de armazenamento (aumentando a capacidade de armazenamento ou mudando de HDD para SSD).

> **Note**
>
> Certos eventos do sistema de arquivos podem consumir recursos de performance de E/S de disco e potencialmente acionar avisos de performance. Por exemplo: .
>
> - A fase de otimização do dimensionamento da capacidade de armazenamento pode gerar maior throughput de disco, conforme descrito em Aumentos da capacidade de armazenamento e performance do sistema de arquivos
> - Para sistemas de arquivos multi-AZ, eventos como o escalonamento da capacidade de throughput, a substituição de hardware ou a interrupção da zona de disponibilidade resultam em eventos automáticos de failover e failback. Todas as alterações de dados que ocorrerem durante esse período precisam ser sincronizadas entre os servidores de arquivos primário e secundário, e o Windows Server executa um trabalho de sincronização de dados que pode consumir recursos de E/S do disco. Para ter mais informações, consulte Como gerenciar a capacidade de throughput.

Minhas métricas estavam temporariamente ausentes, devo me preocupar?

Os sistemas de arquivos single-AZ ficarão indisponíveis durante a manutenção do sistema de arquivos, a substituição de componentes da infraestrutura e quando uma zona de disponibilidade estiver indisponível. Durante esses períodos, as métricas não estarão disponíveis.

Em uma implantação multi-AZ, o Amazon FSx provisiona e mantém automaticamente um servidor de arquivos em espera em uma zona de disponibilidade diferente. Se houver uma manutenção no sistema de arquivos ou uma interrupção não planejada do serviço, o Amazon FSx faz o failover automaticamente para o servidor de arquivos secundário, o que permite que você continue acessando seus dados sem intervenção manual. Durante o breve período em que o seu sistema de arquivos está falhando e voltando a falhar, as métricas podem ficar temporariamente indisponíveis.

Mais informações

Esta seção fornece uma referência de recursos do Amazon FSx com suporte, mas obsoletos.

Tópicos

Como configurar uma programação de backup personalizada

Recomendamos usar AWS Backup para configurar um agendamento de backup personalizado para seu sistema de arquivos. As informações fornecidas aqui são para fins de referência se você precisar agendar backups com mais frequência do que ao usar AWS Backup.

Quando habilitado, o Amazon FSx para Windows File Server faz automaticamente um backup do seu sistema de arquivos, uma vez por dia, durante uma janela diária de backup. O Amazon FSx aplica um período de retenção especificado por você para esses backups automáticos. Além disso, ele oferece suporte a backups iniciados pelo usuário, para que você possa realizar backups a qualquer momento.

A seguir, você encontrará os recursos e a configuração para implantar a programação de backup personalizada. A programação de backup personalizada executa backups iniciados pelo usuário em um sistema de arquivos do Amazon FSx, em uma programação personalizada que você define. Os exemplos de programação podem ser uma vez a cada seis horas, uma vez por semana, e assim por diante. Este script também configura a exclusão de backups anteriores ao período de retenção especificado.

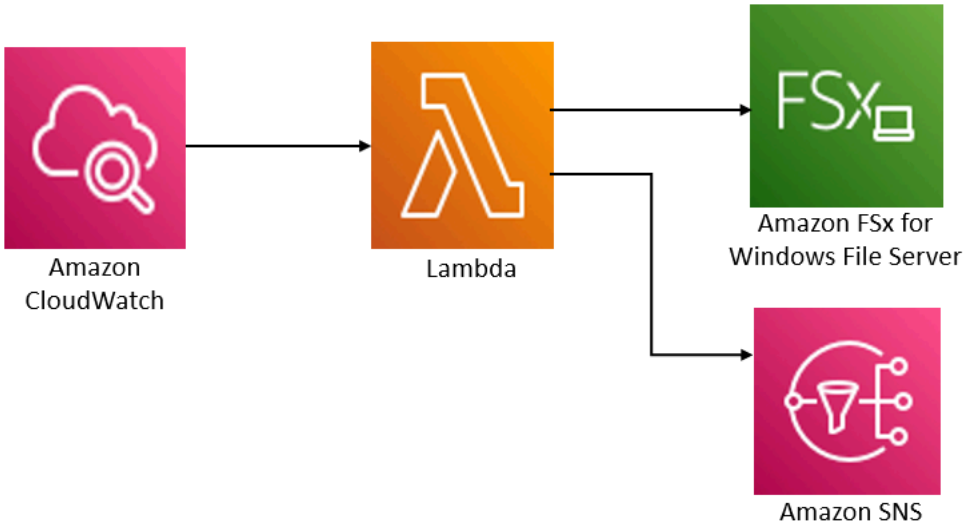
A solução implanta automaticamente todos os componentes necessários e considera os seguintes parâmetros:

- O sistema de arquivos
- Um padrão de programação CRON para realizar backups
- O período de retenção de backups (em dias)
- As tags de nome para backups

Para obter mais informações sobre os padrões de programação do CRON, consulte Expressões de programação para regras no Guia do CloudWatch usuário da Amazon.

Visão geral da arquitetura

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



Essa solução faz o seguinte:

1. O AWS CloudFormation modelo implanta um CloudWatch evento, uma função Lambda, uma fila do Amazon SNS e uma função do IAM. O perfil do IAM concede à função do Lambda permissão para invocar as operações de API do Amazon FSx.
2. O CloudWatch evento é executado em uma programação que você define como um padrão CRON, durante a implantação inicial. Esse evento invoca a função do Lambda do gerenciador de backup da solução, que invoca a operação `CreateBackup` da API do Amazon FSx para iniciar um backup.
3. O gerenciador de backup recupera uma lista de backups existentes que foram iniciados pelo usuário para o sistema de arquivos especificado usando `DescribeBackups`. Em seguida, ele exclui backups anteriores ao período de retenção especificado durante a implantação inicial.
4. O gerenciador de backup envia uma mensagem de notificação para a fila do Amazon SNS em caso de backup com êxito, caso escolha a opção de receber notificação durante a implantação inicial. Uma notificação é sempre enviada em caso de falha.

AWS CloudFormation modelo

Essa solução é usada AWS CloudFormation para automatizar a implantação da solução personalizada de agendamento de backup Amazon FSx. Para usar essa solução, baixe o modelo AWS CloudFormation fsx-scheduled-backup.template.

Implantação automatizada

O procedimento apresentado a seguir configura e implanta essa solução de programação de backup personalizada. A implantação demora cerca de cinco minutos. Antes de começar, você deve ter o ID de um sistema de arquivos Amazon FSx em execução em uma Amazon Virtual Private Cloud (Amazon VPC) em sua conta. AWS Para obter mais informações sobre como criar esses recursos, consulte Introdução ao Amazon FSx para Windows File Server.

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

Iniciar a pilha de soluções de backup personalizadas

1. Baixe o modelo AWS CloudFormation fsx-scheduled-backup.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). No momento, o Amazon FSx está disponível apenas em versões específicas. Regiões da AWS Você deve iniciar essa solução em uma região da AWS na qual o Amazon FSx esteja disponível. Para obter mais informações, consulte a seção do Amazon FSx de Regiões da AWS e endpoints na Referência geral da AWS.

2. Em Parâmetros, analise os parâmetros para o modelo e modifique-os de acordo com as necessidades do seu sistema de arquivos. Essa solução usa os valores padrão apresentados a seguir.

Parâmetro	Padrão	Descrição
ID do sistema de arquivos do Amazon FSx	Nenhum valor padrão	O ID do sistema de arquivos para o sistema de arquivos do qual você deseja realizar o backup.
Padrão de programação CRON para backups.	0 0/4 * * ? *	A programação para realizar o CloudWatch evento, acionando um novo backup e excluindo backups antigos fora do período de retenção.
Retenção de backup (dias)	30	O número de dias em que os backups iniciados pelo usuário serão mantidos. A função do Lambda exclui os backups iniciados pelo usuário que têm mais do que esse número de dias.
Nome para backups	Backups programados pelo usuário	O nome desses backups, que aparece na coluna Nome do backup do console de gerenciamento do Amazon FSx.
Notificações de backups	Sim	Escolha se deseja receber notificações quando os backups forem iniciados com êxito. Uma notificaç ão sempre será enviada se houver um erro.
Endereço de e-mail	Nenhum valor padrão	O endereço de e-mail para assinar as notificações do SNS.

3. 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.

Opções adicionais

Você pode usar a função do Lambda criada por essa solução para realizar backups programados personalizados de mais de um sistema de arquivos do Amazon FSx. O ID do sistema de arquivos é passado para a função Amazon FSx no JSON de entrada do evento. CloudWatch O JSON padrão passado para a função Lambda é o seguinte, onde os valores `FileSystemId` para `SuccessNotification` e são passados dos parâmetros especificados ao iniciar AWS CloudFormation a pilha.

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
}
```

Para programar backups para um sistema de arquivos Amazon FSx adicional, crie outra regra de CloudWatch evento. Você faz isso usando a origem do evento Programação, com a função do Lambda criada por essa solução como o destino. Escolha Constante (texto JSON) em Configurar entrada. Para a entrada JSON, basta substituir o ID do sistema de arquivos do Amazon FSx para fazer backup no lugar do `${FileSystemId}`. Além disso, substitua `Yes` ou `No` no lugar de `${SuccessNotification}` no JSON acima.

Quaisquer regras de CloudWatch eventos adicionais que você crie manualmente não fazem parte da pilha de soluções AWS CloudFormation de backup programado e personalizadas do Amazon FSx. Portanto, eles não serão removidos se você excluir a pilha.

Como usar a replicação do sistema de arquivos distribuído da Microsoft

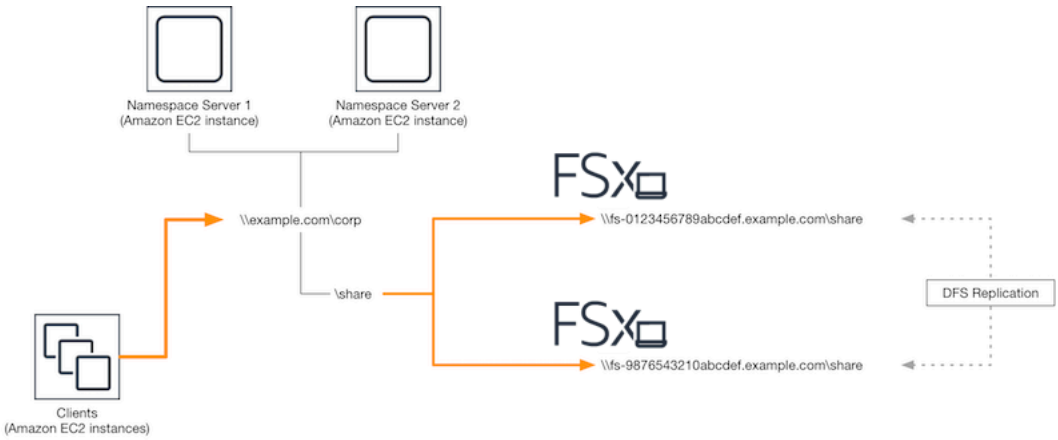
> **Note**
>
> Para implementar a alta disponibilidade de um FSx para Windows File Server, recomendamos o uso do multi-AZ do Amazon FSx. Para obter mais informações sobre o multi-AZ do Amazon FSx, consulte Disponibilidade e durabilidade: sistemas de arquivos single-AZ e multi-AZ

O Amazon FSx suporta o uso do Sistema de Arquivos Distribuído (DFS) da Microsoft para implantações de sistemas de arquivos em várias zonas de disponibilidade (AZs) para obter disponibilidade e durabilidade do multi-AZ. Ao usar a replicação do DFS, você pode replicar dados automaticamente entre dois sistemas de arquivos. Ao usar os namespaces do DFS, você pode configurar um sistema de arquivos como principal e outro como modo de espera, com failover automático para o modo de espera, se o principal deixar de responder.

Antes de usar a Replicação do DFS, execute as seguintes etapas:

- Configure seus grupos de segurança, conforme descrito no Step 8 de Conceitos básicos do Amazon FSx.
- Crie dois sistemas de arquivos Amazon FSx em diferentes AZs dentro de uma região. AWS Para obter mais informações sobre criar sistemas de arquivos, consulte Grave dados em seu compartilhamento de arquivos.
- Certifique-se de que os dois sistemas de arquivos estejam no mesmo AWS Directory Service for Microsoft Active Directory.
- Depois que o sistema de arquivos for criado, anote o ID do sistema de arquivos para uso posterior.

Nos tópicos a seguir, você pode encontrar uma descrição de como configurar e usar a replicação do DFS e o failover de namespaces do DFS entre AZs com o Amazon FSx.



Configurando a replicação do DFS

Você pode usar a replicação do DFS para replicar dados automaticamente entre dois sistemas de arquivos do Amazon FSx. Essa replicação é bidirecional, o que significa que você pode gravar em qualquer sistema de arquivos e as alterações são replicadas no outro.

> **Important**
>
> Você não pode usar a interface de usuário de gerenciamento do DFS nas Ferramentas Administrativas do Microsoft Windows (dfsmgmt.msc) para configurar a replicação do DFS no sistema de arquivos do FSx para Windows File Server.

Configurar a replicação do DFS (com script)

1. Comece o processo de gerenciamento do DFS iniciando sua instância e conectando-a ao Microsoft Active Directory, onde você se juntou aos seus sistemas de arquivos do Amazon FSx. 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 à sua instância como um usuário do Active Directory que é membro do grupo de administradores do sistema de arquivos. No AD AWS gerenciado, esse grupo é chamado de AWS Delegated FSx Administrators. No Microsoft AD autogerenciado, esse grupo é chamado de Administradores de domínio ou o nome personalizado do grupo de administradores que você forneceu durante a criação.

Esse usuário também deve ser membro de um grupo que tenha permissões de administração do DFS delegadas a ele. No AD AWS gerenciado, esse grupo é chamado de Administradores AWS Delegados de Sistemas de Arquivos Distribuídos. Em seu AD autogerenciado, esse usuário deve ser membro de Administradores de domínio ou de outro grupo ao qual você delegou permissões de administração do DFS.

Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.

3. Baixe o script PowerShell FSX-DFSR-Setup.ps1.
4. Abra o menu Iniciar e entre PowerShell. Na lista, escolha Windows PowerShell.
5. Execute o PowerShell script com os seguintes parâmetros especificados para estabelecer a replicação DFS entre seus dois sistemas de arquivos:

   - Os nomes do grupo e da pasta de Replicação do DFS
   - O caminho local para a pasta que você deseja replicar em seus sistemas de arquivos (por exemplo, `D:\share` para o compartilhamento padrão incluído no sistema de arquivos do Amazon FSx)
   - Os nomes DNS dos sistemas de arquivos principal e em espera do Amazon FSx que você criou nas etapas de pré-requisito

   Example

   ```
   FSx-DFSr-Setup.ps1 -group Group -folder Folder -path ContentPath -
   primary FSxFileSystem1-DNS-Name -standby FSxFileSystem2-DNS-Name
   ```

Configurar a replicação do DFS (passo a passo)

1. Comece o processo de gerenciamento do DFS iniciando sua instância e conectando-a ao Microsoft Active Directory, onde você se juntou aos seus sistemas de arquivos do Amazon FSx. 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 à sua instância como um usuário do Active Directory que é membro do grupo de administradores do sistema de arquivos. No AD AWS gerenciado, esse grupo é chamado de AWS Delegated FSx Administrators. No Microsoft AD autogerenciado, esse grupo é chamado de Administradores de domínio ou o nome personalizado do grupo de administradores que você forneceu durante a criação.

   Esse usuário também deve ser membro de um grupo que tenha permissões de administração do DFS delegadas a ele. No AD AWS gerenciado, esse grupo é chamado de Administradores AWS Delegados de Sistemas de Arquivos Distribuídos. Em seu AD autogerenciado, esse usuário deve ser membro de Administradores de domínio ou de outro grupo ao qual você delegou permissões de administração do DFS.

   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 entre PowerShell. Na lista, escolha Windows PowerShell.
4. Se você ainda não tiver instalado as ferramentas de gerenciamento do DFS, instale-as na instância com o comando a seguir.

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

5. No PowerShell prompt, crie um grupo e uma pasta de Replicação DFS com os seguintes comandos.

```
$Group = "Name of the DFS Replication group"
$Folder = "Name of the DFS Replication folder"

New-DfsReplicationGroup –GroupName $Group
New-DfsReplicatedFolder –GroupName $Group –FolderName $Folder
```

6. Determine o nome do computador do Active Directory associado a cada sistema de arquivos com os comandos a seguir.

```
$Primary = "DNS name of the primary FSx file system"
$Standby = "DNS name of the standby FSx file system"

$C1 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -
eq 'HOST/$Primary'").Name
$C2 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -
eq 'HOST/$Standby'").Name
```

7. Adicione seus sistemas de arquivos como membros do grupo de replicação do DFS que você criou com os seguintes comandos.

```
Add-DfsrMember -GroupName $Group -ComputerName $C1
Add-DfsrMember -GroupName $Group -ComputerName $C2
```

8. Use os comandos a seguir para adicionar o caminho local (por exemplo,`D:\share`) para cada sistema de arquivos ao grupo de replicação do DFS. Nesse procedimento, o *`file system 1`* serve como membro principal, o que significa que seu conteúdo inicialmente é sincronizado com o outro sistema de arquivos.

```
$ContentPath1 = "Local path to the folder you want to replicate on file system 1"
$ContentPath2 = "Local path to the folder you want to replicate on file system 2"

Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath1
 -ComputerName $C1 -PrimaryMember $True
Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath2
 -ComputerName $C2 -PrimaryMember $False
```

9. Adicione uma conexão entre os sistemas de arquivos com o comando a seguir.

```
Add-DfsrConnection -GroupName $Group -SourceComputerName $C1 -
DestinationComputerName $C2
```

Em minutos, os dois sistemas de arquivos devem começar a sincronizar o conteúdo do `ContentPath` anterior especificado.

Configurar namespaces do DFS para failover

Você pode usar namespaces do DFS para tratar um sistema de arquivos como principal e o outro como em espera. Ao fazer isso, você pode configurar o failover automático para o modo de espera, se o principal parar de responder. Os namespaces do DFS permitem agrupar pastas compartilhadas em servidores diferentes em um único namespace, onde um único caminho de pasta pode levar a arquivos armazenados em vários servidores. Os namespaces do DFS são gerenciados por servidores de namespace DO DFS, que direcionam instâncias de computação mapeando uma pasta de namespace DO DFS para os servidores de arquivos apropriados.

Configurar os namespaces do DFS para failover (IU)

1. Se você ainda não tiver servidores de Namespace DFS em execução, inicie um par de servidores de Namespace DFS altamente disponíveis usando o modelo Setup-DFSN-Servers.template. AWS CloudFormation 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.
2. Conecte-se a um dos servidores de namespace DFS iniciados na etapa anterior como usuário no grupo Administradores AWS Delegados. Para obter mais informações, consulte Conectando-se à sua instância do Windows no Guia do usuário do Amazon EC2.
3. Abra o Console de gerenciamento do DFS. Abra o menu Iniciar e execute `dfsmgmt.msc`. Essa ação abre a ferramenta GUI de gerenciamento do DFS.
4. Em Ação, escolha Novo namespace e digite o nome do computador do primeiro servidor de namespace do DFS que você iniciou em Servidor e escolha Próximo.
5. Em Nome, insira o namespace que você está criando (por exemplo, **`corp`**).
6. Escolha Editar configurações e defina as permissões apropriadas com base em seus requisitos. Selecione Next (Próximo).
7. Mantenha as opções Namespace com base em domínio e Habilitar modo do Windows Server 2008 selecionadas e escolha Próximo.

   > **Note**
   >
   > O modo Windows Server 2008 é a opção mais recente disponível para namespaces.

8. Analise as configurações do namespace e escolha Criar.
9. Com o namespace recém-criado selecionado em Namespaces na barra de navegação, escolha Ação, em seguida, Adicionar servidor de namespace.
10. Em Servidor de namespace, insira o nome do computador do segundo servidor de namespace do DFS que você iniciou.
11. Escolha Editar configurações, defina as permissões apropriadas com base em seus requisitos e escolha OK.
12. Escolha Adicionar, insira o nome do UNC do compartilhamento de arquivos no sistema de arquivos principal do Amazon FSx (por exemplo *`fs-0123456789abcdef0`*.example.com *`share`*) para Caminho para a pasta de destino e escolha OK.

13. Escolha Adicionar, insira o nome do UNC do compartilhamento do arquivo no sistema de arquivos em espera do Amazon FSx (por exemplo, *fs-fedbca9876543210f*.example.com *share*) para Caminho para a pasta de destino e escolha OK.
14. Na janela Nova pasta, escolha OK. A nova pasta é criada com os dois destinos de pasta em seu namespace.
15. Repita as três últimas etapas para cada compartilhamento de arquivos que você deseja adicionar ao namespace.

Para configurar namespaces DFS para failover () PowerShell

1. Se você ainda não tiver servidores de Namespace DFS em execução, inicie um par de servidores de Namespace DFS altamente disponíveis usando o modelo Setup-DFSN-Servers.template. AWS CloudFormation 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.
2. Conecte-se a um dos servidores de namespace do DFS iniciados na etapa anterior como usuário no grupo de Administradores delegados da AWS . 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 entre PowerShell. O Windows PowerShell aparece na lista de correspondências.
4. Abra o menu de contexto (clique com o botão direito do mouse) do Windows PowerShell e escolha Executar como administrador.
5. Se você ainda não tiver instalado as ferramentas de gerenciamento do DFS, instale-as em sua instância com o comando a seguir.

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

6. Se você ainda não tiver um namespace DFS existente, você pode criar um usando os seguintes comandos. PowerShell

```
$NSS1 = computer name of the 1st DFS Namespace server
$NSS2 = computer name of the 2nd DFS Namespace server

$DNSRoot = fully qualified Active Directory domain name (e.g. mydomain.com)
$Namespace = Namespace name you want to use
$Folder = Folder path you want to use within the Namespace
$FS1FolderTarget = Share path to Folder Target on File System 1
```

```
$FS2FolderTarget = Share path to Folder Target on File System 2

$NSS1,$NSS2 | ForEach-Object { Invoke-Command -ComputerName $_ -ScriptBlock { mkdir
 "C:\DFS\${using:Namespace}";
New-SmbShare -Name ${using:Namespace} -Path "C:\DFS\${using:Namespace}" } }

New-DfsnRoot -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS1}.${DNSRoot}\
${Namespace}" -Type DomainV2
New-DfsnRootTarget -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS2}.
${DNSRoot}\${Namespace}"
```

7. Para criar uma pasta no seu Namespace DFS, você pode usar o comando a seguir. PowerShell Isso cria uma pasta que direciona as instâncias de computação que acessam a pasta para seu sistema de arquivos principal do Amazon FSx por padrão.

```
$FS1 = DNS name of primary FSx file system
New-DfsnFolder -Path "\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath "\\${FS1}\
${FS1FolderTarget}" -EnableTargetFailback $True -ReferralPriorityClass GlobalHigh
```

8. Adicione seu sistema de arquivos do Amazon FSx em espera à mesma pasta de namespace do DFS. As instâncias de computação que acessam a pasta retornam a esse sistema de arquivos se não conseguirem se conectar ao sistema de arquivos principal do Amazon FSx.

```
$FS2 = DNS name of secondary FSx file system
New-DfsnFolderTarget -Path "\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath "\\
${FS2}\${FS2FolderTarget}"
```

Agora você pode acessar seus dados de instâncias de computação usando o caminho remoto da pasta namespace do DFS especificado anteriormente. Isso direciona as instâncias de computação para o sistema de arquivos principal do Amazon FSx (e para o sistema de arquivos em espera, se o principal não estiver respondendo).

Por exemplo, abra o menu Iniciar e insira `PowerShell`. Na lista, escolha `Windows PowerShell` e execute o comando a seguir.

```
net use Z: \\${DNSRoot}\${Namespace}\${Folder} /persistent:yes
```

Trabalhar com janelas de manutenção e multi-AZ do FSx

Para ajudar a garantir a alta disponibilidade da implantação do sistema de arquivos multi-AZ, recomendamos que você escolha janelas de manutenção não sobrepostas para os dois sistemas de arquivos do Amazon FSx em sua implantação multi-AZ. Isso ajuda a garantir que os dados do arquivo continuem disponíveis para suas aplicações e usuários durante as janelas de manutenção do sistema.

> **Note**
>
> Para permitir o tráfego de replicação do DFS de e para os sistemas de arquivos, certifique-se de adicionar regras de entrada e saída do grupo de segurança da VPC, conforme descrito em Grupos de segurança da Amazon VPC.

Histórico do documento

- Versão da API: 1/3/2018
- Última atualização da documentação: 17 de janeiro de 2024

A tabela a seguir descreve as alterações importantes feitas no Guia do usuário do Windows do Amazon FSx. Para receber notificações sobre atualizações da documentação, inscreva-se no feed RSS.

Alteração	Descrição	Data
Support adicionado para níveis mais altos de IOPS em sistemas de arquivos com capacidades de taxa de transferência de 4 Gb/s ou mais	O FSx for Windows File Server está aumentando o IOPS máximo de 130 mil para 150 mil para sistemas de arquivos com capacidade de taxa de transferência de 4 Gb/s ou mais, de 175 mil para 200 mil para sistemas de arquivos com capacidade de transferência de 6 Gb/s ou mais, de 260 mil para 300 mil para sistemas de arquivos com capacidade de transferência de 9 Gb/s ou superior e de 350 mil para 400 mil para sistemas de arquivos com 12 Gb/s de taxa de transferência capacidade de produção ou superior. Para obter mais informações, consulte FSx for Windows File Server performance.	17 de janeiro de 2024
O Amazon FSx atualizou as políticas gerenciadas	O Amazon FSx atualizou as políticas AmazonF,	9 de janeiro de 2024

do AmazonFSxFullAcces s, AmazonF, AmazonFSx ConsoleFullAccess, AmazonF e SxReadOnlyAccess AmazonF SxConsole ReadOnlyAccess SxService RolePolicy AWS	AmazonFSxFullAccess, AmazonFSxConsoleFu llAccess, AmazonF e AmazonF para SxReadOnl yAccess adicionar a permissãoSxConsole ReadOnlyAccess. SxService RolePolicy `ec2:GetSe curityGroupsForVpc` Para obter mais informaçõ es, consulte as atualizações do Amazon FSx para políticas AWS gerenciadas.	
O Amazon FSx atualizou as políticas gerenciadas do AmazonF SxFullAccess e do AmazonF SxConsoleFullAcces s AWS	O Amazon FSx atualizou as políticas do AmazonF SxFullAccess e do AmazonF para adicionar a açãoSxCon soleFullAccess . `ManageCro ssAccountDataRepli cation` Para obter mais informações, consulte as atualizações do Amazon FSx para políticas AWS gerenciad as.	20 de dezembro de 2023
O Amazon FSx atualizou as políticas gerenciadas do AmazonF SxFullAccess e do AmazonF SxConsoleFullAcces s AWS	O Amazon FSx atualizou as políticas do AmazonF SxFullAccess e do AmazonF para adicionar a permissão . SxConsoleFullAccess `fsx:CopySnapshotAn dUpdateVolume` 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 atualizar o tipo de armazenamento do sistema de arquivos	Os sistemas de arquivos do FSx para Windows File Server agora são compatíveis com a atualização do tipo de armazenamento HDD para o tipo de armazenamento SSD. Para obter mais informações, consulte Managing storage type.	9 de agosto de 2023
Suporte adicionado para capacidade de throughput máxima	Os sistemas de arquivos do FSx para Windows File Server agora são compatíveis com capacidade de throughput de até 12 GBps. Para obter mais informações, consulte FSx for Windows File Server performance.	9 de agosto de 2023

Suporte adicionado para provisionamento de IOPS de SSD	Os sistemas de arquivos do FSx para Windows File Server agora são compatíveis com o provisionamento de IOPS de SSD, independentemente da capacidade de armazenamento, até um máximo de 350 mil IOPS. Para obter mais informações, consulte Managing SSD IOPS.	9 de agosto de 2023
O Amazon FSx atualizou a política gerenciada do SxServiceRolePolicy AWS AmazonF	O Amazon FSx atualizou a `cloudwatch:PutMetricData` permissão no AmazonF. SxServiceRolePolicy Para obter mais informações, consulte AmazonF SxServiceRolePolicy.	24 de julho de 2023
O Amazon FSx atualizou a política gerenciada do SxFullAccess AWS AmazonF	O Amazon FSx atualizou a SxFullAccess política da AmazonF para remover a `fsx:*` permissão e adicionar ações específicas. `fsx` Para obter mais informações, consulte a política da Amazon SxFullAccess.	13 de julho de 2023
O Amazon FSx atualizou a política gerenciada do SxConsoleFullAccess AWS AmazonF	O Amazon FSx atualizou a SxConsoleFullAccess política da AmazonF para remover a `fsx:*` permissão e adicionar ações específicas. `fsx` Para obter mais informações, consulte a política da Amazon SxConsoleFullAccess.	13 de julho de 2023

Support adicionado para novas CloudWatch métricas do Amazon FSx for Windows File Server	O FSx for Windows File Server agora fornece métricas CloudWatch adicionais que monitoram o desempenho e o uso da capacidade do servidor de arquivos e do volume de armazenamento. Para obter mais informações, consulte Métricas e dimensões.	22 de setembro de 2022
Suporte adicionado para avisos de performance do sistema de arquivos	O Amazon FSx agora fornece avisos na janela de desempenho e monitoramento quando qualquer um de um conjunto de CloudWatch métricas se aproxima ou ultrapassa limites predeterminados para essas métricas. Cada aviso também fornece uma recomendação prática para melhorar o performance do sistema de arquivos. Para obter mais informações, consulte Performance warnings and recommendations.	22 de setembro de 2022

Suporte adicionado para monitoramento aprimorado da performance do sistema de arquivos	O painel de monitoramento do sistema de arquivos do console do Amazon FSx para sistemas de arquivos do FSx para Windows File Server inclui as novas seções Resumo, Armazenamento e Performance. Essas seções exibem gráficos de novas CloudWatch métricas que fornecem um monitoramento aprimorado do desempenho. Para obter mais informações, consulte Monitoramento de métricas com CloudWatch.	22 de setembro 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 o Amazon Kendra	Agora você pode usar seu sistema de arquivos do FSx para Windows File Server como uma fonte de dados para o Amazon Kendra, permitindo indexar e pesquisar informações contidas em documentos armazenados em seu sistema de arquivos. Para obter mais informaçõ es, consulte Using FSx for Windows File Server with Amazon Kendra.	26 de março de 2022
Suporte adicionado para auditoria de acesso a arquivos	Agora você pode habilitar a auditoria de acessos de usuários finais em arquivos, pastas e compartilhamentos de arquivos. Você pode optar por enviar registros de eventos de auditoria para os serviços Amazon CloudWatch Logs ou Amazon Data Firehose. Para obter mais informações, consulte File access auditing.	8 de junho de 2021
Suporte adicionado para cópia de backups	Agora você pode usar o Amazon FSx para copiar backups dentro da mesma AWS conta para outra Região da AWS (cópias entre regiões) ou dentro da mesma Região da AWS (cópias dentro da região). Para obter mais informações, consulte Copying backups.	12 de abril de 2021

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 capacidade atingir um limite especificado por você. Para obter mais informações, consulte Como aumentar a capacidade de armazenamento de forma dinâmica.	17 de fevereiro de 2021
Suporte adicionado para acesso de clientes usando endereços IP não privados	Você pode acessar os sistemas de arquivos do FSx para Windows File Server com clientes on-premises usando endereços IP não privados. Para obter mais informações, consulte Supported environments. Você pode associar o sistema de arquivos do FSx para Windows File Server a um Microsoft Active Directory autogerenciado com servidores DNS e controladores de domínio do AD que usam endereços IP não privados. Para obter mais informações, consulte Using Amazon FSx with Your Self-Managed Microsoft Active Directory.	17 de dezembro de 2020

Suporte adicionado para usar aliases de DNS	Agora você pode associar aliases de DNS aos seus sistemas de arquivos do FSx para Windows File Server que você pode usar para acessar os dados em seu sistema de arquivos. Para obter mais informações, consulte Managing DNS aliases e Walkthrough 5: Using DNS aliases to access your file system.	9 de novembro de 2020
Suporte adicionado para o Amazon Elastic Container Service	Agora você pode usar o FSx para Windows File Server com o Amazon ECS. Para obter mais informações, consulte Supported Clients.	9 de novembro de 2020
O Amazon FSx agora está integrado com AWS Backup	Agora você pode usá-lo AWS Backup para fazer backup e restaurar seus sistemas de arquivos FSx, além de usar backups nativos do Amazon FSx. Para obter mais informações, consulte Using AWS Backup with Amazon FSx.	9 de novembro de 2020

Suporte adicionado para a escalabilidade da capacidade de throughput	Agora você pode modificar a capacidade de throughput dos sistemas de arquivos do FSx para Windows File Server existentes à medida que seus requisitos de throughput evoluem. Para obter mais informações, consulte Como gerenciar a capacidade de throughput.	1 de junho de 2020
Suporte adicionado para escalabilidade da capacidade de armazenamento	Agora você pode aumentar a capacidade de armazenamento dos sistemas de arquivos do FSx para Windows File Server existentes à medida que seus requisitos de armazenamento evoluem. Para obter mais informações, consulte Managing Storage Capacity.	1 de junho de 2020
Suporte adicionado para armazenamento em unidade de disco rígido (HDD)	O armazenamento em HDD oferece flexibilidade de preço e performance ao usar o FSx para Windows File Server. Para obter mais informações, consulte Optimizing Costs with Amazon FSx.	26 de março de 2020

Support adicionado para transferência de arquivos usando AWS DataSync	Agora você pode usar AWS DataSync para transferir arquivos de e para o FSx for Windows File Server. Para obter mais informações, consulte Migrar arquivos para o Amazon FSx for Windows File Server usando. AWS DataSync	4 de fevereiro de 2020
FSx para Windows File Server lança suporte para tarefas adicionais de administração do sistema de arquivos do Windows	Agora você pode gerenciar e administrar compartilhamentos de arquivos, desduplicação de dados, cotas de armazenamento e criptografia em trânsito para seus compartilhamentos de arquivos usando a CLI do Amazon FSx para gerenciamento remoto ativado. PowerShell Para obter mais informações, consulte Como administrar sistemas de arquivos.	20 de novembro de 2019
FSx para Windows File Server lança suporte nativo de multi-AZ	Você pode usar a implantação multi-AZ para o FSx para Windows File Server para criar mais facilmente sistemas de arquivos com alta disponibilidade que abrangem várias zonas de disponibilidade (AZs). Para obter mais informações, consulte Disponibilidade e durabilidade: sistemas de arquivos Single-AZ e Multi-AZ.	20 de novembro de 2019

FSx para Windows File Server lança suporte para gerenciar sessões de usuários e arquivos abertos	Agora você pode usar a ferramenta Pastas Compartilhadas nativa do Microsoft Windows para gerenciar sessões de usuário e abrir arquivos em seus sistemas de arquivos do FSx para Windows File Server. Para obter mais informações, consulte Managing User Sessions and Open Files.	17 de outubro de 2019
Amazon FSx lança suporte para cópias de sombra do Microsoft Windows	Agora, é possível configurar cópias de sombra do Windows em sistemas de arquivos do FSx para Windows File Server. As cópias de sombra permitem que os usuários desfaçam facilmente alterações em arquivos e comparem versões de arquivos restaurando arquivos para versões anteriores. Para obter mais informações, consulte Working with Shadow Copies.	31 de julho de 2019
Amazon FSx lança suporte compartilhado do Microsoft Active Directory	Agora você pode unir sistemas de arquivos FSx for Windows File Server AWS Managed Microsoft AD a diretórios que estão em uma VPC diferente ou em um sistema de arquivos Conta da AWS diferente. Para obter mais informações, consulte Active Directory Support.	25 de junho de 2019

Amazon FSx lança suporte aprimorado do Microsoft Active Directory	Agora você pode associar os sistemas de arquivos do FSx para Windows File Server aos seus domínios do Microsoft Active Directory autogerenciado, on-premises ou na nuvem. Para obter mais informações, consulte Active Directory Support.	24 de junho de 2019
Amazon FSx está em conformidade com a certificação SOC	O Amazon FSx foi avaliado quanto à conformidade com a certificação SOC. Para obter mais informações, consulte Security and Data Protection.	16 de maio de 2019
Nota esclarecedora adicionada sobre VPN e AWS Direct Connect suporte à conexão de emparelhamento de VPC entre regiões	Os sistemas de arquivos Amazon FSx criados após 22 de fevereiro de 2019 podem ser acessados usando VPN e AWS Direct Connect emparelhamento de VPC entre regiões. Para obter mais informações, consulte Supported Access Methods.	25 de fevereiro de 2019
Suporte adicionado ao AWS Direct Connect, à VPN e à conexão de emparelhamento da VPC entre regiões	Agora você pode acessar os sistemas de arquivos do Amazon FSx para Windows File Server de recursos on-premises e de recursos em outra Amazon VPC ou Conta da AWS. Para obter mais informações, consulte Supported Access Methods.	22 de fevereiro de 2019

O Amazon FSx está agora disponível ao público em geral	O Amazon FSx para Windows File Server fornece servidores de arquivos do Microsoft Windows totalmente gerenciados, baseados em um sistema de arquivos do Windows totalmente nativo. O Amazon FSx para Windows File Server fornece os recursos, a performance e a compatibilidade para mover sem alterações (lift-and-shift) com facilidade aplicações empresariais para a AWS.	28 de novembro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.