



Guia do usuário do Windows

Servidor FSx de arquivos Amazon para Windows



Servidor FSx de arquivos Amazon para Windows: Guia do usuário do Windows

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é FSx para o Windows File Server?	1
FSx Recursos da Amazon	1
Como acessar compartilhamentos de arquivos	2
Segurança e proteção de dados	3
Disponibilidade e durabilidade	3
Como gerenciar sistemas de arquivos	3
Flexibilidade de preço e performance	4
Preços para a Amazon FSx	4
Suposições	4
Pré-requisitos	5
Fóruns do Amazon FSx para Windows File Server	6
Você é usuário da Amazon FSx pela primeira vez?	6
FSx para as melhores práticas do Windows	7
Práticas recomendadas gerais	7
Como criar um plano de monitoramento	7
Garantir que seus sistemas de arquivos tenham recursos suficientes	7
Práticas recomendadas de segurança	7
Segurança de rede	8
Active Directory	8
Evitar perder a disponibilidade devido à configuração incorreta do Active Directory	9
Windows ACLs	10
Como configurar e dimensionar corretamente seu sistema de arquivos	11
Selecionar um tipo de implantação	11
Seleção de uma capacidade de throughput	11
Como aumentar a capacidade de armazenamento e a capacidade de throughput	11
Como modificar a capacidade de throughput durante períodos de inatividade	12
Introdução	13
Configurando seu Conta da AWS	14
.....	14
Etapa 1. Configurar um Active Directory	16
Etapa 2: iniciar uma instância do Windows no EC2 console da Amazon	17
Etapa 3: conectar-se à sua instância	19
Etapa 4: unir sua instância ao seu Directory Service diretório	21
Etapa 5. Criar seu sistema de arquivos	23

Etapa 6. Mapeie seu compartilhamento de arquivos para uma EC2 instância executando o Windows Server	29
Etapa 7. Gravar dados em seu compartilhamento de arquivos	31
Etapa 8. Fazer backup do seu sistema de arquivos.	31
Etapa 9. Limpar os recursos	32
Acessar seus dados	34
Clientes compatíveis	34
Acessar dados diretamente da Nuvem AWS	35
Acesso a dados de uma VPC, Conta da AWS ou Região da AWS diferente	37
Acesso a dados de sistemas on-premises	37
Acessar dados usando nomes de DNS padrão	38
Como usar nomes de DNS com autenticação de Kerberos	39
Compatibilidade com namespaces de Sistemas de Arquivos Distribuídos (DFS)	40
Como acessar dados usando aliases de DNS	40
Como usar autenticação e criptografia do Kerberos com aliases de DNS	41
Associar aliases de DNS ao seu sistema de arquivos	42
Configurar nomes de entidade principal de serviço (SPNs) para o Kerberos	43
Atualizar ou criar um registro CNAME de DNS	46
Aplicar a autenticação de Kerberos usando Objetos de política de grupo (GPOs)	48
Acessar dados usando compartilhamentos de arquivos	49
Mapear compartilhamentos de arquivos	50
Como mapear um compartilhamento de arquivos em uma instância do Amazon EC2 para Windows	50
Como montar um compartilhamento de arquivos em uma instância do Amazon EC2 para Mac	53
Como montar um compartilhamento de arquivos em uma instância do Amazon EC2 para Linux	56
Montar automaticamente compartilhamentos de arquivos em uma instância Linux do Amazon EC2	62
Como gerenciar compartilhamentos de arquivos	65
O comando New-FSxSmbShare falha com uma confiança unidirecional	71
Disponibilidade e durabilidade	72
Como escolher o tipo de implantação do sistema de arquivos single-AZ ou multi-AZ	73
Suporte a recursos por tipo de implantação	73
Processo de failover	74
Experiência de failover em clientes Windows	75

Experiência de failover em clientes Linux	75
Como testar o failover em um sistema de arquivos	75
Recursos do sistema de arquivos single e multi-AZ	76
Sub-redes	76
Interfaces de rede elástica do sistema de arquivos	76
Trabalhar com o Active Directory	78
Usar o AWS Managed Microsoft AD	79
Pré-requisitos de rede	80
Como usar um modelo de isolamento de floresta de recursos	85
Testar sua configuração do Active Directory	85
Como usar o AWS Managed Microsoft AD em outra VPC ou conta	86
Como validar a conectividade com seus controladores de domínio do Active Directory	87
Como usar um Active Directory autogerenciado	90
Pré-requisitos	92
Permissões da conta de serviço	97
Práticas recomendadas ao usar um Active Directory autogerenciado	98
Conta de FSx serviço da Amazon	108
Delegando privilégios à Amazon FSx	109
Como validar a configuração do Active Directory	111
Junte-se FSx a um Active Directory autogerenciado	115
Como obter endereços IP para entradas manuais de DNS	125
Atualizar Active Directory autogerenciado	126
Alterando a conta FSx de serviço da Amazon	128
Como monitorar as atualizações do Active Directory autogerenciado	130
Performance	134
Performance do sistema de arquivos	134
Considerações adicionais sobre performance	135
Latência	136
Throughput e IOPS	136
Performance de um único cliente	136
Desempenho da expansão	136
Capacidade de throughput e performance	137
Escolher a capacidade de throughput	140
Configuração e performance do armazenamento	141
Desempenho da expansão do HDD	142
Exemplo: capacidade de armazenamento e capacidade de throughput	143

Medir a performance usando métricas do CloudWatch	144
Solução de problemas de desempenho	144
Determinar o limite de throughput e IOPS do sistema de arquivos	144
O que é E/S de rede versus E/S de disco? Por que elas são diferentes?	145
Por que o uso da CPU ou da memória é alto quando a E/S de rede é baixa?	145
O que é intermitência? Quanta intermitência meu sistema de arquivos está usando? O que acontece quando os créditos de intermitência se esgotam?	146
Vejo um aviso na página Monitoramento e performance. Preciso alterar a configuração do meu sistema de arquivos?	146
Minhas métricas estavam temporariamente ausentes, devo me preocupar?	147
Como administrar sistemas de arquivos	148
Status FSx do sistema de arquivos da Amazon	149
Usando a Amazon FSx CLI para PowerShell	150
Iniciando uma PowerShell sessão FSx remota da Amazon	152
Tarefas avulsas de configuração do sistema de arquivos	153
Como gerenciar o consumo do armazenamento	153
Ativar cópias de sombra para permitir que os usuários finais recuperem arquivos e pastas das versões anteriores	154
Aplicar a criptografia em trânsito	154
Solução de problemas de acesso à Amazon FSx CLI em PowerShell	155
O grupo de segurança do sistema de arquivos não tem as regras de entrada necessárias para permitir uma conexão remota PowerShell	155
Você tem uma relação de confiança externa configurada entre o Microsoft Active Directory AWS gerenciado e seu Active Directory local	155
Ocorre um erro de localização de idioma ao tentar iniciar uma sessão remota PowerShell ..	156
Janela de manutenção	156
Alterar a janela de manutenção semanal	157
Aliases de DNS	158
Status do alias de DNS	160
Como usar aliases de DNS com o Kerberos	161
Visualizar aliases de DNS existentes	161
Como associar aliases de DNS a sistemas de arquivos	162
Como gerenciar aliases de DNS em sistemas de arquivos atuais	164
Sessões de usuário e arquivos abertos	166
Como usar a GUI para gerenciar usuários e sessões	166
Usando PowerShell para gerenciar sessões de usuários e abrir arquivos	170

Gerenciador de recursos do servidor de arquivos	170
Capacidades gerais	171
Como começar	172
Gerenciamento de cotas	175
Grupos de arquivos	189
Triagem de arquivos	195
Classificação de arquivos	209
Relatórios de armazenamento	229
Tarefas de gerenciamento de arquivos	244
Configurações do FSRM	244
Registros de eventos	250
Casos de uso comuns	251
Gerenciar o armazenamento	258
Otimizar custos do armazenamento	259
Como gerenciar a capacidade de armazenamento	260
Gerenciar tipos de armazenamento	264
Como gerenciar IOPS de SSD	266
Eliminação de duplicação de dados	267
Gerenciar cotas de armazenamento	272
Aumentar a capacidade de armazenamento	273
Monitorar aumentos de armazenamento	275
Como aumentar a capacidade de armazenamento de forma dinâmica	278
Atualização do tipo de armazenamento	284
Como monitorar as atualizações de tipo de armazenamento	285
Atualizar as IOPS SSD	286
Monitorar atualizações de IOPS de SSD provisionadas	287
Como gerenciar a eliminação de duplicação de dados	289
Solução de problemas da eliminação de duplicação dos dados	293
Como usar o namespaces do DFS	295
Como usar o namespaces do DFS	296
Como melhorar o desempenho com fragmentos	296
Agrupar sistemas de arquivos em um namespace	297
Como fragmentar dados usando namespaces do DFS para aumentar a escala do desempenho horizontalmente	299
Como gerenciar a capacidade de throughput	301
Funcionamento da escalabilidade de throughput	301

Saber quando modificar a capacidade de throughput	303
Modificar a capacidade de throughput	303
Como monitorar as atualizações na capacidade de throughput	305
Como gerenciar o tipo de rede	307
Como usar o modo de pilha dupla	308
Como alterar o tipo de rede	308
Marcar recursos	309
Conceitos Básicos de Tags	310
Marcando seus Recursos	311
Restrições de tags	311
Permissões necessárias para marcar recursos	312
Atualizar um sistema de arquivos usando a AWS CLI	312
Como proteger seus dados	314
Proteger seus dados com backups	314
Como trabalhar com backups diários automáticos	316
Como trabalhar com backups iniciados pelo usuário	317
Usando AWS Backup com a Amazon FSx	317
Copiar backups	318
Restaurar backups em um novo sistema de arquivos	321
Como criar backups iniciados pelo usuário	322
Excluir backups	322
Tamanho dos backups	323
Copiar backups	324
Restaurar um backup	325
Como proteger dados com cópias de sombra	326
Práticas recomendadas	327
Como configurar cópias de sombra	329
Configurar cópias de sombra para usar as configurações padrão	333
Definir a quantidade máxima de armazenamento de cópia de sombra	335
Visualizar o armazenamento de cópias de sombra	337
Como criar uma programação de cópias de sombra personalizada	338
Visualizar a programação de cópias de sombra	340
Como criar uma cópia de sombra	340
Como visualizar as cópias de sombra atuais	341
Como excluir cópias de sombra	341
Como excluir uma programação de cópias de sombra	343

Excluir uma configuração de cópia de sombra	343
Solução de problemas com cópias de sombra	344
Replicação programada	345
Como usar o FSx para Windows File Server com o Microsoft SQL Server	346
Como usar o Amazon FSx para arquivos de dados ativos do SQL Server	346
Criar um compartilhamento continuamente disponível	347
Configurar as definições de tempo limite do SMB	347
Como usar o Amazon FSx como testemunha de compartilhamento de arquivos SMB	347
Como migrar para o Amazon FSx	348
Como migrar arquivos para o FSx para Windows File Server	348
Práticas recomendadas para migrar	349
Como migrar arquivos usando o AWS DataSync	349
Como migrar arquivos usando o Robocopy	353
Como migrar as configurações de compartilhamento de arquivos	358
Como migrar a configuração de DNS on-premises para o FSx para Windows File Server	359
Substituir para o FSx para Windows File Server	362
Preparar a substituição para o Amazon FSx	363
Configurar SPNs para autenticação Kerberos	363
Atualizar os registros CNAME do DNS para o sistema de arquivos do Amazon FSx	367
Como monitorar sistemas de arquivos	369
Monitoramento automático e manual	369
Ferramentas automatizadas	370
Ferramentas de monitoramento manual	370
Monitorar com o Amazon CloudWatch	371
Métricas e dimensões	373
Usar métricas do Amazon CloudWatch	378
Avisos e recomendações de performance	383
Acesso a métricas de sistema de arquivos	385
Criar alarmes do CloudWatch	390
Logs do CloudTrail	393
Informações sobre o Amazon FSx no CloudTrail	393
Noções básicas sobre entradas de arquivos de log do Amazon FSx	394
Segurança	397
Proteção de dados	398
Criptografia de dados	399
Criptografia em repouso	399

Criptografia em trânsito	401
Windows ACLs	403
Links relacionados	404
Controle de acesso ao sistema de arquivos com a Amazon VPC	405
Grupos de segurança da Amazon VPC	405
Rede Amazon VPC ACLs	410
Como registrar em log o acesso de usuário final	410
Destinos dos logs de eventos de auditoria	412
Como migrar seus controles de auditoria	413
Como visualizar logs de eventos	413
Como configurar os controles de auditoria de arquivos e pastas	421
Como gerenciar a auditoria de acesso a arquivos	423
Gerenciamento de identidade e acesso	428
Público	428
Autenticação com identidades	429
Gerenciar o acesso usando políticas	430
Como o Amazon FSx para Windows File Server funciona com o IAM	432
Exemplos de políticas baseadas em identidade	437
AWS políticas gerenciadas	441
Solução de problemas	458
Usando tags com a Amazon FSx	460
Uso de perfis vinculados ao serviço	466
Validação de conformidade	472
VPC endpoints de interface	473
Considerações sobre endpoints da VPC de interface do Amazon FSx	473
Como criar um endpoint da VPC de interface para a API do Amazon FSx	474
Como criar uma política de endpoint da VPC para o Amazon FSx	475
Como trabalhar com outros serviços do	476
Usando a Amazon FSx com WorkSpaces aplicativos da Amazon	476
Como fornecer armazenamento pessoal Persistent para cada usuário	477
Como fornecer uma pasta compartilhada entre os usuários	479
Usando o FSx Windows File Server com o Amazon Kendra	481
desempenho do sistema de arquivos	481
Cotas	482
Cotas que podem ser aumentadas	482
Cotas de recursos para cada sistema de arquivos	484

Considerações adicionais	484
Cotas específicas para o Microsoft Windows	485
Solução de problemas	486
Não é possível acessar o sistema de arquivos	486
A interface de rede elástica do sistema de arquivos foi modificada ou excluída	487
O endereço IP elástico anexado à interface de rede elástica do sistema de arquivos foi excluído	487
O grupo de segurança do sistema de arquivos não possui as regras de entrada ou saída necessárias.	487
O grupo de segurança da instância de computação não tem as regras de saída necessárias	487
Instância de computação não associada a um Active Directory	487
O compartilhamento de arquivos não existe	488
O usuário do Active Directory não possui as permissões necessárias	488
Remoção do Permitir controle total de permissões de NTFS ACL	488
Não é possível acessar um sistema de arquivos usando um cliente on-premises	489
O novo sistema de arquivos não está registrado no DNS	489
Não é possível acessar o sistema de arquivos usando um alias de DNS	490
Não é possível acessar o sistema de arquivos usando um endereço IP	491
Como criar falhas no sistema de arquivos	492
Grupo de segurança da VPC configurado incorretamente	492
Nomes duplicados de grupo de administradores de sistemas de arquivos	492
Servidores de DNS ou controladores de domínio inacessíveis	493
Credenciais inválidos da conta de serviço	495
A Amazon não FSx pode acessar as credenciais da sua conta de serviço do Active Directory em AWS Secrets Manager	496
Permissões insuficientes da conta de serviço	498
Capacidade excedida da conta de serviço	499
Não é possível acessar a UO	499
Grupo inválido de administradores do sistema de arquivos	500
A Amazon FSx perdeu a conectividade no domínio	501
A conta de serviço não tem permissões corretas	502
Caracteres Unicode usados em parâmetros de criação	503
Falha ao mudar o tipo de armazenamento para HDD durante a restauração de um backup	503
O sistema de arquivos está em um estado de configuração incorreta	504

Sistema de arquivos configurado incorretamente: a Amazon não FSx consegue acessar os servidores DNS nem os controladores de domínio do seu domínio.	506
Sistema de arquivos com configuração incorreta: as credenciais da conta de serviço são inválidas	506
Sistema de arquivos configurado incorretamente: a chave AWS Secrets Manager secreta ou KMS não está configurada corretamente	507
Sistema de arquivos com configuração incorreta: a conta de serviço fornecida não tem permissão para associar o sistema de arquivos ao domínio	508
Sistema de arquivos com configuração incorreta: a conta de serviço não consegue associar mais computadores ao domínio	508
Sistema de arquivos com configuração incorreta: a conta de serviço não tem acesso à UO	509
Não é possível configurar a DFS-R em um sistema de arquivos multi-AZ ou single-AZ 2	509
Falha nas atualizações da capacidade de armazenamento ou capacidade de throughput	510
O aumento da capacidade de armazenamento falha porque a Amazon não FSx consegue acessar o sistema de arquivos AWS KMS key	510
A atualização da capacidade de armazenamento ou da capacidade de throughput falha porque o Active Directory autogerenciado está com a configuração incorreta	511
O aumento da capacidade de armazenamento falha devido à capacidade de throughput insuficiente	511
A atualização da capacidade de taxa de transferência para 8 falhas MBps	511
Histórico do documento	512
.....	dxxx

O que é FSx para o Windows File Server?

O Amazon FSx para Windows File Server fornece servidores de arquivos Microsoft Windows totalmente gerenciados, apoiados por um sistema de arquivos Windows totalmente nativo. FSx para Windows, o File Server tem os recursos, o desempenho e a compatibilidade para transferir e transferir facilmente os aplicativos corporativos para Nuvem AWS o.

A Amazon FSx oferece suporte a um amplo conjunto de cargas de trabalho corporativas do Windows com armazenamento de arquivos totalmente gerenciado construído no Microsoft Windows Server. FSx A Amazon tem suporte nativo para recursos do sistema de arquivos do Windows e para o protocolo Server Message Block (SMB) padrão do setor para acessar o armazenamento de arquivos em uma rede. FSx A Amazon é otimizada 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 na Amazon FSx, o código, os aplicativos e as ferramentas que os desenvolvedores e administradores do Windows usam atualmente podem continuar funcionando inalterados. Os aplicativos e cargas de trabalho do Windows ideais para a Amazon FSx incluem aplicativos comerciais, diretórios iniciais, serviços na web, gerenciamento de conteúdo, análise de dados, configurações de criação de software e cargas de trabalho de processamento de mídia.

Como um serviço totalmente gerenciado, o File Server FSx para Windows elimina a sobrecarga administrativa de configurar e provisionar servidores de arquivos e volumes de armazenamento. Além disso, a 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 CloudTrail](#).

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

Os principais recursos na 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), SSD IOPS e capacidade de taxa de transferência (in). MBps 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](#).

FSx para Windows file-system-consistent, os backups do servidor de arquivos são altamente duráveis e incrementais. Para garantir a consistência do sistema de arquivos, a 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 obter mais informações, consulte [Proteger seus dados 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 obter mais informações, consulte [Acessar dados usando compartilhamentos de arquivos](#).

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 obter mais informações, consulte [Como gerenciar aliases de DNS](#).

Como acessar compartilhamentos de arquivos

FSx A Amazon pode ser acessada a partir de instâncias computacionais 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 FSx arquivos da Amazon em instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e em WorkSpaces instâncias, instâncias Amazon AppStream 2.0 e VMware Cloud on AWS VMs.

Você pode acessar seus compartilhamentos de arquivos nas instâncias de computação on-premises usando o AWS Direct Connect ou a Site-to-Site VPN. Além de acessar compartilhamentos de arquivos que estão na mesma VPC, AWS conta e Região da AWS sistema de arquivos, você também pode acessar seus compartilhamentos a partir de instâncias computacionais que estão em uma Amazon VPC, conta ou. Região da AWS Isso é feito com o uso do emparelhamento de VPCs ou gateways de trânsito. Para obter mais informações, consulte [Acessar dados diretamente da Nuvem AWS](#).

Segurança e proteção de dados

FSx A Amazon 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.

FSx A Amazon fornece controle de acesso no nível de arquivo e pasta com listas de controle de acesso do Windows (ACLs). 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. A 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 FSx recursos da Amazon.

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 obter mais informações, consulte [Segurança na Amazon FSx](#).

Disponibilidade e durabilidade

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 FSx de arquivos do Windows File Server usando PowerShell comandos personalizados de gerenciamento remoto ou usando a GUI nativa do Windows em

alguns casos. Para saber mais sobre o gerenciamento dos sistemas de FSx arquivos da Amazon, consulte [Administração FSx para sistemas de arquivos Windows](#).

Flexibilidade de preço e performance

FSx para Windows File Server oferece flexibilidade de preço e desempenho, oferecendo tipos de armazenamento em 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 data analytics.

Com FSx o Windows File Server, você pode provisionar armazenamento do sistema de arquivos, IOPS SSD e taxa de transferência de forma independente para obter a combinação certa de custo e desempenho. 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.

Preços para a Amazon FSx

Com a 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 a Amazon FSx, você precisa de uma AWS conta com uma EC2 instância, WorkSpaces instância, instância de WorkSpaces aplicativos ou VM da Amazon em execução na VMware nuvem em AWS ambientes do tipo compatível.

Neste guia, fazemos as seguintes suposições:

- Se você estiver usando a Amazon EC2, presumimos que você esteja familiarizado com a Amazon EC2. Para obter mais informações sobre como usar a 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 on AWS](#).
- Presumimos que você tenha familiaridade com os conceitos do Microsoft Active Directory.

Pré-requisitos

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

- Uma AWS conta com as permissões necessárias para criar um sistema de FSx arquivos da Amazon e uma EC2 instância da Amazon. Para obter mais informações, consulte [Configurando seu Conta da AWS](#).
- Uma EC2 instância da Amazon 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 da Amazon. FSx Para obter informações sobre como criar uma, consulte [Introdução às instâncias EC2 do Amazon Windows](#) no Guia do EC2 usuário da Amazon.
- A Amazon FSx trabalha com o Microsoft Active Directory para realizar a autenticação do usuário e o controle de acesso. Você associa seu sistema de FSx arquivos da Amazon a um Microsoft Active Directory ao criá-lo. Para obter mais informações, consulte [Trabalhar com o Microsoft Active Directory](#).
- Este guia pressupõe que você não alterou as regras do grupo de segurança padrão para sua VPC com base no serviço Amazon VPC. Se tiver, você precisa garantir a adição das regras necessárias para permitir o tráfego de rede da sua EC2 instância da Amazon para o sistema de FSx arquivos da Amazon. Consulte mais detalhes em [Segurança na 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

Se você encontrar problemas ao usar a Amazon FSx, use os [fóruns](#).

Você é usuário da Amazon FSx pela primeira vez?

Se você é um usuário iniciante da Amazon FSx, recomendamos que você leia as seguintes seções na ordem:

1. Se você estiver pronto para criar seu primeiro sistema de FSx arquivos da Amazon, experimente [Introdução ao Amazon FSx para Windows File Server](#) o.
2. Para obter mais informações sobre desempenho, consulte [desempenho do FSx para Windows File Server](#).
3. Para obter detalhes FSx de segurança da Amazon, consulte [Segurança na Amazon FSx](#).
4. Para obter informações sobre a FSx API da Amazon, consulte [Referência de FSx API da Amazon](#).

Práticas recomendadas FSx para Windows File Server

Recomendamos que você siga essas melhores práticas ao trabalhar com o Amazon FSx para Windows File Server.

Tópicos

- [Práticas recomendadas gerais](#)
- [Práticas recomendadas de segurança](#)
- [Active Directory](#)
- [Como configurar e dimensionar corretamente seu sistema de arquivos](#)

Práticas recomendadas gerais

Como criar um plano de monitoramento

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

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 o desempenho e acessar os avisos e recomendações de desempenho, consulte [Avisos e recomendações de performance](#).

Práticas recomendadas 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 a Amazon FSx para atender aos seus objetivos de segurança e conformidade, consulte [Segurança na Amazon FSx](#).

Segurança de rede

Não modificar ou excluir a ENI associada ao seu sistema de arquivos

Seu sistema de FSx arquivos da Amazon 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.

Usando grupos de segurança e rede ACLs

Você pode usar grupos de segurança e listas de controle de acesso à rede (ACLs) para limitar o acesso aos seus sistemas de arquivos. Para [grupos de segurança da VPC](#), o grupo de segurança padrão já está adicionado ao seu sistema de arquivos no console. Certifique-se de que o grupo de segurança e a rede ACLs das sub-redes em que você cria seu sistema de arquivos permitam tráfego nas portas.

Active Directory

Ao criar um sistema de FSx arquivos da Amazon, você pode associá-lo ao seu [domínio do Microsoft Active Directory](#) 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 Active Directory 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 a Amazon FSx sem nenhuma modificação. FSxA Amazon oferece duas opções para o Active Directory: Microsoft Active Directory AWS gerenciado ou Microsoft Active Directory autogerenciado.

Se você estiver usando um Microsoft Active Directory gerenciado pela AWS, recomendamos que deixe as configurações do seu grupo de segurança do Active Directory conforme o padrão. Se você modificar essas configurações, certifique-se de manter uma configuração de rede que atenda aos requisitos de rede. Para obter mais informações, consulte [Pré-requisitos de rede](#).

Se estiver usando um Microsoft Active Directory autogerenciado, há opções adicionais para configurar seu sistema de arquivos. Recomendamos as seguintes melhores práticas para configuração inicial ao usar a Amazon FSx com seu Microsoft Active Directory autogerenciado:

- Atribua sub-redes a um único site do Active Directory: Se seu ambiente do Active Directory 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 FSx arquivos da Amazon a um único site do Active Directory 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 e quaisquer outros controles de roteamento de rede que você tenha na sua infraestrutura do Active Directory permitam a comunicação da Amazon nas portas necessárias. DCs FSx Isso permite que o Windows revertera para outro DCs se não puder usar o site atribuído do Active Directory. Para obter mais informações, consulte [Controle de acesso ao sistema de arquivos com a Amazon VPC](#).

- Use uma unidade organizacional (OU) separada: use uma OU para seus sistemas de FSx arquivos da Amazon que seja separada de qualquer outra unidade organizacional que você possa ter.
- Configure sua conta de serviço com os privilégios mínimos necessários: configure ou delegue a conta de serviço que você fornece à Amazon FSx com os privilégios mínimos necessários. Para obter mais informações, consulte [Usar um Microsoft Active Directory autogerenciado](#).
- Verifique continuamente sua configuração do Active Directory: execute a [ferramenta de validação do Amazon FSx Active Directory](#) em sua configuração do Active Directory antes de criar seu sistema de FSx arquivos da Amazon para verificar se sua configuração é válida para uso com a Amazon FSx e para descobrir quaisquer avisos e erros que a ferramenta possa expor.
- Armazenando credenciais do Active Directory usando AWS Secrets Manager: Você pode usar AWS Secrets Manager para armazenar e gerenciar com segurança suas credenciais da conta de serviço de ingresso no domínio do Microsoft Active Directory. Essa abordagem elimina a necessidade de armazenar credenciais confidenciais em texto simples no código da aplicação ou nos arquivos de configuração, fortalecendo sua postura de segurança. Para obter mais informações, consulte [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#).

Evitar perder a disponibilidade devido à configuração incorreta do Active Directory

Ao usar a Amazon FSx com seu Microsoft Active Directory autogerenciado, é importante ter uma configuração válida do Active Directory 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 transferência, a Amazon reúne FSx os recursos do servidor de arquivos ao seu Active Directory. Se a configuração do Active Directory não for válida durante um evento, seu sistema de arquivos será alterado para o status de Configuração incorreta e corre o risco de ficar indisponível. Aqui estão algumas maneiras de evitar a perda de disponibilidade:

- Mantenha sua configuração do Active Directory atualizada com a 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.
- Monitorar a configuração incorreta do Active Directory: defina notificações de status de configuração incorreta para que você possa redefinir a configuração do Active Directory 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 FSx arquivos da Amazon usando Amazon e. EventBridge AWS Lambda](#)
- Valide sua configuração do Active Directory regularmente: se você quiser detectar proativamente configurações incorretas do Active Directory, recomendamos que você execute a [ferramenta de validação do Active Directory](#) em sua configuração do Active Directory 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 por FSx: FSx A Amazon cria e gerencia objetos de computador em seu Active Directory, 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.

Windows ACLs

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

- Não altere as permissões de NTFS ACL para o usuário SYSTEM: a Amazon FSx exige que o usuário SYSTEM tenha controle total das permissões de NTFS ACL 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

A 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 obter mais informações, consulte [Disponibilidade e durabilidade: sistemas de arquivos single-AZ e multi-AZ](#).

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 obter mais informações, consulte [Impacto da capacidade de throughput na performance](#).

Como aumentar a capacidade de armazenamento e a capacidade 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 20% da capacidade de armazenamento livre em todos os momentos em seu sistema de arquivos. Também recomendamos aumentar a capacidade de throughput em pelo menos 20% antes de aumentar a capacidade de armazenamento para compensar qualquer impacto no desempenho durante um aumento do armazenamento. Você pode usar a FreeStorageCapacity CloudWatch métrica para monitorar a quantidade de armazenamento gratuito disponível e entender suas tendências. Para obter 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 desempenho no FSx console para ver quando as demandas de carga de trabalho se aproximaram ou excederam os limites de desempenho para determinar se seu sistema de arquivos está subprovisionado para sua carga de trabalho.

Para minimizar a duração da escalabilidade do armazenamento e evitar a redução na desempenho 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 no desempenho durante o escalonamento do armazenamento. No entanto, sistemas de arquivos com o tipo de armazenamento em HDD e workloads que envolvam um grande número de usuários finais, altos níveis de E/S ou conjuntos de dados com um grande número de arquivos pequenos podem sofrer uma redução temporária no desempenho. Para obter mais informações, consulte [Aumentos da capacidade de armazenamento e performance do sistema de arquivos](#).

Como 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 alto índice de gravação e de 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 FSx o 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 Directory Service o. Você associará seu sistema de arquivos e sua instância de computação ao Active Directory.
3. Crie uma instância de computação do Amazon Elastic Compute Cloud que execute o Microsoft Windows Server. Você usará essa instância para acessar seu sistema de arquivos.
4. Crie um sistema de arquivos Amazon FSx para Windows File Server usando o FSx console da Amazon.
5. Mapeie seu sistema de arquivos para sua EC2 instância
6. Grave dados no sistema de arquivos.
7. Faça backup do seu sistema de arquivos.
8. Limpe os recursos que você criou.

Tópicos

- [Configurando seu Conta da AWS](#)
- [Etapa 1. Configurar um Active Directory](#)
- [Etapa 2: iniciar uma instância do Windows no EC2 console da Amazon](#)
- [Etapa 3: conectar-se à sua instância](#)
- [Etapa 4: unir sua instância ao seu Directory Service diretório](#)
- [Etapa 5. Criar seu sistema de arquivos](#)
- [Etapa 6. Mapeie seu compartilhamento de arquivos para uma EC2 instância executando o Windows Server](#)
- [Etapa 7. Gravar dados em seu compartilhamento de arquivos](#)
- [Etapa 8. Fazer backup do seu sistema de arquivos.](#)
- [Etapa 9. Limpar os recursos](#)

Configurando seu Conta da AWS

Antes de usar a 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 a <https://portal.aws.amazon.com/billing/inscrição>.
2. Siga as instruções online.

Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWS é 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, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando <https://aws.amazon.com/e> escolhendo 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 Centro de Identidade do AWS IAM, 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 [Console de gerenciamento da AWS](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

Para obter ajuda ao fazer login usando o usuário-raiz, consulte [Fazer login como usuário-raiz](#) no Guia do usuário do Início de Sessão da AWS .

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

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

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

Para obter instruções, consulte [Habilitar o Centro de Identidade do AWS IAM](#) no Guia do usuário do Centro de Identidade do AWS IAM .

2. No Centro de Identidade do IAM, conceda o acesso administrativo a 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 Centro de Identidade do AWS IAM do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

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 [Criar um conjunto de permissões](#) no Guia do usuário do Centro de Identidade do AWS IAM .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de logon único ao grupo.

Para obter instruções, consulte [Adicionar grupos](#) no Guia do usuário do Centro de Identidade do AWS IAM .

Etapa 1. Configurar um Active Directory

Com a Amazon FSx, você pode operar um armazenamento de arquivos totalmente gerenciado para cargas de trabalho baseadas em Windows. Da mesma forma, Directory Service fornece diretórios totalmente gerenciados para uso em sua implantação de carga de trabalho. Se você tiver um domínio corporativo existente do Active Directory em execução AWS em uma nuvem privada virtual (VPC) usando EC2 instâncias, você pode habilitar a autenticação baseada no usuário e o controle de acesso. Você faz isso estabelecendo uma relação de confiança entre seu Microsoft Active Directory AWS gerenciado e seu domínio corporativo. Para a autenticação do Windows na Amazon FSx, você só precisa de uma relação de confiança de floresta direcional unidirecional, na qual a floresta AWS gerenciada confia na floresta de domínio corporativo.

Seu domínio corporativo assume o papel de domínio confiável, e o domínio 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 autenticuem em relação aos recursos compartilhados no domínio gerenciado. Nesse caso, a 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 externo com a Amazon FSx para domínios confiáveis.

Seu grupo de segurança do Active Directory deve habilitar o acesso de entrada do grupo de segurança do sistema de FSx arquivos da Amazon.

Para criar um serviço de AWS diretório para o Microsoft Active Directory

- Se você ainda não tiver um, use o Directory Service para criar seu diretório AWS gerenciado do Microsoft Active Directory. Para obter mais informações, consulte [Criar seu Microsoft Active Directory AWS gerenciado](#) no Guia de AWS Directory Service Administração.

⚠ 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, precisará repetir as etapas deste exercício com o novo Directory Service diretório e o usuário administrador.

- Se você tiver um Active Directory existente, crie uma relação de confiança entre o Microsoft Active Directory AWS gerenciado e o Active Directory existente. Para obter mais informações, consulte [Quando criar uma relação de confiança](#) no Guia de administração do AWS Directory Service .

Etapa 2: iniciar uma instância do Windows no EC2 console da Amazon

Você pode iniciar uma instância do Windows usando o Console de gerenciamento da AWS 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 EC2 console da Amazon em <https://console.aws.amazon.com/ec2/>.
2. No painel do console, selecione Launch Instance.
3. A página Escolha uma imagem de máquina da Amazon (AMI) exibe uma lista de configurações básicas, chamadas Amazon Machine Images (AMIs), que servem como modelos para sua instância. Selecione a AMI para o Windows Server 2016 Base ou posterior. Observe que eles AMIs estão marcados como “Qualificados para o 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 DNS público (IPv4) ou (IPv6) estiver oculta, escolha Mostrar/Ocultar colunas (o ícone em forma de engrenagem) no canto superior direito da página e selecione DNS público () ou (IPv4).) IPv6
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 dele ao criar seu sistema de FSx arquivos da Amazon.

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 [Nomes localizados para contas 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 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 EC2 console da Amazon, selecione a instância e, em seguida, escolha Connect.
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 Detalhes e role para baixo até a entrada Impressão digital em um PC com Windows ou a entrada SHA1 Impressões digitais em um Mac. Esse é o identificador exclusivo do certificado de segurança do computador remoto.
- c. No EC2 console da Amazon, selecione a instância, escolha Ações e, em seguida, escolha Obter registro 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 Directory Service .

Etapa 4: unir sua instância ao seu Directory Service diretório

O procedimento a seguir mostra como unir manualmente uma instância existente EC2 do Amazon Windows ao seu Directory Service diretório.

Para unir uma instância do Windows ao seu Directory Service diretório

1. Conecte-se à instância usando qualquer cliente Remote Desktop Protocol.
2. Abra a caixa de diálogo TCP/ IPv4 ou IPv6 propriedades 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 ou Protocolo de Internet versão 6.
3. (Opcional) Selecione Usar os seguintes endereços de servidor DNS, altere os endereços do servidor DNS preferencial e do servidor DNS alternativo para os IPv6 endereços IPv4 ou dos servidores DNS Directory Service fornecidos e escolha 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, escolha Domínio, insira o nome totalmente qualificado do seu Directory Service diretório e escolha 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 NetBios nome, seguido por uma barra invertida (\) e, em seguida, o nome do usuário, nesse 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 entre na instância usando o nome de usuário e a senha do usuário administrador do seu Directory Service diretório.

Agora que sua instância foi associada ao domínio, você está pronto para criar seu sistema de FSx arquivos da Amazon.

Etapa 5. Criar seu sistema de arquivos

Para criar um sistema de arquivos (console)

1. Abra o FSx console da Amazon 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 Servidor FSx de arquivos do Windows e, em seguida, escolha 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 obter 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.

FSx para Windows File Server oferece tipos de armazenamento em unidade de estado sólido (SSD) e 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 data analytics. 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 obter mais informações, consulte [Sobre os tipos de armazenamento](#).

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

Se você escolher o modo Automático, FSx o Windows File Server escalará automaticamente seu SSD IOPS para manter 3 SSD IOPS por GiB de capacidade de armazenamento. Se você escolher o modo provisionado pelo usuário, insira qualquer número inteiro entre 96 e 400 mil. 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 obter 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 mil e 65.536. Você pode aumentar a capacidade de armazenamento, conforme necessário, a qualquer momento após a criação do sistema de arquivos. Para obter 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 obter mais informações, consulte [desempenho do FSx para Windows File Server](#).

 Note

Se você quiser habilitar a auditoria de acesso a arquivos, deverá escolher uma capacidade de taxa de transferência de 32 MBps ou mais. Para obter mais informações, consulte [Como registrar em log o acesso de usuário final com 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 obter mais informações, consulte [Como gerenciar a capacidade de throughput](#).

Segurança e rede

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 Directory Service diretório e sua instância da 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 na Região da AWS mesmo do seu sistema de arquivos. Para garantir que você possa conectar uma EC2 instância 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 de e para endereços IP ou grupos de segurança IDs associados às instâncias de computação do cliente a partir das quais você deseja acessar seu 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 o tráfego do seu sistema de FSx arquivos da Amazon. 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 obter mais informações, consulte [Controle de acesso ao sistema de arquivos com a Amazon VPC](#).

3. Um sistema de arquivos multi-AZ tem um servidor de arquivos primário e um em espera, cada um nas suas próprias 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 primário 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.

4. Para Tipo de rede, selecione IPv4(somente para IPv4 suporte) ou Dual-Stack (para ambos IPv4 e IPv6 suporte). Você pode alterar o tipo de rede de um sistema de arquivos existente a qualquer momento. Para obter mais informações, consulte [Como alterar o tipo de rede](#).

 Note

Se você pretende criar um sistema de arquivos FSx para Windows File Server que usa o modo de pilha dupla, primeiro atribua um bloco IPv6 CIDR fornecido pela Amazon à sua VPC e sub-redes. Para obter mais informações, consulte [Adicionar IPv6 suporte para sua VPC](#) no Guia do usuário da Amazon Virtual Private Cloud.

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 Directory Service diretório na lista. Para obter mais informações, consulte [Trabalhar com o Microsoft Active Directory](#).

Se você quiser associar o sistema de arquivos a um domínio do Microsoft Active Directory autogerenciado, escolha Microsoft Active Directory autogerenciado e forneça os detalhes a seguir para seu Active Directory. Para obter mais informações, consulte [Usar um 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 Directory Service de domínio autogerenciados do Active Directory.

A 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 Direct Connect associação. AWS Transit Gateway

- Endereços IP do servidor DNS — IPv4 ou IPv6 endereços 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 desabilitado, a criação do seu sistema de arquivos poderá falhar.

- Credenciais para uma conta de serviço do Active Directory que a Amazon FSx usa para unir o sistema de arquivos ao seu domínio. Você pode fornecê-los como:
 - Opção 1: ARN AWS Secrets Manager secreto - O segredo que contém o nome de usuário e a senha de uma conta de serviço no seu domínio do Active Directory. Para obter mais

informações, consulte [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#).

- Opção 2: credenciais em texto não criptografado
 - Nome de usuário da conta de serviço: o nome de usuário da conta de serviço no seu Microsoft Active Directory existente. Não inclua um prefixo ou sufixo de domínio. Por exemplo, para EXAMPLE\ADMIN, use apenas ADMIN.
 - Senha da conta de serviço: a senha da conta de serviço.
- (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 obter mais informações, consulte [Conta de FSx serviço da Amazon](#).

Criptografia, auditoria e acesso (alias 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 obter mais informações, consulte [Criptografia de dados 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 [Como registrar em log o acesso de usuário final com auditoria de acesso a arquivos](#).
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 obter mais informações, consulte [Como gerenciar alias de DNS](#).

Backup e manutenção

Para obter mais informações sobre backups diários automáticos e as configurações desta seção, consulte [Proteger seus dados com backups](#).

1. O backup diário automático está habilitado por padrão. Você pode desativar essa configuração se não quiser que FSx a Amazon faça backups do seu sistema de arquivos automaticamente diariamente.

2. Se os backups automáticos estiverem habilitados, eles ocorrerão durante um período conhecido como janela de backup. Você pode usar a janela padrão ou escolher uma Hora de início da janela de backup automático que seja melhor para seu fluxo de trabalho.
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 a Amazon FSx reterá backups diários automáticos do seu sistema de arquivos. Essa configuração não se aplica a backups iniciados pelo usuário ou a 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 obter mais informações, consulte [Marcação de seus recursos do Amazon FSx](#).

Escolha Próximo.

Revisar sua configuração e criar

1. Verifique a configuração do sistema de arquivos mostrada na página Criar sistema de arquivos. Para sua referência, é possível ver quais configurações do sistema de arquivos você pode ou não modificar após a criação do sistema de arquivos. Escolha Create file system (Criar sistema de arquivos).
2. Depois que a 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 de DNS do seu sistema de arquivos na guia Rede e segurança. Você precisará dela no procedimento a seguir para mapear um compartilhamento para uma EC2 instância.

Etapa 6. Mapeie seu compartilhamento de arquivos para uma EC2 instância executando o Windows Server

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

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

1. Antes de montar um compartilhamento de arquivos em uma instância do Windows, você deve iniciar a EC2 instância e associá-la à instância à AWS Directory Service for Microsoft Active Directory qual seu sistema de arquivos se associou. Para executar essa ação, escolha um dos procedimentos a seguir no Guia de AWS Directory Service Administração:
 - [Junte-se perfeitamente a uma instância do Windows EC2](#)
 - [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 EC2 do usuário da Amazon.
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 seu sistema de arquivos usando o nome DNS padrão atribuído pela 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 [Como acessar dados usando aliases de DNS](#).

Em Pasta, insira o nome DNS do sistema de arquivos e o nome do compartilhamento. O FSx compartilhamento padrão da Amazon é chamado `\share`. Você pode encontrar o nome do DNS no FSx console da Amazon <https://console.aws.amazon.com/fsx/>, na seção Servidor de arquivos do Windows > Rede e segurança ou na resposta de nosso comando de `CreateFileSystem` `DescribeFileSystems` 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.

Etapa 7. Gravar 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: *Hello, World!*
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.

Etapa 8. Fazer backup do seu sistema de arquivos.

Agora que você teve a chance de usar seu sistema de FSx arquivos da Amazon e seus compartilhamentos de arquivos, você pode fazer backup dele. 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 FSx console da Amazon 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.

Etapa 9. Limpar os 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 EC2 console da Amazon, encerre sua instância. Para obter mais informações, consulte [Encerre sua instância](#) no Guia do EC2 usuário da Amazon.
2. No FSx console da Amazon, exclua seu 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 FSx console da Amazon 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.

Seu sistema de FSx arquivos da Amazon e os backups automáticos relacionados agora estão excluídos.

3. Para excluir o Directory Service diretório que você criou para este exercício, consulte [Excluir seu diretório](#) no Guia de AWS Directory Service Administração.

Acessar seus dados

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

Tópicos

- [Clientes compatíveis](#)
- [Acessar dados diretamente da Nuvem AWS](#)
- [Acesso a dados de sistemas on-premises](#)
- [Acessar dados usando nomes de DNS padrão](#)
- [Compatibilidade com namespaces de Sistemas de Arquivos Distribuídos \(DFS\)](#)
- [Como acessar dados usando aliases de DNS](#)
- [Acessar dados usando compartilhamentos de arquivos](#)
- [Criar, atualizar e remover compartilhamentos de arquivos](#)

Clientes compatíveis

O FSx para Windows File Server é compatível com as versões 2.0 a 3.1.1 do protocolo Server Message Block (SMB), proporcionando a flexibilidade de se conectar aos seus sistemas de arquivos usando diversas instâncias de computação e sistemas operacionais.

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 [Mapear 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

Acessar dados diretamente da Nuvem AWS

Cada sistema de arquivos do Amazon FSx está associado a uma nuvem privada virtual (VPC). Você pode acessar o sistema de arquivos do FSx para Windows File Server de qualquer lugar na VPC do sistema de arquivos, independentemente da zona de disponibilidade. Você também pode acessar seu sistema de arquivos de VPCs que estejam em Contas da AWS ou Regiões da AWS diferentes dos respectivos elementos do sistema de arquivos. Além dos requisitos descritos nas próximas seções para acessar os recursos do FSx para Windows File Server, você também precisa garantir que o grupo de segurança da VPC do sistema de arquivos esteja configurado de modo que o tráfego de dados e gerenciamento possa fluir entre o sistema de arquivos e os clientes. Para obter mais informações sobre a configuração de grupos de segurança com as portas necessárias, consulte [Controle de acesso ao sistema de arquivos com a Amazon VPC](#).

Você pode acessar o sistema de arquivos do FSx para Windows File Server de clientes compatíveis que estejam na mesma VPC que seu sistema de arquivos.

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.

Cientes 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		Cientes com endereços IP em um intervalo de endereços IP privados do RFC 1918 :	Cientes com endereços IP fora do seguinte intervalo de blocos CIDR:
Outros CIDRs ou redes emparelhados		• 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	198.19.0.0/16

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 [Proteger seus dados com backups](#).

Acesso a dados de uma VPC, Conta da AWS ou Região da AWS diferente

Com o emparelhamento de VPC ou gateways de trânsito, você pode acessar o sistema de arquivos do FSx para Windows File Server de clientes compatíveis que estejam em uma VPC, Conta da AWS ou Região da AWS diferente do respectivo elemento associado ao seu sistema de arquivos. Ao usar uma conexão de emparelhamento da VPC ou gateway de trânsito para conectar VPCs, as instâncias de computação que estiverem em uma VPC poderão acessar sistemas de arquivos do Amazon FSx que estejam em outra VPC. Esse acesso é possível mesmo que as VPCs pertençam a Contas da AWS 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.

Acesso a dados de sistemas on-premises

O FSx para Windows File Server é compatível com o uso do AWS Direct Connect ou Site-to-Site 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 Site-to-Site 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 sobre o Direct Connect, consulte o [Guia do usuário do Direct Connect](#). Para obter mais informações sobre a configuração de conexões da Site-to-Site VPN, consulte [Conexões VPN](#) no Guia do usuário da Amazon VPC.

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 [Proteger seus dados com backups](#).

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](#).

Note

O Gateway de Arquivos do Amazon FSx não está mais disponível para novos clientes. Os clientes atuais do Gateway de arquivos do FSx podem continuar usando o serviço normalmente. Para recursos semelhantes ao Gateway de Arquivos do FSx, acesse [esta publicação de blog](#).

Acessar dados usando nomes de 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 [Acessar dados usando compartilhamentos de arquivos](#).

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 em entradas DNS manuais](#).

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 de DNS é semelhante ao seguinte formato: `fs-0123456789abcdef0.ad-dns-domain-name`

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

Como usar nomes de DNS com autenticação de 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 Microsoft Active Directory gerenciado pela AWS e o Active Directory on-premises para usar o PowerShell remoto do Amazon FSx com autenticação de 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.

Compatibilidade com namespaces de Sistemas de Arquivos Distribuídos (DFS)

O FSx para Windows File Server é compatível com o uso de namespaces do DFS da Microsoft. Use os namespaces do DFS para organizar os compartilhamentos de arquivos que estejam localizados 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 do FSx para Windows File Server com o namespaces do DFS](#).

Como acessar dados 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 acessar seus compartilhamentos de arquivos usando nomes de DNS diferentes do nome de DNS padrão, registrando aliases de DNS 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 FSx para Windows File Server e continuar usando os nomes de 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. Você pode associar até 50 aliases de DNS a um sistema de arquivos a qualquer momento. Para obter mais informações sobre como associar e desassociar aliases de DNS a um sistema de arquivos do FSx para Windows File Server, consulte [Como gerenciar aliases de DNS](#).

Para configurar o acesso aos seus sistemas de arquivos do FSx para Windows File Server usando aliases de DNS, execute as etapas a seguir:

1. [Associar aliases de DNS ao seu sistema de arquivos](#).
2. [Crie um registro CNAME de DNS](#) para o sistema de arquivos e os aliases de DNS associados a ele.

Para obter mais informações sobre como usar aliases de DNS com sistemas de arquivos do FSx para Windows File Server, consulte [Como gerenciar aliases de DNS](#).

Como usar autenticação e criptografia do Kerberos com aliases de DNS

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 de 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.

Para configurar a autenticação e a criptografia de Kerberos ao acessar seu sistema de arquivos usando aliases de DNS, consulte [Configurar nomes de entidade principal de serviço \(SPNs\) para o Kerberos](#).

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 de 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 de NTLM se a configuração de política Segurança de rede: restringir NTLM: tráfego NTLM de saída para servidores remotos estiver configurada.

Para aplicar a autenticação e a criptografia do Kerberos ao acessar seu sistema de arquivos usando aliases de DNS, consulte [Aplicar a autenticação de Kerberos usando Objetos de política de grupo \(GPOs\)](#).

Para obter mais informações sobre como configurar seu sistema de arquivos para usar aliases de DNS, consulte os procedimentos a seguir:

- [Associar aliases de DNS ao seu sistema de arquivos](#)
- [Configurar nomes de entidade principal de serviço \(SPNs\) para o Kerberos](#)
- [Atualizar ou criar um registro CNAME de DNS](#)
- [Aplicar a autenticação de Kerberos usando Objetos de política de grupo \(GPOs\)](#)

Associar aliases de DNS ao seu sistema de arquivos

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](#).

Para associar aliases de DNS ao criar um novo sistema de arquivos

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 [Etapa 5. Criar 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 hífens (-).
- 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.

Configurar nomes de entidade principal 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 de 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 de 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.

Instalar o módulo Active Directory para PowerShell necessário

1. Faça login em uma instância do Windows associada ao Active Directory ao qual seu sistema de arquivos do Amazon FSx está associado.
2. Abra o PowerShell como administrador.
3. Instale o módulo Active Directory para PowerShell 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

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.

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 [DescribeFileSystems](#).

- 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 the following command to set both the full FQDN and Alias SPNs
Set-AdComputer -Identity $FSxAdComputer -Add @"msDS-AdditionalDnsHostname" =
  @($Alias, $Alias.Split(".")[0])

```

 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 [DescribeFileSystems](#).

```
## 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](#).

Atualizar ou criar um registro CNAME de DNS

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 módulos necessários do PowerShell

1. Faça login em uma instância do Windows associada ao Active Directory ao qual o sistema de arquivos do Amazon FSx esteja associado como um usuário que seja membro de um grupo com permissões de administração de DNS (Administradores do sistema de nomes de domínio delegados da AWS no AWS Managed Microsoft AD e Administradores de domínio ou outro grupo ao qual você tenha delegado permissões de administração de DNS em seu Active Directory autogerenciado).

Para obter mais informações, consulte [Connecting to Your Windows Instance](#) no Amazon EC2 User Guide.

2. Abra o PowerShell como administrador.
3. O módulo do servidor DNS do PowerShell é necessário para a execução das 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 seja membro de um grupo que tenha permissões de administração de DNS (Administradores do sistema de nomes de domínio delegados da AWS no AWS Managed Active Directory e administradores de domínio ou outro grupo ao qual você tenha delegado permissões de administração de DNS em seu Active Directory autogerenciado).

Para obter mais informações, consulte [Connecting to Your Windows Instance](#) no Amazon EC2 User Guide.

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
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
    $DnsServerComputerName -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 obter mais informações, consulte [Não é possível acessar o sistema de arquivos usando um alias de DNS](#).

Aplicar a autenticação de Kerberos usando Objetos de política de grupo (GPOs)

Você pode reforçar a autenticação de 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 de 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 de NTLM se a configuração de política Segurança de rede: restringir NTLM: tráfego NTLM de saída para servidores remotos estiver configurada.

1. Faça login 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.

Acessar dados usando compartilhamentos de arquivos

Um compartilhamento de arquivos do Microsoft Windows é uma pasta ou diretório específico em seu sistema de arquivos. Ele inclui todas as subpastas que possam existir. Os clientes acessam os compartilhamentos de arquivos em seu sistema de arquivos usando o protocolo Server Message Block (SMB). Seu sistema de arquivos do FSx para Windows File Server vem com um compartilhamento de arquivos padrão do Windows, chamado share. Você pode criar e gerenciar quantos compartilhamentos de arquivos do Windows você quiser usando a ferramenta de interface gráfica do usuário (GUI) Pastas Compartilhadas no Windows.

Os compartilhamentos do Microsoft Windows continuamente disponíveis (CA) oferecem o principal benefício de manter o acesso ininterrupto aos arquivos compartilhados, mesmo quando um nó do servidor em um cluster falha. O uso de compartilhamentos de arquivos continuamente disponíveis pode minimizar as interrupções nas aplicações do servidor que estão armazenando seus arquivos de dados nesses compartilhamentos de arquivos durante as janelas de manutenção do sistema de arquivos.

Para obter mais informações sobre como criar e gerenciar compartilhamentos de arquivos em seu sistema de arquivos do FSx para Windows File Server, incluindo compartilhamentos de CAs, consulte [Criar, atualizar e remover compartilhamentos de arquivos](#).

Mapear 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.

Para obter mais informações sobre como mapear e montar compartilhamentos de arquivos para acessar os dados em seu sistema de arquivos, consulte os procedimentos a seguir:

- [Como mapear um compartilhamento de arquivos em uma instância do Amazon EC2 para Windows](#).
- [Como montar um compartilhamento de arquivos em uma instância do Amazon EC2 para Mac](#)
- [Como montar um compartilhamento de arquivos em uma instância do Amazon EC2 para Linux](#)

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

Você pode mapear um compartilhamento de arquivos em uma instância Windows do EC2 usando seu sistema de arquivos do FSx para Windows File Server 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 (Explorador de Arquivos)

1. Inicie a instância do EC2 para 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 EC2 para Windows. Para obter mais informações, consulte [Conectar-se à sua instância baseada no Windows usando RDP](#) 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 da API [CreateFileSystem](#) ou [DescribeFileSystems](#). 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 AWS Managed Microsoft Active Directory, o nome DNS seria como a seguir.

```
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:

```
\\amznfsxaa11bb22.ad-domain.com\share
```

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

```
\\fqn-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 do Windows como um usuário em seu diretório do AWS Managed Microsoft AD. Para obter mais informações, consulte [Conectar-se à sua instância baseada no Windows usando RDP](#) 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 AWS Managed Microsoft Active Directory, o nome DNS seria como a seguir.

```
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: \\amznfsxaa11bb22.ad-domain.com\share /persistent:yes
```

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

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

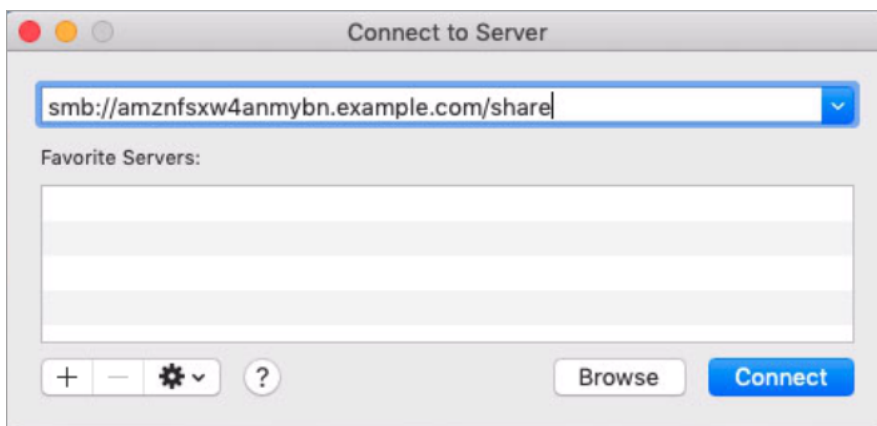
Para montar seu compartilhamento de arquivos em uma instância do Amazon EC2 para Mac que esteja ou não associada ao seu Active Directory para acessar o sistema de arquivos do FSx para Windows File Server. Se a instância não estiver associada ao seu Active Directory, certifique-se de atualizar as opções 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 para Mac (GUI)

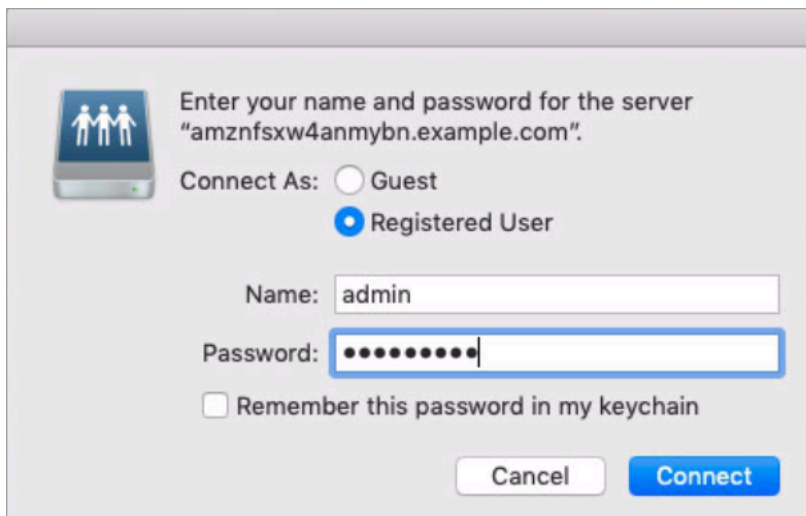
1. Inicie a instância do EC2 para Mac. Para fazer isso, escolha um dos seguintes procedimentos no Guia do usuário do Amazon EC2:

- [Executar uma instância do Mac usando o console](#)
 - [Executar uma instância do Mac usando a AWS CLI](#)
2. Conecte-se à sua instância do EC2 do Mac usando a computação de rede virtual (VNC). Para obter mais informações, consulte [Connect to your instance using 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 da API [CreateFileSystem](#) ou [DescribeFileSystems](#). 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](#)
 - [Executar uma instância do Mac usando a AWS CLI](#)
2. Conecte-se à sua instância do EC2 do Mac usando a computação de rede virtual (VNC). Para obter mais informações, consulte [Connect to your instance using 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 AWS Managed Microsoft Active Directory, o nome DNS seria como a seguir.

```
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 para Linux

Para acessar seu sistema de arquivos do FSx para Windows File Server, você pode montar um compartilhamento de arquivos do FSx para Windows File Server em uma instância do Amazon EC2 para Linux que esteja ou não associada ao seu 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 obter mais informações, consulte [Experiência de failover em clientes Linux](#).

Para montar um compartilhamento de arquivos em uma instância do Amazon EC2 para Linux associada a um 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 [Conectar-se à instância do Linux](#) no Guia do usuário do Amazon EC2.
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,cuid=ad_user,rsize=CIFSMaxBufSize,wsiz=CIFSMaxBufSize,cache=no  
file-server-Id
```

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 AWS Managed Microsoft Active Directory, o nome DNS seria como a seguir.

```
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.
- *cuid=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.
- `rsiz=CIFSMaxBufSize`, `wsiz=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 da CLI `describe-file-systems` ou do comando da API [DescribeFileSystems](#) equivalente.

Para montar um compartilhamento de arquivos em uma instância do Amazon EC2 para Linux não associada a um 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 de 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 [Executar 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 [Conectar-se à instância do Linux](#) no Guia do usuário do Amazon EC2.
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,wsiz=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.
- `rsiz=CIFSMaxBufSize`, `wsiz=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)
```

Montar automaticamente compartilhamentos de arquivos em uma instância Linux do Amazon EC2

Você pode montar automaticamente o compartilhamento de arquivos do FSx para Windows File Server para acessar seu sistema de arquivos do FSx para Windows File Server sempre que a instância Linux do Amazon EC2 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 de NTLM da Microsoft. 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. Você pode recuperar as credenciais da conta de usuário do arquivo `creds.txt` usando o comando a seguir.

```
$ 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 [Executar uma instância](#) no Guia do usuário do Amazon EC2.
2. Conecte-se à sua instância. Para obter mais informações, consulte [Conectar-se à instância do Linux](#) no Guia do usuário do Amazon EC2.
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,wsiz=CIFSMaxBufSize,cache=none 0 0
```

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=ntlmssp1`: especifica o uso da interface do provedor de suporte de segurança do NT LAN Manager para facilitar a autenticação de NTLM 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` a fim de indicar que `fsck` não deve ser executado na inicialização.

Criar, atualizar e remover compartilhamentos de arquivos

Este tópico descreve como gerenciar compartilhamentos de arquivos executando as tarefas a seguir.

- 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 no PowerShell para gerenciar compartilhamentos de arquivos no sistema de arquivos do FSx para 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 o PowerShell para gerenciar compartilhamentos de arquivos localizados em vários sistemas de arquivos.

O Microsoft Windows impõe regras e limitações para nomear 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.

Gerenciar 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 AWS Managed Microsoft Active Directory, esse grupo é denominado Administradores delegados do FSx da AWS. 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 [DescribeFileSystems](#).

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 ao abrir 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 o PowerShell conforme descrito abaixo.

Gerenciar compartilhamentos de arquivos com o PowerShell

Você pode gerenciar compartilhamentos de arquivos usando comandos personalizados de gerenciamento remoto do FSx para Windows File Server para o PowerShell. Esses comandos podem ajudar você a automatizar o gerenciamento de tarefas de compartilhamento de arquivos, como:

- Migrar compartilhamentos de arquivos de servidores de arquivos existentes para o Amazon FSx
- Sincronizar compartilhamentos de arquivos em Regiões da AWS para recuperação de desastres
- Gerenciar programaticamente fluxos de trabalho contínuos de compartilhamentos de arquivos, como provisionamento de compartilhamento de arquivos em equipe

Para saber como usar a CLI do Amazon FSx para gerenciamento remoto no PowerShell, consulte [Usando a Amazon FSx CLI para PowerShell](#).

A tabela a seguir lista os comandos do PowerShell para gerenciamento remoto da CLI do Amazon FSx que você pode usar para gerenciar compartilhamentos de arquivos em sistemas de arquivos do FSx para 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 compartilhamento.
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 -?`.

Passar credenciais para New-FSxSmbShare

Você pode passar credenciais para New-FSxSmbShare para execução em um loop para criar centenas ou milhares de compartilhamentos sem precisar reinserir as credenciais 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 recurso do AWS Secrets Manager, use o comando a seguir.

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

Para criar um compartilhamento continuamente disponível (CA)

Você pode criar compartilhamentos continuamente disponíveis (CA) usando a CLI do Amazon FSx para gerenciamento remoto no 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`.

Determinar se um compartilhamento de arquivos existente está continuamente disponível

Use o comando apresentado a seguir para visualizar o valor da propriedade `Continuamente disponível` para um compartilhamento de arquivos existente.

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -  
scriptblock { get-fsx smbshare -name share_name }
```

Se a propriedade CA estiver habilitada, a saída incluirá a seguinte linha:

```
[...]  
ContinuouslyAvailable : True  
[...]
```

Se a propriedade CA não estiver habilitada, a saída incluirá a seguinte linha:

```
[...]  
ContinuouslyAvailable : False  
[...]
```

Para habilitar a Disponibilidade contínua em um compartilhamento de arquivos existente, use o seguinte comando:

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -  
scriptblock { set-fsx smbshare -name share_name -ContinuouslyAvailable $True }
```

O comando New-FSxSmbShare falha com uma confiança unidirecional

O Amazon FSx não é compatível com a execução do comando New-FSxSmbShare do PowerShell nos casos em que há uma confiança unidirecional e o domínio no qual o usuário reside não está configurado para confiar no domínio associado ao sistema de arquivos do 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 obter mais informações, consulte [Gerenciar compartilhamentos de arquivos com a GUI de Pastas Compartilhadas](#).

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 ajudar você a escolher o tipo certo de implantação para suas workloads. 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 geralmente apresentam cerca de 30 minutos de tempo de inatividade durante eventos de recuperação de falhas e durante a janela de manutenção planejada que você configura para o seu sistema de arquivos. Com os sistemas de arquivos single-AZ, a falha do sistema de arquivos pode ser irreversível 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 o tipo de 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). As workloads com disponibilidade relaxada e necessidades de RPO 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, em casos raros, a perda de atualizações de dados desde o backup mais recente.

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 o tipo de implantação escolhido durante eventos como manutenção do sistema de arquivos, alterações na capacidade de throughput e interrupções não planejadas do serviço.

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 alta disponibilidade do SQL Server.

Processo de failover

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 passando por failback, a E/S pode ser pausada e as métricas do Amazon CloudWatch podem ficar temporariamente indisponíveis. Para sistemas de arquivos multi-AZ, todas as atividades de leitura e gravação de arquivos que ocorrer durante o failover e o failback deverão ser sincronizadas entre os servidores de arquivos primário e secundário. Pode levar várias horas até que os sistemas de arquivos com armazenamento HDD e as workloads com alto índice de gravação e de IOPS concluam esse processo. 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 oferecer serviços 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](#).

Recursos do sistema de arquivos single e multi-AZ

Os sistemas de arquivos single-AZ e multi-AZ consomem sub-redes e interfaces de rede elásticas de forma diferente, conforme explicado nas seções a seguir.

Sub-redes

Quando você cria uma nuvem privada virtual (VPC), ela abrange todas as zonas de disponibilidade (AZs) da Região da AWS. 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. Uma sub-rede consiste em um intervalo de endereços IP na VPC. Cada sub-rede fica alocada em uma única zona de disponibilidade.

Os sistemas de arquivos do FSx para Windows File Server single-AZ exigem uma sub-rede especificada no momento da criação. A sub-rede escolhida define a zona de disponibilidade na qual o sistema de arquivos é criado.

Os sistemas de arquivos multi-AZ exigem 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 dentro da mesma região da AWS.

Para aplicações na AWS, recomendamos que você inicie seus clientes na mesma zona de disponibilidade do seu servidor de arquivos preferencial para minimizar a latência.

Interfaces de rede elástica do sistema de arquivos

[Interfaces de rede elástica](#) são componentes lógicos de rede em uma VPC que representa uma cartão de rede virtual. Quando você cria um sistema de arquivos do Amazon FSx, o Amazon FSx provisiona uma ou mais interfaces de rede elástica na VPC que você associa ao seu sistema de arquivos. A interface de rede elástica permite que os clientes se comuniquem e montem o sistema de arquivos. A interface de rede elástica 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

Não modifique ou exclua 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 utilização de recursos de sistemas de arquivos do FSx para Windows File Server single-AZ e multi-AZ:

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.

Trabalhar com o Microsoft Active Directory

Ao criar um sistema de arquivos do FSx para Windows File Server, você o associa ao seu domínio do Active Directory para fornecer autenticação de usuário e controle de acesso em nível de arquivo e pasta. O Amazon FSx trabalha com o Microsoft Active Directory para se integrar aos seus ambientes do Microsoft Windows existentes. O Amazon FSx oferece duas opções de uso do seu sistema de arquivos do FSx para Windows File Server com o Active Directory: [Como usar o Amazon FSx com o AWS Directory Service for Microsoft Active Directory](#) e [Usar um Microsoft Active Directory autogerenciado](#).

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.

Então, seus usuários poderão usar suas identidades de usuário existentes no Active Directory para se autenticar e acessar o sistema de arquivos do FSx para Windows File Server. Os usuários também podem usar suas identidades existentes para controlar o acesso a arquivos e pastas individuais. Além disso, você pode migrar arquivos e pastas existentes junto com a configuração de lista de controle de acesso (ACL) de segurança para o Amazon FSx sem nenhuma modificação.

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 poderá alterar as seguintes propriedades do Microsoft Active Directory associado após ter criado o sistema de arquivos:

- DomainName

- `OrganizationalUnitDistinguishedName`
- `FileSystemAdministratorsGroup`

No entanto, você pode criar um novo sistema de arquivos de um backup e alterar essas propriedades na configuração de integração do Microsoft Active Directory do novo sistema de arquivos. Para obter mais informações, consulte [Restaurar backups em um novo sistema de arquivos](#).

 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

- [Como usar o Amazon FSx com o AWS Directory Service for Microsoft Active Directory](#)
- [Usar um Microsoft Active Directory autogerenciado](#)

Como usar o Amazon FSx com o AWS Directory Service for Microsoft Active Directory

O AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) fornece diretórios efetivos, totalmente gerenciados e altamente disponíveis do Active Directory na nuvem. Você pode usar esses diretórios do Active Directory em sua implantação da workload.

Se sua organização estiver usando o AWS Managed Microsoft AD para gerenciar identidades e dispositivos, recomendamos que você integre seu sistema de arquivos do Amazon FSx com o AWS Managed Microsoft AD. Ao fazer isso, você obtém uma solução pronta para uso usando o Amazon FSx com o AWS Managed Microsoft AD. A 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 workload de forma eficaz.

Para usar o Amazon FSx com a configuração do 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, escolha AWS Managed Active Directory na seção Autenticação do Windows. Você também escolhe o diretório específico que deseja usar. Para obter mais informações, consulte [Etapa 5. Criar 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 associar seu sistema de arquivos do Amazon FSx diretamente ao seu domínio do Active Directory autogerenciado existente. Para obter mais informações, consulte [Usar um 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 do Amazon FSx, em uma floresta de Active Directory separada daquela em que seus usuários estão.

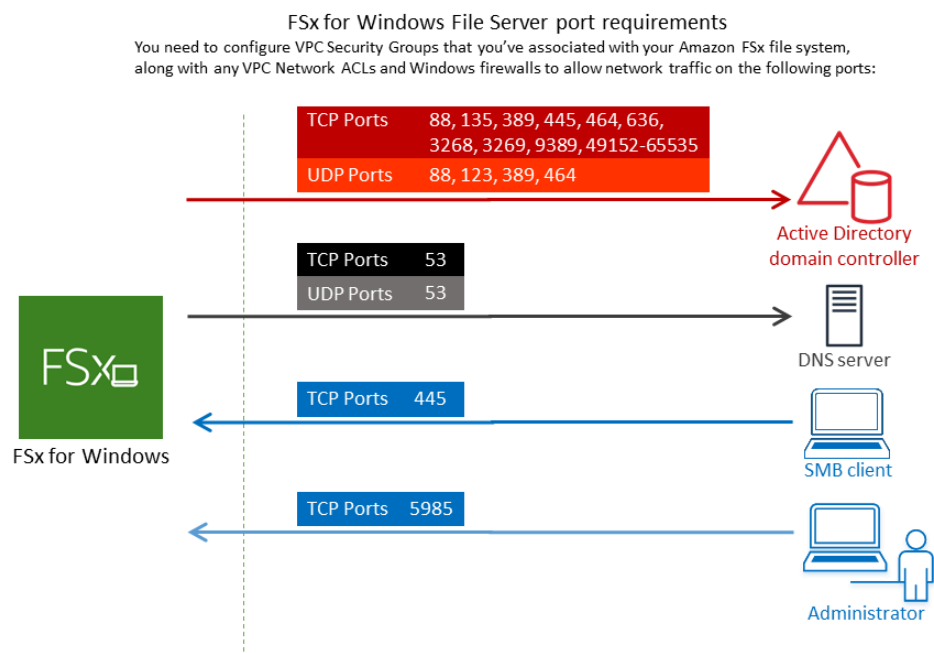
Important

Para sistemas de arquivos single-AZ 2 e todos os sistemas de arquivos multi-AZ, o nome de domínio totalmente qualificado (FQDN) do Active Directory não pode exceder 47 caracteres.

Pré-requisitos de rede

Antes de criar um sistema de arquivos do FSx para Windows File Server associado ao seu domínio do AWS Microsoft Managed Active Directory, verifique se você criou e definiu 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	Função
TCP/UDP	53	Domínio e Nome de Sistema (DNS)
TCP/UDP	88	Autenticação de Kerberos
TCP/UDP	464	Alteração de senha

Protocolo	Portas	Função
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)
UDP	123	Network Time Protocol (NTP)
TCP	135	Distributed Component Environment/Endpoint Mapper (DCE/EPMA P)
TCP	445	Componente de armazenamento de arquivos de rede SMB para serviços de diretório

Protocolo	Portas	Função
TCP	636	Lightweight Directory Access Protocol over TLS/SSL (LDAP)
TCP	3268	Catálogo global da Microsoft
TCP	3269	Catálogo global da Microsoft sobre SSL
TCP	5.985	WinRM 2.0 (Gerenciamento Remoto do Windows)

Protocolo	Portas	Função
TCP	9389	Serviço 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.

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 do Amazon FSx a um AWS Managed Microsoft Active Directory 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 obter mais informações, consulte [Como usar o Amazon FSx com o AWS Managed Microsoft AD em outra VPC ou conta](#).

 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 de confiança de floresta unidirecional entre um domínio do AWS Managed Microsoft AD 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 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 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 pela AWS. Em um cenário de autenticação de Kerberos, as solicitações de autenticação provenientes de um cliente corporativo são validadas pelo domínio corporativo, que então as encaminha para o AWS Managed Microsoft AD, e eventualmente o cliente apresentará seu tíquete de serviço ao seu sistema de arquivos do FSx para Windows File Server. Para obter mais informações sobre confianças, consulte a publicação [Everything you wanted to know about trusts with AWS Managed Microsoft AD](#) no blog de segurança da AWS.

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 obter mais informações, consulte [Como validar a conectividade com seus controladores de domínio do Active Directory](#).

Os recursos relacionados a seguir podem ajudar, conforme você usa o AWS Directory Service for Microsoft Active Directory com o FSx para Windows File Server:

- [O que está Directory Service](#) no Guia de AWS Directory Service Administração
- [Create your AWS Managed Active Directory](#) no Guia de administração do AWS Directory Service
- [Quando criar uma relação de confiança](#) no Guia de administração do AWS Directory Service

Como usar o Amazon FSx com o AWS Managed Microsoft AD em outra VPC ou conta

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

Note

Você só pode selecionar um AWS Managed Microsoft AD no mesmo Região da AWS do seu sistema de arquivos. Se você quiser usar uma configuração de emparelhamento de VPC entre regiões, use um Microsoft Active Directory autogerenciado. Para obter mais informações, consulte [Usar um Microsoft Active Directory autogerenciado](#).

O fluxo de trabalho para associar 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 Directory Service.

Para configurar seu ambiente de rede, você pode usar o AWS Transit Gateway ou o Amazon VPC e criar uma conexão de emparelhamento da 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). É possível usar o emparelhamento de VPC para conectar VPCs dentro da 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.

Há outro pré-requisito quando você associa seu sistema de arquivos a um diretório do AWS Managed Microsoft AD em uma conta diferente daquela do seu sistema de arquivos. Você também precisará compartilhar seu diretório do Microsoft Active Directory com a outra conta. Para fazer isso, você pode usar o recurso de compartilhamento de diretórios do AWS Managed 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 para Windows File Server com o AWS Managed Microsoft Active Directory ou com uma configuração do Active Directory autogerenciado. 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 [Connecting to Your Windows Instance](#) no Amazon EC2 User Guide.
4. Abra uma janela do Windows PowerShell (usando Executar como administrador) na instância do EC2.

Para testar se o módulo do Active Directory necessário para o 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; Result=Listening; Description=DCE / EPMAP (End Point Mapper)}}
Server	10.0.75.243
UdpDetails	{@{Port=88; Result=Timed Out; Description=Kerberos authentication}, @{Port=123; Result=Listening; Description=NetBIOS over TCP/IP}}
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>

#### Note

Como alternativa ao procedimento acima, você pode usar o `AWSSupport-ValidateFSxWindowsADConfig` runbook para validar sua configuração do Active Directory autogerenciado. Para obter mais informações, consulte [AWSSupport-ValidateFSxWindowsADConfig](#) na Referência do runbook do AWS Systems Manager Automation.

## Usar um Microsoft Active Directory autogerenciado

Se sua organização gerencia identidades e dispositivos usando um Active Directory autogerenciado no local ou na nuvem, você pode associar um FSx sistema de arquivos do Windows File Server ao seu domínio do Active Directory no momento da criação.

Quando você une seu sistema de arquivos ao Active Directory autogerenciado, seu FSx sistema de arquivos do Windows File Server reside na mesma floresta do Active Directory (o principal contêiner lógico 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 seus sistemas de arquivos da FSx Amazon, em uma floresta separada do Active Directory daquela em que seus usuários residem. Para fazer isso, associe seu sistema de arquivos a um Microsoft Active Directory gerenciado pela AWS e estabeleça uma relação de confiança de floresta unidirecional entre um Microsoft Active Directory gerenciado pela AWS que você criar e seu Active Directory autogerenciado existente.

- Nome de usuário e senha de uma conta de serviço em seu domínio do Active Directory, para FSx a Amazon usar para unir o sistema de arquivos ao seu domínio do Active Directory. Você pode fornecer essas credenciais como texto simples ou armazená-las AWS Secrets Manager e fornecer o ARN secreto (recomendado).
- (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, a Amazon FSx delegará essa autoridade ao grupo 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. FSx para Windows File Server não criará o grupo de domínio nas seguintes circunstâncias:

- Se já houver um grupo com o nome que você especificar
- Se você não especificar um nome, e já houver um grupo chamado “Administradores de domínio” no seu Active Directory.

Para obter mais informações, consulte [Unindo um sistema de FSx arquivos da Amazon a um domínio autogerenciado do Microsoft Active Directory](#).

## Tópicos

- [Pré-requisitos](#)
- [Permissões da conta de serviço](#)
- [Práticas recomendadas ao usar um Active Directory autogerenciado](#)
- [Conta de FSx serviço da Amazon](#)
- [Delegar permissões para a conta de FSx serviço ou grupo da Amazon](#)
- [Como validar a configuração do Active Directory](#)
- [Unindo um sistema de FSx arquivos da Amazon a um domínio autogerenciado do Microsoft Active Directory](#)
- [Como obter os endereços IP corretos do sistema de arquivos para usar em entradas DNS manuais](#)
- [Como atualizar a configuração de um Active Directory autogerenciado](#)
- [Alterando a conta FSx de serviço da Amazon](#)
- [Como monitorar as atualizações do Active Directory autogerenciado](#)

## Pré-requisitos

Antes de associar um sistema FSx de arquivos do Windows File Server ao seu domínio autogerenciado do Microsoft Active Directory, revise os seguintes pré-requisitos para ajudar a garantir que você possa unir com sucesso seu sistema de FSx arquivos da Amazon ao seu Active Directory autogerenciado.

### Configurações on-premises

Esses são os pré-requisitos para seu Microsoft Active Directory autogerenciado, local ou baseado na nuvem, ao qual você se juntará ao sistema de arquivos da Amazon. FSx

- Os controladores de domínio do Active Directory:
  - Precisa ter um nível funcional de domínio no Windows Server 2008 R2 ou posterior.
  - Precisa ser gravável.
  - Pelo menos um dos controladores de domínio acessíveis deve ser um catálogo global da floresta.
- O servidor DNS deve ser capaz de resolver nomes da seguinte forma:
  - No domínio em que você está associando ao sistema de arquivos



- No domínio raiz da floresta
- Os endereços IP do servidor DNS e do controlador de domínio do Active Directory devem atender aos seguintes requisitos, que variam dependendo de quando o sistema de FSx arquivos da Amazon 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                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Os endereços IP devem estar em um intervalo de endereços IP privados do <a href="#">RFC 1918</a>:</p> <ul style="list-style-type: none"> <li>• 10.0.0.0/8</li> <li>• 172.16.0.0/12</li> <li>• 192.168.0.0/16</li> </ul> | <p>Os endereços IP podem estar em qualquer intervalo, exceto:</p> <ul style="list-style-type: none"> <li>• Endereços IP que entram em conflito com os endereços IP de propriedade da Amazon Web Services na Região da AWS em que o sistema de arquivos está inserido. Para obter uma lista de endereços IP AWS próprios por região, consulte os <a href="#">intervalos de endereços AWS IP</a>.</li> <li>• Endereços IP no intervalo de blocos CIDR de 198.19.0.0/16</li> </ul> |

Se precisar acessar um sistema FSx de arquivos do Windows File Server criado antes de 17 de dezembro de 2020 usando um intervalo de endereços IP não privado, você poderá criar um novo sistema de arquivos restaurando um backup do sistema de arquivos. Para obter mais informações, consulte [Restaurar um backup em um novo sistema de arquivos](#).

- O nome de domínio do Active Directory autogerenciado deve atender aos seguintes requisitos:
  - O nome de domínio que não está no formato de domínio de rótulo único (SLD). A Amazon FSx não oferece suporte a domínios SLD.
  - Para sistemas de arquivos single-AZ 2 e todos os sistemas de arquivos multi-AZ, o nome de domínio não pode exceder 47 caracteres.
- Todos os sites do Active Directory que você definiu devem atender aos seguintes pré-requisitos:
  - As sub-redes na VPC associada ao seu sistema de arquivos devem ser definidas em um site do Active Directory.
  - Não há conflitos entre as sub-redes da VPC e nenhuma das sub-redes do site do Active Directory.

A Amazon FSx exige conectividade com os controladores de domínio ou sites do Active Directory que você definiu em seu ambiente do Active Directory. A Amazon FSx ignorará qualquer controlador de domínio com TCP e UDP bloqueados na porta 389. Para os controladores de domínio restantes em seu Active Directory, certifique-se de que eles atendam aos requisitos de FSx conectividade da Amazon. Além disso, verifique se todas as alterações na conta de serviço são propagadas para todos esses controladores de domínio.

 Important

Não mova objetos de computador que a Amazon FSx cria na OU após a criação do sistema de arquivos. Isso fará com que o sistema de arquivos fique configurado incorretamente.

Você pode validar sua configuração do Active Directory, incluindo testar a conectividade de vários controladores de domínio, usando a ferramenta de [validação do Amazon FSx Active Directory](#). 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 obter mais informações, consulte [Como usar um modelo de isolamento de floresta de recursos](#).

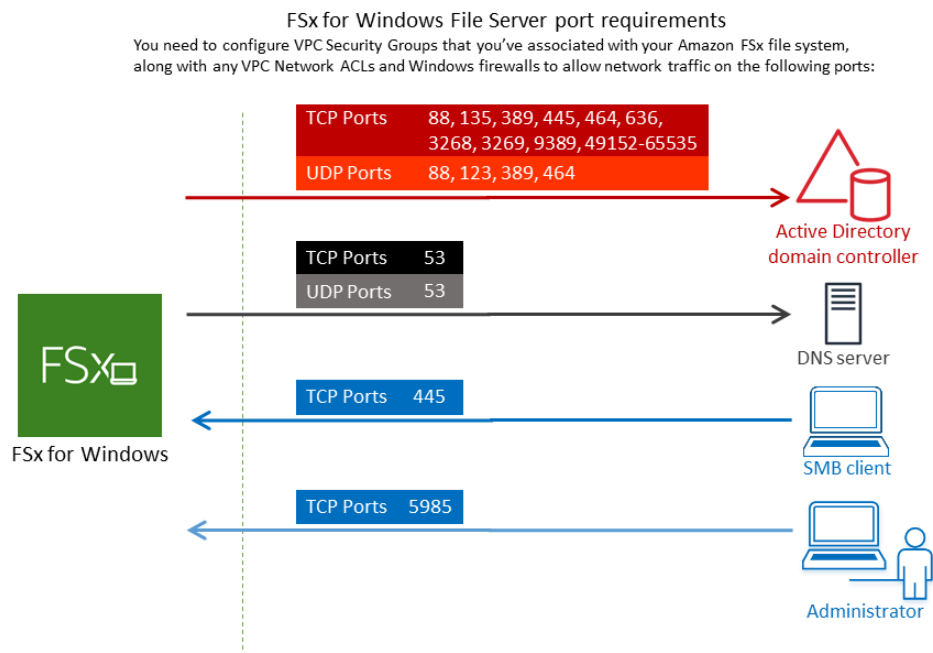
 Important

A Amazon FSx só registra os 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 registro de DNS para seu sistema de arquivos após criá-lo.

## Configurações de rede

Esta seção descreve os requisitos de configuração de rede para associar um sistema de arquivos ao Active Directory autogerenciado. É altamente recomendável que você use a [ferramenta de validação do Amazon FSx Active Directory](#) para testar suas configurações de rede antes de tentar unir seu sistema de arquivos ao seu Active Directory autogerenciado.

- Certifique-se de que suas regras de firewall permitam o tráfego ICMP entre seus controladores de domínio do Active Directory e a Amazon. FSx
- 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 [Direct Connect](#), [AWS Virtual Private Network](#), [emparelhamento da VPC](#) ou [AWS Transit Gateway](#).
- O grupo de segurança VPC padrão para sua Amazon VPC padrão deve ser adicionado ao seu sistema de arquivos usando o console da Amazon. FSx Certifique-se de que o grupo de segurança e a rede ACLs VPC das sub-redes em que você cria seu sistema de arquivos permitam tráfego nas portas e na direção mostrada no diagrama a seguir.



A tabela a seguir identifica o protocolo, as portas e sua função.

| Protocolo | Portas | Perfil                   |
|-----------|--------|--------------------------|
| TCP/UDP   | 53     | Domain Name System (DNS) |
| TCP/UDP   | 88     | Autenticação de Kerberos |
| TCP/UDP   | 464    | Alterar/definir senha    |

| Protocolo                                                                                                                                                                                                                                        | Portas        | Perfil                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|--------------------------------------------------------------------------|
| TCP/UDP                                                                                                                                                                                                                                          | 389           | Lightweight Directory Access Protocol (LDAP)                             |
| UDP                                                                                                                                                                                                                                              | 123           | Network Time Protocol (NTP)                                              |
| TCP                                                                                                                                                                                                                                              | 135           | Mapeador de Environment/End pontos de computação distribuído (DCE/EPMAP) |
| TCP                                                                                                                                                                                                                                              | 445           | Compartilhamento de arquivos de SMB para serviços de diretório           |
| TCP                                                                                                                                                                                                                                              | 636           | LDAPS TLS/SSL (Lightweight Directory Access Protocol over)               |
| 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                |
| <div>  Important<br/> A permissão do tráfego de saída na porta TCP 9389 é necessária para implantações de sistemas de arquivos single-AZ 2 e multi-AZ. </div> |               |                                                                          |
| TCP                                                                                                                                                                                                                                              | 49152 – 65535 | Portas efêmeras para RPC                                                 |

Essas regras de tráfego também precisam ser espelhadas nos firewalls que se aplicam a cada um dos controladores de domínio, servidores DNS, clientes e administradores do Active Directory. FSx FSx

 Note

Se você estiver usando uma rede VPC ACLs, também deverá permitir o tráfego de saída nas portas dinâmicas (49152-65535) do seu sistema de arquivos.

 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, a maioria dos firewalls do Windows e da rede VPC ACLs exigem que as portas sejam abertas em ambas as direções.

## Permissões da conta de serviço

É necessário ter uma conta de serviço em seu Microsoft Active Directory autogerenciado com permissões delegadas para associar objetos de computador ao seu domínio do Active Directory autogerenciado. Uma conta de serviço é uma conta de usuário no Active Directory autogerenciado que recebeu a delegação de certas tarefas.

A seguir está o conjunto mínimo de permissões que devem ser delegadas à conta de FSx serviço da Amazon na OU à qual você está ingressando no sistema de arquivos.

- Se estiver usando o Controle delegado no Console de gerenciamento Microsoft de Computadores e Usuários do Active Directory:
  - Redefinir senhas
  - Restrições de leitura e gravação da conta
  - Gravação validada no nome do host DNS
  - Gravação validada no nome da entidade principal do serviço
- Se estiver usando Recursos avançados no Console de gerenciamento Microsoft de Computadores e Usuários do Active Directory:
  - Modificar permissões
  - Criação de objetos de computador
  - Excluir objetos de computador

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 mais informações sobre como configurar as permissões necessárias, consulte [Delegar permissões para a conta de FSx serviço ou grupo da Amazon](#).

## Práticas recomendadas ao usar um Active Directory autogerenciado

### Tópicos

- [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#)

Recomendamos que você siga essas melhores práticas ao unir um sistema de arquivos Amazon FSx para Windows File Server ao seu Microsoft Active Directory autogerenciado. Essas práticas recomendadas ajudarão a manter a disponibilidade contínua e ininterrupta do sistema de arquivos.

### Use uma conta de serviço separada para a Amazon FSx

Use uma conta de serviço separada para delegar os [privilégios necessários](#) FSx para que a Amazon gerencie totalmente os sistemas de arquivos associados ao seu Active Directory autogerenciado. Não recomendamos o uso de Administradores de domínio para essa finalidade.

### Usar grupo do Active Directory

Use um grupo do Active Directory para gerenciar as permissões e configurações do Active Directory associadas à conta de FSx serviço da Amazon.

### Separar a unidade organizacional (UO)

Para facilitar a localização e o gerenciamento de seus objetos de FSx computador da Amazon, recomendamos que você separe a Unidade Organizacional (OU) que você usa FSx para seus sistemas de arquivos do Windows File Server de outras preocupações com controladores de domínio.

### Mantenha a configuração do Active Directory up-to-date

É fundamental que você mantenha a configuração do Active Directory do seu sistema de arquivos up-to-date com todas as alterações. Por exemplo, se o Active Directory autogerenciado usar uma política de redefinição de senha com base no tempo, atualize a senha da conta de serviço no sistema de arquivos assim que a senha for redefinida. Para obter mais informações, consulte [Como atualizar a configuração de um Active Directory autogerenciado](#).

## Alterando a conta FSx de serviço da Amazon

Se você atualizar o sistema de arquivos com uma nova conta de serviço, ela deverá ter as permissões e os privilégios necessários para associá-la a um Active Directory e ter permissões de Controle total para os objetos de computador atuais associados ao sistema de arquivos. Para obter mais informações, consulte [Alterando a conta FSx de serviço da Amazon](#).

## Atribua sub-redes a um único site do Microsoft Active Directory

Se o seu ambiente do Active Directory 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 FSx arquivos da Amazon a um único site do Active Directory 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 e quaisquer outros controles de roteamento de rede que você tenha na sua infraestrutura do Active Directory permitam a comunicação da Amazon nas portas necessárias. DCs FSx Isso permite que o Windows reverte para outros controladores de domínio, se não puder usar o site do Active Directory atribuído. Para obter mais informações, consulte [Controle de acesso ao sistema de arquivos com a Amazon VPC](#).

## Usar regras de grupo de segurança para limitar o tráfego

Use as regras de grupos de segurança para implementar o princípio do privilégio mínimo na nuvem privada virtual (VPC). Com as regras do grupo de segurança da VPC, você pode limitar o tipo de tráfego de entrada e saída da rede permitido para seu arquivo. Por exemplo, sugerimos que você permita somente o tráfego de saída para os controladores de domínios do Active Directory autogerenciado ou dentro da sub-rede ou do grupo de segurança que esteja usando. Para obter mais informações, consulte [Controle de acesso ao sistema de arquivos com a Amazon VPC](#).

## Não mova objetos de computador criados na Amazon FSx

### Important

Não mova objetos de computador que a Amazon FSx cria na OU após a criação do sistema de arquivos. Isso fará com que o sistema de arquivos fique configurado incorretamente.

## Validar sua configuração do Active Directory

Antes de tentar unir um FSx sistema de arquivos do Windows File Server ao seu Active Directory, é altamente recomendável que você valide sua configuração do Active Directory usando a ferramenta de [validação do Amazon FSx Active Directory](#).

## Armazenando credenciais do Active Directory usando AWS Secrets Manager

Você pode usar AWS Secrets Manager para armazenar e gerenciar com segurança suas credenciais da conta de serviço de ingresso no domínio do Microsoft Active Directory. Essa abordagem elimina a necessidade de armazenar credenciais confidenciais em texto simples no código da aplicação ou nos arquivos de configuração, fortalecendo sua postura de segurança.

Você também pode configurar políticas do IAM para gerenciar o acesso aos seus segredos e configurar políticas de rotação automática para suas senhas.

Armazene as credenciais do Active Directory em AWS Secrets Manager (Console)

Etapa 1: criar uma chave do KMS

Crie uma chave do KMS para criptografar e descriptografar suas credenciais do Active Directory no Secrets Manager.

Para criar uma chave

### Note

Para Chave de criptografia, crie uma nova chave, não use a chave KMS AWS padrão. Certifique-se de criar o AWS KMS key na mesma região que contém o sistema de arquivos que você deseja associar ao seu Active Directory.

1. Abra o AWS KMS console em <https://console.aws.amazon.com/kms>.
2. Escolha Criar chave.
3. Em Tipo de chave, escolha Simétrica.
4. Em Uso da chave, escolha Criptografar e descriptografar.
5. Em Opções avançadas, faça o seguinte:
  - a. Em Origem do material de chaves, escolha Externa.



- b. Em Regionalidade, escolha Chave de região única e escolha Próximo.
6. Escolha Próximo.
7. Em Alias, forneça um nome para a chave do KMS.
8. (Opcional) Em Descrição, forneça uma descrição da chave do KMS.
9. (Opcional) Em Tags, forneça uma tag da chave do KMS e clique em Próximo.
10. (Opcional) Para administradores de chaves, forneça os usuários e usuários e perfis do IAM autorizados a gerenciar essa chave.
11. Em Exclusão de chaves, mantenha a caixa Permitir administradores de chaves selecionada para que eles possam excluir essa chave, e escolha Próximo.
12. (Opcional) Para usuários de chaves, forneça os usuários e perfis do IAM autorizados a usar essa chave em operações criptográficas. Escolha Próximo.
13. Em Política de chaves, escolha Editar e inclua o seguinte na Declaração de política para permitir que FSx a Amazon use a chave KMS e escolha Avançar. Certifique-se de substituir o no local em *us-west-2* Região da AWS que o sistema de arquivos está implantado e *123456789012* pelo seu Conta da AWS ID.

```
{
 "Sid": "Allow FSx to use the KMS key",
 "Version": "2012-10-17",
 "Effect": "Allow",
 "Principal": {
 "Service": "fsx.amazonaws.com"
 },
 "Action": [
 "kms:Decrypt",
 "kms:DescribeKey"
],
 "Resource": "arn:aws:kms:us-west-2:123456789012:key:*",
 "Condition": {
 "StringEquals": {
 "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-west-2:123456789012:secret:*",
 "kms:ViaService": "secretsmanager.us-west-2.amazonaws.com",
 "aws:SourceAccount": "123456789012"
 },
 "ArnLike": {
 "aws:SourceArn": "arn:aws:fsx:us-west-2:123456789012:file-system/*"
 }
 }
}
```

```
}
}
```

#### 14. Escolha Terminar.

##### Note

Você pode definir um controle de acesso mais granular modificando os campos `aws:SourceArn` e `Resource` para alcançar segredos e sistemas de arquivos específicos.

### Etapa 2: criar um AWS Secrets Manager segredo

#### Como criar um segredo

1. Abra o console do Secrets Manager em <https://console.aws.amazon.com/secretsmanager/>.
2. Selecione Armazenar um novo segredo.
3. Em Tipo de segredo, escolha Outro tipo de segredo.
4. Em Pares de chave/valor, faça o seguinte para adicionar suas duas chaves:
  - a. Para a primeira chave, insira `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`.
  - b. Para o valor da primeira chave, insira somente o nome de usuário (sem o prefixo do domínio) do usuário do AD.
  - c. Para a segunda chave, insira `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`.
  - d. Para o valor da segunda chave, insira a senha que você criou para o usuário do AD no domínio.
5. Em Chave de criptografia, insira a chave do KMS que você criou em uma etapa anterior e escolha Próximo.
6. Em Nome do segredo, insira um nome descritivo que ajude você a encontrar o segredo posteriormente.
7. (Opcional) Em Descrição, insira uma descrição para o nome do segredo.
8. Em Permissão de recurso, escolha Editar.

Adicione a política a seguir à política de permissão para permitir que FSx a Amazon use o segredo e escolha Avançar. Certifique-se de substituir o `us-west-2` no local em `us-west-2` Região da AWS que o sistema de arquivos está implantado e `123456789012` pelo seu Conta da AWS ID.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "fsx.amazonaws.com"
 },
 "Action": [
 "secretsmanager:GetSecretValue",
 "secretsmanager:DescribeSecret"
],
 "Resource": "arn:aws:secretsmanager:us-west-2:123456789012:secret:*",
 "Condition": {
 "StringEquals": {
 "aws:SourceAccount": "123456789012"
 },
 "ArnLike": {
 "aws:SourceArn": "arn:aws:fsx:us-west-2:123456789012:file-
system/*"
 }
 }
 }
]
}
```

#### Note

Você pode definir um controle de acesso mais granular modificando os campos `aws:SourceArn` e `Resource` para alcançar segredos e sistemas de arquivos específicos.

9. (Opcional) Você pode configurar o Secrets Manager para alternar suas credenciais automaticamente. Escolha Próximo.
10. Escolha Terminar.

## Armazene as credenciais do Active Directory em AWS Secrets Manager (CLI)

### Etapa 1: criar uma chave do KMS

Crie uma chave do KMS para criptografar e descriptografar suas credenciais do Active Directory no Secrets Manager.

Para criar uma chave KMS, use o AWS CLI comando [create-key](#).

Nesse comando, defina o parâmetro `--policy` para especificar a política de chave que define as permissões para a chave do KMS. A política deve incluir o seguinte:

- O principal serviço da Amazon FSx, qual é `fsx.amazonaws.com`.
- Ações necessárias do KMS: `kms:Decrypt` e `kms:DescribeKey`.
- Padrão de ARN de recurso para sua conta Região da AWS .
- Chaves de condição que restringem o uso da chave:
  - `kms:ViaService` para garantir que as solicitações cheguem por meio do Secrets Manager.
  - `aws:SourceAccount` para limitar sua conta.
  - `aws:SourceArn` para restringir a sistemas de FSx arquivos específicos da Amazon.

O exemplo a seguir cria uma chave KMS de criptografia simétrica com uma política que permite que FSx a Amazon use a chave para operações de descriptografia e descrição da chave. O comando recupera automaticamente seu Conta da AWS ID e região e, em seguida, configura a política de chaves com esses valores para garantir controles de acesso adequados entre a Amazon FSx, o Secrets Manager e a chave KMS. Certifique-se de que seu AWS CLI ambiente esteja na mesma região do sistema de arquivos que se juntará ao Active Directory.

```
Set region and get Account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

Create Key
KMS_KEY_ARN=$(aws kms create-key --policy "{
 \"Version\": \"2012-10-17\",
 \"Statement\": [
 {
 \"Sid\": \"Enable IAM User Permissions\",
 \"Effect\": \"Allow\",
```

```

 \"Principal\": {
 \"AWS\": \"arn:aws:iam::$ACCOUNT_ID:root\"
 },
 \"Action\": \"kms:*\",
 \"Resource\": \"*\"
 },
 {
 \"Sid\": \"Allow FSx to use the KMS key\",
 \"Effect\": \"Allow\",
 \"Principal\": {
 \"Service\": \"fsx.amazonaws.com\"
 },
 \"Action\": [
 \"kms:Decrypt\",
 \"kms:DescribeKey\"
],
 \"Resource\": \"*\",
 \"Condition\": {
 \"StringEquals\": {
 \"kms:ViaService\": \"secretsmanager.$REGION.amazonaws.com\",
 \"aws:SourceAccount\": \"$ACCOUNT_ID\"
 },
 \"ArnLike\": {
 \"aws:SourceArn\": \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\"
 }
 }
 }
]
}" --query 'KeyMetadata.Arn' --output text)

echo "KMS Key ARN: $KMS_KEY_ARN"

```

### Note

Você pode definir um controle de acesso mais granular modificando os campos `aws:SourceArn` e `Resource` para alcançar segredos e sistemas de arquivos específicos.

## Etapa 2: criar um AWS Secrets Manager segredo

Para criar um segredo para FSx a Amazon acessar seu Active Directory, use o AWS CLI comando [create-secret](#) e defina os seguintes parâmetros:

- `--name`: o identificador do seu segredo.
- `--description`: uma descrição da finalidade do segredo.
- `--kms-key-id`: o ARN da chave do KMS que você criou na [Etapa 1](#) para criptografar o segredo em repouso.
- `--secret-string`: uma string JSON contendo suas credenciais do AD no seguinte formato:
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`: o nome de usuário da sua conta de serviço do AD sem o prefixo do domínio, como `svc-fsx`. Não forneça o prefixo do domínio, como `CORP\svc-fsx`.
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`: sua senha da conta de serviço do AD.
- `--region`: O Região da AWS local onde seu sistema de FSx arquivos da Amazon será criado. Isso é padronizado para sua região configurada, se a `AWS_REGION` não estivesse definida.

Depois de criar o segredo, anexe uma política de recursos usando o [put-resource-policy](#) comando e defina os seguintes parâmetros:

- `--secret-id`: o nome ou ARN do segredo para anexar à política. O exemplo a seguir usa **FSxSecret** como `--secret-id`.
- `--region`: O mesmo Região da AWS que seu segredo.
- `--resource-policy`: um documento de política JSON que concede FSx permissão à Amazon para acessar o segredo. A política deve incluir o seguinte:
  - O principal serviço da Amazon FSx, qual é **fsx.amazonaws.com**.
  - Ações necessárias do Secrets Manager: `secretsmanager:GetSecretValue` e `secretsmanager:DescribeSecret`.
  - Padrão de ARN de recurso para sua conta Região da AWS .
  - As seguintes chaves de condição que restringem o acesso:
    - `aws:SourceAccount` para limitar sua conta.
    - `aws:SourceArn` para restringir a sistemas de FSx arquivos específicos da Amazon.

O exemplo a seguir cria um segredo com o formato necessário e anexa uma política de recursos que permite que FSx a Amazon use o segredo. Este exemplo recupera automaticamente seu Conta da AWS ID e região e, em seguida, configura a política de recursos com esses valores para garantir controles de acesso adequados entre a Amazon FSx e o segredo.

Certifique-se de substituir KMS\_KEY\_ARN o pelo ARN da chave que você criou na [Etapa 1](#), CUSTOMER\_MANAGED\_ACTIVE\_DIRECTORY\_USERNAME e CUSTOMER\_MANAGED\_ACTIVE\_DIRECTORY\_PASSWORD pelas credenciais da sua conta de serviço do Active Directory. Além disso, verifique se seu AWS CLI ambiente está configurado para a mesma região do sistema de arquivos que se juntará ao Active Directory.

```
Set region and get account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

Replace with your KMS key ARN from Step 1
KMS_KEY_ARN="arn:aws:kms:us-east-2:123456789012:key/1234542f-d114-555b-9ade-
fec3c9200d8e"

Replace with your Active Directory credentials
AD_USERNAME="Your_Username"
AD_PASSWORD="Your_Password"

Create the secret
SECRET_ARN=$(aws secretsmanager create-secret \
 --name "FSxSecret" \
 --description "Secret for FSx access" \
 --kms-key-id "$KMS_KEY_ARN" \
 --secret-string "{\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME\": \"$AD_USERNAME\",
\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD\": \"$AD_PASSWORD\"}" \
 --region "$REGION" \
 --query 'ARN' \
 --output text)

echo "Secret created with ARN: $SECRET_ARN"

Attach the resource policy with proper formatting
aws secretsmanager put-resource-policy \
 --secret-id "FSxSecret" \
 --region "$REGION" \
 --resource-policy "{
 \"Version\": \"2012-10-17\",
 \"Statement\": [
 {
 \"Effect\": \"Allow\",
 \"Principal\": {
 \"Service\": \"fsx.amazonaws.com\"
 },
```

```
\ "Action\": [
 \ "secretsmanager:GetSecretValue\<",
 \ "secretsmanager:DescribeSecret\<"
],
\ "Resource\": \ "$SECRET_ARN\<",
\ "Condition\": {
 \ "StringEquals\": {
 \ "aws:SourceAccount\": \ "$ACCOUNT_ID\<"
 },
 \ "ArnLike\": {
 \ "aws:SourceArn\": \ "arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*"
 }
}
}
]
}"

echo "Resource policy attached successfully"
```

#### Note

Você pode definir um controle de acesso mais granular modificando os campos `aws:SourceArn` e `Resource` para alcançar segredos e sistemas de arquivos específicos.

## Conta de FSx serviço da Amazon

Os sistemas de FSx arquivos da Amazon associados a um Active Directory autogerenciado exigem uma conta de serviço válida durante toda sua vida útil. A Amazon FSx usa a conta de serviço para gerenciar totalmente seus sistemas de arquivos e realizar tarefas administrativas que exigem a separação e a rejunção de objetos de computador ao seu domínio do Active Directory. Essas tarefas incluem a substituição de um servidor de arquivos com falha e a aplicação de patches no software Microsoft Windows Server. Para FSx que a Amazon execute essas tarefas, a conta de FSx serviço da Amazon deve ter, no mínimo, o conjunto de permissões descrito em [Permissões da conta de serviço](#) Delegado a ela.

Embora os membros do grupo de administradores de domínio tenham privilégios suficientes para realizar essas tarefas, é altamente recomendável que você use uma conta de serviço separada para delegar os privilégios necessários à Amazon. FSx



Para obter mais informações sobre como delegar privilégios usando os recursos Controle de delegado ou Recursos avançados no snap-in do Console de gerenciamento Microsoft de Computadores e Usuários do Active Directory, consulte [Delegar permissões para a conta de FSx serviço ou grupo da Amazon](#).

Se você atualizar o sistema de arquivos com uma nova conta de serviço, a nova conta de serviço deverá ter as permissões e os privilégios necessários para associá-la a um Active Directory e ter permissões de Controle total para os objetos de computador atuais associados ao sistema de arquivos. Para obter mais informações, consulte [Alterando a conta FSx de serviço da Amazon](#).

Recomendamos armazenar as credenciais da conta de serviço do Active Directory no AWS Secrets Manager para aumentar a segurança. Isso elimina a necessidade de armazenar credenciais confidenciais em texto simples e se alinha às práticas de segurança recomendadas. Para obter mais informações, consulte [Usar um Microsoft Active Directory autogerenciado](#).

## Delegar permissões para a conta de FSx serviço ou grupo da Amazon

A conta FSx de serviço ou grupo de administradores da Amazon deve ter [os privilégios necessários](#) FSx para unir os sistemas de arquivos do Windows File Server ao seu domínio autogerenciado do Active Directory. Para delegar essas permissões, você pode usar o Controle de delegado ou os Recursos avançados no snap-in do Active Directory User and Computers MMC, conforme descrito nos procedimentos a seguir.

Para atribuir permissões usando o Controle de delegado

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

1. Faça login no sistema como administrador de domínio para o domínio do Active Directory.
2. Abra o snap-in do MMC de Computadores e Usuários 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 sua conta de FSx serviço ou grupo da Amazon 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. 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 sistema como administrador de domínio para o domínio do Active Directory.
2. Abra o snap-in do MMC de Computadores e Usuários 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 Propriedades.
6. No painel Propriedades da UO, selecione a guia Segurança.
7. Na guia Segurança, selecione Avançado. Em seguida, selecione Adicionar.
8. Na página de entrada de permissão, escolha Selecionar um diretor e insira o nome da sua conta ou grupo de FSx serviços da Amazon. Em Aplica-se a:, escolha Este objeto e todos os computadores 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.

## Como validar a configuração do Active Directory

Antes de criar um sistema de arquivos FSx para Windows File Server associado ao seu Active Directory, recomendamos que você valide sua configuração do Active Directory usando a ferramenta de validação do Amazon FSx Active Directory. 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. Execute uma instância EC2 do Amazon Windows na mesma sub-rede e com os mesmos grupos de segurança da Amazon VPC que você usa para o FSx seu sistema de arquivos do Windows File Server. Certifique-se de que sua EC2 instância tenha as permissões necessárias `AmazonEC2ReadOnlyAccess` do IAM. Você pode validar as permissões de função da EC2 instância 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 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 EC2 instância. Para obter mais informações, consulte [Conectando-se à sua instância do Windows](#) no Guia EC2 do usuário da Amazon.
4. Abra uma PowerShell janela do Windows (usando Executar como administrador) na EC2 instância.

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 FSx arquivos da Amazon (*SUBNET\_1*, por exemplo *SUBNET\_2*), 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   |
| 10.0.128.0/19 | CN=10.0.128.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-ad,DC=local |
| 10.0.64.0/19  | CN=10.0.64.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-ad,DC=local  |

Best match for EC2 subnet subnet-092f4caca69e360e7 is AD site CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test-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 da Amazon FSx](#).

## Unindo um sistema de FSx arquivos da Amazon a um domínio autogerenciado do Microsoft Active Directory

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

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

### Note

FSx Atualmente, a Amazon não oferece suporte a domínios Single Label Domain (SLD).

- Os endereços IP de servidores DNS para o seu domínio.
- Credenciais para uma conta de serviço do Active Directory que a Amazon FSx usa para unir o sistema de arquivos ao seu domínio. Você pode fornecê-los como:
  - Opção 1: ARN AWS Secrets Manager secreto - O segredo que contém o nome de usuário e a senha de uma conta de serviço no seu domínio do Active Directory. Para obter mais informações, consulte [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#).
  - Opção 2: credenciais em texto não criptografado
    - Nome de usuário da conta de serviço: o nome de usuário da conta de serviço no seu Microsoft Active Directory existente. Não inclua um prefixo ou sufixo de domínio. Por exemplo, para EXAMPLE\ADMIN, use apenas ADMIN.
    - Senha da conta de serviço: a senha da conta de serviço.

Opcionalmente, também é possível especificar as seguintes opções:

- Uma Unidade Organizacional (OU) específica dentro do domínio ao qual você deseja que seu sistema de FSx arquivos da Amazon se junte.
- O nome do grupo de domínio cujos membros recebem privilégios administrativos para o sistema de FSx arquivos da Amazon. O nome do grupo de domínio fornecido deve ser exclusivo no Active Directory.

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

#### Important

A Amazon FSx só registra 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 FSx arquivos da Amazon 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 em entradas DNS manuais](#).

## Antes de começar

Garanta que concluiu o [Pré-requisitos](#) detalhado no [Usar um Microsoft Active Directory autogerenciado](#).

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

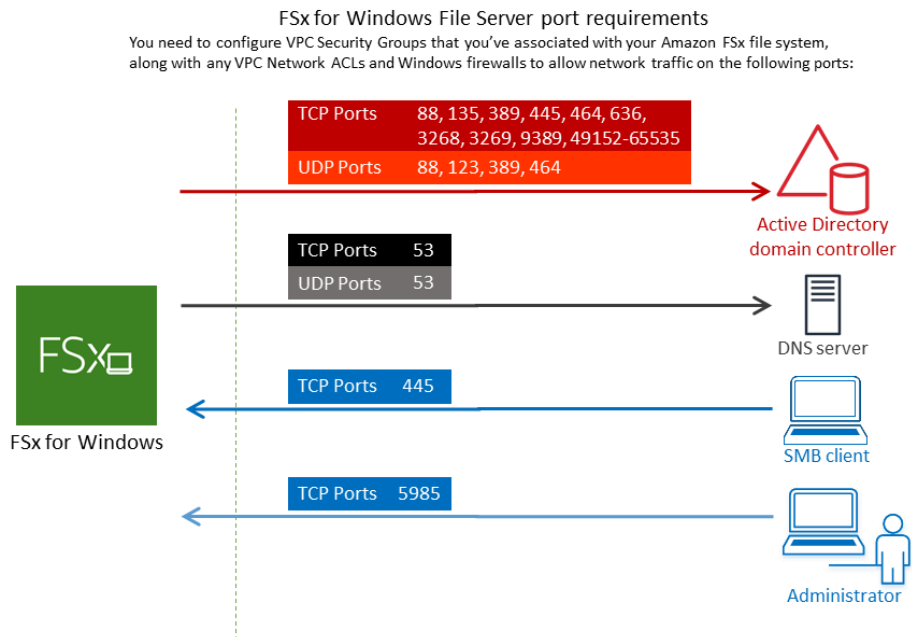
1. Abra o FSx console da Amazon em <https://console.aws.amazon.com/fsx/>.
2. No painel, escolha Create file system (Criar sistema de arquivos) para iniciar o assistente de criação de sistemas de arquivos.
3. Escolha Windows FSx File Server e, em seguida, escolha Avançar. A página Criar sistema de arquivos 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 mil e 65.536. Você pode aumentar a capacidade de armazenamento, conforme necessário, a qualquer momento após a criação do sistema de arquivos. Para obter 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 obter mais informações, consulte [desempenho 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 obter 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 para seu Directory Service diretório e instância da 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 a rede VPC da (s) sub-rede ACLs (s) em que você está criando seu sistema de FSx arquivos permitam tráfego nas portas e nas direções mostradas no diagrama a seguir.



A tabela a seguir identifica o perfil de cada porta.

| Protocolo | Portas | Perfil                              |
|-----------|--------|-------------------------------------|
| TCP/UDP   | 53     | Domínio<br>Nome<br>Sistema<br>(DNS) |
| TCP/UDP   | 88     | Autenticação<br>de<br>Kerberos      |
| TCP/UDP   | 464    | Alteração<br>de<br>senha            |

| Protocolo | Portas | Perfil                                                            |
|-----------|--------|-------------------------------------------------------------------|
| TCP/UDP   | 389    | Lightweight Directory Access Protocol (LDAP)                      |
| UDP       | 123    | Network Time Protocol (NTP)                                       |
| TCP       | 135    | Distributed Component Environment/Endpoint Mapper (DCERPM)        |
| TCP       | 445    | Component-based File System (CIFS) for SMB services and directory |

| Protocolo | Portas | Perfil                                                                    |
|-----------|--------|---------------------------------------------------------------------------|
| TCP       | 636    | LDAP<br>TLS/<br>SSL<br>(Light<br>ght<br>Direct<br>Acces<br>Proto<br>over) |
| TCP       | 3268   | Catálo<br>global<br>da<br>Micros                                          |
| TCP       | 3269   | Catálo<br>global<br>da<br>Micros<br>sobre<br>SSL                          |
| TCP       | 5985   | WinRM<br>2.0<br>(Gere<br>mento<br>Remo<br>do<br>Micros<br>Wind            |

| Protocolo | Portas        | Perfil                                                   |
|-----------|---------------|----------------------------------------------------------|
| TCP       | 9389          | Serviço Web do Microsoft Active Directory 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.

#### Note

Se você estiver usando uma rede VPC ACLs, também deverá permitir o tráfego de saída nas portas dinâmicas (49152-65535) do seu sistema de arquivos. 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](#).

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

 **Note**

Se você tiver sites do Active Directory definidos, deverá garantir que as sub-redes na VPC associadas ao seu sistema de arquivos da FSx Amazon estejam definidas em um site do Active Directory e que não existam 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 somente na direção em que o tráfego de rede é iniciado, a maioria dos firewalls do Windows e da rede VPC ACLs exigem que as portas sejam abertas em ambas as 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). FSx Atualmente, a Amazon não oferece suporte a domínios 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. Credenciais da conta de serviço: escolha como fornecer as credenciais da sua conta de serviço:
- Opção 1: ARN AWS Secrets Manager secreto - O segredo que contém o nome de usuário e a senha de uma conta de serviço no seu domínio do Active Directory. Para obter mais informações, consulte [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#).
  - Opção 2: credenciais em texto não criptografado
    - Nome de usuário da conta de serviço: o nome de usuário da conta de serviço no seu Microsoft Active Directory existente. Não inclua um prefixo ou sufixo de domínio. Por exemplo, para EXAMPLE\ADMIN, use apenas ADMIN.
    - Senha da conta de serviço: a senha da conta de serviço.
    - Confirmar senha: a senha da conta de serviço.

 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. 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, a Amazon FSx usa o Domain Admins grupo Builtin. Observe que FSx a Amazon 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 delegado de administradores do sistema de arquivos, por padrão, a Amazon FSx tentará usar o Domain Admins grupo integrado no 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\ FSx Admins) ou sufixo de domínio (FSxAdmins@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= FSx Admins, OU=Example, DC=corp, DC=com.

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

O exemplo a seguir cria um sistema de arquivos FSx para Windows File Server com um SelfManagedActiveDirectoryConfiguration na Zona de us-east-2 Disponibilidade.

```
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 que a Amazon FSx cria na OU após a 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 em entradas DNS manuais

A Amazon FSx só registra registros DNS para um sistema de arquivos se você estiver usando o Microsoft DNS como o serviço DNS padrão. Se você estiver usando um DNS de terceiros, precisará configurar manualmente as entradas de DNS para seus sistemas de FSx arquivos da Amazon. 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. No <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, escolha a interface de rede elástica mostrada em Interface de rede para abrir a página Interfaces de rede no EC2 console da Amazon.
    - O endereço IP do sistema de arquivos Single-AZ 1 a ser usado é mostrado na coluna IPv4 IP 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 EC2 console da Amazon.
    - O endereço IP da sub-rede preferencial a ser usada é mostrado na coluna IPv4 IP privado secundário.
    - No painel de sub-rede Amazon FSx Standby, escolha a interface de rede elástica mostrada em Interface de rede para abrir a página Interfaces de rede no console da Amazon EC2 .

- O endereço IP a ser usado pela sub-rede em espera é mostrado na coluna IPv4 IP 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 IPv4 endereço privado primário para a interface de rede elástica de sua sub-rede preferencial. Para obter mais informações, consulte [Usando a Amazon FSx CLI para PowerShell](#).

## Como atualizar a configuração de um Active Directory autogerenciado

Para ajudar a garantir a disponibilidade contínua e ininterrupta do seu sistema de FSx arquivos da Amazon, você deve atualizar a configuração do Active Directory do sistema de arquivos quando qualquer uma das seguintes propriedades do Active Directory for alterada:

- Os endereços IP do servidor DNS
- As credenciais da conta de serviço do Active Directory autogerenciado

Quando você atualiza a configuração autogerenciada do Active Directory para seu sistema de FSx arquivos da Amazon, o estado do seu 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 obter 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.

 Important

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.

Para obter informações sobre a solução de possíveis problemas relacionados às configurações do Active Directory autogerenciado, consulte [O sistema de arquivos está em um estado de configuração incorreta](#).

Você pode usar a Console de gerenciamento da AWS FSx API da Amazon ou AWS CLI para atualizar as credenciais 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 Console de gerenciamento da AWS CLI e a API. Para obter mais informações, consulte [Como monitorar as atualizações do Active Directory autogerenciado](#).

Atualizar a configuração do Active Directory autogerenciado (console)

1. Abra o FSx console da Amazon 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 (nome de usuário e senha) ou o ARN secreto na caixa de diálogo exibida. Você pode usar AWS Secrets Manager para armazenar suas credenciais. Para obter mais informações, consulte [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#).
5. Selecione Atualizar para iniciar a atualização da configuração do Active Directory.

Você pode [monitorar o progresso da atualização](#) usando o Console de gerenciamento da AWS ou AWS CLI o.

## Atualizar a configuração do Active Directory autogerenciado (CLI)

- Para atualizar a configuração autogerenciada do Active Directory de um sistema FSx de arquivos do Windows File Server, use o AWS CLI comando [update-file-system](#). Defina os seguintes parâmetros:
  - `--file-system-id` para o ID do sistema de arquivos que você está atualizando.
  - `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.
  - `DomainJoinServiceAccountSecret` AWS Secrets Manager segredo contendo o nome de usuário e a senha de uma conta de serviço no seu domínio do Active Directory

### Note

Você não pode fornecer ambos username/password e um segredo de conta de serviço de ingresso no domínio para se conectar ao seu Active Directory. Forneça somente um conjunto de credenciais.

- `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 objeto `AdministrativeActions` na resposta descreve a solicitação e seu status.

## Alterando a conta FSx de serviço da Amazon

Se você atualizar o sistema de arquivos com uma nova conta de serviço, a nova conta de serviço deverá ter as permissões e os privilégios necessários para associá-la a um Active Directory e ter permissões de Controle total para os objetos de computador atuais associados ao sistema de arquivos. Além disso, verifique se a nova conta de serviço está nas contas confiáveis com a configuração de Política de grupo Controlador de domínio: permitir a reutilização da conta de computador durante a associação ao domínio habilitada.

Recomendamos fortemente usar um grupo do Active Directory para gerenciar as permissões e configurações do Active Directory associadas a contas de serviço.

Ao alterar a conta de serviço da Amazon FSx, certifique-se de que as contas de serviço tenham as seguintes configurações:

- A nova conta de serviço (ou o grupo do Active Directory ao qual ela pertence) tem permissões de Controle total para os objetos de computador atuais associados ao sistema de arquivos.
- As contas de serviço novas e anteriores (ou o grupo do Active Directory ao qual elas pertencem) fazem parte das contas confiáveis (ou do grupo confiável do Active Directory) com a configuração da Política de grupo Controlador de domínio: Permitir a reutilização da conta de computador durante a associação ao domínio habilitada em todos os controladores de domínio no Active Directory.

Se as contas de serviço não atenderem a esses requisitos, o sistema poderá apresentar as seguintes condições:

- Para sistemas de arquivos single-AZ, o sistema de arquivos poderá ficar [MISCONFIGURED\\_UNAVAILABLE](#).
- Para sistemas de arquivos Multi-AZ, o sistema de arquivos pode ficar [MAL CONFIGURADO](#) e o nome do RemotePowerShell endpoint pode mudar.

## Como configurar a Política de grupo de um controlador de domínio

O seguinte [procedimento recomendado pela Microsoft](#) descreve como usar a Política de grupo do controlador de domínio para configurar a política de lista de permissões.

Para configurar a política de lista de permissões de um controlador de domínio

1. Instale as atualizações de 12 de setembro de 2023 ou posteriores do Microsoft Windows em todos os computadores membros e controladores de domínio no Microsoft Active Directory autogerenciado.
2. Em uma política de grupo nova ou existente aplicável a todos os controladores de domínio em seu Active Directory autogerenciado, defina as seguintes configurações.
  - a. Acesse Configuração do Computador > Políticas > Configurações do Windows > Configurações de Segurança > Políticas Locais > Opções de Segurança.

- b. Clique duas vezes em Controlador de domínio: permitir a reutilização da conta do computador durante a associação ao domínio.
- c. Selecione Definir esta configuração de política e <Edit Security...>.
- d. Use o seletor de objetos para adicionar usuários ou grupos de criadores e proprietários de contas de computador confiáveis à permissão Permitir. (Como prática recomendada, recomendamos que você use grupos para obter permissões.) Não adicione a conta de usuário que realiza a associação ao domínio.

 **Warning**

Limite a associação à política a usuários e contas de serviço confiáveis. Não adicione usuários autenticados, todos ou outros grupos grandes a essa política. Em vez disso, adicione usuários confiáveis e contas de serviço específicos aos grupos e adicione esses grupos à política.

3. Aguarde o intervalo de atualização da Política de grupo ou execute `gpupdate /force` em todos os controladores de domínio.
4. Verifique se a chave de registro `HKLM\System\CCS\Control\SAM — “ComputerAccountReuseAllowList”` está preenchida com o SDDL desejado. Não edite o registro manualmente.
5. Tente se conectar a um computador que tenha as atualizações de 12 de setembro de 2023 ou posteriores instaladas. Certifique-se de que uma das contas listadas na política seja proprietária da conta do computador. Certifique-se também de que seu registro não tenha a `NetJoinLegacyAccountReuse` ativada (definida como 1). Se a associação ao domínio falhar, verifique o `c:\windows\debug\netsetup.log`.

## Como monitorar as atualizações do Active Directory autogerenciado

Você pode monitorar o progresso de uma atualização de configuração autogerenciada do Active Directory usando a Console de gerenciamento da AWS, a API ou a AWS CLI, conforme descrito nos procedimentos a seguir.

Quando você atualiza a configuração do Active Directory autogerenciado do seu sistema de arquivos, o estado do sistema de arquivos muda de Disponível para Atualizando enquanto a atualização é aplicada. Quando a atualização for concluída, o estado voltará para Disponível. A conclusão de atualização de configuração do Active Directory pode levar vários minutos.

## 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.

| Updates (10) <span>↻</span>                                                         |                |             |              |                           |
|-------------------------------------------------------------------------------------|----------------|-------------|--------------|---------------------------|
| <input type="text" value="Filter updates"/> <span>&lt; 1 &gt;</span> <span>⚙</span> |                |             |              |                           |
| Update type ▼                                                                       | Target value ▼ | Status ▼    | Progress % ▼ | Request time ▲            |
| Storage capacity                                                                    | 154            | ✓ Completed | -            | 2020-05-22T12:14:58-04:00 |
| Throughput capacity                                                                 | 64             | ✓ Completed | -            | 2020-05-22T12:14:50-04:00 |
| Throughput capacity                                                                 | 128            | ✓ Completed | -            | 2020-05-21T13:55:58-04:00 |
| Storage capacity                                                                    | 140            | ✓ Completed | -            | 2020-05-21T13:55:30-04:00 |
| Storage capacity                                                                    | 122            | ✓ Completed | -            | 2020-05-18T11:36:33-04:00 |

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 — a Amazon FSx recebeu a solicitação de atualização, mas ainda não começou a processá-la.
- Em andamento — a 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

A hora em que a 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 [describe-file-systems](#) AWS CLI comando e a ação da [DescribeFileSystems](#) API. A matriz AdministrativeActions lista as dez ações de atualização mais recentes para cada tipo de ação administrativa.

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

```
{
 "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."
 }
 }
],
 .
 .
 .
```

# desempenho 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 desempenho. 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.

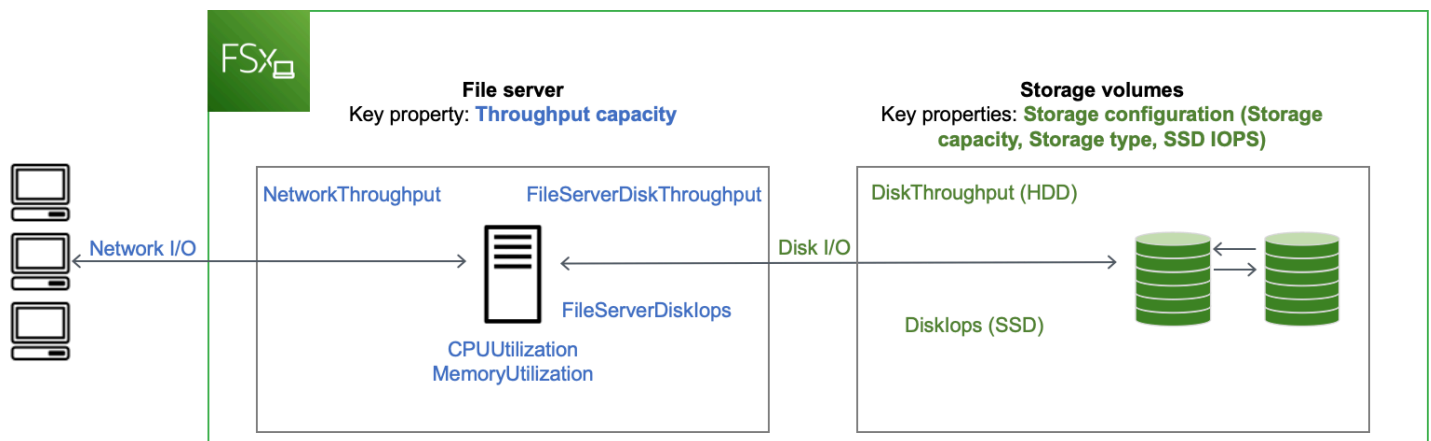
## Tópicos

- [Performance do sistema de arquivos](#)
- [Considerações adicionais sobre performance](#)
- [Impacto da capacidade de throughput na performance](#)
- [Escolher o nível certo de capacidade de throughput](#)
- [Impacto da configuração de armazenamento na performance](#)
- [Exemplo: capacidade de armazenamento e capacidade de throughput](#)
- [Medir a performance usando métricas do CloudWatch](#)
- [Solução de problemas de desempenho do sistema de arquivos](#)

## 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 em 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 em 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 em 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 em 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 em 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 do Amazon FSx fornecem até 2 GBps e 80 mil IOPS em todas as Regiões da AWS nas quais o Amazon FSx está disponível, além de 12 GBps de throughput e 400 mil IOPS 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). 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 atributo permite que ele forneça um throughput de até vários GBps 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 de SMB suportadas pelo Windows, esse limite está na casa dos milhões e você pode ter praticamente um número ilimitado de conexões de SMB.

## Desempenho da 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 throughput 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 workloads de teste e desenvolvimento, não a workloads 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), Europa (Irlanda), Ásia-Pacífico (Tóquio) e Ásia-Pacífico (Singapura).

## Memória e E/S de rede

| Capacidade de throughput do FSx (MBps) | Throughput da rede (MBps) |                                       | 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 throughput do FSx (MBps) | Throughput de disco (MBps) |                                   | 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                               | 10K               | 20K                               |
| 512                                    | 512                        | –                                 | 20K               | –                                 |
| 1.024                                  | 1,024                      | –                                 | 40K               | –                                 |
| 2.048                                  | 2,048                      | –                                 | 80K               | –                                 |
| 4.608                                  | 4,608                      | –                                 | 150K              | –                                 |
| 6.144                                  | 6,144                      | –                                 | 200K              | –                                 |
| 9.216                                  | 9,216 <sup>1</sup>         | –                                 | 300K <sup>1</sup> | –                                 |
| 12.288                                 | 12,288 <sup>1</sup>        | –                                 | 400K <sup>1</sup> | –                                 |

### Note

<sup>1</sup>Se você tiver um sistema de arquivos multi-AZ com uma capacidade de throughput de 9.216 ou 12.288 MBps, o desempenho será limitado a 9 mil MBps e 262.500 IOPS somente para o 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 desempenho 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 configurar uma quantidade específica de capacidade de throughput para atender às necessidades da sua workload. 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. A tabela a seguir fornece o nível mínimo de capacidade de throughput recomendado para um sistema de arquivos com base na quantidade de capacidade de armazenamento provisionada.

| Capacidade de armazenamento SSD (GiB) | Capacidade de armazenamento HDD (GiB) | Capacidade de throughput mínima recomendada (MBps) |
|---------------------------------------|---------------------------------------|----------------------------------------------------|
| Até 640                               | Até 3.200                             | 32                                                 |
| 641 - 1.280                           | 3.201 - 6.400                         | 64                                                 |
| 1.281 - 2.560                         | 6.401 - 12.800                        | 128                                                |
| 2.561 - 5.120                         | 12.801 - 25.600                       | 256                                                |
| 5.121 - 10.240                        | 25.601 - 51.200                       | 512                                                |
| 10.241 - 20.480                       | > 51.200                              | 1.024                                              |
| > 20.480                              | NA                                    | 2.048                                              |

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 obter 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 desempenho durante esses eventos. Para obter mais informações, consulte [Acesso a métricas de sistema de arquivos](#).

## 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 obter mais informações, consulte [Gerenciar o tipo de armazenamento do seu sistema de arquivos](#).

Seu sistema de arquivos fornece os seguintes níveis padrão de throughput de disco e IOPS:

| Tipo de armazenamento | Throughput de disco (MBps por TiB de armazenamento) | IOPS de disco (por TiB de armazenamento) |
|-----------------------|-----------------------------------------------------|------------------------------------------|
| SSD                   | 750                                                 | 3 mil <sup>1</sup>                       |

| Tipo de armazenamento | Throughput de disco (MBps por TiB de armazenamento)                                   | IOPS de disco (por TiB de armazenamento) |
|-----------------------|---------------------------------------------------------------------------------------|------------------------------------------|
| HDD                   | Linha de base de 12; expansão de 80 (até um máximo de 1 GBps por sistema de arquivos) | Linha de base de 12; expansão de 80      |

#### Note

<sup>1</sup>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 mil IOPS por sistema de arquivos.

## Desempenho da 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 o 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 o 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:

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

Para um volume de HDD de 1 TiB, o throughput de expansão limita-se a 80 MiB/s, o bucket é preenchido com créditos a 12 MiB/s e pode suportar até 1 TiB equivalente em créditos.

Volumes de armazenamento em HDD podem sofrer variações significativas de desempenho de acordo com a workload. Picos repentinos nas IOPS ou no throughput podem levar à degradação do desempenho do disco. A métrica [DiskThroughputBalance](#) fornece informações sobre o saldo máximo de crédito para o throughput do disco e a utilização de IOPS do disco. Por exemplo, se a workload exceder os limites básicos de IOPS do HDD (12 IOPS por TiB de armazenamento), a

utilização de IOPS em disco (HDD) ficará acima de 100% e resultará no esgotamento do saldo de crédito intermitente, que você poderá ver na métrica `DiskThroughputBalance`. Para que sua workload continue gerando altos níveis de E/S, talvez seja necessário fazer o seguinte:

- Reduza as demandas de E/S de sua workload para que o saldo de crédito estourado seja reabastecido.
- Aumente a capacidade de armazenamento do sistema de arquivos para fornecer um nível básico mais alto de IOPS de disco.
- Atualize o sistema de arquivos para usar o armazenamento SSD, que fornece um nível básico mais alto de IOPS de disco para melhor atender aos requisitos de sua workload.

## 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 throughput de expansão para operações de arquivo executadas em dados acessados ativamente armazenados em cache no cache em 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.

## Medir a performance usando métricas do CloudWatch

Você pode usar o Amazon CloudWatch para medir e monitorar o throughput e as IOPS do seu sistema de arquivos. Para obter mais informações, consulte [Monitorar com o Amazon CloudWatch](#).

## Solução de problemas de desempenho do sistema de arquivos

O desempenho do sistema de arquivos do seu FSx para Windows File Server depende de vários fatores, inclusive do tráfego que você direciona para o sistema de arquivos, de como você provisiona o sistema de arquivos e os recursos que são consumidos pelos recursos habilitados, como a Eliminação da duplicação dos dados ou Cópias de sombra. Para obter informações sobre como entender a desempenho do seu sistema de arquivos, consulte [desempenho do FSx para Windows File Server](#).

### Tópicos

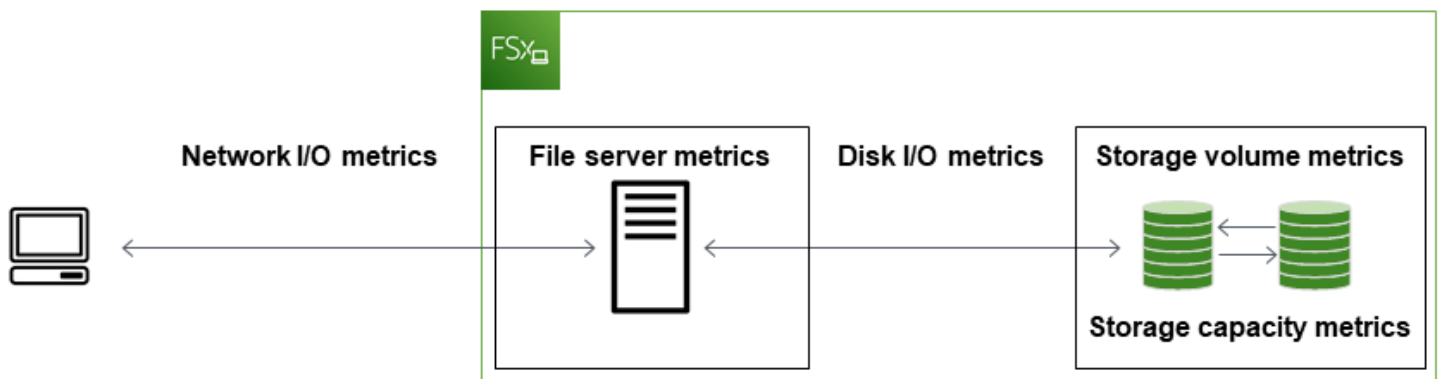
- [Como posso determinar os limites de throughput e IOPS do meu sistema de arquivos?](#)
- [Qual é a diferença entre E/S de rede e E/S de disco? Por que a E/S da minha rede é diferente da E/S do meu disco?](#)
- [Por que o uso da CPU ou da memória está alto, mesmo quando a E/S de rede está baixa?](#)
- [O que é intermitência? Quanta intermitência meu sistema de arquivos está usando? O que acontece quando os créditos de intermitência se esgotam?](#)
- [Vejo um aviso na página Monitoramento e performance. Preciso alterar a configuração do meu sistema de arquivos?](#)
- [Minhas métricas estavam temporariamente ausentes, devo me preocupar?](#)

## 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 em 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 obter mais informações, consulte [Monitorar com o 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 obter mais informações, consulte [Reduzir os custos de armazenamento com desduplicação 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 [desempenho 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 obter 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.

# Administração FSx para sistemas de arquivos Windows

FSx A Amazon fornece uma ampla variedade de recursos administrativos que ajudam você a gerenciar e expandir facilmente seus sistemas de arquivos Amazon FSx para Windows File Server para atender às mudanças de carga de trabalho e requisitos de usuários, bem como às necessidades regulatórias e de conformidade de sua organização. A seguir está uma lista de algumas das configurações do sistema de arquivos que você pode gerenciar usando a API Console de gerenciamento da AWS, a FSx CLI da Amazon para gerenciamento remoto AWS CLI e as interfaces PowerShell gráficas nativas do Microsoft Windows Server.

- Capacidade de armazenamento
- Tipo de armazenamento
- IOPS SSD
- Capacidade de produção
- Aliases de DNS
- Eliminação de duplicação de dados
- Cópias de sombra
- Cotas de armazenamento
- Auditoria de acesso a arquivos
- Compartilhar arquivos

As seções a seguir fornecem informações sobre as configurações e os recursos administrativos do sistema de arquivos que estão disponíveis para você. Incluímos orientações para ajudar você a determinar quais opções são melhores para sua situação e as melhores práticas, quando aplicável.

## Tópicos

- [Status FSx do sistema de arquivos da Amazon](#)
- [Usando a Amazon FSx CLI para PowerShell](#)
- [Iniciando uma PowerShell sessão FSx remota da Amazon](#)
- [Tarefas únicas de configuração do sistema de arquivos usando a Amazon FSx CLI para gerenciamento remoto em PowerShell](#)
- [Solução de problemas de acesso à Amazon FSx CLI em PowerShell](#)
- [Janela de manutenção do sistema de arquivos](#)



- [Alterar a janela de manutenção semanal](#)
- [Como gerenciar aliases de DNS](#)
- [Sessões de usuário e arquivos abertos](#)
- [Gerenciador de recursos de servidor de arquivos ativado FSx para Windows File Server](#)
- [Gerenciar armazenamento no FSx para Windows File Server](#)
- [Como usar o namespaces do DFS](#)
- [Como gerenciar a capacidade de throughput](#)
- [Como gerenciar o tipo de rede](#)
- [Marcação de seus recursos do Amazon FSx](#)
- [Atualizar um sistema de arquivos usando a AWS CLI](#)

## Status FSx do sistema de arquivos da Amazon

Você pode visualizar o status de um sistema de FSx arquivos da Amazon usando o FSx console da Amazon, o AWS CLI comando [describe-file-systems](#) ou a operação da API [DescribeFileSystems](#).

| Status do sistema de arquivos | Description                                                                                                                                                                                                                                                              |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DISPONÍVEL                    | O sistema de arquivos está em um estado íntegro e está acessível e disponível para uso.                                                                                                                                                                                  |
| CRIANDO                       | A Amazon FSx está criando um novo sistema de arquivos.                                                                                                                                                                                                                   |
| EXCLUINDO                     | A 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 |

| Status do sistema de arquivos | Description                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | restauração da disponibilidade, consulte <a href="#">O sistema de arquivos está em um estado de configuração incorreta.</a>                                                                                                                                                                                                               |
| MISCONFIGURED_UNAVAILABLE     | O sistema de arquivos não está disponível no momento devido a uma alteração no ambiente do Active Directory. Para obter informações sobre a restauração da disponibilidade, consulte <a href="#">O sistema de arquivos está em um estado de configuração incorreta.</a>                                                                   |
| FAILED                        | <ul style="list-style-type: none"> <li>Ao criar um novo sistema de arquivos, a Amazon não FSx conseguiu criar o novo sistema de arquivos.</li> <li>O sistema de arquivos não está disponível.</li> <li>O sistema de arquivos falhou e a Amazon não FSx consegue recuperá-lo.</li> <li>FSx A Amazon não consegue criar backups.</li> </ul> |

## Usando a Amazon FSx CLI para PowerShell

Este capítulo descreve como acessar a Amazon FSx CLI para gerenciamento remoto e realizar tarefas administrativas do sistema de arquivos FSx para sistemas de arquivos Windows. PowerShell Você também pode usar a interface gráfica de usuário (GUI) nativa do Microsoft Windows para realizar algumas tarefas administrativas.

O Amazon FSx CLI 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 FSx sistema de arquivos do 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 FSx de arquivos do 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 FSxAdministradores AWS Delegados. Se você estiver usando um Microsoft Active Directory autogerenciado, trata-se do grupo Domain Admins ou de um grupo personalizado que você especificou para a administração quando criou o sistema de arquivos. Para obter mais informações, consulte [Práticas recomendadas ao usar um Active Directory autogerenciado](#).

- Que as regras de entrada do grupo de segurança do sistema de arquivos da sua VPC permitam tráfego na porta 5985.

A Amazon FSx CLI para gerenciamento remoto PowerShell usa os seguintes recursos de segurança:

- As credenciais de usuário são autenticadas usando a autenticação de 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 FSx arquivos da Amazon:

- 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.

Caso queira definir e transmitir variáveis como parâmetros para o comando de gerenciamento remoto, você precisará usar o Invoke-Command.

#### Note

Para sistemas de arquivos Multi-AZ, você só pode usar o Amazon FSx CLI para gerenciamento remoto enquanto o sistema de arquivos estiver usando seu servidor de arquivos preferido. Para obter 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 para acessar o Remoto PowerShell. O endpoint de administração remota tem o formato de `amznfsxctlyaa1k.ActiveDirectory-DNS-name`, por exemplo, `amznfsxctlyaa1k.corp.example.com`. Você pode encontrar o nome do endpoint usando

o Console de gerenciamento da AWS na página Detalhes do sistema de arquivos na guia Rede e segurança. Use o AWS CLI [describe-file-systems](#) comando para visualizar a RemoteAdministrationEndpoint propriedade retornada na resposta.

Você pode usar o Get-Command cmdlet para recuperar 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 FSx CLI da Amazon 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 FSx de arquivos do Windows File Server, consulte [Iniciando uma PowerShell sessão FSx remota da Amazon](#)

## Iniciando uma PowerShell sessão FSx remota da Amazon

Este tópico fornece instruções para iniciar uma PowerShell sessão remota de longa duração em seu servidor FSx de arquivos do 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 FSx Administradores delegados 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 no seu sistema de FSx arquivos da Amazon. *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 do 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 Grupo de FSx Administradores. Se sua instância estiver associada ao domínio, você não precisará fornecer credenciais.

#### Important

O PowerShell endpoint remoto do Windows pode mudar se você estiver usando a configuração autogerenciada do Active Directory e alterar a conta de serviço sem as configurações adequadas da Política de Grupo do Active Directory. Para obter mais informações, consulte [Alterando a conta FSx de serviço da Amazon](#).

## Tarefas únicas de configuração do sistema de arquivos usando a Amazon FSx CLI para gerenciamento remoto em PowerShell

Use a seguinte Amazon FSx CLI para gerenciamento remoto em PowerShell comandos para implementar rapidamente as tarefas de administração do sistema de arquivos seguindo nossas melhores práticas.

### 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 obter mais informações, consulte [Reduzir os custos de armazenamento com deduplicação 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 obter mais informações, consulte [Gerenciar 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 obter mais informações, consulte [Configurar 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](#).

## Solução de problemas de acesso à Amazon FSx CLI em 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 obter 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 florestal. 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")
```

## Janela de manutenção do sistema de arquivos

O Amazon FSx para Windows File Server executa correções de software de rotina para o software Microsoft Windows Server que ele gerencia. A janela de manutenção especifica o dia da semana e a hora do dia em que esse processo de manutenção começa. Você pode especificar o período inicial da janela de manutenção durante a criação do sistema de arquivos. Se você não especificar uma, será atribuída uma janela inicial de manutenção padrão de 30 minutos. A duração da janela de manutenção depende de vários fatores, incluindo o escopo da manutenção e o processo de sincronização de qualquer atividade de leitura e gravação de arquivos que ocorra durante a manutenção entre os servidores primário e secundário dos sistemas de arquivos multi-AZ. Para obter mais informações, consulte [Processo de failover](#).

FSx para Windows File Server permite ajustar a hora de início da janela de manutenção para acomodar sua carga de trabalho e seus requisitos operacionais. É possível mover o horário de início da janela de manutenção com a frequência necessária, desde que o horário de início da janela de manutenção seja programada, no mínimo, uma vez a cada 14 dias. Se um patch for lançado e você não tiver agendado uma janela de manutenção em 14 dias, FSx o Windows File Server prosseguirá com a manutenção no sistema de arquivos para garantir sua segurança e confiabilidade. Para obter mais informações sobre como ajustar o horário de início da janela de manutenção do sistema de arquivos, consulte [Alterar a janela de manutenção semanal](#).



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 os servidores de arquivos em espera e o preferencial. Para obter mais informações, consulte [Processo de failover](#). Como a aplicação de patches em sistemas de arquivos multi-AZ envolve failover e failback entre servidores de arquivos, qualquer atividade de leitura e gravação que ocorra durante esse período deve ser sincronizado entre servidores 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 for Windows File Server conclui todas as operações de gravação pendentes nos volumes de armazenamento subjacentes que hospedam seu sistema de arquivos antes do início da manutenção.

## Alterar a janela de manutenção semanal

FSx para Windows File Server permite que você ajuste quando a janela de manutenção do sistema de arquivos começa para acomodar sua carga de trabalho e seus requisitos operacionais. Você pode usar a FSx API Console de gerenciamento da AWS, AWS CLI, e da Amazon para alterar o início da janela de manutenção semanal, descrita no procedimento a seguir.

Para alterar o horário de início da janela de manutenção semanal (console)

1. Abra o FSx console da Amazon 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 Salvar para salvar as alterações. A nova hora de início da manutenção é exibida no painel Configurações de administração.

Para alterar a hora de início da janela de manutenção semanal usando o comando [update-file-system](#) CLI, consulte. [Atualizar um sistema de arquivos usando a AWS CLI](#)

## Como gerenciar aliases de DNS

Além do nome padrão do Sistema de Nomes de Domínio (DNS) FSx fornecido pela Amazon, você também pode associar os aliases de DNS de sua escolha aos seus sistemas de arquivos. Com os aliases de DNS, você pode continuar usando nomes DNS existentes para acessar dados armazenados na Amazon FSx ao [migrar o armazenamento do sistema de arquivos do](#) local para a Amazon FSx, sem precisar atualizar nenhuma ferramenta ou aplicativo.

Você pode associar aliases de DNS a sistemas FSx de arquivos novos e existentes do Windows File Server e, ao restaurar um backup em um novo sistema de arquivos, usando o Console de gerenciamento da AWS CLI. Você pode associar até 50 aliases de DNS a um sistema de arquivos a qualquer momento.

### Note

O suporte para aliases de DNS está disponível nos sistemas FSx de arquivos do 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 obter mais informações, consulte [Como trabalhar com backups iniciados pelo usuário](#).
2. Restaure o backup em um novo sistema de arquivos. Para obter mais informações, consulte [Restaurar backups em um novo sistema de arquivos](#).

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.

A Amazon FSx só registra 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 FSx arquivos da Amazon 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 em entradas DNS manuais](#).

Você pode associar aliases de DNS aos sistemas FSx de arquivos existentes do Windows File Server, ao criar novos sistemas de arquivos e ao criar um novo sistema de arquivos a partir de 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 os nomes principais do serviço (SPNs) para autenticação e criptografia Kerberos.
- Configure um registro DNS CNAME para o alias de DNS que é resolvido para o nome DNS padrão do seu sistema de arquivos da Amazon. FSx

Para obter mais informações, consulte [Como acessar dados usando aliases de DNS](#).

Um nome de alias de DNS FSx para seu sistema de arquivos do Windows File Server precisa atender aos seguintes requisitos:

- Deve ser formatado como um nome de domínio totalmente qualificado (FQDN).
- Pode conter caracteres alfanuméricos e hífens (-).
- Não pode começar ou terminar com um hífen (-).
- Pode começar com um caractere numérico.

Para nomes de alias de DNS, a Amazon FSx armazena caracteres alfabéticos como letras minúsculas (a-z), independentemente de como você os especifica: como letras maiúsculas, letras minúsculas ou as letras correspondentes nos 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, a Amazon FSx responderá com um erro de solicitação incorreta.

#### Note

Quando a Amazon FSx adiciona ou remove aliases em um sistema de arquivos, os clientes conectados são temporariamente desconectados e se reconectam automaticamente ao sistema de arquivos. Todos os arquivos que foram abertos por clientes mapeando um compartilhamento non-Continuously-Available (não CA) no momento da desconexão devem ser reabertos pelo cliente.

## Tópicos

- [Status do alias de DNS](#)
- [Como usar aliases de DNS com autenticação de Kerberos](#)
- [Visualizar aliases de DNS para sistemas de arquivos e backups](#)
- [Como associar aliases de DNS a sistemas de arquivos](#)
- [Como gerenciar aliases de DNS em sistemas de arquivos atuais](#)

## Status do alias de DNS

Aliases de DNS podem ter um dos seguintes valores de status:

- Disponível — O alias DNS está associado a um sistema de FSx arquivos da Amazon.
- Criação — A Amazon FSx está criando o alias DNS e o associando ao sistema de arquivos.
- Excluindo — A Amazon FSx está desassociando o alias DNS do sistema de arquivos e o excluindo.
- Falha na criação — a Amazon não FSx conseguiu associar o alias de DNS ao sistema de arquivos.
- Falha na exclusão — a Amazon não FSx conseguiu desassociar o alias DNS do sistema de arquivos.

## Como usar aliases de DNS com autenticação de Kerberos

Recomendamos que você use autenticação e criptografia baseadas em Kerberos em trânsito com a 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 FSx arquivos da Amazon usando um alias de DNS, você deve configurar os nomes principais do serviço (SPNs) que correspondam ao alias DNS no objeto de computador do Active Directory do seu sistema de arquivos.

Se você SPNs configurou o alias de DNS que você atribuiu a outro sistema de arquivos em um objeto de computador no Active Directory, você deve primeiro removê-lo SPNs antes de SPNs adicioná-lo ao objeto de computador do seu sistema de arquivos. Para obter mais informações, consulte [Configurar nomes de entidade principal de serviço \(SPNs\) para o Kerberos](#).

## Visualizar aliases de DNS para sistemas de arquivos e backups

Você pode visualizar os aliases de DNS atualmente associados aos seus sistemas FSx de arquivos e backups do Windows File Server usando a API Console de gerenciamento da AWS AWS CLI, the e, conforme descrito nos procedimentos a seguir.

Para visualizar aliases de DNS associados a 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 visualizar aliases de DNS associados a backups

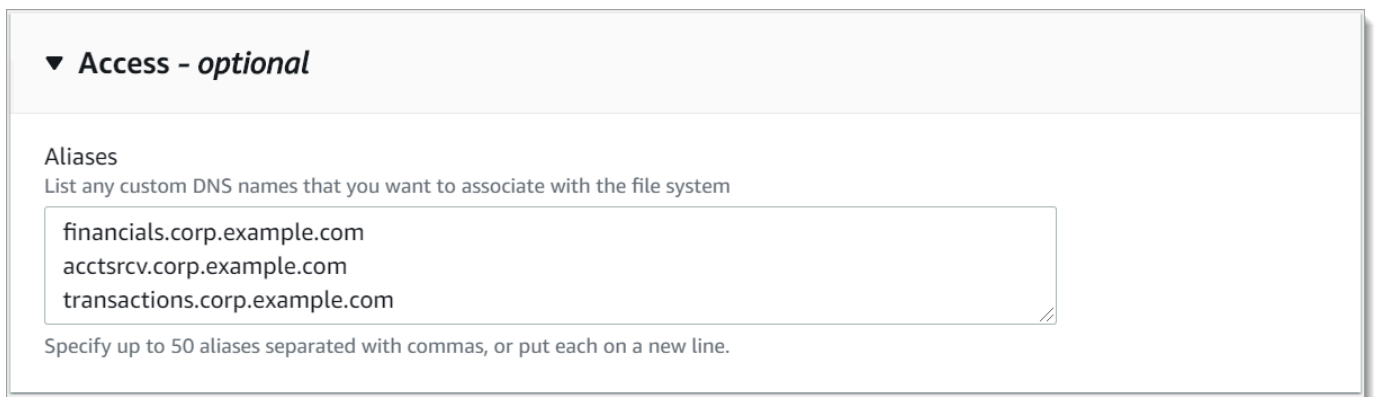
- Como usar o console: no painel de navegação, escolha Backups e, em seguida, escolha o backup que você deseja visualizar. No painel Resumo, visualize o campo Aliases de DNS.
- Usando a CLI ou a API — Use o comando da `describe-backups` CLI ou a operação da API. [DescribeBackups](#)

## Como associar aliases de DNS a sistemas de arquivos

Você pode associar aliases de DNS ao criar um novo FSx sistema de arquivos do Windows File Server do zero ou ao restaurar um backup em um novo sistema de arquivos usando a API, Console de gerenciamento da AWS AWS CLI, e descrita nos procedimentos a seguir.

Para associar aliases de DNS ao criar um novo sistema de arquivos (console)

1. Abra o FSx console da Amazon em <https://console.aws.amazon.com/fsx/>.
2. Siga o procedimento para a criação de um novo sistema de arquivos descrito na [Etapa 5. Criar 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.



▼ **Access - optional**

Aliases  
List any custom DNS names that you want to associate with the file system

financials.corp.example.com  
acctsrcv.corp.example.com  
transactions.corp.example.com

Specify up to 50 aliases separated with commas, or put each on a new line.

4. Quando o sistema de arquivos está disponível, você pode acessá-lo usando o alias DNS configurando os nomes principais do serviço (SPNs) e atualizando ou criando um registro DNS CNAME para o alias. Para obter mais informações, consulte [Como acessar dados usando aliases de DNS](#).

Para associar aliases de DNS ao criar um novo sistema de FSx arquivos da Amazon (CLI)

1. Ao criar um novo sistema de arquivos, use a propriedade [Alias](#) com a operação da [CreateFileSystem](#) API 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 \
 --alias financials.corp.example.com,acctsrcv.corp.example.com,transactions.corp.example.com
```

```
--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 DNS configurando os nomes principais do serviço (SPNs) e atualizando ou criando um registro DNS CNAME para o alias. Para obter mais informações, consulte [Como acessar dados usando aliases de DNS](#).

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 [CreateFileSystemFromBackup](#) API 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 CLI a seguir associa dois aliases ao sistema de arquivos que a Amazon FSx está criando a partir de 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 DNS configurando os nomes principais do serviço (SPNs) e atualizando ou criando um registro DNS CNAME para o alias. Para obter mais informações, consulte [Como acessar dados usando aliases de DNS](#).

## Como gerenciar aliases de DNS em sistemas de arquivos atuais

Você pode adicionar e remover aliases nos sistemas FSx de arquivos existentes do Windows File Server usando o Console de gerenciamento da AWS e AWS CLI, conforme descrito nos procedimentos a seguir.

Para gerenciar aliases de DNS de sistema de arquivos atual (console)

1. Abra o FSx console da Amazon 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 janela 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 seu sistema de arquivos usando o alias DNS configurando os nomes principais do serviço (SPNs) e atualizando ou criando um registro DNS CNAME para o alias. Para obter mais informações, consulte [Como acessar dados usando aliases de DNS](#).

Para associar aliases de DNS a sistemas de arquivos existentes (CLI)

1. Use o comando `associate-file-system-aliases` CLI ou a operação da [AssociateFileSystemAliases](#) API 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 fs-0123456789abcdef0 fs-0123456789abcdef0
```



```
--aliases financials.corp.example.com transfers.corp.example.com
```

A resposta mostra o status dos aliases que a 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 ([DescribeFileSystemAliases](#) é a operação de API equivalente) para monitorar o status dos aliases que você está associando.
3. Quando o `Lifecycle` valor de `AVAILABLE` (um processo que pode levar até 2,5 minutos), você pode acessar seu sistema de arquivos usando o alias DNS configurando os nomes principais do serviço (SPNs) e atualizando ou criando um registro DNS CNAME para o alias. Para obter mais informações, consulte [Como acessar dados usando aliases de DNS](#).

## Desassociar aliases de DNS de sistemas de arquivos (CLI)

- Use o comando `disassociate-file-system-aliases` CLI ou a operação da [DisassociateFileSystemAliases](#) API 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 a Amazon FSx está desassociando do sistema de arquivos.

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

Use o comando `describe-file-system-aliases` CLI ([DescribeFileSystemAliases](#) é a operação equivalente da API) para monitorar o status dos aliases. Leva até 2,5 minutos para que o alias seja excluído.

## Sessões de usuário e arquivos abertos

Você pode monitorar sessões de usuários conectados e abrir arquivos em seu sistema FSx de arquivos do 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 FSx CLI da Amazon para gerenciamento remoto para gerenciar sessões de usuários e abrir arquivos em PowerShell seu FSx sistema de arquivos do Windows File Server.

## Como usar a GUI para gerenciar usuários e sessões

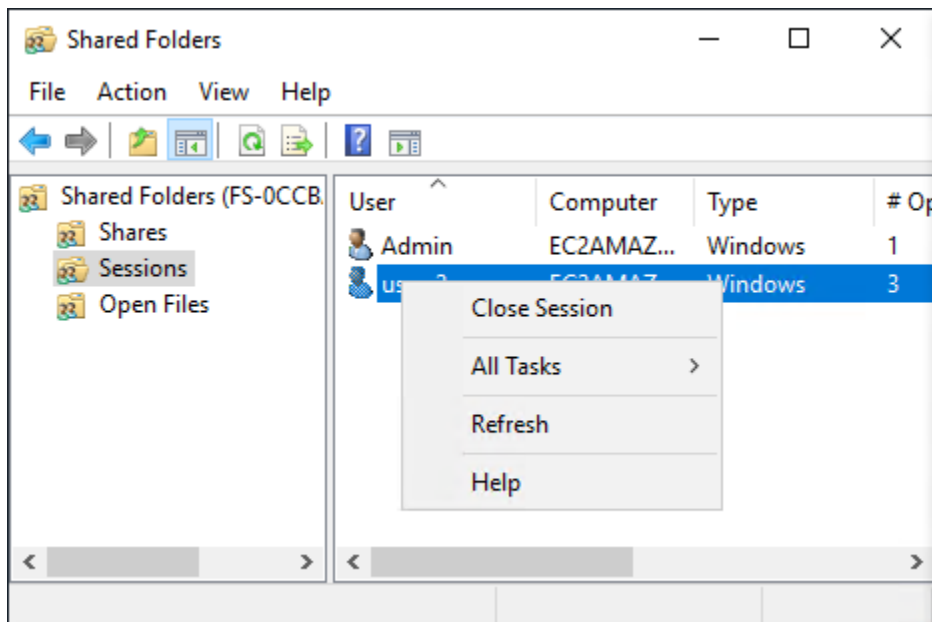
Os procedimentos a seguir detalham como você pode gerenciar sessões de usuário e abrir arquivos no sistema de FSx arquivos da Amazon usando a ferramenta de pastas compartilhadas do Microsoft Windows.

## Iniciar a ferramenta de pastas compartilhadas

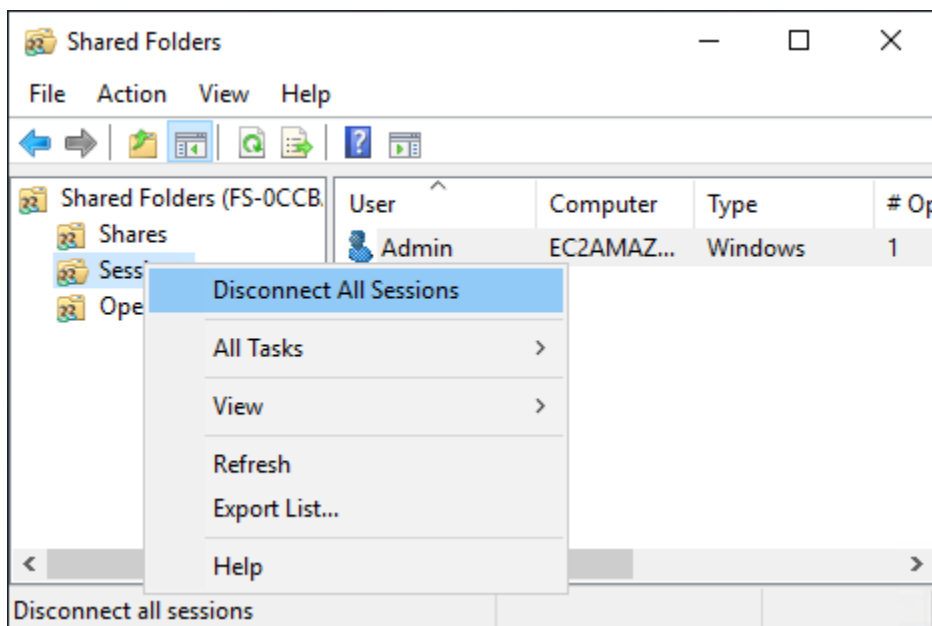
1. Inicie sua EC2 instância da Amazon e conecte-a ao Microsoft Active Directory ao qual seu sistema de FSx arquivos da Amazon está associado. Para fazer isso, escolha um dos seguintes procedimentos no Guia de administração do AWS Directory Service :
  - [Junte-se perfeitamente a uma instância do Windows EC2](#)
  - [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 FSx Administradores 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 EC2 do usuário da Amazon.
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 DNS do seu sistema de FSx arquivos da Amazon, por exemplo `fs-012345678901234567.ad-domain.com`.
6. Escolha OK. Em seguida, uma entrada para o sistema de FSx arquivos da Amazon aparece na lista da ferramenta de pastas compartilhadas.

## Para gerenciar sessões de usuário (GUI)

Na ferramenta Pastas compartilhadas, escolha Sessões para visualizar todas as sessões de usuário conectadas ao seu sistema FSx de arquivos do Windows File Server. Se um usuário ou aplicativo estiver acessando um compartilhamento de arquivos no seu sistema de FSx arquivos da Amazon, esse snap-in mostrará a sessão dele. Você pode desconectar as sessões abrindo o menu de contexto (clique com o botão direito) de uma sessão e escolhendo Fechar sessão.



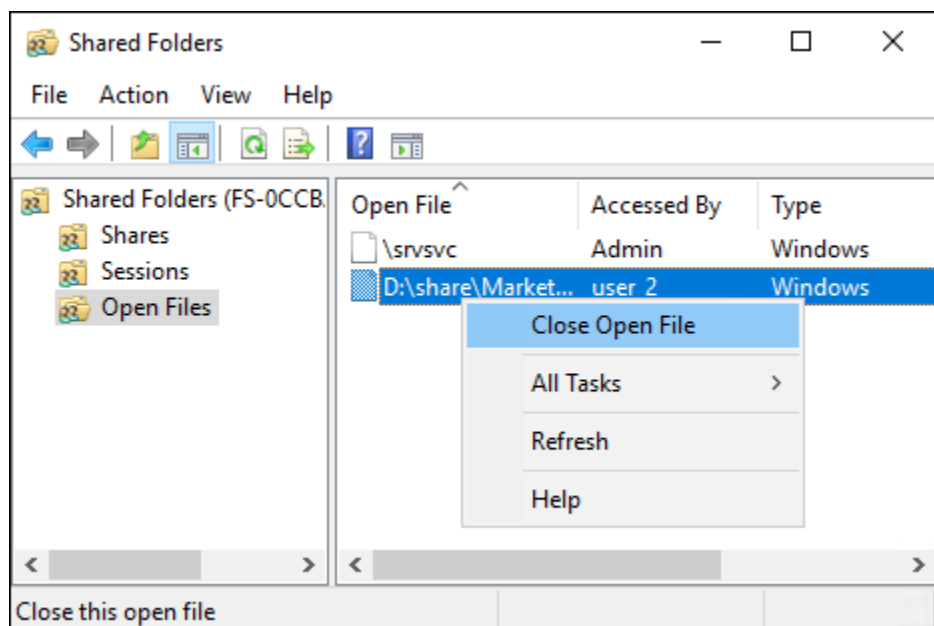
Para desconectar todas as sessões abertas, abra o menu de contexto (clique com o botão direito) de Sessões, escolha Desconectar todas as sessões e confirme a ação.



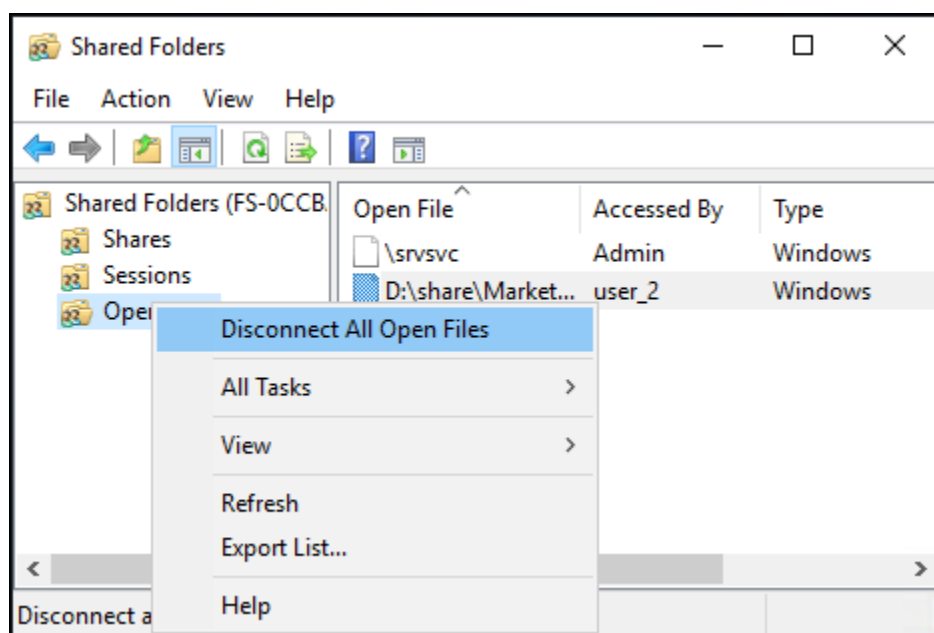
### Para gerenciar arquivos abertos (GUI)

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 a 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 o Amazon FSx CLI para gerenciamento remoto ativado. PowerShell Para saber como usar essa CLI, consulte [Usando a Amazon FSx CLI para PowerShell](#).

A seguir estão os comandos que você pode usar para a sessão do usuário e para o gerenciamento de arquivos abertos.

| Command              | Description                                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 -?`.

## Gerenciador de recursos de servidor de arquivos ativado FSx para Windows File Server

O File Server Resource Manager (FSRM) é um recurso do Windows Server que ajuda você a gerenciar e classificar dados armazenados em seu sistema de arquivos Amazon FSx for Windows File Server. O FSRM fornece recursos automatizados de imposição de políticas e emissão de relatórios que ajudam a controlar os custos de armazenamento, manter a conformidade com as políticas de gerenciamento de dados e organizar arquivos com base nas regras de negócios.

Com o FSRM, você pode definir limites de armazenamento para evitar que os usuários consumam armazenamento excessivo, identificar e classificar automaticamente dados confidenciais, impedir que

tipos de arquivos não autorizados sejam salvos em pastas comerciais e gerar relatórios detalhados sobre padrões de uso do armazenamento. Esses recursos ajudam você a manter um sistema de arquivos organizado, eficiente e compatível sem exigir intervenção manual para cada arquivo ou pasta.

O FSRM é particularmente valioso para organizações que precisam:

- Controle os custos de armazenamento limitando a quantidade de espaço em disco que os usuários e departamentos podem armazenar
- Identifique dados confidenciais, como informações de identificação pessoal ou registros financeiros
- Aplique políticas sobre quais tipos de arquivo são permitidos em pastas específicas
- Gere relatórios de conformidade sobre retenção de dados, propriedade de arquivos ou uso de armazenamento
- Mantenha a visibilidade de como o armazenamento está sendo usado em toda a organização

## Capacidades gerais

- [Gerenciamento de cotas](#)- Defina limites de armazenamento nas pastas para controlar quanto espaço os usuários e aplicativos podem consumir. Você pode configurar cotas fixas que impedem que os usuários excedam os limites ou cotas flexíveis que permitem excedentes ao enviar notificações. As cotas ajudam você a gerenciar os custos de armazenamento e evitar que usuários ou departamentos consumam quantidades desproporcionais de armazenamento.
- [Triagem de arquivos](#)- Controle quais tipos de arquivos os usuários podem salvar em pastas específicas. Você pode bloquear tipos de arquivo não autorizados, como arquivos executáveis, arquivos de mídia ou documentos pessoais em pastas comerciais. A triagem de arquivos ajuda a aplicar políticas de gerenciamento de dados, reduzir os riscos de segurança e evitar o desperdício de armazenamento de arquivos não comerciais.
- [Classificação de arquivos](#)- Atribua automaticamente propriedades de metadados aos arquivos com base em seu conteúdo ou localização. A classificação ajuda você a organizar arquivos, identificar dados confidenciais, aplicar políticas de retenção e gerar relatórios com base nas características do arquivo. Você pode classificar arquivos por confidencialidade de dados, departamento, período de retenção ou qualquer outra propriedade personalizada que você definir.
- [Relatórios de armazenamento](#)- Gere relatórios detalhados sobre o uso do sistema de arquivos, incluindo arquivos grandes, arquivos duplicados, arquivos por proprietário, arquivos por tipo e uso de cotas. Os relatórios de armazenamento ajudam você a entender como o armazenamento está

sendo consumido, identificar arquivos que podem ser arquivados ou excluídos e tomar decisões informadas sobre o gerenciamento do armazenamento.

## Tópicos

- [Introdução ao Gerenciador de Recursos do Servidor de Arquivos](#)
- [Gerenciamento de cotas](#)
- [Grupos de arquivos](#)
- [Triagem de arquivos](#)
- [Classificação de arquivos](#)
- [Relatórios de armazenamento](#)
- [Tarefas de gerenciamento de arquivos](#)
- [Configurações do FSRM](#)
- [Registros de eventos](#)
- [Casos de uso comuns](#)

## Introdução ao Gerenciador de Recursos do Servidor de Arquivos

Você pode ativar o File Server Resource Manager (FSRM) ao criar um novo sistema de arquivos Amazon FSx para Windows File Server ou pode atualizar seu sistema de arquivos existente para habilitar o FSRM.

O FSRM é suportado somente nos sistemas de arquivos Amazon FSx para Windows File Server com armazenamento SSD e uma capacidade de taxa de transferência de 128 ou mais. MB/s Você pode atualizar o tipo de armazenamento para SSD e modificar a capacidade de taxa de transferência a qualquer momento depois de criar o sistema de arquivos. Para obter mais informações, consulte [Atualização do tipo de armazenamento de um sistema de arquivos do FSx para Windows](#) e [Como gerenciar a capacidade de throughput](#).

Para habilitar o FSRM ao criar um sistema de arquivos (console)

1. Abra o FSx console da Amazon 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 Amazon FSx para Windows File Server e, em seguida, escolha Avançar.



4. Selecione a opção Criar padrão
5. Forneça as informações necessárias
6. Abra o bloco Gerenciador de Recursos do Servidor de Arquivos e escolha Ativado.
7. Em Destino do registro de eventos, escolha uma das seguintes opções:
  - CloudWatch Registros - Selecione um grupo de CloudWatch registros de registros para receber registros de eventos do FSRM. O nome do grupo de CloudWatch registros de registros deve começar com o '/aws/fsx/' prefixo.
  - Kinesis Data Firehose — Selecione um stream de entrega do Kinesis Data Firehose para receber registros de eventos do FSRM
8. Conclua as seções restantes e escolha Criar sistema de arquivos.

Para habilitar o FSRM ao criar um sistema de arquivos (CLI)

Para habilitar o FSRM ao criar um sistema de arquivos FSx para Windows File Server, use o comando CLI `AWS . create-file-system` Inclua a seguinte configuração de FSRM no `-- windows-configuration` parâmetro:

- `FsrmserviceEnabled`: definir como `true`
- `EventLogDestination`- O Amazon Resource Name (ARN) que especifica o destino dos registros de eventos do FSRM. Pode ser um ARN do grupo de CloudWatch registros do Logs ou um ARN do stream de distribuição do Kinesis Data Firehose.

```
aws fsx create-file-system \
 --file-system-type WINDOWS \
 --storage-capacity 300 \
 --storage-type SSD \
 --subnet-ids subnet-0123456789abcdef0 \
 --windows-configuration
 "ThroughputCapacity=128,WindowsFsrmsConfiguration={FsrmserviceEnabled=true,EventLogDestination=
 east-1:123456789012:log-group:/aws/fsx/fsrm}"
```

Para modificar a configuração do FSRM em um sistema de arquivos existente (console)

1. Abra o FSx console da Amazon em <https://console.aws.amazon.com/fsx/>.
2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do Windows que você deseja modificar.

3. Escolha a guia Administração.
4. Na seção Gerenciador de recursos do servidor de arquivos, escolha Gerenciar.
5. Faça as alterações necessárias:
  - Para alterar o destino do registro de eventos, selecione outro grupo de registros de CloudWatch registros ou stream de entrega do Kinesis Data Firehose
  - Para ativar o FSRM, escolha Ativado
  - Para desativar o FSRM, escolha Desativado

 Important

Os sistemas de arquivos Multi-AZ sofrerão eventos automáticos de failover e failback durante esse processo, enquanto os sistemas de arquivos Single-AZ passarão por um breve período de indisponibilidade.

6. Escolha Salvar.

Você pode monitorar o progresso da atualização na página de detalhes dos sistemas de arquivos, na guia Atualizações.

Para modificar a configuração do FSRM em um sistema de arquivos (CLI) existente

Para habilitar e desabilitar o FSRM em um sistema de arquivos existente FSx para Windows File Server, use o comando CLI AWS `aws fsx update-file-system`

Habilitando o FSRM

Para ativar o FSRM, inclua a seguinte configuração do FSRM no parâmetro: `--windows-configuration`

- `FsrmServiceEnabled`: definir como `true`
- `EventLogDestination`- O Amazon Resource Name (ARN) que especifica o destino dos registros de eventos do FSRM. Pode ser um ARN do grupo de CloudWatch registros do Logs ou um ARN do stream de distribuição do Kinesis Data Firehose.

```
aws fsx update-file-system \
```

```
--file-system-id fs-0123456789abcdef0 \
--windows-configuration
FsrConfiguration='{FsrServiceEnabled=true,EventLogDestination="arn:aws:logs:us-
east-1:123456789012:log-group:/aws/fsx/fsrm"}'
```

## Desativando o FSRM

Para desativar o FSRM:

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--windows-configuration FsrConfiguration='{FsrServiceEnabled=false}'
```

### Important

Os sistemas de arquivos Multi-AZ sofrerão eventos automáticos de failover e failback durante esse processo, enquanto os sistemas de arquivos Single-AZ passarão por um breve período de indisponibilidade.

## FSx controle remoto PowerShell

Para configurar e usar os recursos do FSRM, você deve usar o Amazon FSx CLI para gerenciamento remoto ativado. PowerShell Para mais informações, consulte [Iniciando uma PowerShell sessão FSx remota da Amazon](#).

## Gerenciamento de cotas

Você pode usar o gerenciamento de cotas do Gerenciador de Recursos do Servidor de Arquivos (FSRM) para controlar a quantidade de espaço de armazenamento que os usuários consomem no seu FSx sistema de arquivos do Windows File Server. As cotas ajudam você a gerenciar a capacidade de armazenamento limitando a quantidade de dados que podem ser armazenados em pastas específicas e gerando notificações quando o uso do armazenamento se aproxima ou excede os limites definidos.

### Como funciona o gerenciamento de cotas

O gerenciamento de cotas fornece dois tipos de cotas que você pode aplicar às pastas em seu sistema de arquivos:

## Cotas fixas

Impeça que os usuários salvem arquivos após o limite da cota ser atingido. Quando um usuário tenta salvar um arquivo que excederia o limite da cota, a operação falha e o usuário recebe uma mensagem de erro.

## Cotas flexíveis

Permita que os usuários excedam o limite da cota ao registrar a violação. As cotas flexíveis são úteis para monitorar o uso do armazenamento sem impor limites rígidos.

## Modelos de cota

Os modelos de cota fornecem uma configuração reutilizável que define as configurações de cota, incluindo limites de tamanho, tipo de cota (fixa ou temporária) e notificações de limite. Depois de criar um modelo de cota, você pode aplicá-lo a várias pastas sem precisar redefinir as mesmas configurações todas as vezes. Ao atualizar um modelo de cota, você pode, opcionalmente, aplicar as alterações a todas as cotas criadas a partir desse modelo.

O uso de modelos de cotas oferece vários benefícios:

- Consistência - Certifique-se de que pastas semelhantes tenham configurações de cotas idênticas
- Eficiência - aplique configurações de cota a várias pastas rapidamente
- Manutenção - Atualize as configurações de cota em várias pastas modificando o modelo

## Aplicação automática de cotas

A aplicação automática de cotas cria automaticamente cotas para subpastas com base em um modelo especificado. Quando você cria uma cota de aplicação automática em uma pasta principal, o FSRM gera automaticamente uma cota para cada subpasta existente e para qualquer nova subpasta que os usuários criem no futuro. Essa abordagem é útil para cenários em que você deseja aplicar limites de cota consistentes em vários diretórios de usuários ou pastas departamentais.

## Notificações de limite

Os limites definem os níveis de uso nos quais o FSRM executa ações específicas. Você pode configurar vários limites para cada cota, com cada limite definido como uma porcentagem do limite da cota. Quando o uso do armazenamento atinge uma porcentagem limite, o FSRM pode realizar as seguintes ações:

## Registro em log de eventos

Registre um evento na Amazon CloudWatch ou no Amazon Kinesis Data Firehose para monitoramento e análise. Você pode especificar o nível de gravidade do evento (informação, aviso ou erro) e fornecer um corpo de mensagem personalizado. O registro de eventos é útil para monitorar o uso da cota e integrar-se aos sistemas de monitoramento existentes.

## Relatórios de armazenamento

Gere um relatório de uso de armazenamento que forneça informações detalhadas sobre os arquivos e pastas que consomem espaço de armazenamento. Os relatórios de armazenamento ajudam você a identificar quais usuários ou aplicativos estão consumindo mais armazenamento e a tomar decisões informadas sobre o gerenciamento do armazenamento. Para obter mais informações, consulte [Relatórios de armazenamento](#).

Você pode configurar vários limites com ações diferentes para cada cota. Por exemplo, você pode configurar uma cota com um evento de informação com 75% de uso e um evento de aviso com 90% de uso.

## Comandos de gerenciamento de cotas

Você pode acessar três famílias de PowerShell comandos FSx remotos para gerenciar cotas:

1. Comandos de cota - Crie, recupere, modifique, remova e atualize cotas em pastas específicas. Use esses comandos quando precisar gerenciar cotas em uma folder-by-folder base.
2. Comandos do modelo de cota - Crie, recupere e modifique modelos de cota que definem configurações de cotas reutilizáveis. Use esses comandos para estabelecer políticas de cotas padrão que você pode aplicar em várias pastas.
3. Comandos de cota automática - Crie, recupere, modifique, remova e atualize cotas de aplicação automática que geram cotas automaticamente para subpastas. Use esses comandos quando precisar aplicar limites de cota consistentes em várias subpastas sem criar cotas individuais manualmente.

## Lista de comandos FSx remotos PowerShell de gerenciamento de cotas

### Note

Todos os exemplos nesta página pressupõem que você tenha definido a `$FSxWindowsRemotePowerShellEndpoint` variável com o PowerShell endpoint remoto

do Windows do seu sistema de arquivos. Você pode encontrar esse endpoint no FSx console da Amazon na página de detalhes do seu sistema de arquivos ou usando o AWS CLI `describe-file-systems` comando.

## Comandos de cota

### Novo- FSx FSRMQuota

Cria uma nova cota em uma pasta. Uma cota limita a quantidade de dados que os usuários podem armazenar em uma pasta. Opcionalmente, você pode configurar a cota para gerar notificações quando os usuários excederem os limites da cota.

#### Parâmetros:

- **Folder (string):** obrigatório. O caminho da pasta em que a cota será aplicada.
- **Size (string):** Obrigatório quando não está usando um modelo: o limite do tamanho da cota.
- **Template (string):** opcional. O nome de um modelo de cota existente a ser usado. Ao especificar um modelo, você só pode usar o parâmetro Descrição; todas as outras configurações são herdadas do modelo.
- **Description (string):** opcional. Uma descrição da cota.
- **SoftLimit (boolean):** opcional. Se definido como verdadeiro, cria uma cota flexível que permite que os usuários excedam o limite ao registrar violações.
- **Disabled (boolean):** opcional. Se definido como verdadeiro, cria a cota em um estado desativado.
- **ThresholdConfigurations (array):** opcional. Uma matriz de configurações de limite que especificam ações a serem tomadas em diferentes níveis de uso. Cada configuração tem as seguintes propriedades:
  - **ThresholdPercentage (number):** a porcentagem do limite de cota em que as ações devem ser acionadas. Insira um valor entre 0 e 250.
  - **Action (array):** Uma ou mais ações a serem tomadas quando o limite for atingido. Cada ação tem as seguintes propriedades:
    - **ActionType:** O tipo de ação a ser executada. Especifique os seguintes valores:
      1. **Event:** registra um evento no registro de eventos do sistema de arquivos. Ao especificar Evento, você também deve especificar as seguintes propriedades:
        - **EventType:** Informação, aviso ou erro

- **MessageBody:** o texto da mensagem a ser registrada com o evento.
2. **Report:** gera um relatório de uso do armazenamento.

## Exemplos:

1. Crie uma cota rígida de 5 GB sem usar um modelo de cota.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMQuota -Folder "share\test" -Size 5GB
}
```

2. Crie uma cota flexível com uma notificação de limite

```
$thresholds = [System.Collections.ArrayList]@()
$warning = @{
 ThresholdPercentage = 75
 Action = @{
 @{
 ActionType = "Event"
 EventType = "Warning"
 MessageBody = "Quota usage has reached 75%"
 }
 }
}
$thresholds.Add($warning)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList ($thresholds) -ScriptBlock {
 param($thresholds)
 New-FSxFSRMQuota -Folder "share/test" -Size 1GB -Description "Test quota" -
SoftLimit -ThresholdConfigurations $Using:thresholds
}
```

## Obtenha- FSx FSRMQuota

Recupera uma ou mais cotas do seu sistema de arquivos. O comando retorna detalhes sobre as configurações de cotas, incluindo limites de tamanho, limites e uso atual.

## Parâmetros:

- **Folder (string)**: opcional. O caminho da pasta a partir da qual recuperar as cotas. Se você não especificar um caminho de pasta, o comando retornará todas as cotas no sistema de arquivos.

Exemplos:

1. Obtenha todas as cotas existentes no sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMQuota
}
```

### Remover- FSx FSRMQuota

Remove uma cota de uma pasta especificada em seu sistema de arquivos.

Parâmetros:

- **Folder (string)**: obrigatório. O caminho da pasta da qual remover a cota.
- **PassThru (boolean)**: opcional. Se definido como verdadeiro, retorna o objeto de cota removido.

Exemplos:

1. Remova uma cota.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMQuota -Folder "share\test" -PassThru
}
```

### Conjunto- FSx FSRMQuota

Modifica a configuração de uma cota existente.

Parâmetros:

- **Folder (string)**: obrigatório. O caminho da pasta que contém a cota a ser modificada.
- **Description (string)**: opcional. Uma nova descrição para a cota.



- **Size (string):** opcional. O novo limite de tamanho da cota.
- **SoftLimit (boolean):** opcional. Se definido como verdadeiro, altera a cota para um limite flexível, permitindo que os usuários excedam o limite enquanto registram violações.
- **Disabled (boolean):** opcional. Se definido como verdadeiro, desativa a cota. Se definido como falso, ativa a cota.
- **ThresholdConfigurations (array):** opcional. Uma variedade de novas configurações de limites. Cada configuração de limite tem as seguintes propriedades:
  - **ThresholdPercentage (number):** a porcentagem do limite de cota em que as ações devem ser acionadas. Insira um valor entre 0 e 250.
  - **Action (array):** Uma ou mais ações a serem tomadas quando o limite for atingido. Cada ação tem as seguintes propriedades:
    - **ActionType:** O tipo de ação a ser executada. Especifique os seguintes valores:
      1. **Event:** registra um evento no registro de eventos do sistema de arquivos. Ao especificar **Evento**, você também deve especificar as seguintes propriedades:
        - **EventType:** Informação, aviso ou erro
        - **MessageBody:** o texto da mensagem a ser registrada com o evento.
      2. **Report:** gera um relatório de uso do armazenamento.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de cota modificado.

## Exemplos:

### 1. Modifique o tamanho e a descrição da cota.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMQuota -Folder "share\department" -Size 2GB -Description "Updated
quota for department share"
}
```

### 2. Desativar uma cota

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMQuota -Folder "share\department" -Disabled: $true
```

```
}
```

## Atualizar- FSx FSRMQuota

Recalcula as estatísticas de uso atuais de uma cota examinando a pasta para determinar a quantidade real de espaço que está sendo usada.

Parâmetros:

- **Folder (string):** obrigatório. O caminho da pasta que contém a cota a ser atualizada.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de cota atualizado.

Exemplos:

1. Recalcula as estatísticas de uso atuais para uma cota especificada.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Update-FSxFSRMQuota -Folder "share\department" -PassThru
}
```

## Comandos do modelo de cota

### Novo - FSx FSRMQuota Modelo

Cria um novo modelo de cota que define uma configuração reutilizável para cotas.

Parâmetros:

- **Name (string):** obrigatório. Um nome para o modelo de cota.
- **Size (string):** obrigatório. O limite de tamanho que o modelo de cota impõe.
- **Description (string):** opcional. Uma descrição para o modelo de cota.
- **SoftLimit (boolean):** opcional. Se definido como verdadeiro, cria um modelo para cotas flexíveis que relatam o uso, mas não impõem o limite.
- **ThresholdConfigurations (array):** opcional. Uma matriz de configurações de limite que especificam ações a serem tomadas em diferentes níveis de uso. Cada configuração tem as seguintes propriedades:

- **ThresholdPercentage (number):** a porcentagem do limite de cota em que as ações devem ser acionadas. Insira um valor entre 0 e 250.
- **Action (array):** Uma ou mais ações a serem tomadas quando o limite for atingido. Cada ação tem as seguintes propriedades:
  - **ActionType:** O tipo de ação a ser executada. Especifique os seguintes valores:
    1. **Event:** registra um evento no registro de eventos do sistema de arquivos. Ao especificar **Evento**, você também deve especificar as seguintes propriedades:
      - **EventType:** Informação, aviso ou erro
      - **MessageBody:** o texto da mensagem a ser registrada com o evento.
    2. **Report:** gera um relatório de uso do armazenamento.

### Exemplos:

1. Crie um modelo rígido de limite de 1 GB.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMQuotaTemplate -Name "1GB Hard Limit" -Size 1GB -Description "Standard
1GB hard limit template"
}
```

2. Crie um modelo de limite flexível de 5 GB com um limite de aviso de 90% de uso

```
$threshold = @{
 ThresholdPercentage = 90
 Action = @(
 @{
 ActionType = "Event"
 EventType = "Warning"
 MessageBody = "Quota usage has reached 90% of the limit"
 }
)
}

$thresholds = [System.Collections.ArrayList]@()
$thresholds.Add($threshold)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $thresholds -ScriptBlock {
```

```
param($thresholds)

New-FSxFSRMQuotaTemplate -Name "5GB Soft Limit" -Size 5GB -Description "5GB soft
limit with 90% warning" -SoftLimit -ThresholdConfigurations $Using:thresholds
}
```

Obtenha um FSx FSRMQuota modelo

Recupera um ou mais modelos de cota do seu sistema de arquivos.

Parâmetros:

- **Name (string):** opcional. O nome de um modelo de cota específico a ser recuperado. Se você não especificar um nome, o comando retornará todos os modelos de cota.

Exemplos:

1. Recupere todos os modelos de cota no sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMQuotaTemplate
}
```

Conjunto - FSx FSRMQuota Modelo

Modifica as propriedades de um modelo de cota.

Parâmetros:

- **Name (string):** obrigatório. O nome do modelo de cota a ser modificado.
- **Description (string):** opcional. Uma nova descrição para o modelo.
- **Size (string):** opcional. O novo limite de tamanho para o modelo.
- **SoftLimit (boolean):** opcional. Se definido como verdadeiro, altera o modelo para criar cotas flexíveis que relatam o uso, mas não impõem o limite.
- **ThresholdConfigurations (array):** opcional. Uma matriz de configurações de limite que especificam ações a serem tomadas em diferentes níveis de uso. Cada configuração tem as seguintes propriedades:
  - **ThresholdPercentage (number):** a porcentagem do limite de cota em que as ações devem ser acionadas. Insira um valor entre 0 e 250.

- **Action (array):** Uma ou mais ações a serem tomadas quando o limite for atingido. Cada ação tem as seguintes propriedades:
  - **ActionType:** O tipo de ação a ser executada. Especifique os seguintes valores:
    1. **Event:** registra um evento no registro de eventos do sistema de arquivos. Ao especificar **Evento**, você também deve especificar as seguintes propriedades:
      - **EventType:** Informação, aviso ou erro
      - **MessageBody:** o texto da mensagem a ser registrada com o evento.
    2. **Report:** gera um relatório de uso do armazenamento.
- **UpdateDerived (boolean):** opcional. Se definido como verdadeiro, atualiza todas as cotas criadas a partir desse modelo.
- **UpdateDerivedMatching (boolean):** opcional. Se definido como verdadeiro, atualiza somente as cotas que foram criadas a partir desse modelo e que não foram modificadas desde a criação.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de modelo modificado.

## Exemplos:

### 1. Modifica o tamanho e a descrição de um modelo de cota.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMQuotaTemplate -Name "5GB Soft Limit" -Size 10GB -Description "Updated to
 10GB soft limit"
}
```

### 2. Modifica um modelo de cota e atualiza todas as cotas criadas a partir do modelo.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMQuotaTemplate -Name "1GB Hard Limit" -Size 2GB -UpdateDerived
}
```

## Reiniciar- FSx FSRMQuota

Redefine uma cota para corresponder às configurações de um modelo especificado.

## Parâmetros

- **Folder (string):** obrigatório. O caminho da pasta que contém a cota a ser redefinida.
- **Template (string):** obrigatório. O nome do modelo de cota a ser aplicado.

## Exemplos

Exemplos: redefinir uma cota para corresponder às configurações definidas em um modelo de cota.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Reset-FSxFSRMQuota -Folder "share\department" -Template "1GB Hard Limit"
}
```

## Comandos de cota automática

### Nova FSx FSRMAuto cota

O `New-FSxFSRMAutoQuota` comando cria uma cota de aplicação automática em uma pasta especificada. Uma cota de aplicação automática gera automaticamente cotas com base no modelo especificado para cada subpasta existente e quaisquer novas subpastas criadas na pasta especificada.

## Parâmetros

- **Folder (string):** obrigatório. O caminho da pasta em que a cota de aplicação automática será criada.
- **Template (string):** opcional. O nome de um modelo de cota existente a ser usado para a cota de aplicação automática.
- **Disabled (boolean):** opcional. Se definido como verdadeiro, cria a cota de aplicação automática em um estado desativado.

## Exemplos

1. Crie uma cota de aplicação automática que aplique automaticamente um modelo especificado a todas as subpastas.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
```

```
New-FSxFSRMAutoQuota -Folder "share\department" -Template "250 MB Extended Limit"
}
```

## Obtenha uma FSx FSRMAuto cota

O `Get-FSxFSRMAutoQuota` comando recupera uma ou mais cotas de aplicação automática do seu sistema de arquivos.

### Parâmetros

- **Folder (string)**: opcional. O caminho da pasta a partir da qual recuperar as cotas de aplicação automática. Você também pode usar `...` no final do caminho para incluir todas as subpastas.

Se você não especificar um caminho de pasta, o comando retornará todas as cotas de aplicação automática no sistema de arquivos.

### Exemplos

1. Recupere todas as cotas de aplicação automática no sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMAutoQuota
}
```

## Remover - FSx FSRMAuto Cota

O `Remove-FSxFSRMAutoQuota` comando remove uma cota de aplicação automática de uma pasta especificada. Quando você remove uma cota de aplicação automática, o comando também remove todas as cotas das subpastas derivadas do modelo de cota associado.

### Parâmetros

- **Folder (string)**: obrigatório. O caminho da pasta da qual remover a cota de aplicação automática.
- **PassThru (boolean)**: opcional. Se definido como verdadeiro, retorna o objeto de cota de aplicação automática removido.

## Exemplos

### 1. Remova uma cota de aplicação automática de uma pasta específica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMAutoQuota -Folder "share\department" -PassThru
}
```

## Definir FSx FSRMAuto cota

O `Set-FSxFSRMAutoQuota` comando modifica as configurações de uma cota de aplicação automática.

## Parâmetros

- `Folder (string)`: obrigatório. O caminho da pasta que contém a cota de aplicação automática a ser modificada.
- `Template (string)`: opcional. O nome de um modelo de cota a ser aplicado.
- `Disabled (boolean)`: opcional. Se definido como verdadeiro, desativa a cota de aplicação automática. Se definido como falso, ativa a cota de aplicação automática.
- `UpdateDerived (boolean)`: opcional. Se definido como verdadeiro, atualiza todas as cotas existentes derivadas dessa cota de aplicação automática.
- `UpdateDerivedMatching (boolean)`: opcional. Se definido como verdadeiro, atualiza somente as cotas derivadas que não foram modificadas desde a criação.
- `PassThru (boolean)`: opcional. Se definido como verdadeiro, retorna o objeto de cota de aplicação automática modificado.

## Exemplos

### 1. Altere o modelo de cota usado por uma cota de aplicação automática.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMAutoQuota -Folder "share\department" -Template "100 MB Limit"
}
```

### 2. Desative uma cota de aplicação automática e atualize todas as cotas derivadas dela.



```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMAutoQuota -Folder "share\department" -Disabled: $true -UpdateDerived
}
```

## Atualização - FSx FSRMAuto Cota

O `Update-FSxFSRMAutoQuota` comando recalcula as propriedades de uma cota de aplicação automática e as cotas derivadas dela examinando a pasta para determinar a quantidade real de espaço que está sendo usada.

### Parâmetros

- `Folder (string)`: obrigatório. O caminho da pasta que contém a cota de aplicação automática a ser atualizada.
- `PassThru (boolean)`: opcional. Se definido como verdadeiro, retorna o objeto de cota de aplicação automática atualizado.

### Exemplos

1. Recalcule as estatísticas de uso e retorne o objeto de cota de aplicação automática atualizado.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Update-FSxFSRMAutoQuota -Folder "share\department" -PassThru
}
```

## Grupos de arquivos

Os grupos de arquivos definem coleções lógicas de padrões de nome de arquivo que você deve usar ao configurar a [triagem de arquivos](#) e que você pode usar opcionalmente ao gerar relatórios [de armazenamento](#). Um grupo de arquivos contém padrões de inclusão (arquivos a serem combinados) e padrões de exclusão (arquivos a serem excluídos das correspondências), aos quais você faz referência pelo nome do grupo de arquivos em vez de especificar padrões individuais a cada vez.

### Como os grupos de arquivos são usados

Grupos de arquivos são necessários para os seguintes recursos do FSRM:

- Triagem de arquivos - Você deve especificar um ou mais grupos de arquivos para definir quais tipos de arquivo bloquear ou monitorar.
- Exceções de filtragem de arquivos - Você deve especificar um ou mais grupos de arquivos para definir quais tipos de arquivo permitir, apesar de bloquear a triagem de arquivos nas pastas principais.
- Modelos de triagem de arquivos - Você deve especificar um ou mais grupos de arquivos para definir quais tipos de arquivo o modelo bloqueará ou monitorará.

Os grupos de arquivos são opcionais para os seguintes recursos do FSRM:

- Relatórios de armazenamento - você pode, opcionalmente, filtrar relatórios por grupo de arquivos para analisar o uso do armazenamento para tipos de arquivo específicos. Por exemplo, você pode gerar um relatório mostrando somente arquivos de áudio e vídeo.

## Padrões de nome de arquivo

Os grupos de arquivos usam padrões curinga para corresponder aos nomes dos arquivos. Você pode especificar padrões de inclusão (arquivos a serem combinados) e padrões de exclusão (arquivos a serem excluídos das correspondências).

O FSRM oferece suporte aos seguintes curingas:

- Asterisco (\*) - Corresponde a zero ou mais caracteres
- Ponto de interrogação (?) - Combina exatamente com um personagem

Por exemplo, o padrão \*.doc\* corresponde a arquivos como report.doc, report.docx, edocument.doc, enquanto o padrão de ~\$\* exclusão exclui arquivos temporários criados por aplicativos do Microsoft Office.

## Grupos de arquivos padrão

Quando você ativa o FSRM em seu sistema de arquivos, os seguintes grupos de arquivos são criados automaticamente:

### Arquivos de áudio e vídeo

Corresponde aos formatos comuns de arquivo de áudio e vídeo \*.mp3 \*.wav, incluindo \*.avi, \*.mp4, \*.mpeg, e \*.wmv

## Arquivos de backup

Corresponde aos formatos de arquivo de backup\* .bak, incluindo\* .backup, e \* .old

## Arquivos compactados

Corresponde aos formatos de arquivo compactado e arquivado\* .zip, incluindo  
\* .rar,\* .7z,\* .gz, e \* .tar

## Arquivos de e-mail

Corresponde aos formatos de mensagem de e-mail e caixa de correio\* .eml, incluindo \* .msg, e  
\* .pst

## Arquivos executáveis

Corresponde aos formatos de arquivo executável e de script\* .exe, incluindo  
\* .dll,\* .com,\* .bat,\* .cmd, e \* .vbs

## Arquivos de imagem

Corresponde aos formatos de arquivo de imagem comuns \* .jpg \* .jpeg,  
incluindo\* .png,\* .gif,,\* .bmp, e \* .tif

## Arquivos do Office

Corresponde aos formatos de documentos do Microsoft Office \* .doc \* .docx,  
incluindo\* .xls,\* .xlsx,,\* .ppt, e \* .pptx

## Arquivos do sistema

Corresponde aos formatos de arquivo do sistema Windows\* .sys, incluindo \* .dll,\* .ocx, e  
\* .drv

## Arquivos temporários

Corresponde aos formatos de arquivo temporários\* .tmp, incluindo\* .temp, e ~\*

## Arquivos de texto

Corresponde aos formatos de arquivo baseados em texto\* .txt, incluindo,\* .log, e \* .csv  
\* .xml

## Arquivos de páginas da Web

Corresponde aos formatos de arquivo de conteúdo da web \* .html \* .htm,  
incluindo\* .asp,\* .aspx,\* .php,, e \* .js

Você pode usar esses grupos de arquivos padrão imediatamente nas triagens de arquivos e nos relatórios de armazenamento, ou pode modificá-los para atender às suas necessidades específicas.

## Comandos de gerenciamento de grupos de arquivos

O FSRM fornece PowerShell comandos para criar e gerenciar grupos de arquivos. Use esses comandos para definir grupos de arquivos personalizados que correspondam às políticas de gerenciamento de arquivos da sua organização.

### Note

Todos os exemplos nesta página pressupõem que você tenha definido a `$FSxWindowsRemotePowerShellEndpoint` variável com o PowerShell endpoint remoto do Windows do seu sistema de arquivos. Você pode encontrar esse endpoint no AWS FSx console na página de detalhes do seu sistema de arquivos ou usando o comando AWS `describe-file-systems` CLI.

### Novo- FSx FSRMFile Grupo

Cria um grupo de arquivos que define uma coleção lógica de padrões de nomes de arquivos. Esses padrões podem ser usados para triagens de arquivos, exceções de triagem de arquivos e relatórios de armazenamento.

Parâmetros:

- **Name (string):** obrigatório. Um nome para o grupo de arquivos.
- **Description (string):** opcional. Uma descrição para o grupo de arquivos.
- **IncludePattern (array):** opcional. Uma matriz de cadeias de caracteres de padrões que especificam os arquivos a serem incluídos.
- **ExcludePattern (array):** opcional. Uma matriz de cadeias de caracteres de padrões que especificam arquivos a serem excluídos.

Exemplos:

1. Crie um grupo de arquivos para arquivos de texto.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
```

```
New-FSxFSRMFileGroup -Name "My Text Files" -IncludePattern "*.txt"
}
```

2. Crie um grupo de arquivos para o código-fonte com padrões de inclusão e exclusão.

```
$includePatterns = @("*.cpp", "*.h", "*.cs", "*.py")
$excludePatterns = @("*.tmp", "*.bak")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList @($includePatterns, $excludePatterns) -ScriptBlock {
 param($includePatterns, $excludePatterns)
 New-FSxFSRMFileGroup -Name "Source Code" -Description "Programming source files"
 -IncludePattern $includePatterns -ExcludePattern $excludePatterns
}
```

## FSxFSRMFileGrupo Get

Recupera um ou mais grupos de arquivos do seu sistema de arquivos. Os grupos de arquivos definem coleções de padrões de arquivo usados na triagem e geração de relatórios de arquivos.

Parâmetros:

- **Name (array):** opcional. Uma matriz de nomes de grupos de arquivos a serem recuperados. Se você não especificar um nome, o comando retornará todos os grupos de arquivos no sistema de arquivos.

Exemplos:

1. Recupere todos os grupos de arquivos no sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMFileGroup
}
```

## Remover - FSx FSRMFile Grupo

Remove um ou mais grupos de arquivos do seu sistema de arquivos. Após a remoção, o grupo de arquivos não pode ser usado em triagens de arquivos ou exceções de triagem de arquivos.

## Parâmetros:

- **Name (array):** obrigatório. Uma matriz de nomes de grupos de arquivos a serem removidos.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto do grupo de arquivos removido.

## Exemplos:

1. Remova um único grupo de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMFileGroup -Name "My Text Files" -PassThru
}
```

## Conjunto - FSx FSRMFile Grupo

Modifica as propriedades dos grupos de arquivos existentes.

## Parâmetros:

- **Name (array):** obrigatório. Uma matriz de nomes de grupos de arquivos a serem modificados.
- **Description (string):** opcional. Uma nova descrição para o grupo de arquivos.
- **IncludePattern (array):** opcional. Uma nova matriz de cadeias de caracteres de padrões que especificam os arquivos a serem incluídos.
- **ExcludePattern (array):** opcional. Uma nova matriz de cadeias de caracteres de padrões que especificam arquivos a serem excluídos.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto do grupo de arquivos modificado.

## Exemplos:

1. Atualize a descrição e os padrões de um grupo de arquivos.

```
$includePatterns = @"*.docx", "*.pdf", "*.rtf"
$excludePatterns = @"~$*", "*.tmp"
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList @($includePatterns, $excludePatterns) -ScriptBlock {
 param($includePatterns, $excludePatterns)
 Set-FSxFSRMFileGroup -Name "Documents" -Description "Updated document types" -
 IncludePattern $includePatterns -ExcludePattern $excludePatterns -PassThru
}
```

## Triagem de arquivos

A triagem de arquivos controla quais tipos de arquivos os usuários podem salvar nas pastas do seu sistema de arquivos. A triagem de arquivos ajuda a aplicar políticas de armazenamento, evitar tipos de arquivos não autorizados e manter a conformidade com os requisitos organizacionais.

### Note

As filtragens de arquivos usam grupos de arquivos para definir quais tipos de arquivo devem ser bloqueados ou monitorados. Para obter mais informações sobre como criar e gerenciar grupos de arquivos, consulte [Grupos de arquivos](#).

O FSRM oferece suporte a dois tipos de filtragem de arquivos:

1. Triagem ativa de arquivos - Impeça que os usuários salvem arquivos que correspondam aos grupos de arquivos especificados e gere notificações quando os usuários tentarem salvar arquivos bloqueados. Use triagens de arquivos ativas quando precisar aplicar políticas rígidas sobre quais tipos de arquivo são permitidos em pastas específicas.
2. Telas passivas de arquivos - Monitore e registre quando os usuários salvam arquivos que correspondem aos grupos de arquivos especificados, mas não impedem a operação de salvamento. Use telas de arquivos passivas quando quiser monitorar os padrões de uso de arquivos sem interromper os fluxos de trabalho do usuário.

## Modelos de triagem de arquivos

Os modelos de triagem de arquivos fornecem uma configuração reutilizável que define as configurações de triagem de arquivos, incluindo quais grupos de arquivos bloquear ou monitorar e quais notificações gerar. Depois de criar um modelo de triagem de arquivos, você pode aplicá-lo a várias pastas sem precisar redefinir as mesmas configurações todas as vezes. Ao atualizar um

modelo de triagem de arquivos, você pode, opcionalmente, aplicar as alterações a todas as triagens de arquivo criadas a partir desse modelo.

O uso de modelos de triagem de arquivos oferece vários benefícios:

- **Consistência** - Certifique-se de que pastas semelhantes tenham configurações de triagem de arquivos idênticas
- **Eficiência** - Aplique configurações de triagem de arquivos a várias pastas rapidamente
- **Manutenção** - Atualize as configurações de triagem de arquivos em várias pastas modificando o modelo

## Exceções de triagem de arquivos

As exceções de filtragem de arquivos substituem as regras de triagem de arquivos que, de outra forma, se aplicariam a uma pasta e a todas as suas subpastas. Ao criar uma exceção de filtragem de arquivos, você especifica quais grupos de arquivos permitir, apesar de qualquer bloqueio na triagem de arquivos nas pastas principais. As exceções de filtragem de arquivos são úteis quando você precisa permitir tipos de arquivo específicos em determinadas subpastas e, ao mesmo tempo, manter restrições mais amplas em níveis mais altos da hierarquia de pastas.

Por exemplo, você pode bloquear arquivos executáveis em um compartilhamento inteiro, mas criar uma exceção para uma subpasta específica na qual os administradores precisam armazenar arquivos de instalação.

## Notificações de seleção de arquivos

Quando os usuários tentam salvar arquivos bloqueados por uma triagem de arquivos ativa, o FSRM pode gerar notificações para alertar os administradores ou fornecer informações aos usuários. Você pode configurar os seguintes tipos de notificações:

- **Registro de eventos** — registre um evento na Amazon CloudWatch ou no Amazon Kinesis Data Firehose para monitoramento e análise. Você pode especificar o nível de gravidade do evento (informação, aviso ou erro) e fornecer um corpo de mensagem personalizado. O registro de eventos é útil para rastrear violações da triagem de arquivos e integrar-se aos sistemas de monitoramento existentes.
- **Relatórios de armazenamento** - Gere um relatório de uso de armazenamento que forneça informações detalhadas sobre a atividade de triagem de arquivos. Os relatórios de armazenamento ajudam você a identificar padrões nas tentativas de salvar arquivos e a tomar



decisões informadas sobre as políticas de triagem de arquivos. Para obter mais informações, consulte [Relatórios de armazenamento](#).

## Comandos de gerenciamento de triagem de arquivos

Você pode acessar três famílias de PowerShell comandos FSx remotos para gerenciar a triagem de arquivos:

1. Comandos de filtragem de arquivos - Crie, recupere, modifique, remova e redefina triagens de arquivos individuais em pastas específicas. Use esses comandos quando precisar gerenciar a triagem de arquivos em uma folder-by-folder base.
2. Comandos do modelo de triagem de arquivos - Crie, recupere, modifique e remova modelos de triagem de arquivos que definem configurações de triagem de arquivos reutilizáveis. Use esses comandos para estabelecer políticas padrão de triagem de arquivos que você pode aplicar em várias pastas.
3. Comandos de exceção de filtragem de arquivos - Crie, recupere, modifique e remova exceções de triagem de arquivos que substituem as regras de triagem de arquivos nas pastas principais. Use esses comandos quando precisar permitir tipos de arquivo específicos em determinadas subpastas, mantendo restrições mais amplas.

### Lista de PowerShell comandos FSx remotos de filtragem de arquivos

#### Note

Todos os exemplos nesta página pressupõem que você tenha definido a `$FSxWindowsRemotePowerShellEndpoint` variável com o PowerShell endpoint remoto do Windows do seu sistema de arquivos. Você pode encontrar esse endpoint no FSx console da Amazon na página de detalhes do seu sistema de arquivos ou usando o AWS CLI `describe-file-systems` comando.

## Comandos de tela de arquivos

### Nova FSx FSRMFile tela

Cria uma triagem de arquivo que impede que os usuários salvem tipos específicos de arquivos em uma pasta.

## Parâmetros:

- **Folder (string):** obrigatório. O caminho da pasta em que a tela do arquivo será aplicada.
- **Description (string):** opcional. Uma descrição para a triagem do arquivo.
- **IncludeGroup (array):** opcional. Uma matriz de nomes de grupos de arquivos que especificam quais arquivos bloquear ou monitorar.
- **Active (boolean):** opcional. Se definido como verdadeiro, cria uma triagem de arquivo ativa que bloqueia os arquivos. Se definido como false, cria uma tela de arquivo passiva que monitora somente os arquivos. O padrão é true (verdadeiro).
- **Template (string):** opcional. O nome de um modelo de triagem de arquivo existente a ser usado.
- **NotificationConfigurations (array):** opcional. Uma variedade de configurações para notificações quando os usuários tentam salvar arquivos bloqueados. Cada configuração tem as seguintes propriedades:
  - **ActionType (string):** O tipo de ação a ser executada. Especifique os seguintes valores:
    1. **Event:** registra um evento no registro de eventos do sistema de arquivos. Ao especificar Evento, você também deve especificar as seguintes propriedades:
      - **EventType (string):** Informação, aviso ou erro
      - **MessageBody (string):** o texto da mensagem a ser registrada com o evento.
    2. **Report:** gera um relatório de uso do armazenamento. Ao especificar Relatório, você também deve especificar:
      - **ReportType (string):** O tipo de relatório. Você pode especificar os seguintes valores: DuplicateFiles, FilesByFileGroup, FilesByOwner, FilesByProperty, LargeFiles, Leases ou QuotaUsage.

## Exemplos:

1. Crie uma tela de arquivo ativa básica que bloqueie arquivos de áudio.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMFileScreen -Folder "share\department" -IncludeGroup "Audio and Video
Files"
}
```

2. Crie uma tela de arquivo que bloqueie arquivos de vídeo e gere uma entrada de registro de eventos quando um usuário tentar salvar um arquivo de vídeo.

```
$notifications = [System.Collections.ArrayList]@()
$eventNotification = @{
 ActionType = "Event"
 EventType = "Warning"
 MessageBody = "File screen violation detected"
}
$null = $notifications.Add($eventNotification)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
 param($notifications)
 New-FSxFSRMFileScreen -Folder "share\projects" -IncludeGroup "Audio and Video
Files" -NotificationConfigurations $Using:notifications
}
```

## FSxFSRMFileEcrã Get

Recupera uma ou mais filtragens de arquivos do seu sistema de arquivos.

Parâmetros:

- **Folder (string):** opcional. O caminho da pasta a partir da qual recuperar as filtragens de arquivos. Se você não especificar um caminho de pasta, o comando retornará todas as filtragens de arquivos no sistema de arquivos.

Exemplos:

1. Recupere todas as telas de arquivos no sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMFileScreen
}
```

## FSxFSRMFileEcrã do conjunto

Modifica as propriedades de uma triagem de arquivos existente.

## Parâmetros:

- **Folder (string):** obrigatório. O caminho da pasta que contém a triagem do arquivo a ser modificada.
- **Description (string):** opcional. Uma nova descrição para a triagem do arquivo.
- **IncludeGroup (array):** opcional. Uma nova matriz de nomes de grupos de arquivos que definem quais arquivos bloquear ou monitorar.
- **Active (boolean):** opcional. Se definido como verdadeiro, define a tela do arquivo para o modo ativo (bloqueio). Se definido como falso, define a tela do arquivo para o modo passivo (somente monitoramento). O padrão é true (verdadeiro).
- **NotificationConfigurations (array):** opcional. Uma nova variedade de configurações de notificação.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de filtragem de arquivos modificado.

## Exemplos:

1. Modifique a descrição e os grupos de arquivos para uma triagem de arquivos.

```
$includeGroups = @"Audio and Video Files"
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
 param($includeGroups)
 Set-FSxFSRMFileScreen -Folder "share\projects" -Description "Updated screen" -
 IncludeGroup $includeGroups
}
```

2. Defina uma tela de arquivo para o modo ativo e adicione notificações.

```
$notifications = [System.Collections.ArrayList]@()
$eventNotification = @{
 ActionType = "Event"
 EventType = "Warning"
 MessageBody = "File screen violation detected"
}
$null = $notifications.Add($eventNotification)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
```

```
param($notifications)
Set-FSxFSRMFileScreen -Folder "share\projects" -Active: $true -
NotificationConfigurations $Using:notifications -PassThru
}
```

## Remover - FSx FSRMFile Tela

Remove uma triagem de arquivo de uma pasta especificada.

Parâmetros:

- **Folder (string)**: obrigatório. O caminho da pasta da qual remover a tela do arquivo.
- **PassThru (boolean)**: opcional. Se definido como verdadeiro, retorna o objeto de filtragem de arquivos removido.

Exemplos:

1. Remova uma triagem de arquivo de uma pasta específica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMFileScreen -Folder "share\projects" -PassThru
}
```

## Redefinir - FSx FSRMFile Tela

Redefine a triagem de um arquivo para corresponder às configurações de um modelo especificado.

Parâmetros:

- **Folder (string)**: obrigatório. O caminho da pasta que contém a tela do arquivo a ser redefinida.
- **Template (string)**: obrigatório. O nome de um modelo de triagem de arquivo existente a ser aplicado.

Exemplos:

1. Redefina uma triagem de arquivo para que corresponda às configurações definidas em um modelo de triagem de arquivo.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Reset-FSxFSRMFileScreen -Folder "share\department" -Template "Block Audio Files"
}
```

## Comandos do modelo de triagem de arquivos

### Obtenha- FSx FSRMFile ScreenTemplate

O `Get-FSxFSRMFileScreenTemplate` comando recupera um ou mais modelos de triagem de arquivos do seu sistema de arquivos.

#### Parâmetros

- **Name (array):** opcional. Uma matriz de nomes de modelos de triagem de arquivos a serem recuperados. Se você não especificar um nome, o comando retornará todos os modelos de triagem de arquivos no sistema de arquivos.

## Exemplos

1. Recupere todos os modelos de triagem de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMFileScreenTemplate
}
```

### Novo- FSx FSRMFile ScreenTemplate

O `New-FSxFSRMFileScreenTemplate` comando cria um modelo de triagem de arquivo que define uma configuração reutilizável para triagem de arquivos. O modelo especifica quais grupos de arquivos bloquear e quais notificações gerar quando os usuários tentarem salvar arquivos bloqueados.

#### Parâmetros

- **Name (string):** obrigatório. Um nome para o modelo de triagem de arquivos.

- **Description (string):** opcional. Uma descrição para o modelo de triagem de arquivos.
- **IncludeGroup (array):** opcional. Uma matriz de nomes de grupos de arquivos que especificam quais arquivos bloquear ou monitorar.
- **Active (boolean):** opcional. Se definido como verdadeiro, cria um modelo de triagem de arquivos ativo que bloqueia os arquivos. Se definido como false, cria um modelo passivo que monitora somente arquivos. O padrão é true (verdadeiro).
- **NotificationConfigurations (array):** opcional. Uma variedade de configurações para notificações quando os usuários tentam salvar arquivos bloqueados. Cada configuração tem as seguintes propriedades:
  - **ActionType (string):** O tipo de ação a ser executada. Especifique os seguintes valores:
    1. **Event:** registra um evento no registro de eventos do sistema de arquivos. Ao especificar Evento, você também deve especificar as seguintes propriedades:
      - **EventType (string):** Informação, aviso ou erro
      - **MessageBody (string):** o texto da mensagem a ser registrada com o evento.
    2. **Report:** gera um relatório de uso do armazenamento. Ao especificar Relatório, você também deve especificar:
      - **ReportType (string):** O tipo de relatório. Você pode especificar os seguintes valores: DuplicateFiles, FilesByFileGroup, FilesByOwner, FilesByProperty, LargeFiles, Leases ou QuotaUsage

## Exemplos

1. Crie um modelo de triagem de arquivos com notificações.

```
$notifications = [System.Collections.ArrayList]@()
$eventNotif = @{
 ActionType = "Event"
 EventType = "Warning"
 MessageBody = "Blocked file detected"
}
$null = $notifications.Add($eventNotif)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
 param($notifications)
```

```
New-FSxFSRMFileScreenTemplate -Name "Block Executables" -Description
"Blocks executable files" -IncludeGroup "Executable Files" -Active: $true -
NotificationConfigurations $Using:notifications
}
```

## Remover- FSx FSRMFile ScreenTemplate

O `Remove-FSxFSRMFileScreenTemplate` comando remove um ou mais modelos de triagem de arquivos do seu sistema de arquivos. Quando você remove um modelo, as triagens de arquivo criadas a partir desse modelo permanecem inalteradas.

### Parâmetros

- **Name (array):** obrigatório. Uma matriz de nomes de modelos de triagem de arquivos a serem removidos.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de modelo de triagem de arquivo removido.

### Exemplos

1. Remova um único modelo de triagem de arquivo.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMFileScreenTemplate -Name "Block Executables" -PassThru
}
```

## Conjunto- FSx FSRMFile ScreenTemplate

O `Set-FSxFSRMFileScreenTemplate` comando modifica as propriedades dos modelos de filtragem de arquivos existentes. Opcionalmente, atualiza as filtragens de arquivos que foram criadas usando os modelos modificados.

### Parâmetros

- **Name (array):** obrigatório. Uma matriz de nomes de modelos de triagem de arquivos a serem modificados.
- **Description (string):** opcional. Uma nova descrição para o modelo.
- **IncludeGroup (array):** opcional. Uma nova matriz de nomes de grupos de arquivos que definem quais arquivos bloquear ou monitorar.



- **Active** (boolean): opcional. Se definido como verdadeiro, define o modelo para o modo ativo (bloqueio). Se definido como falso, define o modelo para o modo passivo (monitoramento). O padrão é true (verdadeiro).
- **NotificationConfigurations** (array): opcional. Uma nova variedade de configurações de notificação.
- **UpdateDerived** (boolean): opcional. Se definido como verdadeiro, atualiza todas as filtragens de arquivos existentes criadas a partir desse modelo, independentemente de quaisquer modificações feitas nessas filtragens de arquivo.
- **UpdateDerivedMatching** (boolean): opcional. Se definido como verdadeiro, atualiza somente as filtragens de arquivos que não foram modificadas desde sua criação a partir desse modelo.
- **PassThru** (boolean): opcional. Se definido como verdadeiro, retorna o objeto de modelo de triagem de arquivo modificado.

## Exemplos

1. Atualize um modelo de triagem de arquivos com novos grupos de arquivos.

```
$includeGroups = @("Audio and Video Files")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
 param($includeGroups)
 Set-FSxFSRMFileScreenTemplate -Name "Block Executables" -IncludeGroup
 $includeGroups
 }
```

2. Atualize um modelo de triagem de arquivos para o modo ativo e atualize todas as filtragens de arquivos derivadas.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMFileScreenTemplate -Name "Block Executables" -Active: $true -
 UpdateDerived
 }
```

## Comandos de exceção de filtragem de arquivos

### Novo- FSx FSRMFile ScreenException

O `New-FSxFSRMFileScreenException` comando cria uma exceção de filtragem de arquivos que substitui todas as regras de triagem de arquivos que, de outra forma, se aplicariam a uma pasta e a todas as suas subpastas. Isso permite que tipos de arquivo específicos sejam criados na pasta de exceções, mesmo que estejam bloqueados por filtrações de arquivos nas pastas principais.

### Parâmetros

- **Folder (string)**: obrigatório. O caminho da pasta em que a exceção de triagem de arquivos será aplicada. A exceção se aplica a essa pasta e a todas as suas subpastas.
- **Description (string)**: opcional. Uma descrição para a exceção de triagem de arquivos.
- **IncludeGroup (array)**: opcional. Uma matriz de nomes de grupos de arquivos que especificam quais arquivos permitir, apesar de qualquer bloqueio de arquivos que, de outra forma, se aplicaria às pastas principais.

### Exemplos

1. Crie uma exceção de filtragem de arquivos para uma pasta e um grupo de arquivos específicos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMFileScreenException -Folder "share\department" -IncludeGroup "Text
Files"
}
```

2. Crie uma exceção de filtragem de arquivos com vários grupos de arquivos.

```
$includeGroups = @("Audio and Video Files", "Documents")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
 param($includeGroups)
 New-FSxFSRMFileScreenException -Folder "share\projects" -Description "Allow media
files in project folder" -IncludeGroup $includeGroups
}
```

## Obtenha- FSx FSRMFile ScreenException

O `Get-FSxFSRMFileScreenException` comando recupera uma ou mais exceções de triagem de arquivos do seu sistema de arquivos.

### Parâmetros

- **Folder (string):** opcional. O caminho da pasta a partir da qual recuperar as exceções da triagem de arquivos. Se você não especificar um caminho de pasta, o comando retornará todas as exceções de filtragem de arquivos no sistema de arquivos.

### Exemplos

1. Recupere todas as exceções da triagem de arquivos no sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMFileScreenException
}
```

2. Recupere a exceção de triagem de arquivos para uma pasta específica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMFileScreenException -Folder "share\department"
}
```

## Remover- FSx FSRMFile ScreenException

O `Remove-FSxFSRMFileScreenException` comando remove uma exceção de filtragem de arquivos de uma pasta especificada. Após a remoção, a pasta e suas subpastas estarão sujeitas a todas as regras de triagem de arquivos das pastas principais que foram anteriormente substituídas pela exceção.

### Parâmetros

- **Folder (string):** obrigatório. O caminho da pasta da qual remover a exceção de triagem de arquivos.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de exceção da triagem de arquivos removido.

## Exemplos

### 1. Remova uma exceção de filtragem de arquivos de uma pasta específica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMFileScreenException -Folder "share\projects" -PassThru
}
```

## Conjunto- FSx FSRMFile ScreenException

O Set-FSxFSRMFileScreenException comando modifica as propriedades de uma exceção de filtragem de arquivos.

## Parâmetros

- **Folder (string):** obrigatório. O caminho da pasta que contém a exceção de filtragem de arquivos a ser modificada.
- **Description (string):** opcional. Uma nova descrição para a exceção de filtragem de arquivos.
- **IncludeGroup (array):** opcional. Uma nova matriz de nomes de grupos de arquivos que definem quais arquivos permitir, apesar de qualquer bloqueio de arquivos que, de outra forma, se aplicaria às pastas principais.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de exceção da triagem de arquivos modificado.

## Exemplos

### 1. Atualize os grupos de arquivos permitidos para uma exceção de triagem de arquivos.

```
$includeGroups = @("Audio and Video Files")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
 param($includeGroups)
 Set-FSxFSRMFileScreenException -Folder "share\projects" -IncludeGroup
 $includeGroups -PassThru
}
```

## Classificação de arquivos

A classificação de arquivos atribui automaticamente propriedades de metadados aos arquivos com base em seu conteúdo, localização ou outros atributos. A classificação ajuda você a organizar arquivos, aplicar políticas de gerenciamento de dados e atender aos requisitos de conformidade, identificando arquivos que contêm informações confidenciais, pertencem a categorias comerciais específicas ou exigem períodos de retenção.

### Como funciona a classificação de arquivos

A classificação de arquivos usa um processo de três etapas:

1. Definir propriedades - Crie definições de propriedades de classificação que especifiquem os tipos de metadados que você deseja atribuir aos arquivos, como "Data Sensitivity" ou "ContainsPII".
2. Crie regras - configure regras de classificação que atribuam automaticamente valores de propriedade aos arquivos com base em critérios que você especifica, como padrões de conteúdo de arquivo ou localização de pastas. Por exemplo, arquivos que contêm um padrão, como um número de previdência social, (XXX-XX-XXXX) podem ser classificados automaticamente como ContainsPII=Yes.
3. Executar classificação - Execute o processo de classificação para verificar arquivos e aplicar as regras. Você pode executar a classificação manualmente sob demanda, em um cronograma ou continuamente em segundo plano.

Depois que a classificação for concluída, você poderá usar as propriedades atribuídas para gerar relatórios de armazenamento [Tarefas de gerenciamento de arquivos](#), aplicar ou pesquisar arquivos com características específicas.

### Definições de propriedades de classificação

As definições de propriedades de classificação especificam os tipos de metadados que podem ser atribuídos aos arquivos. Cada definição de propriedade tem um nome, um tipo de propriedade e, opcionalmente, uma lista de valores permitidos. Por exemplo, você pode criar uma propriedade chamada "Data Sensitivity" com um `OrderedList` Tipo e valores possíveis: `Public`, `InternalConfidential`, `Restricted` e.

Os seguintes tipos de propriedades são compatíveis:

- **OrderedList**- Uma lista ordenada em que os valores têm uma sequência específica (por exemplo, Baixa, Média, Alta). Use esse tipo quando a ordem dos valores for importante para relatórios ou decisões políticas.
- **MultiChoice**- Permite que vários valores sejam selecionados em uma lista (por exemplo, um arquivo pode ser marcado com as categorias “Financeiro” e “Jurídico”).
- **SingleChoice**- Permite que somente um valor seja selecionado em uma lista.
- **String**- Um único valor de texto sem opções predefinidas.
- **MultiString**- Vários valores de texto sem opções predefinidas.
- **Integer**- Um valor numérico.
- **YesNo**- Um valor booleano (verdadeiro ou falso).
- **DateTime**- Um valor de data e hora.

As definições de propriedade são reutilizáveis em várias regras de classificação. Depois de criar uma definição de propriedade, você pode referenciá-la em qualquer regra de classificação que precise atribuir valores para essa propriedade.

## Regras de classificação

As regras de classificação definem a lógica para atribuir automaticamente os valores das propriedades aos arquivos. Cada regra especifica:

- Qual propriedade definir
- Qual valor atribuir a essa propriedade
- Onde aplicar a regra (quais pastas)
- Como identificar arquivos que devem receber o valor da propriedade. Você pode usar dois mecanismos de classificação:

### Classificador de conteúdo

O Classificador de conteúdo verifica o conteúdo do arquivo em busca de padrões de texto ou expressões regulares específicos. Use esse mecanismo para identificar arquivos com base no que eles contêm. O Classificador de conteúdo fornece três maneiras de combinar o conteúdo do arquivo:

- **ContentString**- Pesquisa cadeias de texto que não diferenciam maiúsculas de minúsculas. Use essa opção quando quiser encontrar palavras ou frases específicas, independentemente

da capitalização. Por exemplo, pesquisar por “confidencial” corresponderá a “Confidencial”, “CONFIDENCIAL” e “confidencial”.

- **ContentStringCaseSensitive**- Pesquisa sequências de texto com distinção entre maiúsculas e minúsculas. Use essa opção quando a capitalização for importante para sua pesquisa. Por exemplo, pesquisar por “SSN” corresponderá a “SSN”, mas não a “ssn” ou “Ssn”. Isso é útil para acrônimos, códigos de produtos ou outros identificadores em que a maiúscula e minúscula é significativa.
- **ContentRegularExpression**- Pesquisa padrões usando expressões regulares. Use essa opção quando precisar combinar padrões complexos ou formatos variáveis. Por exemplo, você pode usar expressões regulares para detectar:
  - Números de previdência social no formato 123-45-6789: `\b\d{3}-\d{2}-\d{4}\b`
  - Números de cartão de crédito com espaços ou traços opcionais: `\b\d{4}[\s-]?\d{4}[\s-]?\d{4}[\s-]?\d{4}\b`
  - Endereços de e-mail, números de telefone ou outros dados estruturados

Você pode especificar várias sequências de caracteres ou padrões em uma única regra e os arquivos serão classificados se o conteúdo corresponder a qualquer um dos valores especificados.

## Classificador de pastas

O classificador de pastas atribui valores de propriedade com base em onde os arquivos são armazenados. Use esse mecanismo para classificar os arquivos por sua localização na hierarquia de pastas. Por exemplo:

- Defina uma propriedade de período de retenção para todos os arquivos na pasta Documentos legais
- Marque todos os arquivos em uma pasta de projeto específica com um identificador de projeto

Além disso, você pode usar o `ReevaluateProperty` parâmetro para controlar o que acontece quando a classificação é executada em um arquivo que já tem um valor para a propriedade. Você pode selecionar as seguintes configurações:

- **Never**- Classifique somente arquivos que não tenham um valor para essa propriedade
- **Overwrite**- Substitua os valores existentes quando os arquivos são alterados
- **Aggregate**- Combine novos valores com valores existentes (para propriedades de vários valores)

## Propriedades de gerenciamento

As propriedades de gerenciamento são propriedades de classificação que se aplicam a pastas em vez de arquivos. Você usa propriedades de gerenciamento para organizar e categorizar pastas na hierarquia do sistema de arquivos. Ao contrário das propriedades do arquivo que são atribuídas automaticamente por meio de regras de classificação, você define as propriedades de gerenciamento manualmente usando o [Conjunto - FSx FSRMMgmt Propriedade](#) comando.

Para classificar pastas, use a FolderUsage\_MS propriedade. Especifique os seguintes valores:

- User Files
- Group Share
- Application Files
- Backup and Archival

## Classificação em execução

Você pode executar a classificação de arquivos de três maneiras:

1. Classificação manual - Use [Começar- FSx FSRMClassification](#) para executar a classificação imediatamente. Essa abordagem é útil para testar novas regras ou realizar tarefas de classificação únicas.
2. Classificação programada - Use [Conjunto- FSx FSRMClassification](#) para configurar uma programação para classificação automática. Você pode programar a classificação para ser executada semanalmente ou mensalmente em horários específicos. A classificação programada é apropriada para a maioria dos ambientes de produção em que você deseja execuções de classificação regulares e previsíveis.
3. Classificação contínua - Use [Conjunto- FSx FSRMClassification](#) com o Continuous parâmetro para ativar a classificação em segundo plano que seja executada continuamente. A classificação contínua classifica automaticamente os arquivos novos e modificados logo após serem criados ou alterados. Essa abordagem fornece a maior up-to-date classificação, mas consome mais recursos do sistema.

Ao iniciar a classificação, você pode especificar um RunDuration para limitar o tempo de execução do processo. Se a classificação não for concluída dentro do tempo especificado, ela



será interrompida e retomada durante a próxima execução programada ou quando você a reiniciar manualmente.

Depois que a classificação for concluída, você poderá visualizar as propriedades de classificação atribuídas aos arquivos clicando com o botão direito do mouse em um arquivo no Explorador de Arquivos do Windows, selecionando Propriedades e escolhendo a guia Classificação. Essa guia exibe todas as propriedades de classificação e seus valores para o arquivo.

## Gerenciamento do processo de classificação

Você pode monitorar e controlar o processo de classificação com os seguintes comandos:

- [Obtenha- FSx FSRMClassification](#)- Verifique o status atual da classificação (RunningQueued,NotRunning, ouUnknown)
- [Pare- FSx FSRMClassification](#)- Interromper um trabalho de classificação em execução ou em fila
- [Espere... FSx FSRMClassification](#)- Pausa a execução do script até que a classificação seja concluída ou o tempo limite expire

Use esses comandos para coordenar a classificação com outras tarefas. Por exemplo, você pode esperar a conclusão da classificação antes de gerar um relatório de armazenamento que dependa das propriedades do arquivo classificado.

## Práticas recomendadas de classificação

Siga essas práticas recomendadas para garantir uma classificação de arquivos eficiente e eficaz.

### 1. Considerações sobre a performance

A classificação baseada em conteúdo consome muitos recursos porque o FSRM deve ler e verificar o conteúdo do arquivo.

- Teste primeiro as regras em um pequeno conjunto de dados — Antes de aplicar as regras de classificação em todo o sistema de arquivos, teste-as em uma amostra representativa de arquivos para verificar se funcionam conforme o esperado e estimar quanto tempo levará para a classificação.
- Limite o escopo da varredura de conteúdo - A classificação baseada em conteúdo consome muitos recursos porque exige a leitura do conteúdo do arquivo. Use o Namespace parâmetro para limitar as regras a pastas específicas em vez de escanear todo o sistema de arquivos.

- Use a classificação de pastas quando possível - o Classificador de pastas é muito mais rápido do que o Classificador de conteúdo porque não precisa ler o conteúdo do arquivo. Quando os arquivos puderem ser classificados com base em sua localização, use o Classificador de pastas em vez do Classificador de conteúdo.
- Programar a classificação fora do horário de pico - Execute a classificação programada durante períodos de baixa atividade do sistema para minimizar o impacto no desempenho do usuário. Evite executar a classificação durante janelas de backup ou outras tarefas de manutenção.
- Defina `RunDuration` limites apropriados - Use o `RunDuration` parâmetro para evitar que a classificação seja demorada demais e afete o desempenho do sistema. Se a classificação não for concluída dentro do limite de tempo, ela será retomada durante a próxima corrida programada.
- Monitore o desempenho da classificação - Use `Get-FSxFSRMClassification` para verificar o status da classificação e identificar se a classificação está demorando mais do que o esperado. A classificação de longa duração pode indicar que as regras precisam ser otimizadas ou que o sistema precisa de mais recursos.

## 2. Design de regras

- Use expressões regulares específicas - Ao usar `ContentRegularExpression`, escreva padrões que sejam tão específicos quanto possível para evitar correspondências falsas. Teste as expressões regulares minuciosamente antes de implantá-las na produção.
- Combine vários padrões de forma eficiente - Em vez de criar regras separadas para padrões semelhantes, combine-as em uma única regra com vários `ContentRegularExpression` valores `ContentString` ou. Isso reduz o número de vezes que o FSRM precisa escanear cada arquivo.
- Excluir pastas desnecessárias - Use o `ExcludeNamespace` parâmetro em `Set-FSxFSRMClassification` para excluir diretórios temporários e outros locais que não precisam de classificação.

## 3. Gestão de propriedades

- Planeje seu esquema de propriedade - Projete suas propriedades de classificação antes de criar regras. Considere quais propriedades você precisa para políticas de emissão de relatórios, conformidade e gerenciamento de arquivos.
- Definições de propriedade do documento - Use o campo `Descrição` para explicar o que cada propriedade significa e como ela deve ser usada. Isso ajuda outros administradores a entender seu esquema de classificação.

## 4. Manutenção contínua

- Analise os resultados da classificação regularmente — gere relatórios de armazenamento para verificar se a classificação está funcionando conforme o esperado e se os arquivos estão recebendo os valores corretos das propriedades.
- Atualize as regras conforme necessário — à medida que os requisitos de gerenciamento de dados da sua organização mudarem, atualize as regras de classificação para refletir novas políticas ou requisitos de conformidade.
- Limpe propriedades não utilizadas - Remova as definições e regras de propriedades que não são mais necessárias para manter sua configuração de classificação gerenciável.

## Comandos de gerenciamento de classificação

Você pode acessar quatro famílias de PowerShell comandos FSx remotos para gerenciar a classificação de arquivos:

1. Comandos de definição de propriedade - Crie e gerencie definições de propriedades de classificação que especificam os tipos de metadados que você pode atribuir aos arquivos.
2. Comandos de regras de classificação - Crie e gerencie regras de classificação automática que atribuem valores de propriedades com base no conteúdo ou na localização do arquivo.
3. Comandos de propriedades de gerenciamento - defina e recupere propriedades de classificação em pastas em vez de arquivos.
4. Comandos do processo de classificação - Inicie, interrompa, monitore e configure o processo de classificação.

## Lista de PowerShell comandos FSx remotos de classificação de arquivos

### Note

Todos os exemplos nesta página pressupõem que você tenha definido a `$FSxWindowsRemotePowerShellEndpoint` variável com o PowerShell endpoint remoto do Windows do seu sistema de arquivos. Você pode encontrar esse endpoint no FSx console da Amazon na página de detalhes do seu sistema de arquivos ou usando o AWS CLI `describe-file-systems` comando.

## Comandos de definição de propriedade

### Novo- FSx FSRMClassification PropertyDefinition

**New-FSxFSRMClassificationPropertyDefinition:** cria uma definição de propriedade de classificação que pode ser usada para classificar arquivos. As definições de propriedades definem os atributos que podem ser atribuídos aos arquivos por meio de regras de classificação.

#### Parâmetros:

- **Name (string):** obrigatório. Um nome para a definição da propriedade.
- **DisplayName (string):** opcional. Um nome de exibição para a definição da propriedade.
- **Description (string):** opcional. Uma descrição para a definição da propriedade.
- **Type (string):** obrigatório. O tipo da propriedade de classificação. Especifique os seguintes valores:
  - **OrderedList:** uma lista ordenada de valores possíveis
  - **MultiChoice:** Seleção de múltipla escolha a partir de valores possíveis
  - **SingleChoice:** Escolha única entre os valores possíveis
  - **String:** Cadeia de texto única
  - **MultiString:** Várias sequências de texto
  - **Integer:** Valor numérico
  - **YesNo:** valor booleano
  - **DateTime:** valor de data e hora
- **PossibleValueConfigurations (array):** opcional. Uma variedade de configurações para **OrderedList** **MultiChoice**, ou tipos de **SingleChoice** propriedades. Cada configuração tem as seguintes propriedades:
  - **Name (string):** O nome do valor (obrigatório)
  - **Description (string):** uma descrição do valor (opcional)
- **Parameters (array):** opcional. Uma matriz de strings em "name=value" formato para configuração adicional.

#### Exemplos:

##### 1. Crie uma lista de propriedades para dados de PII.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMClassificationPropertyDefinition -Name "ContainsPII" -Type OrderedList -
PossibleValueConfigurations @(
 @{ Name = "Yes" },
 @{ Name = "No" })
}
```

## 2. Crie uma propriedade de lista ordenada para Data Sensibility.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMClassificationPropertyDefinition -Name "DataSensitivity" -Type
 OrderedList -PossibleValueConfigurations @(
 @{ Name = "Public" },
 @{ Name = "Internal" },
 @{ Name = "Confidential" },
 @{ Name = "Restricted" }
)
}
```

## Obtenha- FSx FSRMClassification PropertyDefinition

**Get-FSxFSRMClassificationPropertyDefinition:** recupera uma ou mais definições de propriedades de classificação do seu sistema de arquivos.

### Parâmetros:

- **Name (array):** opcional. Uma matriz de nomes de definições de propriedades a serem recuperadas. Se você não especificar um nome, o comando retornará todas as definições de propriedades no sistema de arquivos.

### Exemplos:

#### 1. Recupere todas as definições de propriedades de classificação no sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMClassificationPropertyDefinition
}
```

## Conjunto- FSx FSRMClassification PropertyDefinition

Modifica as propriedades de uma definição de propriedade de classificação existente.

### Parâmetros

- **Name (array):** obrigatório. Uma matriz de nomes de propriedades para modificar.
- **DisplayName (string):** opcional. Um novo nome de exibição para a definição da propriedade.
- **Description (string):** opcional. Uma nova descrição para a definição da propriedade.
- **PossibleValueConfigurations (array):** opcional. Uma nova matriz de configurações para **OrderedList**, **MultiChoice**, ou **SingleChoice** propriedades. Cada configuração tem as seguintes propriedades:
  - **Name (string):** O nome do valor (obrigatório)
  - **Description (string):** uma descrição do valor (opcional)
- **Parameters (array):** opcional. Uma nova matriz de strings no formato "nome=valor".
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de definição de propriedade modificado.

### Exemplos:

1. Atualize os valores possíveis com descrições em uma definição de propriedade existente.

```
$values = [System.Collections.ArrayList]@()
$null = $values.Add(@{
 Name = "High"
 Description = "High Risk Content"
})
$null = $values.Add(@{
 Name = "Medium"
 Description = "Medium Risk Content"
})

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $values -ScriptBlock {
 param($values)
 Set-FSxFSRMClassificationPropertyDefinition -Name "RiskLevel" -
PossibleValueConfigurations $Using:values -PassThru
}
```

## Remover- FSx FSRMClassification PropertyDefinition

Remove uma ou mais definições de propriedades de classificação do seu sistema de arquivos. Somente definições de propriedades definidas localmente podem ser removidas.

### Parâmetros

- **Name (array):** obrigatório. Uma matriz de nomes de propriedades a serem removidos.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de definição de propriedade removido.

### Exemplos:

1. Remova uma única definição de propriedade.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMClassificationPropertyDefinition -Name "RiskLevel" -PassThru
}
```

## Comandos da regra de classificação

### Nova FSx FSRMClassification regra

Cria uma regra de classificação automática que atribui valores de propriedade aos arquivos com base em critérios especificados. Cada regra define um valor para uma única propriedade.

### Parâmetros

- **Name (string):** obrigatório. Um nome para a regra de classificação.
- **Description (string):** opcional. Uma descrição da regra de classificação.
- **Property (string):** obrigatório. O nome da propriedade de classificação a ser definida. Deve ser um nome de definição de propriedade existente.
- **PropertyValue (string):** opcional. O valor a ser atribuído à propriedade. Deve ser válido para o mecanismo de classificação especificado.
- **Namespace (array):** obrigatório. Uma matriz de caminhos ou tipos de pasta em que a regra se aplica.
- **Disabled (boolean):** opcional. Se definido como verdadeiro, cria a regra em um estado desativado.

- **ReevaluateProperty (string)**: opcional. Especifica quando reavaliar os arquivos. Especifique os seguintes valores:
  - **Never**: avalie somente arquivos sem valor de propriedade existente
  - **Overwrite**: reavale quando os arquivos são alterados e sobrescreva o valor existente
  - **Aggregate**: reavale quando os arquivos são alterados e combinados com o valor existente
- **Flags (array)**: opcional. Especifica comportamentos especiais para a regra. Especifique os seguintes valores:
  - **ClearAutomaticallyClassifiedProperty**
  - **ClearManuallyClassifiedProperty**
  - **Deprecated**
- **ContentRegularExpression (array)**: opcional. Uma matriz de expressões regulares para corresponder ao conteúdo do arquivo.
- **ContentString (array)**: opcional. Uma matriz de sequências de caracteres que não diferenciam maiúsculas de minúsculas para pesquisar no conteúdo do arquivo.
- **ClassificationMechanism (string)**: obrigatório. O mecanismo a ser usado para classificar arquivos. Especifique os seguintes valores:
  - **Content Classifier**: verifica o conteúdo do arquivo em busca de sequências de caracteres específicas ou padrões de expressão regular. Ao especificar o Classificador de conteúdo, você pode usar os ContentRegularExpression parâmetros ContentString ContentStringCaseSensitive, ou para definir o conteúdo a ser pesquisado.
  - **Folder Classifier**: classifica os arquivos com base na localização da pasta
- **Parameters (array)**: opcional. Uma matriz de "name=value" strings para configuração adicional.

## Exemplos:

### 1. Detecte números de previdência social usando uma expressão regular.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMCClassificationRule -Name "Detect_SSN" -Property "ContainsPII" -
 PropertyValue "Yes" -Namespace "share" -ClassificationMechanism "Content Classifier" -
 ContentRegularExpression "\b\d{3}-\d{2}-\d{4}\b"
}
```



## 2. Detecte números de cartão de crédito usando uma expressão regular.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMClassificationRule -Name "Detect_CreditCard" -Property "ContainsPII" -
Property "Yes" -Namespace "share" -ClassificationMechanism "Content Classifier" -
ContentRegularExpression "\b\d{4}[\s-]?\d{4}[\s-]?\d{4}[\s-]?\d{4}\b"
}
```

## 3. Classifique cada arquivo em uma pasta com uma propriedade de período de retenção de 7 anos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMClassificationRule -Name "Contracts_Records_7Year" -Property
"RetentionPeriod" -Property "7 years" -Namespace "share/Legal Documents" -
ClassificationMechanism "Folder Classifier"
}
```

## FSxFSRMClassificationRegra Get

Recupera uma ou mais regras de classificação do seu sistema de arquivos.

### Parâmetros

- **Name (array):** opcional. Uma matriz de nomes de regras de classificação a serem recuperadas. Se você não especificar um nome, o comando retornará todas as regras no sistema de arquivos.

### Exemplos:

#### 1. Recupere todas as regras de classificação no sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMClassificationRule
}
```

## Definir uma FSx FSRMClassification regra

Modifica as propriedades das regras de classificação existentes.

## Parâmetros

- **Name (array):** obrigatório. Uma matriz de nomes de regras de classificação a serem modificadas.
- **Description (string):** opcional. Uma nova descrição para a regra.
- **Property (string):** opcional. O nome da propriedade de classificação a ser definida.
- **PropertyValue (string):** opcional. Um novo valor a ser atribuído à propriedade.
- **Namespace (array):** opcional. Uma nova matriz de caminhos ou tipos de pasta em que a regra se aplica.
- **Disabled (boolean):** opcional. Se definido como verdadeiro, desativa a regra. Se definido como falso, ativa a regra.
- **ReevaluateProperty (string):** opcional. Altera quando reavaliar os arquivos. Especifique os seguintes valores:
  - **Never:** avalie somente arquivos sem valor de propriedade existente
  - **Overwrite:** reavale quando os arquivos são alterados e sobrescreva o valor existente
  - **Aggregate:** reavale quando os arquivos são alterados e combinados com o valor existente
- **Flags (array):** opcional. Novos comportamentos especiais para a regra. Especifique os seguintes valores:
  - **ClearAutomaticallyClassifiedProperty**
  - **ClearManuallyClassifiedProperty**
  - **Deprecated**
- **ContentRegularExpression (array):** opcional. Uma nova matriz de expressões regulares.
- **ContentString (array):** opcional. Uma nova matriz de sequências de pesquisa que não diferenciam maiúsculas de minúsculas.
- **ContentStringCaseSensitive (array):** opcional. Uma nova matriz de sequências de pesquisa com distinção entre maiúsculas e minúsculas.
- **ClassificationMechanism (string):** opcional. Um novo mecanismo de classificação a ser usado. Especifique os seguintes valores:
  - **Content Classifier:** verifica o conteúdo do arquivo em busca de sequências de caracteres específicas ou padrões de expressão regular. Ao especificar o Classificador de conteúdo, você pode usar os ContentRegularExpression parâmetros ContentString ContentStringCaseSensitive, ou para definir o conteúdo a ser pesquisado.
  - **Folder Classifier:** classifica os arquivos com base na localização da pasta

- **Parameters (array):** opcional. Uma nova matriz de cadeias de caracteres de "name=value" configuração.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de regra modificado.

### Exemplos:

1. Atualize as propriedades da regra e o namespace de uma regra de classificação existente.

```
$namespaces = @("share\finance", "share\accounting")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $namespaces -ScriptBlock {
 param($namespaces)
 Set-FSxFSRMClassificationRule -Name "Detect_CreditCard" -Description "Updated PII
detection" -Namespace $Using:namespaces -ReevaluateProperty "Overwrite"
}
```

### Remover - FSx FSRMClassification Regra

Remove uma ou mais regras de classificação do seu sistema de arquivos.

### Parâmetros

- **Name (array):** obrigatório. Uma matriz de nomes de regras de classificação a serem removidas.
- **PassThru (boolean):** opcional. Se definido como verdadeiro, retorna o objeto de regra removido.

### Exemplos:

1. Remova uma única regra de classificação.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMClassificationRule -Name "Find Confidential Files" -PassThru
}
```

## Comandos de propriedade de gerenciamento

### Obter uma FSx FSRMMgmt propriedade

Recupera as propriedades de gerenciamento das pastas especificadas. As propriedades de gerenciamento são propriedades de classificação que se aplicam às pastas e não aos arquivos.

#### Parâmetros

- **Namespace (string):** opcional. Um caminho para uma pasta.
- **Name (string):** opcional. O nome de uma propriedade de gerenciamento a ser recuperada. Se você não especificar um nome, o comando recuperará todas as propriedades de gerenciamento.
- **Recurse (boolean):** opcional. Se definido como verdadeiro, recupera as propriedades de gerenciamento de todas as pastas dentro do namespace. Requer o parâmetro Namespace.
- **Effective (boolean):** opcional. Se definido como verdadeiro, recupera a propriedade de gerenciamento da pasta mais próxima com o nome especificado. A pesquisa inclui o namespace especificado e sua hierarquia principal. Requer o parâmetro Name.

#### Exemplos:

1. Recupere todas as propriedades de gerenciamento no sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMMgmtProperty
}
```

2. Recupere as propriedades de gerenciamento de uma pasta específica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMMgmtProperty -Namespace "share\department"
}
```

### Remover- FSx FSRMMgmt Propriedade

Remove as propriedades de gerenciamento das pastas especificadas.

#### Parâmetros

- **Namespace (string):** opcional. Um caminho para uma pasta.

- **Name (string):** obrigatório. O nome da propriedade de gerenciamento a ser removida.
- **Recurse (boolean):** opcional. Se definido como verdadeiro, remove as propriedades de gerenciamento de todas as pastas dentro do namespace. Requer o parâmetro Namespace.

#### Exemplos:

1. Remova todas as instâncias de uma propriedade de gerenciamento.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMMgmtProperty -Name "FolderUsage_MS"
}
```

2. Remova uma propriedade de gerenciamento de uma pasta específica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMMgmtProperty -Name "FolderUsage_MS" -Namespace "share\department"
}
```

#### Conjunto - FSx FSRMMgmt Propriedade

Altera o valor de uma propriedade de gerenciamento para um namespace especificado. As propriedades de gerenciamento são propriedades de classificação que se aplicam às pastas e não têm o sinalizador Seguro definido.

#### Parâmetros

- **Namespace (string):** opcional. O caminho da pasta.
- **Name (string):** obrigatório. O nome da propriedade de gerenciamento a ser modificada. Deve ser uma propriedade de classificação existente que se aplique às pastas.
- **Value (string):** obrigatório. O novo valor a ser atribuído à propriedade de gerenciamento.

#### Exemplos:

1. Defina uma propriedade de uso da pasta.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
```

```
Set-FSxFSRMMgmtProperty -Namespace "share\department" -Name "FolderUsage_MS" -Value
"User Files"
}
```

## Comandos do processo de classificação

### Obtenha- FSx FSRMClassification

Recupera o status do processo de classificação de arquivos em execução. O status pode ser um dos valores a seguir:

- **Unknown:** O status da classificação não pode ser determinado
- **NotRunning:** Nenhuma classificação está em execução no momento
- **Queued:** A classificação está na fila para começar
- **Running:** A classificação está atualmente em andamento

### Parâmetros

Nenhum

### Exemplos:

#### 1. Recupere o status atual da classificação.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMClassification
}
```

### Começar- FSx FSRMClassification

Inicia o processo de classificação de arquivos, que aplica regras de classificação aos arquivos e gera um relatório de classificação.

### Parâmetros

- **Queue (boolean):** opcional. Se definido como verdadeiro, adiciona a tarefa de classificação a uma fila para ser executada nos próximos 5 minutos. Todas as tarefas enfileiradas durante esse período serão executadas juntas. Se definido como falso ou não especificado, a classificação começa imediatamente.

- **RunDuration (number):** opcional. Especifica quantas horas o processo de classificação deve ser executado antes de ser cancelado. Valores válidos: -1 a 2147483. Valores especiais:
  - -1: Executar até ser cancelado
  - 0: Executar até a conclusão
  - Se não for especificado, é executado até a conclusão.

Exemplos:

1. Comece a classificação sem limite de tempo.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Start-FSxFSRMClassification -RunDuration 0
}
```

Pare- FSx FSRMClassification

Interrompe qualquer tarefa de classificação em execução ou em fila no seu sistema de arquivos.

Parâmetros

Nenhum

Exemplos:

1. Interrompa uma classificação em execução.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Stop-FSxFSRMClassification
}
```

Espere... FSx FSRMClassification

Aguarda a conclusão do processo de classificação de arquivos. Use esse comando quando precisar executar ações que dependam do acabamento da classificação, como gerar relatórios com base em arquivos classificados.

## Parâmetros

- **Timeout (number)**: opcional. Especifica quanto tempo esperar, em segundos, para que a classificação seja concluída. Se o tempo limite expirar antes que a classificação termine, o comando retornará, mas a classificação continuará sendo executada em segundo plano. Valores válidos: -1 a 2147483. Valores especiais:
  - -1: Aguarde indefinidamente até que a classificação seja concluída (padrão)
  - 0: Verifique o status atual e retorne imediatamente sem esperar

## Exemplos:

1. Aguarde indefinidamente até que a classificação seja concluída.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Wait-FSxFSRMClassification
}
```

## Conjunto- FSx FSRMClassification

Modifica as definições de configuração para classificação de arquivos.

## Parâmetros

- **ExcludeNamespace (array)**: opcional. Uma matriz de pastas adicionais a serem excluídas da classificação.
- **ScheduleConfigurations (hashtable)**: opcional. Uma tabela de hash contendo a configuração do cronograma com as seguintes propriedades:
  - **Time (datetime)**: DateTime objeto que especifica quando executar a tarefa (obrigatório)
  - **RunDuration (number)**: Número de horas para executar a tarefa (opcional)
  - **Weekly (array)**: matriz de dias da semana (opcional)
  - **Monthly (array)**: matriz de dias do mês, use -1 para o último dia (opcional)
- **Continuous (boolean)**: opcional. Se definido como verdadeiro, habilita a classificação contínua em segundo plano.
- **PassThru (boolean)**: opcional. Se definido como verdadeiro, retorna o objeto de configuração de classificação modificado.



## Exemplos:

### 1. Permita a classificação contínua.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMClassification -Continuous $true
}
```

### 2. Defina um cronograma semanal para executar a classificação.

```
$schedule = @{
 Time = ("12:00am")
 Weekly = @('Monday', 'Wednesday', 'Friday')
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
 param($schedule)
 Set-FSxFSRMClassification -ScheduleConfigurations $schedule
}
```

### 3. Defina uma programação mensal com exclusões personalizadas.

```
$schedule = @{
 Time = ("12:00am")
 Monthly = @(1, 15, -1) # 1st, 15th, and last day
 RunDuration = 4
}
$excludeNamespaces = @("share\folder /s")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList @($schedule, $excludeNamespaces) -ScriptBlock {
 param($schedule, $excludeNamespaces)
 Set-FSxFSRMClassification -ScheduleConfigurations $schedule -ExcludeNamespace
$excludeNamespaces
}
```

## Relatórios de armazenamento

Os relatórios de armazenamento fornecem uma análise detalhada do uso do sistema de arquivos, ajudando você a entender como o armazenamento está sendo consumido, identificar arquivos que

podem ser arquivados ou excluídos e monitorar a conformidade com as políticas de gerenciamento de arquivos. Você pode gerar vários tipos de relatórios que analisam a propriedade do arquivo, tipos de arquivo, arquivos duplicados, arquivos grandes, triagem de arquivos e uso de cotas.

## Tipos de relatório

Você pode criar os seguintes tipos de relatório:

- DuplicateFiles

Identifica arquivos com conteúdo idêntico com base no tamanho do arquivo e na comparação de hash. Use esse relatório para encontrar arquivos redundantes que consomem espaço de armazenamento desnecessário. O relatório agrupa arquivos duplicados e mostra o espaço total que pode ser recuperado com a remoção de duplicatas.

- FilesByFileGroup

Agrupa arquivos por associação ao [grupo](#) de arquivos e mostra o consumo de armazenamento de cada grupo de arquivos. Use esse relatório para entender quais tipos de arquivos (documentos, mídia, executáveis etc.) consomem mais espaço de armazenamento.

- FilesByOwner

Agrupa arquivos por proprietário e mostra quanto armazenamento cada usuário ou grupo consome. Use esse relatório para identificar os usuários que estão consumindo mais espaço de armazenamento e para alocar custos ou cotas de armazenamento de forma adequada.

- FilesByProperty

Agrupa arquivos por valores de propriedade de classificação e mostra a contagem de arquivos e o consumo de armazenamento para cada valor de propriedade. Use esse relatório para analisar arquivos com base em sua classificação, como nível de sensibilidade de dados, departamento ou período de retenção. Este relatório exige que os arquivos tenham sido classificados usando [Regras de classificação](#).

- FileScreenAuditFiles

Lista as [Triagem de arquivos](#) violações em que os usuários tentaram salvar arquivos que foram bloqueados pelas triagens de arquivos ativas. Use esse relatório para monitorar a conformidade com as políticas de triagem de arquivos e identificar usuários que frequentemente tentam salvar tipos de arquivo não autorizados.

- FoldersByProperty

Agrupa pastas por valores de propriedade de gerenciamento e mostra o consumo de armazenamento para cada valor de propriedade. Use esse relatório para analisar o uso do armazenamento por finalidade da pasta, como arquivos de usuário, compartilhamentos de grupos ou arquivos de aplicativos.

- **LargeFiles**

Lista os arquivos que excedem um limite de tamanho especificado. Use esse relatório para identificar arquivos que consomem espaço de armazenamento significativo e podem ser candidatos para arquivamento, compactação ou exclusão.

- **LeastRecentlyAccessed**

Lista os arquivos que não foram acessados por um determinado número de dias. Use esse relatório para identificar arquivos inativos que podem ser arquivados ou movidos para níveis de armazenamento de menor custo.

- **MostRecentlyAccessed**

Lista os arquivos que foram acessados em um determinado número de dias.

- **QuotaUsage**

Mostra estatísticas de uso de cotas para pastas com [cotas configuradas](#). Use esse relatório para monitorar a conformidade da cota e identificar pastas que estão se aproximando de seus limites de cota.

## Formatos de relatório

Você pode gerar relatórios em vários formatos para se adequar a diferentes casos de uso:

- **DHTML**- Formato HTML dinâmico com recursos interativos, como classificação e filtragem.
- **HTML**- Formato HTML estático adequado para arquivamento ou envio por e-mail.
- **XML**- Formato de dados estruturados para processamento programático.
- **CSV**- Formato de valores separados por vírgula para importação em aplicativos de planilhas.
- **Text**- Formato de texto simples para visualização ou processamento simples.

Você pode especificar vários formatos para um único relatório.

## Relatórios interativos e programados

Você pode criar dois tipos de relatórios de armazenamento:

1. Relatórios interativos - Executados imediatamente quando criados e executados somente uma vez. Use relatórios interativos para análise ad-hoc ou solução de problemas. Os relatórios interativos não têm agendas e não podem ser modificados após a criação. Para executar outro relatório interativo, você deve criar um novo relatório com um nome diferente.
2. Relatórios agendados - Executados automaticamente de acordo com uma programação configurada. Use relatórios programados para monitoramento regular e relatórios de conformidade. Você pode programar relatórios para serem executados semanalmente ou mensalmente em horários específicos. Os relatórios agendados podem ser modificados para alterar sua configuração, e você também pode executá-los sob demanda usando o [Início - FSx FSRMStorage Relatório](#) comando sem esperar pelo horário agendado.

## Executando relatórios

Depois de criar um relatório agendado, você pode executá-lo de várias maneiras:

- Execução automática - Os relatórios programados são executados automaticamente no horário de agendamento configurado.
- Execução manual - Use [Início - FSx FSRMStorage Relatório](#) para executar um relatório programado sob demanda sem esperar pelo horário agendado.

Você pode monitorar a execução do relatório usando [Obter- FSx FSRMStorage Relatório](#) para verificar o status.

## Acessando relatórios de armazenamento

Depois que o FSRM gera relatórios de armazenamento, os arquivos de relatório são salvos em um local padrão em seu sistema de arquivos. Para acessar esses relatórios, você precisa mapear o compartilhamento administrativo de D\$ do seu sistema de arquivos.

Para acessar relatórios de armazenamento

1. Mapeie o compartilhamento administrativo D\$ usando o seguinte formato de caminho:

```
\\file-system-dns-name\D$
```

Por exemplo:

```
\\amznfsxaa11bb22.corp.example.com\D$
```

2. Navegue até a StorageReports pasta. Essa pasta contém subpastas organizadas por tipo de relatório e data de execução.

#### Note

O acesso ao compartilhamento administrativo do D\$ requer credenciais de administrador.

## Práticas recomendadas de relatórios de armazenamento

Siga estas práticas recomendadas para garantir relatórios de armazenamento eficientes e eficazes:

### Considerações sobre a performance

A geração de relatórios de armazenamento consome muitos recursos porque o FSRM deve verificar grandes quantidades de arquivos.

- Limitar o escopo do relatório - Use o Namespace parâmetro para limitar os relatórios a pastas específicas em vez de escanear todo o sistema de arquivos. A varredura de grandes estruturas de diretórios consome muitos recursos e pode levar horas para ser concluída.
- Agende relatórios fora do horário de pico - Execute relatórios programados durante períodos de baixa atividade do sistema, para minimizar o impacto no desempenho. Evite a execução de relatórios durante janelas de backup ou outras tarefas de manutenção.
- Defina limites razoáveis - Use parâmetros de limite para limitar a saída do relatório a dados acionáveis. Por exemplo, LargeFileMinimum defina um valor que identifique arquivos que valem a pena investigar, nem todos os arquivos com mais de 1 MB.
- RunDuration Limites de uso - defina o RunDuration parâmetro para evitar que os relatórios sejam executados por muito tempo e afetem o desempenho do sistema. Se um relatório não for concluído dentro do limite de tempo, ele será retomado durante a próxima execução programada.
- Monitore o desempenho do relatório - Use [Obter- FSx FSRMStorage Relatório](#) para verificar quanto tempo os relatórios demoram para serem concluídos. Se os relatórios sempre demorarem muito, considere restringir seu escopo ou executá-los com menos frequência.

## Design do relatório

- Use nomes descritivos - dê aos relatórios nomes claros e descritivos que indiquem o que eles analisam e quando são executados, como “Arquivos grandes semanais - Compartilhamento financeiro” ou “Arquivos duplicados mensais - Todos os compartilhamentos”.
- Combine análises relacionadas - Ao gerar vários tipos de relatórios para o mesmo namespace, crie um único relatório com vários ReportType valores em vez de relatórios separados. Isso é mais eficiente porque o FSRM só precisa examinar a estrutura de diretórios uma vez.
- Filtrar por padrões de arquivo - Use parâmetros de padrão de arquivo para focar os relatórios em tipos de arquivo específicos. Por exemplo, ao analisar arquivos grandes, você pode criar relatórios separados para arquivos de vídeo, arquivos de banco de dados e arquivos de arquivamento para entender melhor os padrões de consumo de armazenamento.
- Aproveite as propriedades de classificação - Use FilesByProperty relatórios para analisar arquivos com base em sua classificação. Isso fornece insights mais significativos.

## Gerenciamento de relatórios

- Analise os relatórios regularmente - Agende um horário para analisar os resultados do relatório e tomar medidas sobre as descobertas. Os relatórios só são valiosos se você os usar para tomar decisões de gerenciamento de armazenamento.
- Arquive relatórios antigos - os arquivos de relatório se acumulam com o tempo e consomem espaço de armazenamento. Estabeleça uma política de retenção para arquivos de relatórios e exclua ou archive relatórios antigos que não são mais necessários.
- Teste os relatórios antes do agendamento - Crie relatórios interativos para testar as configurações dos relatórios e verificar se eles produzem os resultados esperados antes de criar versões programadas.

## Comandos de gerenciamento de relatórios de armazenamento

Você pode acessar duas famílias de PowerShell comandos FSx remotos para gerenciar relatórios de armazenamento:

1. Comandos de definição de relatório - Crie, recupere, modifique e remova configurações de relatórios de armazenamento que especificam quais dados analisar, quando executar relatórios e quais formatos gerar.

2. Comandos de execução de relatórios — inicie, interrompa, monitore e aguarde a geração do relatório de armazenamento. Use esses comandos para executar relatórios sob demanda ou gerenciar trabalhos de relatórios de longa duração.

## Lista de PowerShell comandos FSx remotos do Storage Report

### Note

Todos os exemplos nesta página pressupõem que você tenha definido a `$FSxWindowsRemotePowerShellEndpoint` variável com o PowerShell endpoint remoto do Windows do seu sistema de arquivos. Você pode encontrar esse endpoint no FSx console da Amazon na página de detalhes do seu sistema de arquivos ou usando o AWS CLI `describe-file-systems` comando.

## Comandos de definição de relatório

### Novo - FSx FSRMStorage Relatório

Novo - FSx FSRMStorage Relatório: cria um relatório de armazenamento que analisa diretórios especificados para gerar um ou mais tipos de relatório.

#### Parâmetros:

- **Name (string):** obrigatório. Um nome para o relatório de armazenamento.
- **Namespace (array):** obrigatório. Uma matriz de caminhos ou tipos de pastas para analisar. Você pode especificar caminhos em vários formatos:
  - Caminho da pasta
  - [Classificação de pastas](#). Por exemplo, `[FolderUsage_ms="Arquivos do usuário "]`
- **ReportType (array):** obrigatório. Uma matriz de tipos de relatórios a serem gerados. Especifique os seguintes valores:
  - **DuplicateFiles:** identifica arquivos duplicados com base no tamanho e no conteúdo do arquivo
  - **FilesByFileGroup:** Agrupa arquivos por associação ao grupo de arquivos
  - **FilesByOwner:** Agrupa arquivos por proprietário
  - **FilesByProperty:** agrupa arquivos por propriedade de classificação
  - **FileScreenAuditFiles:** Lista as violações da triagem de arquivos

- **FoldersByProperty**: agrupa pastas por propriedade de gerenciamento
- **LargeFiles**: lista arquivos acima de um limite de tamanho especificado
- **LeastRecentlyAccessed**: lista arquivos que não foram acessados recentemente
- **MostRecentlyAccessed**: lista os arquivos que foram acessados recentemente
- **QuotaUsage**: mostra estatísticas de uso da cota
- **ReportFormat (array)**: opcional. Uma variedade de formatos de saída. Especifique os seguintes valores:
  - **DHTML**: Formato HTML dinâmico
  - **HTML**: formato HTML estático
  - **XML**: formato XML
  - **CSV**: formato de valores separados por vírgula
  - **Text**: Formato de texto sem formatação
- **Interactive (boolean)**: opcional. Se definido como verdadeiro, gera um relatório interativo. Os relatórios interativos não podem ser modificados após a criação.
- **ScheduleConfigurations (hashtable)**- Obrigatório, a menos que o relatório seja interativo. Uma tabela de hash contendo a configuração do cronograma com as seguintes propriedades:
  - **Time (datetime)**: DateTime objeto que especifica quando executar a tarefa (obrigatório)
  - **RunDuration (number)**: Número de horas para executar a tarefa (opcional)
  - **Weekly (array)**: matriz de dias da semana (opcional)
  - **Monthly (array)**: matriz de dias do mês, use -1 para o último dia (opcional)

#### Parâmetros específicos do relatório:

- **FileScreenAuditDaysSince (number)**: opcional. Para FileScreenAuditFiles relatórios, especifica há quantos dias devem ser incluídos os eventos de auditoria.
- **FileScreenAuditUser (array)**: opcional. Para FileScreenAuditFiles relatórios, especifica uma matriz de contas de usuário a serem incluídas no relatório. Somente violações de triagem de arquivos cometidas por esses usuários serão incluídas.
- **FileGroupIncluded (array)**: opcional. Para FilesByFileGroup relatórios, especifica quais grupos de arquivos incluir.
- **FileOwnerFilePattern (string)**: opcional. Para FilesByOwner relatórios, especifica um padrão de arquivo para filtrar os resultados.



- **PropertyName (string)**: opcional. Para **FilesByProperty** relatórios, especifica a propriedade de classificação pela qual agrupar.
- **FolderPropertyName (string)**: opcional. Para **FoldersByProperty** relatórios, especifica a propriedade da pasta pela qual agrupar.
- **PropertyFilePattern (string)**: opcional. Para **FilesByProperty** e **FoldersByProperty**, especifica um padrão de arquivo para filtrar os resultados.
- **LargeFileMinimum (number)**: opcional. Para **LargeFiles** relatórios, especifica o tamanho mínimo do arquivo em bytes.
- **LargeFilePattern (string)**: opcional. Para **LargeFiles** relatórios, especifica um padrão de arquivo para filtrar os resultados.
- **LeastAccessedMinimum (number)**: opcional. Para **LeastRecentlyAccessed** relatórios, especifica o número mínimo de dias desde o último acesso.
- **LeastAccessedFilePattern (string)**: opcional. Para **LeastRecentlyAccessed** relatórios, especifica um padrão de arquivo para filtrar os resultados.
- **MostAccessedMaximum (number)**: opcional. Para **MostRecentlyAccessed** relatórios, especifica o número máximo de dias desde o último acesso.
- **MostAccessedFilePattern (string)**: opcional. Para **MostRecentlyAccessed** relatórios, especifica um padrão de arquivo para filtrar os resultados.
- **QuotaMinimumUsage (number)**: opcional. Para **QuotaUsage** relatórios, especifica a porcentagem mínima de uso da cota a ser incluída.

## Exemplos:

### 1. Crie um relatório mensal de arquivos grandes.

```
$schedule = @{
 Time = ("3:00 AM")
 Monthly = @(1) # Run on first day
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
 param($schedule)
 New-FSxFSRMStorageReport -Name "Monthly Large Files" -Namespace "share
\data" -ReportType "LargeFiles" -LargeFileMinimum 100MB -ReportFormat "HTML" -
ScheduleConfigurations $schedule
```

```
}
```

## 2. Crie um relatório semanal de arquivos duplicados com vários namespaces e formatos.

```
$schedule = @{
 Time = ("12:00 AM")
 Weekly = @('Sunday')
 RunDuration = 4
}

$namespaces = @("share\docs", "[FolderUsage_MS=User Files]")
$reportFormats = @("HTML", "CSV")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($schedule, $namespaces, $reportFormats) -ScriptBlock {
 param($schedule, $namespaces, $reportFormats)
 New-FSxFSRMStorageReport -Name "Weekly Duplicates" -Namespace $namespaces -
 ReportType "DuplicateFiles" -ReportFormat $reportFormats -ScheduleConfigurations
 $schedule
}
```

## 3. Crie um relatório interativo que seja executado imediatamente.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMStorageReport -Name "Find large files" -Namespace "share" -Interactive
 $true -ReportType "QuotaUsage"
}
```

## Obter- FSx FSRMStorage Relatório

Get- FSx FSRMStorage Report: recupera um ou mais relatórios de armazenamento do seu sistema de arquivos. Retorna detalhes sobre configurações e status do relatório.

Parâmetros:

- Name (array): opcional. Uma matriz de nomes de relatórios a serem recuperados. Se você não especificar um nome, o comando retornará todos os relatórios de armazenamento no sistema de arquivos.

Exemplos:

### 1. Recupere todos os relatórios de armazenamento no sistema de arquivos.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMStorageReport
}
```

## Remover - FSx FSRMStorage Denunciar

Remover - FSx FSRMStorage Relatório: remove um ou mais relatórios de armazenamento do seu sistema de arquivos. Você não pode remover relatórios que estão sendo executados no momento.

### Parâmetros:

- Name (array): obrigatório. Uma matriz de nomes de relatórios a serem removidos.
- PassThru (boolean): opcional. Se definido como verdadeiro, retorna o objeto de relatório removido.

### Exemplos:

#### 1. Remova um único relatório de armazenamento.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Remove-FSxFSRMStorageReport -Name "Monthly Report" -PassThru
}
```

## Conjunto - FSx FSRMStorage Relatório

### Parâmetros

- Name (array): obrigatório. Uma matriz de nomes de relatórios a serem modificados.
- Namespace (array): opcional. Uma matriz de caminhos ou tipos de pastas para analisar. Você pode especificar caminhos em vários formatos:
  - Caminho da pasta
  - [Classificação de pastas](#). Por exemplo, [FolderUsage\_ms="Arquivos do usuário"]
- ReportType (array): opcional. Uma matriz de tipos de relatórios a serem gerados. Especifique os seguintes valores:
  - DuplicateFiles: identifica arquivos duplicados com base no tamanho e no conteúdo do arquivo

- `FilesByFileGroup`: Agrupa arquivos por associação ao grupo de arquivos
- `FilesByOwner`: Agrupa arquivos por proprietário
- `FilesByProperty`: agrupa arquivos por propriedade de classificação
- `FileScreenAuditFiles`: Lista as violações da triagem de arquivos
- `FoldersByProperty`: agrupa pastas por propriedade de gerenciamento
- `LargeFiles`: lista arquivos acima de um limite de tamanho especificado
- `LeastRecentlyAccessed`: lista arquivos que não foram acessados recentemente
- `MostRecentlyAccessed`: lista os arquivos que foram acessados recentemente
- `QuotaUsage`: mostra estatísticas de uso da cota
- `ReportFormat` (array): opcional. Uma variedade de formatos de saída. Especifique os seguintes valores:
  - `DHTML`: Formato HTML dinâmico
  - `HTML`: formato HTML estático
  - `XML`: formato XML
  - `CSV`: formato de valores separados por vírgula
  - `Text`: Formato de texto sem formatação
- `ScheduleConfigurations` (hashtable)- Obrigatório, a menos que o relatório seja interativo. Uma tabela de hash contendo a configuração do cronograma com as seguintes propriedades:
  - `Time` (datetime): DateTime objeto que especifica quando executar a tarefa (obrigatório)
  - `RunDuration` (number): Número de horas para executar a tarefa (opcional)
  - `Weekly` (array): matriz de dias da semana (opcional)
  - `Monthly` (array): matriz de dias do mês, use -1 para o último dia (opcional)
- `PassThru` (boolean): opcional. Se definido como verdadeiro, retorna o objeto de relatório modificado.

### Parâmetros específicos do relatório

- `FileScreenAuditDaysSince` (number): opcional. Para `FileScreenAuditFiles` relatórios, especifica há quantos dias devem ser incluídos os eventos de auditoria.
- `FileScreenAuditUser` (array): opcional. Para `FileScreenAuditFiles` relatórios, especifica uma matriz de contas de usuário a serem incluídas no relatório. Somente violações de triagem de arquivos cometidas por esses usuários serão incluídas.

- **FileGroupIncluded** (array): opcional. Para **FilesByFileGroup** relatórios, especifica quais grupos de arquivos incluir.
- **FileOwnerFilePattern** (string): opcional. Para **FilesByOwner** relatórios, especifica um padrão de arquivo para filtrar os resultados.
- **PropertyName** (string): opcional. Para **FilesByProperty** relatórios, especifica a propriedade de classificação pela qual agrupar.
- **FolderPropertyName** (string): opcional. Para **FoldersByProperty** relatórios, especifica a propriedade da pasta pela qual agrupar.
- **PropertyFilePattern** (string): opcional. Para **FilesByProperty** e **FoldersByProperty**, especifica um padrão de arquivo para filtrar os resultados.
- **LargeFileMinimum** (number): opcional. Para **LargeFiles** relatórios, especifica o tamanho mínimo do arquivo em bytes.
- **LargeFilePattern** (string): opcional. Para **LargeFiles** relatórios, especifica um padrão de arquivo para filtrar os resultados.
- **LeastAccessedMinimum** (number): opcional. Para **LeastRecentlyAccessed** relatórios, especifica o número mínimo de dias desde o último acesso.
- **LeastAccessedFilePattern** (string): opcional. Para **LeastRecentlyAccessed** relatórios, especifica um padrão de arquivo para filtrar os resultados.
- **MostAccessedMaximum** (number): opcional. Para **MostRecentlyAccessed** relatórios, especifica o número máximo de dias desde o último acesso.
- **MostAccessedFilePattern** (string): opcional. Para **MostRecentlyAccessed** relatórios, especifica um padrão de arquivo para filtrar os resultados.
- **QuotaMinimumUsage** (number): opcional. Para **QuotaUsage** relatórios, especifica a porcentagem mínima de uso da cota a ser incluída.

## Exemplos:

1. Atualize o cronograma e o formato de um relatório existente.

```
$schedule = @{
 Time = ("3:00 AM")
 Monthly = @(1)
}
$reportFormats = @("HTML", "CSV")
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList @($schedule, $reportFormats) -ScriptBlock {
 param($schedule, $reportFormats)
 Set-FSxFSRMStorageReport -Name "Monthly Report" -ScheduleConfigurations $schedule -
ReportFormat $reportFormats -PassThru
}
```

## Comandos de execução de relatórios

### Início - FSx FSRMStorage Relatório

#### Parâmetros

- **Name (array):** obrigatório. Uma matriz de nomes de relatórios para começar.
- **Queue (boolean):** opcional. Se definido como verdadeiro, adiciona o relatório a uma fila para ser executado nos próximos 5 minutos. Todos os relatórios colocados na fila durante esse período serão executados juntos. Se definido como falso ou não especificado, o relatório será iniciado imediatamente.
- **RunDuration (number):** opcional. Especifica quantas horas o relatório deve ser executado antes de ser cancelado. Valores válidos: -1 a 2147483. Valores especiais:
  - 0: Executar até a conclusão
  - -1: Executar até ser cancelado

Se não for especificado, é executado até a conclusão.

## Exemplos

### 1. Inicie um relatório de armazenamento imediatamente.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Start-FSxFSRMStorageReport -Name "Monthly Report"
}
```

### 2. Coloque na fila um relatório de armazenamento com um limite de duração.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
```

```
Start-FSxFSRMStorageReport -Name "Quarterly Report" -Queue: $true -RunDuration 4
}
```

## Parar - FSx FSRMStorage Denunciar

### Parâmetros

- **Name (array):** obrigatório. Uma matriz de nomes de relatórios a serem interrompidos.

### Exemplos:

#### 1. Interrompa um único relatório de armazenamento.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Stop-FSxFSRMStorageReport -Name "Monthly Report"
}
```

## Aguarde - FSx FSRMStorage Denuncie

### Parâmetros

- **Name (array):** obrigatório. Uma variedade de nomes de relatórios a serem aguardados.
- **Timeout (number):** opcional. Especifica quanto tempo esperar, em segundos, para que os relatórios sejam concluídos. Se o tempo limite expirar antes da conclusão dos relatórios, o comando retornará, mas a geração do relatório continuará sendo executada em segundo plano. Valores válidos: -1 a 2147483. Valores especiais:
  - -1: aguarde indefinidamente até que os relatórios sejam concluídos (padrão)
  - 0: Verifique o status atual e retorne imediatamente sem esperar

### Exemplos:

#### 1. Aguarde indefinidamente a conclusão de um relatório de armazenamento.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Wait-FSxFSRMStorageReport -Name "Monthly Report"
}
```

## Tarefas de gerenciamento de arquivos

O Amazon FSx para Windows File Server não oferece suporte às tarefas de gerenciamento de arquivos do FSRM. No entanto, você pode obter casos de uso comuns, como políticas de arquivamento e retenção de dados, usando PowerShell comandos nativos de máquinas clientes que têm acesso de rede ao seu sistema de arquivos.

Por exemplo, você pode usar PowerShell scripts em máquinas clientes para:

- Mova ou archive arquivos com base na idade ou na hora do último acesso
- Excluir arquivos classificados que excedam um período de retenção
- Copiar arquivos para armazenamento de arquivos com base nas propriedades de classificação

Você pode acessar as propriedades dos arquivos usando o `Get-FsrmClassification` comando e realizar ações com base nos valores.

Para acessar as propriedades de classificação do FSRM ou outros metadados do FSRM a partir de PowerShell scripts do lado do cliente, a máquina cliente também deve ter o FSRM instalado.

## Configurações do FSRM

As configurações do FSRM fornecem uma configuração em todo o sistema que permite que você personalize o comportamento e simplifique o gerenciamento de recursos. Use essas configurações para controlar como o FSRM opera em seu sistema de arquivos e para definir valores padrão que simplificam a criação e a configuração de recursos, como relatórios de armazenamento e triagem de arquivos.

### Categorias de configurações

As configurações do FSRM são organizadas em três categorias:

#### Auditoria de tela de arquivos

A auditoria de filtragem de arquivos registra quando os usuários tentam salvar arquivos que estão bloqueados pela triagem ativa de arquivos. Essas informações são essenciais para monitorar a conformidade com as políticas de triagem de arquivos e identificar usuários que frequentemente tentam salvar tipos de arquivos não autorizados.

- `ReportFileScreenAuditEnable`- Essa configuração controla se o FSRM registra violações de triagem de arquivos. Se desativado, o FSRM não registra violações da triagem de arquivos



e `FileScreenAuditFiles` os relatórios não terão dados para exibir. Você deve habilitar essa configuração para usar relatórios de auditoria de triagem de arquivos.

- `ReportFileScreenAuditDaysSince`- Essa configuração fornece o intervalo de tempo padrão para relatórios de auditoria de tela de arquivos. Quando você cria um `FileScreenAuditFiles` relatório sem especificar a distância a ser examinada, o FSRM usa esse valor. Definir um padrão apropriado (como 30 dias) garante que os relatórios se concentrem nas violações recentes sem incluir dados históricos excessivos.
- `ReportFileScreenAuditUser`- Essa configuração fornece a lista padrão de usuários a serem incluídos nos relatórios de auditoria da tela de arquivos. Quando você cria um `FileScreenAuditFiles` relatório sem especificar quais usuários incluir, o FSRM usa essa lista. Se estiverem vazios, os relatórios incluirão todos os usuários por padrão. Você pode usar essa configuração para concentrar os relatórios em grupos de usuários ou departamentos específicos.

### Filtros de relatório padrão

As configurações padrão do filtro de relatório fornecem valores que são usados quando você cria relatórios de armazenamento sem especificar determinados parâmetros. Esses padrões simplificam a criação de relatórios e garantem a consistência em relatórios semelhantes.

Cada tipo de relatório tem configurações padrão associadas:

- Relatórios de arquivos grandes - `ReportLargeFileMinimum` define o tamanho mínimo padrão do arquivo e `ReportLargeFilePattern` define o filtro padrão de arquivo.
- Relatórios de arquivos menos acessados - `ReportLeastAccessedMinimum` define o número padrão de dias desde o último acesso e `ReportLeastAccessedFilePattern` define o filtro padrão de arquivo.
- Relatórios de arquivos mais acessados - `ReportMostAccessedMaximum` define o número máximo padrão de dias desde o último acesso e `ReportMostAccessedFilePattern` define o filtro padrão de arquivo.
- Arquivos por relatórios do proprietário - `ReportFileOwnerFilePattern` define o filtro padrão de arquivo padrão e `ReportFileOwnerUser` define a lista padrão de usuários a serem incluídos.
- Arquivos por relatórios de propriedades - `ReportPropertyName` define a propriedade de classificação padrão a ser analisada e `ReportPropertyFilePattern` define o filtro padrão de arquivo padrão.
- Relatórios de arquivos por grupo de arquivos - `ReportFileGroupIncluded` define a lista padrão de grupos de arquivos a serem incluídos.

- **Relatórios de uso da cota** - `ReportQuotaMinimumUsage` define a porcentagem mínima padrão de uso da cota.

Ao criar um relatório, você pode substituir qualquer um desses padrões especificando o parâmetro explicitamente na configuração do relatório. Os padrões globais só se aplicam quando você não especifica um valor.

## Limites de relatório

As configurações de limite de relatórios controlam o número máximo de itens a serem incluídos nos relatórios de armazenamento. Esses limites têm dois propósitos:

1. **Gerenciamento de desempenho** - Limitar o número de itens nos relatórios evita que os relatórios demorem muito para gerar ou consumam recursos excessivos do sistema. Grandes relatórios que analisam milhões de arquivos podem levar horas para serem concluídos e afetar o desempenho do sistema.
2. **Usabilidade do relatório** - Relatórios com milhares de entradas são difíceis de revisar e analisar. Os limites dos relatórios garantem que os relatórios permaneçam focados nos dados mais relevantes.

Você pode configurar um controle granular sobre os limites do relatório:

- **Limites gerais** - `ReportLimitMaxFile` limita o número total de arquivos em qualquer relatório, independentemente do tipo.
- **Per-report-type limites** - Configurações como `ReportLimitMaxFileGroup`, `ReportLimitMaxOwner`, e `ReportLimitMaxPropertyValue` limitam o número de grupos, proprietários ou valores de propriedades a serem incluídos em tipos de relatórios específicos.
- **Limites por grupo** - Configurações como `ReportLimitMaxFilesPerFileGroup`, `ReportLimitMaxFilesPerOwner`, e `ReportLimitMaxFilesPerPropertyValue` limitam quantos arquivos serão exibidos em cada grupo no relatório.

Quando um relatório atinge um limite, o FSRM inclui os itens que consomem mais espaço de armazenamento ou são mais relevantes para o tipo de relatório e indica no relatório que o limite foi atingido.

## Comandos de configurações do FSRM

Você pode acessar comandos para recuperar e modificar as configurações globais. Use esses comandos para configurar o comportamento do FSRM em todo o sistema.

Lista de comandos remotos de configurações FSx do FSRM PowerShell

### Note

Todos os exemplos nesta página pressupõem que você tenha definido a `$FSxWindowsRemotePowerShellEndpoint` variável com o PowerShell endpoint remoto do Windows do seu sistema de arquivos. Você pode encontrar esse endpoint no FSx console da Amazon na página de detalhes do seu sistema de arquivos ou usando o AWS CLI `describe-file-systems` comando.

Obtenha- FSx FSRMSetting

`Get-FSxFSRMSetting`: recupera as configurações atuais do Gerenciador de Recursos do Servidor de Arquivos em seu sistema de arquivos. Retorna somente as configurações que podem ser modificadas usando `Set-FSxFSRMSetting`.

Parâmetros:

Nenhum

Exemplos:

1. Recupere todas as configurações atuais do FSRM.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMSetting
}
```

Conjunto- FSx FSRMSetting

`Set-FSxFSRMSetting`: modifica as configurações globais do Gerenciador de Recursos do Servidor de Arquivos em seu sistema de arquivos. Essas configurações fornecem valores padrão para relatórios de armazenamento e controlam o comportamento do FSRM.

## Parâmetros:

### Configurações de auditoria da tela de arquivos:

- `ReportFileScreenAuditEnable` (boolean): opcional. Controla se os eventos de auditoria de triagem de arquivos estão incluídos nos relatórios do FSRM.
- `ReportFileScreenAuditDaysSince` (number): opcional. O número padrão de dias para verificar as violações da triagem de arquivos ao gerar `FileScreenAuditFiles` relatórios.
- `ReportFileScreenAuditUser` (array): opcional. Uma matriz da lista padrão de contas de usuário a serem incluídas nos `FileScreenAuditFiles` relatórios.

### Configurações padrão do filtro de relatório:

- `ReportFileGroupIncluded` (array): opcional. Uma matriz de nomes de grupos de arquivos para incluir nos relatórios por padrão.
- `ReportFileOwnerFilePattern` (string): opcional. O padrão de arquivo padrão para arquivos de relatórios do proprietário. Suporta curingas (\*e?).
- `ReportFileOwnerUser` (array): opcional. Uma matriz de usuários no formato Domínio\Usuário para arquivos por relatórios do proprietário.
- `ReportLargeFileMinimum` (number): opcional. O tamanho mínimo padrão do arquivo em bytes para relatórios de arquivos grandes.
- `ReportLargeFilePattern` (string): opcional. O padrão de arquivo padrão para relatórios de arquivos grandes. Suporta curingas (\*e?).
- `ReportLeastAccessedFilePattern` (string): opcional. O padrão de arquivo padrão para relatórios de arquivos menos acessados. Suporta curingas (\*e?).
- `ReportLeastAccessedMinimum` (number): opcional. O número mínimo padrão de dias desde o último acesso para relatórios de arquivos menos acessados.
- `ReportMostAccessedFilePattern` (string): opcional. O padrão de arquivo padrão para os relatórios de arquivos mais acessados. Suporta curingas (\*e?).
- `ReportMostAccessedMaximum` (number): opcional. O número máximo padrão de dias desde o último acesso para os relatórios de arquivos mais acessados.
- `ReportPropertyFilePattern` (string): opcional. O padrão de arquivo padrão para relatórios de propriedades. Suporta curingas (\*e?).
- `ReportPropertyName` (string): opcional. O nome padrão da propriedade para relatórios de propriedades.

- `ReportQuotaMinimumUsage (number)`: opcional. A porcentagem mínima padrão de uso da cota para relatórios de uso da cota.

#### Configurações de limite de relatórios:

- `ReportLimitMaxDuplicateGroup (number)`: opcional. O número máximo de grupos de arquivos duplicados a serem incluídos nos relatórios de arquivos duplicados.
- `ReportLimitMaxFile (number)`: opcional. O número máximo de arquivos a serem incluídos nos relatórios de armazenamento.
- `ReportLimitMaxFileGroup (number)`: opcional. O número máximo de grupos de arquivos a serem incluídos nos relatórios.
- `ReportLimitMaxFileScreenEvent (number)`: opcional. O número máximo de eventos de triagem de arquivos a serem incluídos nos relatórios de auditoria de triagem de arquivos.
- `ReportLimitMaxFilesPerDuplicateGroup (number)`: opcional. O número máximo de arquivos por grupo duplicado em relatórios de arquivos duplicados.
- `ReportLimitMaxFilesPerFileGroup (number)`: opcional. O número máximo de arquivos por grupo de arquivos nos relatórios de arquivos por grupo de arquivos.
- `ReportLimitMaxFilesPerOwner (number)`: opcional. O número máximo de arquivos por proprietário nos relatórios de arquivos por proprietário.
- `ReportLimitMaxFilesPerPropertyValue (number)`: opcional. O número máximo de arquivos por valor de propriedade em arquivos por relatórios de propriedade.
- `ReportLimitMaxOwner (number)`: opcional. O número máximo de proprietários a serem incluídos nos arquivos por relatórios do proprietário.
- `ReportLimitMaxPropertyValue (number)`: opcional. O número máximo de valores de propriedades a serem incluídos nos arquivos por meio de relatórios de propriedades.
- `ReportLimitMaxQuota (number)`: opcional. O número máximo de cotas a serem incluídas nos relatórios de uso de cotas.

#### Outras configurações:

- `PassThru (boolean)`: opcional. Se definido como verdadeiro, retorna o objeto de configurações modificado.

#### Exemplos:

## 1. Configure a auditoria de triagem de arquivos padrão com um histórico de 30 dias.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMSetting -ReportFileScreenAuditDaysSince 30 -PassThru
}
```

## 2. Defina as configurações padrão do relatório de arquivos grandes.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMSetting -ReportLargeFileMinimum 100MB -ReportLargeFilePattern "*.iso"
 -PassThru
}
```

# Registros de eventos

Quando você ativa o FSRM em seu sistema de arquivos, o File Server AWS FSx para Windows gera registros de eventos para atividades de gerenciamento de arquivos e os envia para o destino que você configurou (AWS CloudWatch Logs ou AWS Kinesis Data Firehose). Esses registros ajudam você a monitorar as operações do FSRM, solucionar problemas e manter trilhas de auditoria das atividades de gerenciamento de arquivos.

## Quais registros do FSRM

Quando você habilita o FSRM em seu sistema de arquivos, o File Server AWS FSx para Windows registra eventos e os envia para o destino configurado. Os seguintes eventos serão registrados:

- Violações de triagem de arquivos - Quando os usuários tentam salvar arquivos que são monitorados por telas de arquivos que têm ações de notificação de eventos
- Notificações de limite de cota - Quando o uso da cota atinge limites configurados que têm ações de notificação de eventos
- Eventos de serviço do FSRM — confirmação das configurações de notificação, erros de serviço e falhas operacionais

## Acessando registros do FSRM

O local em que você acessa os registros do FSRM depende do destino que você configurou ao habilitar o FSRM:

### CloudWatch Registros

Visualize os registros no console de CloudWatch registros navegando até o grupo de registros que você especificou. Você pode pesquisar, filtrar e analisar registros usando o CloudWatch Logs Insights e configurar CloudWatch alarmes para notificá-lo sobre eventos específicos.

### Kinesis Data Firehose

Os registros são entregues ao destino configurado em seu stream de distribuição do Kinesis Data Firehose, como Amazon S3 AWS, Redshift ou Service. AWS OpenSearch Você pode processar e analisar registros usando as ferramentas e os serviços integrados ao seu fluxo de entrega.

## Casos de uso comuns

Este tópico fornece step-by-step exemplos de tarefas comuns do Gerenciador de Recursos do Servidor de Arquivos. Esses exemplos demonstram como usar e implementar os recursos do FSRM para resolver os desafios típicos de gerenciamento de arquivos.

### Note

Todos os exemplos nesta página pressupõem que você tenha definido a `$FSxWindowsRemotePowerShellEndpoint` variável com o PowerShell endpoint remoto do Windows do seu sistema de arquivos. Você pode encontrar esse endpoint no FSx console da Amazon na página de detalhes do seu sistema de arquivos ou usando o AWS CLI `describe-file-systems` comando.

## Definindo uma cota fixa em uma pasta

Este exemplo mostra como criar uma cota fixa que impede que os usuários armazenem mais de 10 GB em uma pasta de “departamento”.

Para definir uma cota em uma pasta:

1. Crie uma cota fixa com um limite de 10 GB:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMQuota -Folder "share\department" -Size 10GB -Description "10 GB hard
limit for department folder"
}
```

2. (Opcional) Modifique a cota para adicionar uma notificação de limite com 85% de uso:

```
$thresholds = [System.Collections.ArrayList]@()
$threshold = @{
 ThresholdPercentage = 85
 Action = @(
 @{
 ActionType = "Event"
 EventType = "Warning"
 MessageBody = "Department folder has reached 85% of quota limit"
 }
)
}

>null = $thresholds.Add($threshold)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList ($thresholds) -ScriptBlock {
 param($thresholds)
 Set-FSxFSRMQuota -Folder "share\department" -ThresholdConfigurations
$Using:thresholds
}
```

3. Verifique se a cota foi criada:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMQuota -Folder "share\department"
}
```

## Restringindo tipos de arquivos específicos usando grupos de arquivos

Este exemplo mostra como impedir que os usuários salvem arquivos de áudio e vídeo em uma pasta de documentos comerciais usando o grupo de arquivos padrão Audio and Video Files "".



Para restringir os tipos de arquivo usando grupos de arquivos:

1. Crie uma tela de arquivo ativa que bloqueie arquivos de áudio e vídeo:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
New-FSxFSRMFileScreen -Folder "share\business-documents" -IncludeGroup "Audio and
Video Files" -Description "Block media files in business documents folder"
}
```

2. (Opcional) Atualize a tela do arquivo para adicionar uma notificação quando os usuários tentarem salvar arquivos bloqueados:

```
$notifications = [System.Collections.ArrayList]@()

$eventNotification = @{
 ActionType = "Event"
 EventType = "Warning"
 MessageBody = "User attempted to save blocked media file"
}
$null = $notifications.Add($eventNotification)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
 param($notifications)
 Set-FSxFSRMFileScreen -Folder "share\business-documents" -
NotificationConfigurations $Using:notifications
}
```

3. Verifique se a tela do arquivo foi criada:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMFileScreen -Folder "share\business-documents"
}
```

## Identifique e classifique dados de PII

Este exemplo mostra como identificar automaticamente arquivos contendo números de previdência social e classificá-los como contendo informações de identificação pessoal (PII).

## Para identificar e classificar dados de PII:

### 1. Crie uma propriedade de classificação para PII:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMClassificationPropertyDefinition -Name "ContainsPII" -Type
 OrderedList -PossibleValueConfigurations @(
 @{ Name = "Yes" },
 @{ Name = "No" })
}
```

### 2. Crie uma regra de classificação para detectar números do Seguro Social:

#### Note

A expressão regular a seguir pesquisará arquivos em busca de texto com o padrão XXX-XX-XXXX. Para uso em produção, considere usar padrões mais sofisticados ou combinar vários métodos de detecção.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMClassificationRule -Name "Detect_SSN" -Property "ContainsPII"
 -PropertyValue "Yes" -Namespace "share" -ClassificationMechanism "Content
 Classifier" -ContentRegularExpression "\b\d{3}-\d{2}-\d{4}\b"
}
```

### 3. Classificação da corrida:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Start-FSxFSRMClassification
}
```

### 4. (Opcional) Configure a classificação contínua para classificar automaticamente os novos arquivos:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMClassification -Continuous $true
}
```

```
}
```

5. Verifique o status (1 significa concluído):

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMClassification
}
```

6. Depois que a classificação for concluída, você poderá visualizar as propriedades de classificação atribuídas aos arquivos clicando com o botão direito do mouse em um arquivo no Explorador de Arquivos do Windows, selecionando Propriedades e escolhendo a guia Classificação. Essa guia exibe todas as propriedades de classificação e seus valores para o arquivo.

## Criação de uma política de retenção para arquivos

Este exemplo mostra como classificar arquivos por período de retenção com base na localização da pasta, que você pode usar com PowerShell scripts do lado do cliente para arquivar ou excluir arquivos.

Para criar uma política de retenção para arquivos:

1. Crie uma propriedade de classificação para o período de retenção:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMClassificationPropertyDefinition -Name "RetentionPeriod" -Type
 String -Description "File retention period"
}
```

2. Crie regras de classificação para diferentes períodos de retenção:

- Retenção de 7 anos para documentos legais na pasta Documentos Legais:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMClassificationRule -Name "Legal_7Year" -Property
 "RetentionPeriod" -PropertyValue "7 years" -Namespace "share/Legal Documents" -
 ClassificationMechanism "Folder Classifier"
}
```

- Retenção de 3 anos para registros financeiros na pasta Finanças:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
 New-FSxFSRMClassificationRule -Name "Finance_3Year" -Property
 "RetentionPeriod" -PropertyValue "3 years" -Namespace "share/Finance" -
 ClassificationMechanism "Folder Classifier"
}
```

Você também pode classificar por conteúdo de arquivo e pesquisar sequências de caracteres como “Período de retenção de sete anos”. Para conseguir isso, use o `ClassificationMechanism "Content Classifier" ContentString "Retention seven years"` e.

3. Execute a classificação para aplicar as propriedades de retenção:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Start-FSxFSRMClassification
}
```

4. (Opcional) Configure a classificação contínua para classificar automaticamente os novos arquivos:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Set-FSxFSRMClassification -Continuous $true
}
```

5. Verifique o status (1 significa concluído):

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Get-FSxFSRMClassification
}
```

6. Depois que a classificação for concluída, você poderá visualizar as propriedades de classificação atribuídas aos arquivos clicando com o botão direito do mouse em um arquivo no Explorador de Arquivos do Windows, selecionando Propriedades e escolhendo a guia

Classificação. Essa guia exibe todas as propriedades de classificação e seus valores para o arquivo.

- Depois que os arquivos são classificados com períodos de retenção, você pode usar PowerShell scripts do lado do cliente para arquivar ou excluir arquivos com base em sua `RetentionPeriod` propriedade e idade. Por exemplo, você pode escanear o sistema de arquivos e comparar a idade do arquivo com a classificação do período de retenção. Para obter mais informações, consulte [Tarefas de gerenciamento de arquivos](#).

## Configurando relatórios comuns de armazenamento

Esta seção mostra como criar dois relatórios de armazenamento comumente usados: um relatório de arquivos grandes e um relatório de arquivos por proprietário.

### Relatório de arquivos grandes

Este exemplo cria um relatório mensal que identifica arquivos maiores que 200 MB.

Para criar um relatório de arquivos grandes:

- Crie um relatório programado de arquivos grandes:

```
$schedule = @{
 Time = "2:00 AM"
 Monthly = @(1) # Run on the 1st of each month
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
 param($schedule)
 New-FSxFSRMStorageReport -Name "Monthly Large Files Report" -Namespace "share"
 -ReportType "LargeFiles" -LargeFileMinimum 200MB -ReportFormat "HTML","CSV" -
 ScheduleConfigurations $schedule
}
```

- (Opcional) Execute o relatório imediatamente para testar:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
 Start-FSxFSRMStorageReport -Name "Monthly Large Files Report"
}
```

## Relatório de arquivos por proprietário

Este exemplo cria um relatório semanal que mostra o consumo de armazenamento por usuário.

Para criar um relatório de arquivos por proprietário:

1. Crie um relatório de arquivos agendados por proprietário:

```
$schedule = @{
 Time = "3:00 AM"
 Weekly = @('Sunday')
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
 param($schedule)
 New-FSxFSRMStorageReport -Name "Weekly Files by Owner Report" -
 Namespace "share" -ReportType "FilesByOwner" -ReportFormat "HTML","CSV" -
 ScheduleConfigurations $schedule
}
```

2. (Opcional) Execute o relatório imediatamente para testar:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
 Start-FSxFSRMStorageReport -Name "Weekly Files by Owner Report"
}
```

Acesse os relatórios gerados mapeando o compartilhamento administrativo de D\$. Para obter mais informações, acesse [Acessando relatórios de armazenamento](#).

## Gerenciar armazenamento no FSx para Windows File Server

A configuração de armazenamento do seu sistema de arquivos inclui a quantidade de capacidade de armazenamento provisionado, o tipo de armazenamento e, se o tipo de armazenamento for uma unidade de estado sólido (SSD), a quantidade de IOPS SSD. Durante e após a criação do sistema de arquivos, é possível configurar esses recursos junto com a capacidade de throughput do sistema de arquivos para atingir o nível de desempenho desejado para sua workload. Explore os tópicos a seguir e aprenda a gerenciar o armazenamento do seu sistema de arquivos e o desempenho

relacionado ao armazenamento usando o Console de gerenciamento da AWS, a AWS CLI e a API do Amazon FSx para gerenciamento remoto no PowerShell.

## Tópicos

- [Otimizar custos do armazenamento](#)
- [Como gerenciar a capacidade de armazenamento](#)
- [Gerenciar o tipo de armazenamento do seu sistema de arquivos](#)
- [Como gerenciar IOPS de SSD](#)
- [Reduzir os custos de armazenamento com deduplicação de dados](#)
- [Gerenciar cotas de armazenamento](#)
- [Aumentar a capacidade de armazenamento do sistema de arquivos](#)
- [Como monitorar os aumentos da capacidade de armazenamento](#)
- [Como aumentar dinamicamente a capacidade de armazenamento de um sistema de arquivos do FSx para Windows File Server](#)
- [Atualização do tipo de armazenamento de um sistema de arquivos do FSx para Windows](#)
- [Como monitorar as atualizações de tipo de armazenamento](#)
- [Atualizar as IOPS SSD de um sistema de arquivos](#)
- [Monitorar atualizações de IOPS de SSD provisionadas](#)
- [Como gerenciar a eliminação de duplicação de dados](#)
- [Solução de problemas da eliminação de duplicação dos dados](#)

## Otimizar custos do armazenamento

Você pode otimizar seus custos com armazenamento usando as opções de configuração de armazenamento disponíveis no FSx para Windows.

Opções de tipo 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 a relação entre custo e desempenho para atender às necessidades da sua 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 data analytics. Para obter mais informações sobre os tipos de armazenamento e o desempenho do sistema de arquivos, consulte [desempenho do FSx para Windows File Server](#).

**Desduplicação de dados:** grandes conjuntos de dados costumam ter 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 [Reduzir os custos de armazenamento com desduplicação de dados](#).

## Como gerenciar a capacidade de armazenamento

Você pode aumentar a capacidade de armazenamento do sistema de arquivos do FSx para Windows de acordo com as mudanças dos seus requisitos de armazenamento. Para fazê-lo, você pode usar o console do Amazon FSx, a API do Amazon FSx ou a AWS Command Line Interface (AWS CLI). Os fatores a levar em consideração ao planejar um aumento na capacidade de armazenamento incluem saber quando você precisa aumentar a capacidade de armazenamento, entender como o Amazon FSx processa os aumentos de capacidade de armazenamento e acompanhar o andamento de uma solicitação de aumento de armazenamento. Você só pode aumentar a capacidade de armazenamento de um sistema de arquivos, não sendo possível 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.

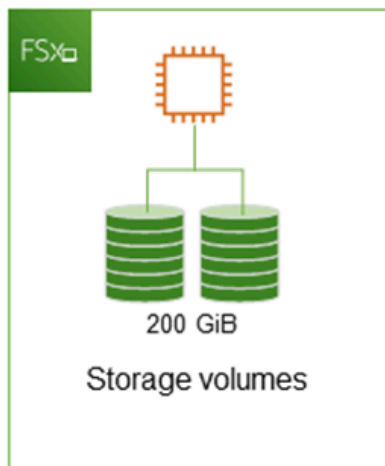
Quando você aumenta a capacidade de armazenamento de um sistema de arquivos do Amazon FSx, o Amazon FSx adiciona automaticamente um conjunto de discos novo e maior ao sistema de arquivos. Em seguida, o Amazon FSx executa um processo de otimização de armazenamento em segundo plano para migrar de forma transparente os dados dos discos antigos para os novos discos. Dependendo do tipo de armazenamento e de outros fatores, a otimização do armazenamento pode



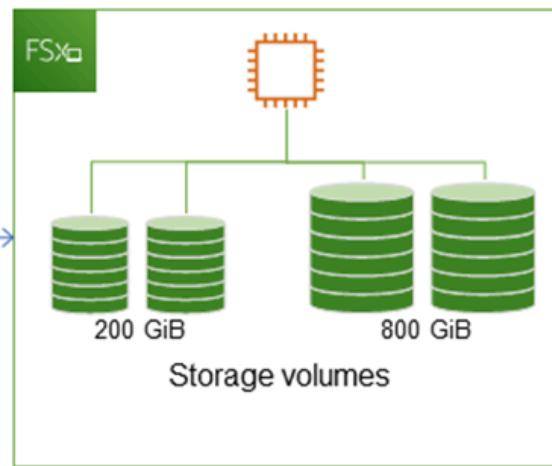
levar de algumas horas a vários dias, com um impacto mínimo perceptível sobre o desempenho da workload. Durante essa otimização, o uso do backup é temporariamente maior, porque os volumes de armazenamento antigos e novos estão incluídos nos backups no nível de sistema de arquivos. Ambos os conjuntos 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.

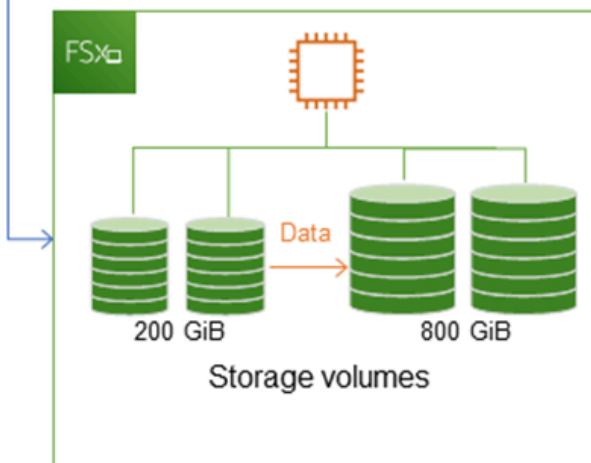
Step 1: Storage capacity increase request to 800 GiB.



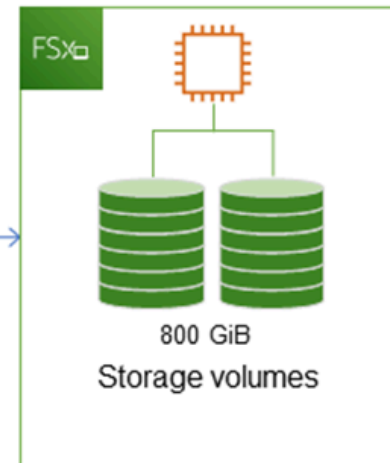
Step 2: Amazon FSx adds the new, larger disks.



Step 3: Amazon FSx migrates data to larger disks.



Step 4: Amazon FSx removes smaller disks.



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](#).

## O que saber sobre o aumento da capacidade de armazenamento de um sistema de arquivos

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 MBps. 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](#).

## Saber 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 [Monitorar com o Amazon CloudWatch](#).

Recomendamos manter pelo menos 20% 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 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. Porém, sistemas de arquivos com o tipo de armazenamento em HDD e workloads 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 podem sofrer uma redução temporária no desempenho. Nesses casos, recomendamos que você aumente a capacidade de throughput do sistema de arquivos antes da capacidade de armazenamento. Para esses tipos de workloads, também recomendamos alterar a capacidade de throughput durante períodos ociosos quando houver uma carga mínima no sistema de arquivos. 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](#).

## Gerenciar o tipo de armazenamento do seu sistema de arquivos

Você pode alterar o tipo de armazenamento do sistema de arquivos de HDD para SSD usando o Console de gerenciamento da AWS e a AWS CLI. Ao alterar o tipo de armazenamento para SSD, lembre-se de que você não poderá atualizar a configuração do sistema de arquivos novamente

até 6 horas após a solicitação do último aumento ou até que o processo de otimização do armazenamento seja concluído, o que demorar mais. 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. Para obter mais informações, consulte [Atualização do tipo de armazenamento de um sistema de arquivos do FSx para Windows](#).

Você não pode alterar o tipo de armazenamento do sistema de arquivos de SSD para HDD. Se você quiser alterar o tipo de armazenamento de um sistema de arquivos de SSD para HDD, precisará restaurar um backup do sistema de arquivos em um novo sistema de arquivos configurado para usar o armazenamento em HDD. Para obter mais informações, consulte [Restaurar backups em um novo sistema de arquivos](#).

## Sobre os tipos de armazenamento

Você pode configurar o sistema de arquivos do FSx para Windows File Server para usar o tipo de armazenamento de unidade de estado sólido (SSD) ou de unidade de disco rígido (HDD) magnético.

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, data analytics, 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.

O armazenamento HDD foi desenvolvido para um amplo espectro de workloads, incluindo diretórios iniciais, compartilhamentos de arquivos de usuários e departamentos, além de sistemas de gerenciamento de conteúdo. 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 obter mais informações, consulte [Configuração e performance do armazenamento](#).

## Como gerenciar IOPS de SSD

Para sistemas de arquivos configurados com armazenamento SSD, a quantidade de IOPS SSD determina a quantidade de E/S de disco disponível quando seu sistema de arquivos precisa ler e gravar dados no disco, ao contrário dos dados que estão no cache. Você pode selecionar e escalar a quantidade de IOPS SSD 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 as IOPS SSD acima do limite compatível com a capacidade de throughput, talvez seja necessário aumentar a capacidade de throughput para alcançar esse nível de IOPS SSD. Para obter mais informações, consulte [desempenho do FSx para Windows File Server](#) e [Como gerenciar a capacidade de throughput](#).

Veja alguns itens importantes que você precisa saber sobre como atualizar as IOPS SSD de um sistema de arquivos:

- Como escolher um modo de IOPS, pois há dois modos de IOPS para escolher:
  - Automática: escolha esse modo e o Amazon FSx escalará automaticamente suas IOPS SSD para manter 3 IOPS SSD por GiB de capacidade de armazenamento, até 400 mil IOPS SSD por sistema de arquivos.
  - Provisionada pelo usuário: escolha esse modo para especificar o número de IOPS SSD no intervalo de 96 a 400 mil. 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). A solicitação vai falhar quando você escolher o modo provisionado pelo usuário e a quantidade de IOPS SSD que você especifica não é pelo menos 3 IOPS por GiB. 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 do sistema de arquivos e a quantidade exigir, por padrão, uma quantidade de IOPS SSD que seja superior ao nível atual de IOPS SSD, o Amazon FSx alternará automaticamente o sistema de arquivos para o modo Automático e o sistema de arquivos terá no mínimo 3 IOPS SSD por GiB de capacidade de armazenamento.
- 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.

- Frequência dos aumentos de IOPS SSD: não é possível fazer aumentos adicionais de IOPS SSD, aumentos da capacidade de throughput ou atualizações no tipo de armazenamento em um sistema de arquivos até 6 horas após a última solicitação de aumento ou até que o processo de otimização de armazenamento tenha sido concluído, o que for mais demorado. 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).

Para obter mais informações sobre como atualizar a quantidade de IOPS SSD do sistema de arquivos do FSx para Windows File Server, consulte [Atualizar as IOPS SSD de um sistema de arquivos](#).

## Reduzir os custos de armazenamento com desduplicação de dados

A desduplicação de dados, geralmente chamada de deduplicação, ajuda os administradores de armazenamento a reduzir os custos associados a dados duplicados. Com o FSx para Windows File Server, você pode usar a Eliminação de Duplicação de Dados da Microsoft 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:

- Os compartilhamentos de arquivos do usuário podem ter várias cópias dos mesmos arquivos ou de arquivos semelhantes.
- Os repositórios 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 habilitando 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. Ao habilitar a eliminação de duplicação de dados, a compressão de dados é habilitada por padrão, comprimindo os dados após a desduplicação para promover ainda mais economia. A desduplicação de dados otimiza as redundâncias sem comprometer a fidelidade ou a integridade dos dados. 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 da desduplicação usando o comando `Measure-FSxDedupFileMetadata` do PowerShell remoto 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 os trabalhos de desduplicação podem consumir recursos do servidor de arquivos, recomendamos monitorar o status dos trabalhos de desduplicação usando o `Get-FSxDedupStatus`.

Para obter informações sobre como configurar a desduplicação de dados em seu sistema de arquivos, consulte [Como gerenciar a eliminação de duplicação de dados](#).

Para obter informações sobre como solucionar problemas relacionados à desduplicação de dados, consulte

[Use as informações a seguir para ajudar a solucionar alguns problemas comuns ao configurar e usar a desduplicação de dados.](#)

---

## 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

Para ver o status atual da desduplicação de dados, execute o comando `Get-FSxDedupStatus` do PowerShell para visualizar o status de conclusão dos trabalhos de desduplicação 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.

- Levando em conta um cenário ideal, a Microsoft recomenda ter 1 GB de memória para cada 1 TB de dados lógicos (ou no mínimo 350 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. Caso contrário, você precisará aumentar a capacidade de throughput do sistema de arquivos para um nível que atenda aos requisitos de memória de 1 GB por 1 TB de dados lógicos.
- 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`). Lembre-se de que usar uma alocação maior de memória para a desduplicação pode afetar o desempenho do sistema de arquivos.
- Você pode modificar a configuração dos trabalhos de desduplicação para reduzir a quantidade de memória necessária. 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.

Para obter mais informações sobre a eliminação de duplicação de dados, consulte a documentação da Microsoft [Noções básicas da eliminação de duplicação de 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 [Reduzir os custos de armazenamento com deduplicação de dados](#).

## Gerenciar 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 monitorar 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.

Você pode gerenciar cotas de armazenamento do usuário em seu sistema de arquivos usando a CLI do Amazon FSx para gerenciamento remoto no PowerShell. Para saber como usar essa CLI, consulte [Usando a Amazon FSx CLI 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 -?`.

## Aumentar a capacidade de armazenamento do sistema de arquivos

Você pode aumentar a capacidade de armazenamento do sistema de arquivos do FSx para Windows File Server de acordo com as mudanças dos seus requisitos de armazenamento. Use o console, a AWS CLI ou a API do Amazon FSx para aumentar a capacidade de armazenamento de um sistema de arquivos, conforme descrito nos procedimentos a seguir. Para obter mais informações, consulte [Como gerenciar a capacidade de armazenamento](#).

## 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

Depois de aumentar a capacidade de armazenamento do sistema de arquivos, você poderá monitorar o andamento do aumento da capacidade de armazenamento usando o console, a API ou a AWS CLI do Amazon FSx conforme descrito nos procedimentos a seguir.

### 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 mil 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

Como alternativa ao aumento manual da capacidade de armazenamento do sistema de arquivos do FSx para Windows File Server conforme a quantidade de dados armazenados aumenta, você pode usar um modelo do CloudFormation para aumentar o armazenamento automaticamente. A solução apresentada nesta seção aumenta dinamicamente a capacidade de armazenamento de um sistema de arquivos quando a capacidade de armazenamento livre ficar 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 usa os seguintes parâmetros:

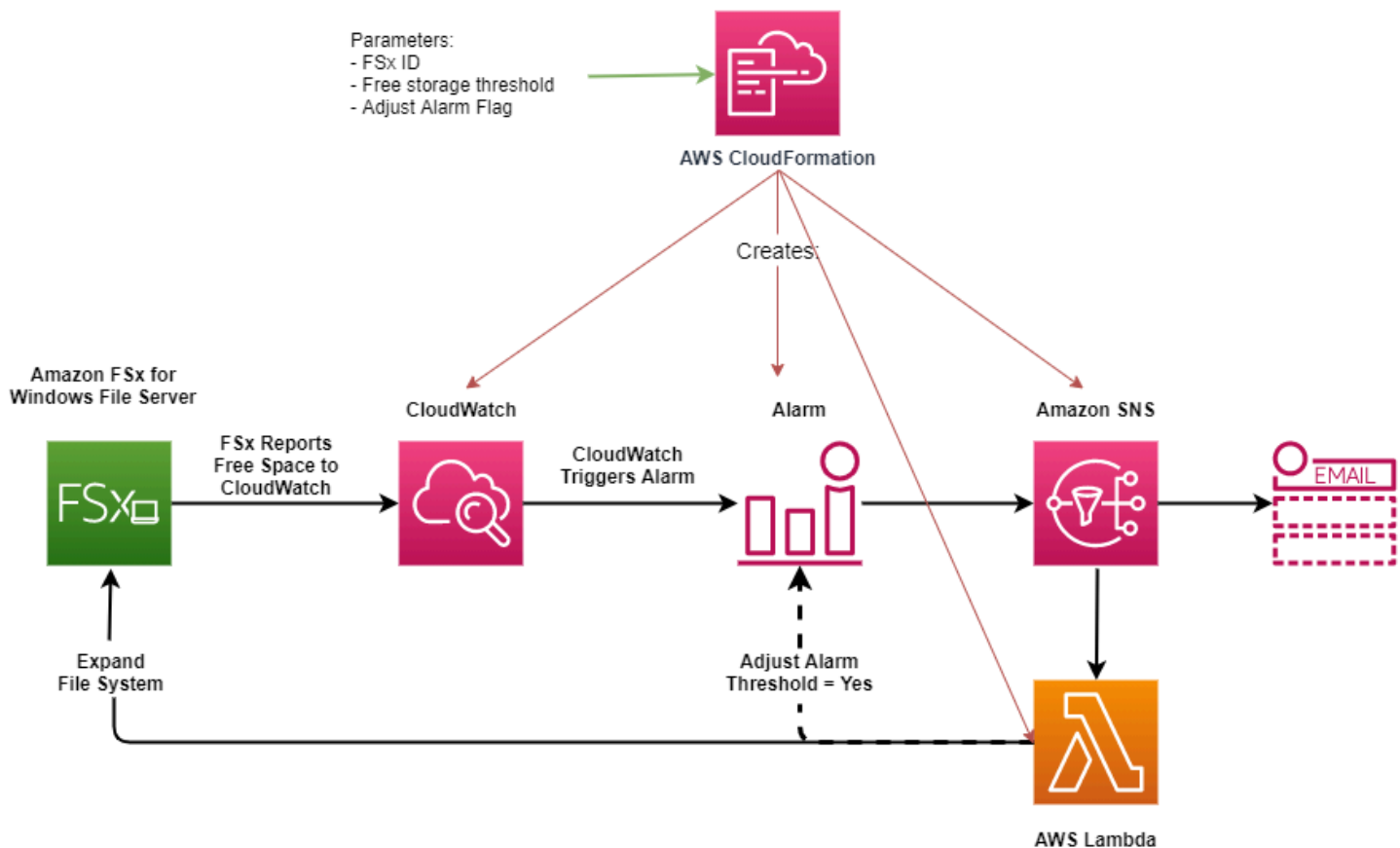
- O ID do sistema de arquivos
- O limite de capacidade de armazenamento livre (valor numérico)
- Unidade de medida (porcentagem [padrão] ou GiB)
- A porcentagem em que a capacidade de armazenamento (%) será aumentada
- O endereço de e-mail da assinatura do SNS
- Ajustar o limite do alarme (Sim/Não)

## Tópicos

- [Visão geral da arquitetura](#)
- [Modelo do CloudFormation](#)
- [Implantação automatizada com o CloudFormation](#)

## 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 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 do CloudFormation

Essa solução usa o 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 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 CloudFormation

O procedimento a seguir configura e implanta uma pilha do 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 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.

## Specify stack details

### Stack name

Stack name

FSxWindows-Dynamically-Increase-Storage-Capacity

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

### Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

#### File System Parameters

FileSystemId

Amazon FSx file system ID

fs-0123456789abcdef0

#### Alarm Notification

LowFreeDataStorageCapacityThreshold

Low free data storage capacity threshold (GiB or %)

200

LowFreeDataStorageCapacityThresholdUnit

Specify the Storage Capacity threshold Unit (GiB or %)

GiB

EmailAddress

The email address for alarm notification.

mmajor@example.com

#### Other parameters

AlarmModificationNotification

Would you like to adjust the percent increase for the next FSx storage increase event proportionate to the requested increase?

Yes

PercentIncrease

Provide the percent increase for File System Storage. This value should be between 10 and 100

30

Cancel

Previous

Next

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 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 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.

## Atualização do tipo de armazenamento de um sistema de arquivos do FSx para Windows

Você pode alterar o tipo de armazenamento de um sistema de arquivos que usa armazenamento HDD para usar armazenamento SSD. Você pode usar o console, a AWS CLI ou a API do Amazon FSx para alterar o tipo de armazenamento de um sistema de arquivos, conforme apresentado nos procedimentos a seguir. Para obter mais informações, consulte [Gerenciar o tipo de armazenamento do seu sistema de arquivos](#).

Para 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.

Você pode [monitorar o andamento](#) de uma atualização do tipo de armazenamento usando o console e a CLI.

Para 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

Depois de atualizar de HDD para SSD o tipo de armazenamento do seu sistema de arquivos, você poderá monitorar o andamento da atualização do tipo de armazenamento usando o console, a AWS CLI ou a API do Amazon FSx conforme descrito nos procedimentos a seguir.

Monitorar as atualizações do sistema de arquivos 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: o desempenho do armazenamento SSD está disponível para operações de gravação. A atualização entrará em um estado de otimização atualizada, que normalmente durará algumas horas, e durante o qual as operações de leitura terão níveis de desempenho 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.

## Atualizar as IOPS SSD de um sistema de arquivos

Para sistemas de arquivos configurados com armazenamento SSD, o nível provisionado de IOPS SSD determina a quantidade de E/S de disco disponível quando seu sistema de arquivos precisa ler e gravar dados no disco, ao contrário da leitura ou gravação de dados que estão no cache. Você pode atualizar as IOPS SSD de um sistema de arquivos usando o console, a AWS CLI ou a API do Amazon FSx, conforme descrito nos procedimentos a seguir. Para obter mais informações sobre o gerenciamento de IOPS SSD, consulte [Como gerenciar IOPS de SSD](#).

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 será exibida.

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 entre 96 e 400 mil.
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 IOPS SSD, use `Iops=number_of_IOPS` até um máximo de 400 mil nas regiões compatíveis da AWS e com `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 IOPS SSD por GiB de capacidade de armazenamento no sistema de arquivos, até um máximo de 400 mil nas regiões compatíveis da AWS.

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](#).

## Monitorar atualizações de IOPS de SSD provisionadas

Depois de atualizar a quantidade de IOPS SSD provisionadas para seu sistema de arquivos, você poderá monitorar o andamento da atualização de IOPS SSD usando o console, a AWS CLI e a API do Amazon FSx, conforme descrito nos procedimentos 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 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 IOPS de SSD 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 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 eliminação de duplicação de dados

Você pode gerenciar as [configurações de deduplicação de dados](#) em seu sistema de arquivos usando a CLI do Amazon FSx para gerenciamento remoto no PowerShell. Para obter mais informações sobre como usar o gerenciamento remoto da CLI do Amazon FSx no PowerShell, consulte [Usando a Amazon FSx CLI 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                                                                                                                                                                                                                                                       |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Enable-FSxDedup</a>              | Permite a eliminação de duplicação de dados no compartilhamento 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.                                |
| <code>Disable-FSxDedup</code>                | Desativa a eliminação de duplicação de dados no compartilhamento de arquivos.                                                                                                                                                                                   |
| <code>Get-FSxDedupConfiguration</code>       | 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.                                                    |
| <code>Set-FSxDedupConfiguration</code>       | 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.                                                                         |
| <a href="#">Get-FSxDedupStatus</a>           | Recupere o status da eliminação de duplicação e inclua propriedades somente leitura que descrevam a economia e o status da otimização no sistema de arquivos, os horários e o status de conclusão dos últimos trabalhos de deduplicação no sistema de arquivos. |

| Comando de eliminação de duplicação de dados | Descrição                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                                                                                                                                    |
| <a href="#">New-FSxDedupSchedule</a>         | Crie e personalize uma programação de desduplicação de dados.                                                                                                                                                                                                                                                           |
| <a href="#">Set-FSxDedupSchedule</a>         | Altere as configurações das programações de eliminação de duplicação de dados existentes.                                                                                                                                                                                                                               |
| Remove-FSxDedupSchedule                      | Exclua uma programação de desduplicação.                                                                                                                                                                                                                                                                                |
| Get-FSxDedupJob                              | Obtenha o status e as informações de todos os trabalhos de desduplicação em execução ou na 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 amznfsxxxxxxx.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 uma nova programação de deduplicação usando o comando `New-FSxDedupSchedule`, apresentado a seguir. As programações de eliminação de duplicação de dados usam o horário UTC.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxxxxxxx.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 amznfsxxxxxxx.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 amznfsxxxxxxx.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 amznfsxxxxxxx.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: Capacity, FreeSpace, UsedSpace, UnoptimizedSize e SavingsRate.

## Solução de problemas da eliminação de duplicação dos dados

Use as informações a seguir para ajudar a solucionar alguns problemas comuns ao configurar e usar a deduplicação de dados.

### 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

Para ver o status atual da deduplicação de dados, execute o comando `Get-FSxDedupStatus` do PowerShell para visualizar o status de conclusão dos trabalhos de deduplicação 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.

- Levando em conta um cenário ideal, a Microsoft [recomenda](#) ter 1 GB de memória para cada 1 TB de dados lógicos (ou no mínimo 350 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. Caso contrário, você precisará [aumentar a capacidade de throughput do sistema de arquivos](#) para um nível que atenda aos requisitos de memória de 1 GB por 1 TB de dados lógicos.
- 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`). Lembre-se de que usar uma alocação maior de memória para a deduplicação pode afetar o desempenho do sistema de arquivos.

- Você pode modificar a configuração dos trabalhos de deduplicação para reduzir a quantidade de memória necessária. 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.

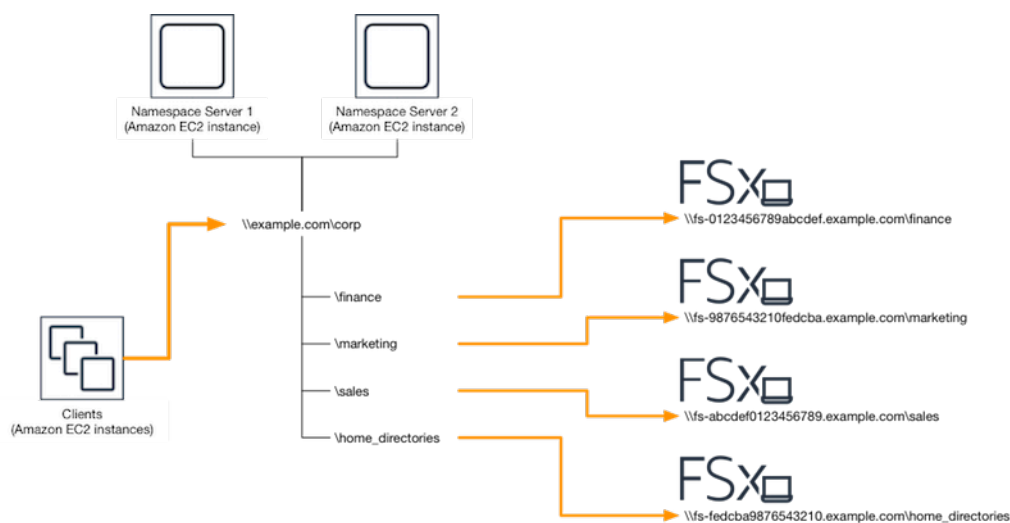
## Como usar o namespaces do DFS

O namespaces do DFS é um serviço de função do Windows Server que você usa para agrupar pastas compartilhadas localizadas em diferentes servidores em um ou mais namespaces estruturados logicamente. Isso torna possível oferecer aos usuários uma visão virtual das pastas compartilhadas, com um único caminho levando a arquivos localizados em vários sistemas de arquivos, conforme apresentado no diagrama a seguir. Além de organizar e unificar o acesso aos compartilhamentos de arquivos em vários sistemas de arquivos,

## Agrupar vários sistemas de arquivos do FSx para Windows File Server com os namespaces do DFS

Você pode usar os namespaces do Sistema de Arquivos Distribuído (DFS) da Microsoft para agrupar compartilhamentos de arquivos em vários sistemas de arquivos do FSx para Windows File Server em uma estrutura de pastas ou namespace comum. Ao usar os namespaces do DFS, é possível escalar o armazenamento de arquivos além da capacidade máxima de armazenamento de um único sistema de arquivos (64 TiB) para grandes conjuntos de dados de arquivos, alcançando até centenas de petabytes. Esta seção mostra como configurar os namespaces do DFS em vários sistemas de arquivos do FSx para Windows File Server.

O namespaces do DFS é um serviço de função do Windows Server que você usa para agrupar pastas compartilhadas localizadas em diferentes servidores em um ou mais namespaces estruturados logicamente. Isso torna possível oferecer aos usuários uma visão virtual das pastas compartilhadas, com um único caminho levando a arquivos localizados em vários sistemas de arquivos, conforme apresentado no diagrama a seguir. Além de organizar e unificar o acesso aos compartilhamentos de arquivos em vários sistemas de arquivos,



Para obter um procedimento passo a passo para agrupar FSx para sistemas de arquivos Windows usando namespaces do DFS, consulte [Agrupar vários sistemas de arquivos em um único namespace](#).

## Como melhorar o desempenho 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 a solução fornecida em [Como fragmentar dados usando namespaces do DFS para aumentar a escala do desempenho horizontalmente](#) para distribuir uniformemente o acesso de leitura/gravação aos seus dados em vários sistemas de arquivos do FSx para Windows File Server.

## Agrupar vários sistemas de arquivos em um único namespace

Neste procedimento, você criará um único namespace baseado em domínio (example.com \corp) em dois servidores de namespace, a fim de consolidar compartilhamentos de arquivos armazenados em vários sistemas de arquivos do FSx para Windows (finanças, marketing, vendas, home\_directories). Você também vai configurar quatro compartilhamentos de arquivos no namespace, cada um redirecionando os usuários de maneira transparente para compartilhamentos hospedados em sistemas de arquivos distintos do FSx para Windows. Isso permite que os usuários acessem os compartilhamentos de arquivos usando um namespace comum em vez de precisar especificar os nomes do DNS 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.

## Agrupar vários sistemas de arquivos em um namespace comum do DFS

1. Se você ainda não tiver servidores do namespace do DFS em execução, poderá iniciar um par de servidores do namespace do DFS altamente disponíveis usando o modelo [setup-DFSN-servers.template](#) do 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.
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 [Connecting to Your Windows Instance](#) no Amazon EC2 User Guide.

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. Escolha 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

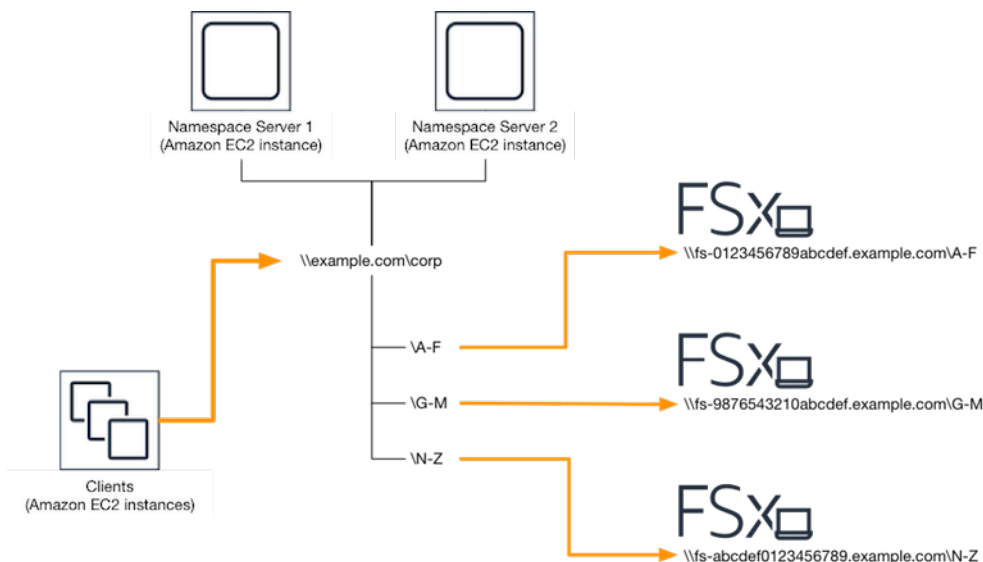
O modo Windows Server 2008 é a opção mais recente disponível para namespaces.

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 fragmentar dados usando namespaces do DFS para aumentar a escala do desempenho horizontalmente

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 tiver servidores do namespace do DFS em execução, você pode iniciar um par de servidores do namespace do DFS altamente disponíveis usando o modelo [setup-DFS-servers.template](#) do 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.
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 [Connecting to Your Windows Instance](#) no Amazon EC2 User Guide.
  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. Escolha 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.

## Como gerenciar a capacidade de throughput

Você pode aumentar e diminuir a capacidade de throughput do sistema de arquivos a qualquer momento para ajudar a gerenciar seu desempenho. A capacidade de throughput é uma das dimensões que determina a velocidade com a qual o servidor de arquivos que hospeda o sistema de arquivos do FSx para Windows File Server 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 uma quantidade maior de memória para armazenamento em cache no servidor de arquivos. Para obter mais informações, consulte [desempenho do FSx para Windows File Server](#).

### Tópicos

- [Funcionamento da escalabilidade de throughput](#)
- [Saber quando modificar a capacidade de throughput](#)
- [Modificar a capacidade de throughput](#)
- [Como monitorar as atualizações na capacidade de throughput](#)

## Funcionamento da escalabilidade de throughput

Quando você modifica a capacidade de throughput do seu sistema de arquivos, o Amazon FSx troca o servidor de arquivos do sistema de arquivos por outro com mais ou menos throughput nos bastidores. Para sistemas de arquivos multi-AZ, alternar para um novo servidor de arquivos aciona failover e failback automáticos, enquanto o Amazon FSx substitui os servidores de arquivos preferenciais e secundários. Sistemas de arquivos single-AZ ficarão indisponíveis por alguns minutos enquanto o servidor de arquivos for alternado durante o ajuste de escala da capacidade de throughput. Você receberá uma cobrança pela nova quantidade de capacidade de throughput quando ela ficar disponível para o seu sistema de arquivos.

 Note

Durante uma operação de manutenção no back-end, as modificações do sistema (incluindo modificações na capacidade de throughput) podem ter atrasos. As operações de manutenção podem fazer com que as modificações do sistema fiquem na fila para processamento.

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 resincronização para garantir que os dados sejam resincronizados com o servidor de arquivos recém-substituído.

O FSx para Windows foi projetado para minimizar o impacto dessa atividade de resincronização na aplicação e nos usuários. No entanto, o processo de resincronização 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 resincronização depende não apenas do nível da rotatividade de dados, mas também da natureza da rotatividade de dados no sistema de arquivos. Se a workload tiverem um alto índice 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.

## Saber 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. O desempenho (throughput e IOPS) que você pode promover usando o sistema de arquivos depende das características específicas da workload, junto com a capacidade de throughput, da capacidade de armazenamento e do tipo de armazenamento do seu 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 [Monitorar com o Amazon CloudWatch](#).

O FSx para Windows File Server fornece alertas de desempenho com base nos valores das métricas do CloudWatch para seu sistema de arquivos no painel de monitoramento e desempenho na página de detalhes do sistema de arquivos no console do Amazon FSx. Isso inclui a capacidade de throughput e outras métricas do sistema de arquivos que podem se beneficiar do aumento da capacidade de throughput. Para obter mais informações, consulte [Avisos e recomendações de performance](#).

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 desempenho necessários para oferecer suporte aos atributos 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 obter mais informações, consulte [Impacto da capacidade de throughput na performance](#).

## Modificar a capacidade de throughput

Você pode aumentar ou diminuir a capacidade de throughput do seu sistema de arquivos usando o console, o AWS Command Line Interface (AWS CLI) ou a API do Amazon FSx, conforme descrito nos procedimentos a seguir.

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 atualizações na capacidade de throughput](#).

## Modificar a capacidade de throughput de um sistema de arquivos (CLI)

Para aumentar ou diminuir 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` até o valor desejado; os valores válidos são 8, 16, 32, 64, 128, 256, 512, 1.024, 2.048, 4.608, 6.144, 9.216 e 12.288 MBps.

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 atualizações na capacidade de throughput](#).

## Como monitorar as atualizações 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.

| Updates (10)                                |                |             |              |                           |        |
|---------------------------------------------|----------------|-------------|--------------|---------------------------|-------------------------------------------------------------------------------------------|
| <input type="text" value="Filter updates"/> |                |             |              |                           | < 1 >  |
| Update type ▼                               | Target value ▼ | Status ▼    | Progress % ▼ | Request time ▲            |                                                                                           |
| Storage capacity                            | 154            | ✓ Completed | -            | 2020-05-22T12:14:58-04:00 |                                                                                           |
| Throughput capacity                         | 64             | ✓ Completed | -            | 2020-05-22T12:14:50-04:00 |                                                                                           |
| Throughput capacity                         | 128            | ✓ Completed | -            | 2020-05-21T13:55:58-04:00 |                                                                                           |
| Storage capacity                            | 140            | ✓ Completed | -            | 2020-05-21T13:55:30-04:00 |                                                                                           |
| Storage capacity                            | 122            | ✓ Completed | -            | 2020-05-18T11:36:33-04:00 |                                                                                           |

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 MBps e a capacidade de throughput de destino de 256 MBps.

```
.
.
.
 "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](#).

## Como gerenciar o tipo de rede

Ao criar um sistema de arquivos do FSx para Windows, você deve especificar um tipo de rede, que deve ser uma das seguintes opções:

- O IPv4 permite que seu sistema de arquivos se comunique usando somente o protocolo de Internet versão 4 (IPv4).
- O Dual-stack permite que seu sistema de arquivos se comunique por Protocolo de Internet versão 6 (IPv6) e IPv4.

É possível alterar o tipo de rede de um sistema de arquivos do FSx para Windows a qualquer momento usando o console de gerenciamento do Amazon FSx, a AWS CLI, a API da AWS ou um

dos SDKs da AWS. Por exemplo, se suas sub-redes oferecem suporte para endereçamento de IPv4 e IPv6, você pode atualizar seu sistema de arquivos existente de somente IPv4 para o modo de pilha dupla. Também é possível atualizar seu sistema de arquivos de pilha dupla para somente IPv4.

## Como usar o modo de pilha dupla

Você deve usar o modo de pilha dupla se precisar acessar e gerenciar seus sistemas de arquivos do Amazon FSx de forma nativa de clientes IPv6. Ao configurar seu sistema de arquivos do Amazon FSx para usar endereçamento de pilha dupla, você pode acessar seus dados de arquivos de clientes IPv6, bem como de clientes IPv4, na mesma Amazon VPC, em outra VPC da Conta da AWS ou em sua rede on-premises. Por exemplo, com um sistema de arquivos do Amazon FSx configurado para usar pilha dupla, é possível ter clientes IPv4 existentes e novos clientes IPv6 acessando seus dados de arquivos armazenados em seu sistema de arquivos.

Por padrão, o Amazon FSx e a Amazon VPC usam o protocolo de endereçamento IPv4. Portanto, como pré-requisito para usar IPv6, você deve primeiro atribuir um bloco Classless Inter-Domain Range (CIDR) IPv6 fornecido pela Amazon à sua VPC e sub-redes antes de poder usar o IPv6 com seus sistemas de arquivos Amazon FSx. Para obter mais informações sobre como habilitar o IPv6 para sua VPC, consulte [Adicionar suporte ao IPv6 para sua VPC](#) no Guia do usuário da Amazon Virtual Private Cloud.

## Como alterar o tipo de rede

Você pode modificar o tipo de rede de um sistema de arquivos usando o console do Amazon FSx, o AWS Command Line Interface (AWS CLI) ou a API do Amazon FSx.

Para alterar o tipo de rede de um sistema de arquivos (console)

1. Abra o console do Amazon FSx em <https://console.aws.amazon.com/fsx/>.
2. Navegue até Sistemas de arquivos e escolha o sistema de arquivos do FSx para Windows em que você deseja alterar o tipo de rede.
3. Em Ações, escolha Atualizar tipo de rede. Ou, no painel Rede e segurança, escolha Gerenciar ao lado de Tipo de rede do sistema de arquivos.

A janela Atualizar tipo de rede é exibida.

4. Em Tipo de rede desejado, escolha IPv4 ou Pilha dupla.
  - Se você escolher IPv4, nenhuma outra configuração é necessária.



- Se você escolher `Dual-stack`, especifique o intervalo de endereços IPv6 que os endpoints do sistema de arquivos usarão:
- Intervalo de endereços IPv6 não alocados da sua VPC: o Amazon FSx escolhe um intervalo de endereços IP /118 disponível entre um dos intervalos de CIDR de IPv6 da VPC para usar como intervalo de endereços IPv6 do endpoint para o sistema de arquivos.

## 5. Selecione Atualizar.

Para modificar o tipo de rede de um sistema de arquivos (CLI)

- Para modificar um tipo de rede do sistema de arquivos, use o comando da CLI [update-file-system](#) (ou a operação de API equivalente [UpdateFileSystem](#)), conforme exibido no exemplo a seguir.

```
aws fsx update-file-system \
 --file-system-id fs-0123456789abcdef0 \
 --network-type DUAL
```

## Marcação de seus recursos do Amazon FSx

Para ajudar você a gerenciar seus sistemas de arquivos e outros recursos do FSx para Windows File Server, 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-las.

### Tópicos

- [Conceitos Básicos de Tags](#)
- [Marcando seus Recursos](#)
- [Restrições de tags](#)
- [Permissões necessárias para marcar recursos](#)

## Conceitos Básicos de Tags

Uma tag um rótulo atribuído a um recurso 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 FSx para Windows File Server da sua conta que ajuda a rastrear o proprietário e o nível da pilha de cada instância.

Recomendamos que você desenvolva um conjunto de chave de tags que atenda suas necessidades para cada tipo de recurso. Usar um conjunto consistente de chaves de tags facilita para você gerenciar seus recursos. É possível pesquisar e filtrar os recursos de acordo com as tags que adicionar. Para obter mais informações sobre como implementar uma estratégia eficaz de marcação de recursos com tags, consulte o whitepaper da AWS , [Práticas recomendadas de marcação com tags](#).

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 FSx para Windows File Server, 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](#).

## Marcando seus Recursos

É possível marcar os recursos do FSx para Windows File Server que existem em sua conta. Caso esteja usando o console do Amazon FSx, você poderá aplicar tags aos recursos ao usar a guia Tags na tela do recurso relevante. Ao criar recursos, você pode aplicar a chave Nome com um valor e aplicar tags de sua escolha ao criar um sistema de arquivos. O console pode organizar os recursos de acordo com a tag Nome, mas ela não tem nenhum significado semântico para o serviço do FSx para Windows File Server.

Você pode aplicar permissões no nível do recurso com base em tags nas suas políticas do IAM para as ações de API do FSx para Windows File Server 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 APIs do FSx para Windows File Server `TagResource` e `UntagResource` 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 a tags:

- Número máximo de tags por recurso — 50
- Em todos os recursos, cada chave de tag deve ser exclusiva e possuir 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 FSx para Windows File Server 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 necessárias para marcar recursos

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 [Usando tags para controlar o acesso aos seus FSx recursos da Amazon](#).

## Atualizar um sistema de arquivos usando a AWS CLI

Há três elementos que você pode atualizar usando os procedimentos deste tutorial 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
```

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

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

- FSx Os backups nativos da Amazon oferecem suporte às suas necessidades de retenção e conformidade de backup na Amazon FSx.
- AWS Backup os backups dos seus sistemas de FSx arquivos da Amazon fazem parte de uma solução de backup centralizada e automatizada em todos os AWS 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 FSx arquivos da Amazon em um segundo sistema de arquivos fornece proteção e recuperação de dados.

## Tópicos

- [Proteger seus dados com backups](#)
- [Como proteger seus dados com cópias de sombra](#)
- [Replicação programada usando AWS DataSync](#)

## Proteger seus dados com backups

Você pode proteger os dados em seu sistema FSx de arquivos do Windows File Server fazendo backups regulares do sistema de arquivos. FSx A Amazon oferece várias opções para fazer backup de seus sistemas de arquivos. Você pode usar backups diários automáticos para fazer um backup todos os dias. Você pode fazer um backup do sistema de arquivos iniciado pelo usuário a qualquer momento. Você também pode usar AWS Backup como parte de uma solução de backup centralizada para seus AWS recursos. Essas soluções de backup podem ajudar você a atender 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.

Com a Amazon FSx file-system-consistent, os backups são 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, a Amazon FSx usa o Volume Shadow Copy Service (VSS) no Microsoft Windows. Para garantir alta durabilidade, a Amazon FSx armazena backups no Amazon Simple Storage Service (Amazon S3).

Os FSx backups da Amazon são incrementais, sejam eles gerados usando o backup diário automático ou 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, o armazenamento I/O pode ser suspenso 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 aplicativos experimentará essa I/O suspensão como uma breve I/O pausa. 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 for Windows File Server executa em seu sistema de arquivos. FSx Os backups da Amazon ajudam a suportar suas necessidades de retenção e conformidade de backup. Trabalhar com FSx os backups da Amazon é fácil, seja criando backups, copiando um backup, restaurando um sistema de arquivos a partir de um backup ou excluindo 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](#)
- [Como trabalhar com backups iniciados pelo usuário](#)
- [Usando AWS Backup com a Amazon FSx](#)
- [Copiar backups](#)

- [Restaurar backups em um novo sistema de arquivos](#)
- [Como criar backups iniciados pelo usuário](#)
- [Excluir backups](#)
- [Tamanho dos backups](#)
- [Copiar backups na mesma conta](#)
- [Restaurar um backup em um novo sistema de arquivos](#)

## Como trabalhar com backups diários automáticos

Por padrão, a 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 a janela de backup diário, recomendamos que você escolha um horário conveniente do dia fora do horário normal de operação para as aplicações que usam o sistema de arquivos. Também recomendamos escolher uma janela de backup fora da de manutenção, pois os backups automatizados podem não ocorrer se houver manutenção contínua do sistema de arquivos.

Os backups diários automáticos são mantidos por um determinado período, conhecido como período de retenção. Quando você cria um sistema de arquivos no FSx console da Amazon, o período padrão de retenção diária de backup automático é de 30 dias. O período de retenção padrão é diferente na FSx API e na CLI da Amazon. 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 obter mais informações, consulte [Atualizar um sistema de arquivos usando a AWS CLI](#).



 Important

Reduzir o período de retenção dos backups diários automáticos resultará na exclusão permanente dos backups fora da nova janela de retenção. Antes de continuar, certifique-se de que não precisará desses backups mais antigos.

## Como trabalhar com backups iniciados pelo usuário

Com a Amazon FSx, você pode fazer backups manualmente dos seus sistemas de arquivos a qualquer momento. Você pode fazer isso usando o FSx console da Amazon, a API ou o AWS Command Line Interface (AWS CLI). Seus backups dos sistemas de FSx arquivos da Amazon iniciados pelo usuário nunca expiram e estão 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 FSx console, a API ou a CLI da Amazon. Eles nunca são excluídos automaticamente pela Amazon FSx. Para obter 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.

Para aprender a fazer backups iniciados pelo usuário de seus sistemas de arquivos, consulte [Como criar backups iniciados pelo usuário](#).

## Usando AWS Backup com a Amazon FSx

AWS Backup é uma forma simples e econômica de proteger seus dados fazendo backup dos sistemas de FSx arquivos da Amazon. 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 da 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 FSx console da Amazon. Os backups feitos AWS Backup são incrementais em relação a quaisquer outros FSx backups da Amazon 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 por AWS Backup são considerados backups iniciados pelo usuário e contam para a cota de backup iniciada pelo usuário para a Amazon. FSx Você pode ver e restaurar os backups feitos AWS Backup no FSx console, na CLI e na API da Amazon. No entanto, você não pode excluir backups feitos AWS Backup no FSx console, na CLI ou na API da Amazon. Para obter mais informações sobre como usar AWS Backup para fazer backup de seus sistemas de FSx arquivos da Amazon, consulte Como [trabalhar com sistemas de FSx arquivos da Amazon](#) no Guia do AWS Backup desenvolvedor.

## Copiar backups

Você pode usar FSx a Amazon para copiar manualmente backups dentro da mesma AWS conta para outra AWS região (cópias entre regiões) ou dentro da mesma AWS região (cópias dentro da região). Você pode fazer cópias entre regiões somente dentro da mesma AWS partição. Você pode criar cópias de backup iniciadas pelo usuário usando o FSx console ou a AWS CLI API da Amazon. 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 FSx console da Amazon ou a API AWS CLI da 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:

- 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.

### JSON

```
{
 "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).

Para aprender a fazer backups de cópia de seus sistemas de arquivos, consulte [Copiar backups na mesma conta](#).

## Restaurar backups em um novo sistema de arquivos

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 AWS CLI console ou um dos AWS SDKs. 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 acessando 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 Active Directory do sistema de arquivos original. Para obter mais informações sobre o Active Directory, consulte [Trabalhar com o Microsoft Active Directory](#).

Para saber como restaurar um backup em um novo sistema FSx de arquivos do Windows, consulte [Restaurar um backup em um novo sistema de arquivos](#).

### Note

Só é possível restaurar o backup de um sistema de arquivos para um novo sistema de arquivos com o mesmo tipo de implantação e capacidade de armazenamento que o original. Você poderá aumentar a capacidade de armazenamento do novo sistema de arquivos depois que ele estiver disponível. Para obter mais informações, consulte [Como gerenciar a capacidade de armazenamento](#).

Você pode alterar qualquer uma das seguintes configurações do sistema de arquivos ao restaurar um backup em um novo sistema de arquivos:

- Tipo de armazenamento
- Capacidade de throughput
- VPC
- Zona de disponibilidade

- Sub-rede
- VPC security groups (Grupos de segurança da VPC)
- Configuração do Active Directory
- AWS KMS chave de criptografia
- Hora de início do backup automático diário
- Janela de manutenção semanal

## Como criar backups iniciados pelo usuário

Além dos backups diários automáticos do sistema de arquivos, você pode criar um backup do sistema de arquivos iniciado pelo usuário a qualquer momento, usando o FSx console da Amazon, conforme descrito no procedimento a seguir.

Criar um backup do sistema de arquivos iniciado pelo usuário

1. Abra o FSx console da Amazon 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 seus backups no FSx console da Amazon escolhendo Backups na navegação do lado esquerdo. Seu novo backup iniciado pelo usuário terá o tipo USER\_INITIATED e o status CREATING até que se torne AVAILABLE. Para obter mais informações, consulte [Como trabalhar com backups iniciados pelo usuário](#).

## Excluir backups

Você pode excluir qualquer backup diário automático e iniciado pelo usuário do seu sistema de arquivos usando o FSx console, a CLI ou a API da Amazon, descritos nos procedimentos a seguir. Para excluir backups feitos por AWS Backup, que têm o tipo de AWS Backup, você deve usar o AWS Backup console, a CLI ou a API. A exclusão de um backup é uma ação permanente e irreversível.

Todos os dados em um backup excluído também são excluídos. Não exclua um backup, a menos que tenha certeza de que não precisará dele novamente no futuro.

Para excluir um backup (console)

1. Abra o FSx console da Amazon 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 irreversível.

## 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.

Para fornecer backups duráveis e incrementais, a Amazon FSx faz backup dos dados no nível do bloco. file-system-consistent 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.

Use etiquetas para organizar sua AWS fatura de forma a refletir sua própria estrutura de custos. Para fazer isso, inscreva-se para receber sua Conta da AWS fatura com os valores-chave da etiqueta incluídos. Então, para ver o custo de recursos combinados, organize suas informações de faturamento de acordo com recursos com os mesmos valores de chave de tags. Por exemplo,

é possível marcar vários recursos com um nome de aplicação específico, e depois organizar suas informações de faturamento para ver o custo total daquela aplicação em vários serviços. Para obter mais informações, consulte [Usar tags de alocação de custos](#) no Guia do usuário do AWS Billing .

#### Note

Ao [aumentar a capacidade de armazenamento](#), o processo de migração de dados do antigo conjunto de discos de armazenamento para o novo e maior conjunto de discos de armazenamento pode resultar em um aumento temporário no uso do backup até que os backups associados ao antigo conjunto de discos de armazenamento sejam excluídos. Se o armazenamento do seu sistema de arquivos foi apenas parcialmente usado antes de você aumentar sua capacidade, o tamanho dos dados que precisam ser migrados para os novos discos pode ser maior do que o tamanho dos dados existentes nos discos de armazenamento originais. Isso pode ocasionar um aumento no uso do backup até o novo nível de capacidade de armazenamento. Você deve considerar o impacto do aumento da capacidade de armazenamento em seu planejamento de backup.

## Copiar backups na mesma conta

Você pode usar o Console de gerenciamento da AWS e AWS CLI para copiar manualmente os backups da mesma AWS conta para outra Região da AWS (cópias entre regiões) ou dentro da mesma Região da AWS (cópias dentro da região) usando os procedimentos a seguir.

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

1. Abra o FSx console da Amazon 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 [CopyBackup](#) API 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 FSx console da Amazon ou programaticamente usando o comando da describe-backups CLI ou a operação da API. [DescribeBackups](#)

## Restaurar um backup em um novo sistema de arquivos

Você pode restaurar um backup do sistema de arquivos para criar um novo sistema de arquivos usando a Console de gerenciamento da AWS CLI e a API, conforme descrito no procedimento a seguir.

Restaurar um sistema de arquivos de um backup

1. Abra o FSx console da Amazon 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 seu sistema de FSx arquivos da Amazon e, em seguida, escolha Criar sistema de arquivos.

FSx A Amazon está criando um novo sistema de arquivos e, quando seu status mudar paraAVAILABLE, você poderá usar o sistema de arquivos normalmente.

## Como proteger 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 habilitadas, 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 sistema de arquivos e, portanto, consomem a capacidade de armazenamento do sistema de arquivos somente para as partes modificadas dos arquivos. Todas as cópias de sombra armazenadas em seu sistema de arquivos são incluídas em backups do sistema de arquivos.

### Note

As cópias de sombra não estão habilitadas FSx para o Windows File Server por padrão. Para proteger os dados em seu sistema de arquivos usando cópias de sombra, é necessário habilitar as cópias de sombra e configurar uma programação de cópia de sombra no sistema

de arquivos. Para obter mais informações, consulte [Configurar 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](#)
- [Como configurar cópias de sombra](#)
- [Configurar cópias de sombra para usar o armazenamento e a programação padrão](#)
- [Definir a quantidade máxima de armazenamento de cópia de sombra](#)
- [Visualizar o armazenamento de cópias de sombra](#)
- [Como criar uma programação de cópias de sombra personalizada](#)
- [Visualizar a programação de cópias de sombra](#)
- [Como criar uma cópia de sombra](#)
- [Como visualizar as cópias de sombra atuais](#)
- [Como excluir cópias de sombra](#)
- [Como excluir uma programação de cópias de sombra](#)
- [Como excluir o armazenamento de cópias de sombra, a programação e todas as cópias de sombra](#)
- [Solução de problemas com cópias de sombra](#)

## 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. A 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: 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 I/O operações 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 FSx necessidade de o Windows executar verificações de consistência no armazenamento de cópias de sombra. Você também pode experimentar uma maior latência das I/O operações devido à FSx necessidade de o 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](#) para sistemas de arquivos Multi-AZ, FSx o Windows executa uma verificação de consistência que exige a verificação do armazenamento de cópias paralelas em seu sistema de arquivos antes que o novo servidor de arquivos ativo 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.

## Como configurar cópias de sombra

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

- Configurar a quantidade máxima de armazenamento que as cópias de sombra podem consumir em seu sistema de arquivos
- (Opcional) Configurar o número máximo de cópias de sombra que pode ser armazenado em seu sistema de arquivos O valor padrão é 20.
- (Opcional) Configurar uma programação que define os horários e intervalos para fazer cópias de sombra, 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 habilitar e programar rapidamente cópias paralelas periódicas usando FSx as configurações padrão da Amazon, consulte [Configurar 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 [Definir 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 obter mais informações, consulte [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 armazenado 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 I/O desempenho para manter 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 em até 500. No entanto, se você tiver um grande número de cópias de sombra ou cópias de sombra que ocupem uma grande quantidade de armazenamento (escala de TB) em um único sistema de arquivos, processos como failover e failback poderão levar mais tempo do que o esperado. Isso ocorre porque o Windows precisa executar verificações de consistência no armazenamento de cópias paralelas. Você também pode experimentar uma maior latência das I/O operações 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. A Amazon FSx oferece o recurso Shadow Copies 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 I/O operations for every file write operation. If Windows is unable to keep up with the incoming rate of I/O operations per second, it can cause all shadow copies to be deleted because it can no longer maintain the shadow copies via copy-on-write. Therefore, it is important that you provision sufficient I/O performance capacity for your workload needs on your file system (both the throughput capacity dimension that determines the file server I/O performance, and the storage type and capacity that determine the storage I/O desempenhos).
- Geralmente, recomendamos que você use sistemas de arquivos configurados com armazenamento SSD em vez de armazenamento em HDD ao habilitar cópias de sombra, já que o Windows consome um I/O desempenho maior para manter as cópias de sombra e porque o armazenamento em HDD fornece menor capacidade de desempenho 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.

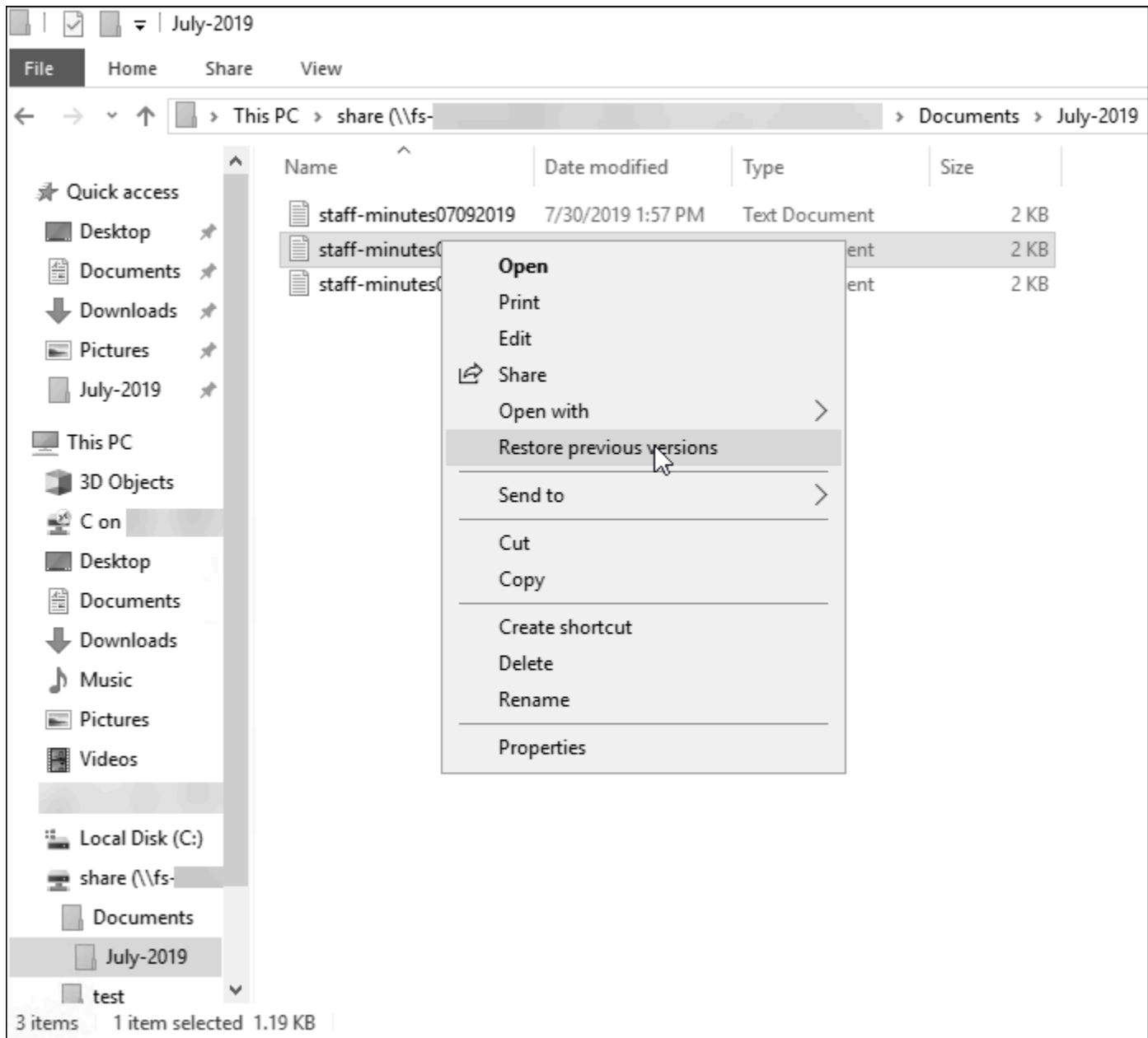
#### Warning

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](#).

## Como restaurar arquivos e pastas individuais

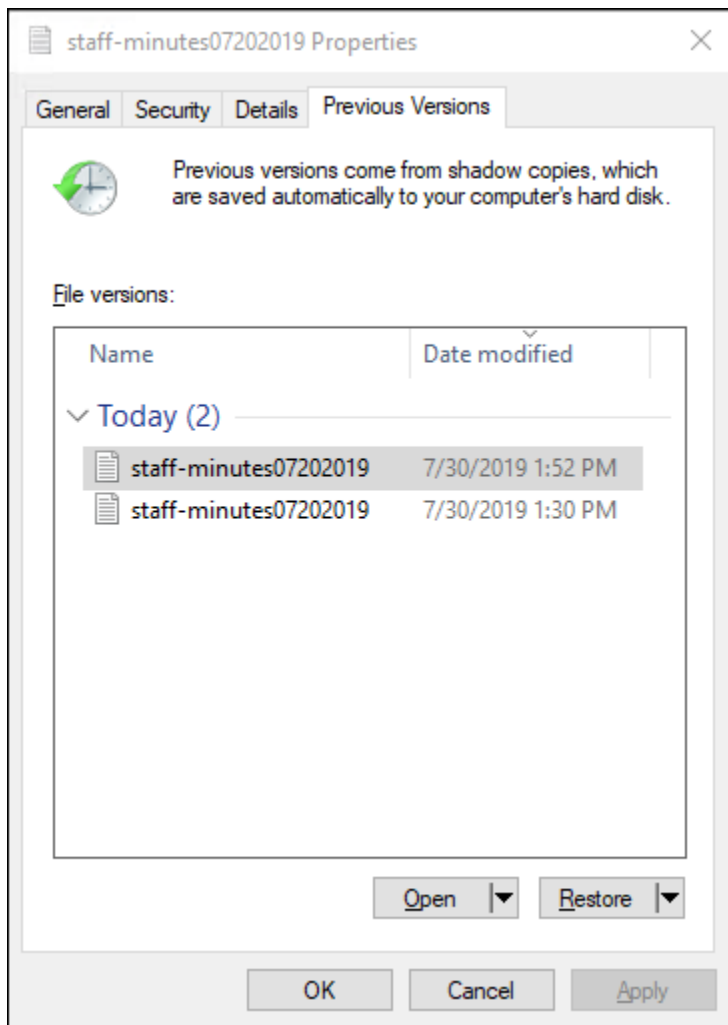
Depois de configurar cópias de sombra em seu sistema de FSx arquivos da Amazon, seus usuários podem restaurar rapidamente versões anteriores de arquivos ou pastas individuais e recuperar arquivos excluídos.

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.





## Configurar cópias de sombra para usar o armazenamento e a programação padrão

Você pode configurar rapidamente as cópias de sombra em seu sistema de arquivos usando a configuração e a programação padrão para cópias 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 sistema de arquivos, a quantidade de armazenamento de cópias de sombra atualmente alocada não será aumentada 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.

## Para definir 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 FSx Administradores AWS Delegados. 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 EC2 do usuário da Amazon.
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 FSx console da Amazon, na seção Rede e Segurança da tela de detalhes do sistema de arquivos ou na resposta da operação da DescribeFileSystem 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 a programação 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 FSx Administradores AWS Delegados. 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 EC2 do usuário da Amazon.

- Defina a programação padrão da 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](#).

## Definir 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 até o qual as cópias de sombra podem crescer usando os parâmetros -Maxsize ou -Default. O uso de Default define o máximo de 10% da capacidade de armazenamento do sistema de arquivos. Não é possível especificar os parâmetros -Maxsize e -Default 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 [Configurar cópias de sombra para usar o armazenamento e a programação padrão](#).

Para definir a quantidade de armazenamento de cópia de sombra em um sistema FSx de arquivos do 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 `FSxAdministradores AWS Delegados`. 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 EC2 do usuário da Amazon.
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 FSx arquivos da Amazon. `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 FSx console da Amazon, na seção Rede e Segurança da tela de detalhes do sistema de arquivos ou na resposta da operação da `DescribeFileSystem` 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% do volume e o número máximo de cópias de sombra como 20 usando a opção `-Default`.

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
FSx Shadow Storage Configuration
```

| AllocatedSpace | UsedSpace | MaxSpace | MaxShadowCopyNumber |
|----------------|-----------|----------|---------------------|
| -----          | -----     | -----    | -----               |

0

0 32530536858

20

É possível limitar o número máximo de cópias de sombra permitido no sistema de arquivos ao usar o comando `Set-FsxShadowStorage` com o parâmetro `-MaxShadowCopyNumber` e especificar um valor de 1 a 500. Por padrão, o número máximo de cópias de sombra é definido como 20, conforme recomendado pela Microsoft para workloads ativas.

## 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, consulte [Usando a Amazon FSx CLI 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 alocada para cópias de sombra no momento. Inicialmente, esse valor é 0.
- **UsedSpace:** a quantidade de armazenamento, em bytes, usada pelas cópias de sombra no momento. Inicialmente, esse valor é 0.
- **MaxSpace:** a quantidade máxima de armazenamento, em bytes, até a qual o armazenamento de sombra 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 quantidade `UsedSpace` 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 configurada (MaxShadowCopyNumber), a próxima cópia de sombra que você faz substitui 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 de modo automático ou manual, elas usam a quantidade de armazenamento de cópia de sombra que você configurou como o 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 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 [Configurar 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 FSx console da Amazon, na seção Rede e Segurança da tela de detalhes do sistema de arquivos ou na resposta da operação da `DescribeFileSystem` 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

```

## 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, consulte [Usando a Amazon FSx CLI 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 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, consulte [Usando a Amazon FSx CLI 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, consulte [Usando a Amazon FSx CLI 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, consulte [Usando a Amazon FSx CLI 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. Ocorre um erro se você não especificar qual cópia de sombra excluir, se especificar várias cópias IDs de sombra ou se especificar uma ID de cópia de sombra inválida.

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 número específico das cópias de sombra mais antigas em seu sistema de arquivos, atualize seu parâmetro `-MaxShadowCopyNumber` para o número desejado de cópias de sombra que gostaria de manter. No entanto, essa alteração entrará em vigor somente após a captura do snapshot 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                   |

## 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, consulte [Usando a Amazon FSx CLI 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 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, consulte [Usando a Amazon FSx CLI 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.
```

## 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](#)
- [Todas as minhas cópias de sombra estão ausentes](#)
- [Não é possível criar FSx backups da Amazon ou acessar cópias de sombra em um sistema de arquivos restaurado ou atualizado recentemente](#)

### 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

Ter capacidade de I/O desempenho insuficiente em seu sistema de arquivos (por exemplo, porque você está usando armazenamento em HDD, porque a capacidade de armazenamento em HDD esgotou ou porque a capacidade de transferência é insuficiente) pode fazer com que todas as cópias de sombra sejam excluídas pelo Windows Server porque ele não consegue manter as cópias de sombra com a capacidade de desempenho disponível. I/O Considere as seguintes recomendações para ajudar a evitar esse problema:

- Se você estiver usando armazenamento em HDD, use o FSx console da Amazon ou a FSx API da Amazon para passar a usar o armazenamento SSD. Para obter mais informações, consulte [Gerenciar o tipo de armazenamento do seu sistema de arquivos](#).
- 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 obter mais informações, consulte [Recomendações do sistema de arquivos para cópias de sombra](#).

Não é possível criar FSx backups da Amazon ou acessar cópias de sombra em um sistema de arquivos restaurado ou atualizado recentemente

Esse comportamento é esperado. A Amazon FSx reconstrói o estado de cópia de sombra em um sistema de arquivos restaurado recentemente e não permite o acesso a cópias de sombra ou backups enquanto a reconstrução ainda está em andamento.

## Replicação programada usando AWS DataSync

Você pode usar AWS DataSync para agendar a replicação periódica do seu FSx sistema de arquivos do Windows File Server para 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 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 obter mais informações, consulte [Para criar um compartilhamento continuamente disponível \(CA\)](#).

## Configurar as definições de tempo limite do SMB

Conforme descrito em [Processo de failover](#), 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 migrar o armazenamento de arquivos atual para o Amazon FSx

O Amazon FSx para Windows File Server tem os recursos, o desempenho e a compatibilidade para ajudar você a mover sem alterações (lift-and-shift) aplicações empresariais com facilidade para a Nuvem Amazon Web Services. O processo para migrar seu armazenamento on-premises do Microsoft Windows File Server para o FSx para Windows File Server tem as quatro etapas básicas a seguir:

1. Migre seus arquivos para o FSx para Windows File Server. Para obter 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 obter mais informações, consulte [Como migrar configurações de compartilhamento de arquivos on-premises 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 obter mais informações, consulte [Operações de substituição para o Amazon FSx para Windows File Server](#).

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](#)
- [Como migrar configurações de compartilhamento de arquivos on-premises para o Amazon FSx](#)
- [Como migrar a configuração de DNS on-premises para o FSx para Windows File Server](#)
- [Operações de substituição para o Amazon FSx para Windows File Server](#)

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

Para migrar seus arquivos atuais para sistemas de arquivos do FSx para Windows File Server, recomendamos o uso do AWS DataSync, que é um serviço de transferência de dados on-line projetado para simplificar, automatizar e acelerar a cópia de grandes quantidades de dados que



envolvam serviços de armazenamento da AWS. O DataSync copia dados na Internet ou no Direct Connect. Como serviço totalmente gerenciado, o DataSync reduz a necessidade de modificar aplicações, desenvolver scripts ou gerenciar a infraestrutura. Para obter 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.

Execute as etapas a seguir para mover dados de um sistema de arquivos do Amazon FSx usando armazenamento SSD para armazenamento em HDD. (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 obter mais informações, consulte [Como criar backups iniciados pelo usuário](#).
2. Restaure o backup em um sistema de arquivos usando o armazenamento HDD. Para obter mais informações, consulte [Restaurar backups em um novo sistema de arquivos](#).

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

Recomendamos usar o AWS DataSync para transferir dados entre sistemas de arquivos do FSx para Windows File Server. O DataSync é um serviço de transferência de dados que simplifica, automatiza e acelera a movimentação e a replicação de dados entre sistemas de armazenamento on-premises e outros serviços de armazenamento da AWS pela internet ou pelo Direct Connect. O DataSync pode

transferir dados e metadados do sistema de arquivos, como propriedade, carimbos de data e hora e permissões de acesso.

O DataSync oferece suporte à cópia de listas de controle de acesso (ACLs) do NTFS e também à cópia de informações de controle de auditoria de arquivos, também conhecidas como system access control lists (SACL - listas de controle de acesso do sistema) do NTFS, que são usadas por administradores para controlar o registro em log da auditoria das tentativas do usuário de acessar arquivos.

Você pode usar o DataSync para transferir arquivos entre dois sistemas de arquivos do FSx para Windows File Server e também transferir dados para um sistema de arquivos em uma Região da AWS ou conta da AWS diferente. É possível usar o DataSync com sistemas de arquivos do FSx para Windows File Server 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.

No AWS DataSync, um local para o FSx para Windows File Server é um endpoint para um FSx para 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.

O DataSync acessa seu FSx para Windows File Server usando o protocolo Server Message Block (SMB). A autenticação é executada com o nome de usuário e a senha configurada no console do AWS DataSync ou na AWS CLI.

## Pré-requisitos

Para migrar dados para a configuração do Amazon FSx para Windows File Server, você precisa de um servidor e de uma rede que atendam aos requisitos do DataSync. Para obter mais informações, consulte [Requirements for DataSync](#) no Guia do usuário do AWS DataSync.

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 se explica porque as tarefas do DataSync envolvem varreduras de metadados de arquivos que podem esgotar os limites de IOPS de disco dos sistemas de arquivos HDD, ocasionando migrações de execução prolongada e impacto na performance do sistema de arquivos. Para ter mais informações, consulte [Práticas recomendadas para migrar o armazenamento de arquivos atual para o FSx para Windows File Server](#).

Se o conjunto de dados consistir principalmente em arquivos pequenos, com milhões de arquivos, ou se você tiver mais largura de banda da rede disponível do que uma única tarefa do DataSync pode consumir, também poderá acelerar as transferências de dados com uma arquitetura de aumento horizontal da escala. Para obter mais informações, consulte: [Como acelerar as transferências de dados com arquiteturas de aumento da escala na horizontal do AWS DataSync](#).

Você pode monitorar a utilização de E/S de disco do sistema de arquivos usando [Métricas de performance do FSx](#).

## Primeiros passos para migrar arquivos usando o DataSync

Para transferir arquivos de um local de origem para um local de destino usando o DataSync, execute 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 atual on-premises para o FSx para Windows File Server, consulte [Transferência de dados entre um armazenamento autogerenciado e a AWS](#), [Criar um local para SMB](#) e [Criar um local para o Amazon FSx para Windows File Server](#) no Guia do usuário do 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 o DataSync para migrar dados entre dois sistemas de arquivos do 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 o DataSync para dividir sua workload entre dois sistemas de arquivos.

Veja um exemplo de visão geral do processo de migração:

1. Crie locais do DataSync para os sistemas de arquivos de origem e de 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 tarefa do DataSync 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 que você estime a duração do processo de transferência de dados e solucione problemas de erros do DataSync com antecedência.

Para minimizar o tempo de substituição, você pode executar tarefas do DataSync com antecedência, transferindo 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 tarefas do DataSync para serem executadas somente em determinados diretórios ou para incluírem ou excluírem 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: [Como acessar dados usando aliases de DNS](#).

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 processos de tarefas do DataSync, monitore a utilização da performance dos sistemas de arquivos de origem e de destino. Para ter mais informações, consulte: [Monitorar com o Amazon CloudWatch](#).
- Configure o [Monitoramento do DataSync](#) para ajudar no entendimento do progresso das tarefas em andamento. Você também pode enviar logs do DataSync para o grupo do Amazon CloudWatch Logs para ajudar na depuração das tarefas, se encontrar 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 para migração de arquivos com o Robocopy

Antes de começar, faça o seguinte:

- Estabeleça conectividade de rede (usando o Direct Connect ou a VPN) entre o Active Directory on-premises e a VPC na qual você deseja criar o sistema de arquivos do 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 (on-premises ou na AWS) que contém os arquivos atuais 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.

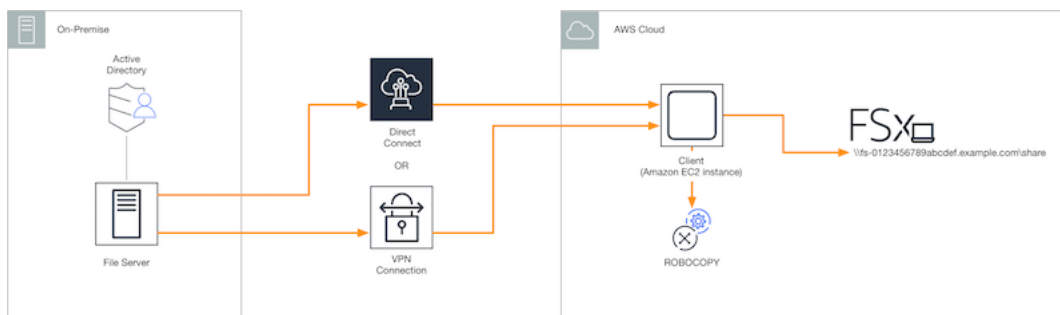
A tabela a seguir resume os requisitos de acessibilidade do sistema de arquivos de origem e de destino para três modelos de acesso do usuário da migração.

| 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 de Operadores de backup do Active Directory on-premises e usar o sinalizador /b com o RoboCopy. | O usuário precisa ser membro do grupo de administradores* do sistema de arquivos do Amazon FSx e usar o sinalizador /b com o 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 do Amazon                                             |

| 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 |
|-----------------------------------------|---------------------------------------------------------------|------------------------------------------------------------------------|
|                                         |                                                               | FSx e usar o sinalizador /b com o RoboCopy                             |

### Note

\* Para sistemas de arquivos associados a um Microsoft AD gerenciado pela AWS, o grupo de administradores do sistema de arquivos do Amazon FSx é Administradores delegados do FSx da AWS. 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 usando o Robocopy

Aplique o seguinte procedimento para migrar os arquivos existentes dos sistemas de arquivos on-premises para os sistemas de arquivos do FSx para Windows File Server.

Para migrar arquivos atuais para o Amazon FSx usando o Robocopy

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 no servidor de arquivos atual (on-premises ou na AWS) para uma letra de unidade (por exemplo, Y:) como



mostrado a seguir. 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 AWS Managed Microsoft AD, 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 para migração de arquivos com o Robocopy](#).

```
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 comando Robocopy a seguir 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 on-premises 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 obter 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 denominado `SmbShares.xml` ao executar os comandos a seguir 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 recurso do AWS Secrets Manager, 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
 amznfsxxxxxxxxxx.corp.com -ErrorVariable errormsg -ScriptBlock { New-FSxSmbShare -
 Credential $Using:credential @Using:param }
}
```

## Como migrar a configuração de DNS on-premises para o FSx para Windows File Server

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 obter 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 [Como associar 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.

## Manage DNS aliases

Associate new DNS aliases

transactions.corp.example.com

Specify up to 50 aliases separated with commas, or put each on a new line.

Associate

### Current DNS aliases (1)

filesystem.domain.name.com

< 1 >

| <input type="checkbox"/> | DNS name                    | Status    |
|--------------------------|-----------------------------|-----------|
| <input type="checkbox"/> | financials.corp.example.com | Available |

If you associate or disassociate DNS aliases, your file system will experience a temporary loss of availability.

Close

- Na caixa Associar novos aliases, insira os aliases de DNS que você deseja associar.
- 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` da CLI ou a operação de API [AssociateFileSystemAliases](#) para associar aliases de DNS a um sistema de arquivos atual.

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 estão sendo associados, use o comando `describe-file-system-aliases` da CLI ([DescribeFileSystemAliases](#) é 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).

## Operações de substituição para o Amazon FSx para Windows File Server

Após migrar o armazenamento de arquivos on-premises, a configuração de compartilhamento de arquivos e a configuração de DNS, a próxima etapa é substituir suas operações para os sistemas de arquivos do FSx para Windows File Server. 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](#)
- [Configurar SPNs para autenticação Kerberos](#)
- [Atualizar os registros CNAME do DNS para o sistema de arquivos do Amazon FSx](#)

## 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 ou o Robocopy. Para obter 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 obter mais informações, consulte [Como migrar configurações de compartilhamento de arquivos on-premises 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.

Instalar o módulo Active Directory para PowerShell necessário

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 o PowerShell como administrador.
3. Instale o módulo Active Directory para PowerShell 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 on-premises para o FSx para Windows File Server](#).

```
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 on-premises para o FSx para Windows File Server](#).
  - 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 on-premises para o FSx para Windows File Server](#).

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 [DescribeFileSystems](#).

- Substitua *alias\_fqdn* pelo alias de DNS completo que você associou ao sistema de arquivos em [Como migrar a configuração de DNS on-premises para o FSx para Windows File Server](#).

```
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 [DescribeFileSystems](#).

```
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 on-premises para o FSx para Windows File Server](#).

 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 [Aplicar a autenticação de Kerberos usando Objetos de política de grupo \(GPOs\)](#) 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.

Instalar os cmdlets necessários do PowerShell

1. Faça login em uma instância do Windows associada ao Active Directory ao qual seu sistema de arquivos do Amazon FSx está associado como um usuário e que seja membro de um grupo que tenha permissões de administração de DNS (Administradores de sistema de nomes de domínio delegados da AWS no AWS Managed Microsoft Active Directory e Administradores de domínio ou outro grupo ao qual você tenha delegado permissões de administração de DNS no Active Directory autogerenciado).

Para obter mais informações, consulte [Conectar-se à sua instância baseada no Windows usando RDP](#) no Guia do usuário do Amazon EC2.

2. Abra o PowerShell como administrador.
3. O módulo do servidor DNS do PowerShell é necessário para a execução das 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 on-premises para o FSx para Windows File Server](#).

# Monitorar sistemas de arquivos do FSx para Windows File Server

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do FSx para Windows File Server e de suas soluções da AWS. Você deve coletar dados de monitoramento de todas as partes de sua solução da AWS para facilitar a depuração de uma falha, caso ela ocorra. No entanto, antes de iniciar o monitoramento do FSx para Windows File Server, é necessário criar um plano 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

- [Monitoramento automático e manual](#)
- [Monitorar com o Amazon CloudWatch](#)
- [Registrar em log as chamadas de API do Amazon FSx para Windows File Server usando o AWS CloudTrail](#)

## Monitoramento automático e manual

A AWS fornece várias ferramentas que você pode usar para monitorar o FSx para Windows File Server. 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 automatizadas para observar o FSx para Windows File Server e gerar relatórios quando algo estiver errado:

- Amazon CloudWatch Alarms: observe uma única métrica ao longo de um período que você especificar e realize uma ou mais ações com base no valor da métrica em relação a um limite ao longo de vários períodos. A ação é uma notificação enviada para um tópico do Amazon Simple Notification Service (Amazon SNS) ou uma política do Amazon EC2 Auto Scaling. Os alarmes do CloudWatch não invocam ações simplesmente por estarem em um estado específico. O estado deve ter sido alterado e mantido por um número específico de períodos. Para obter mais informações, consulte [Monitorar com o Amazon CloudWatch](#).
- Amazon CloudWatch Logs: monitore, armazene e acesse seus arquivos de log do AWS CloudTrail ou de outras origens. Para obter mais informações, consulte [O que é o Amazon CloudWatch Logs?](#) no Guia do usuário do Amazon CloudWatch Logs.
- Monitoramento de log AWS CloudTrail: compartilhe arquivos de log entre contas, monitore os arquivos de log do CloudTrail em tempo real enviando-os para o CloudWatch Logs, escreva aplicações de processamento de logs em Java e confirme se os arquivos de log não foram alterados após a entrega pelo CloudTrail. Para obter mais informações, consulte [Trabalhando com arquivos de log do CloudTrail](#) no Guia do usuário do AWS CloudTrail.

## Ferramentas de monitoramento manual

Outra parte importante do monitoramento do FSx para Windows File Server é o monitoramento manual dos itens que os alarmes do Amazon CloudWatch não abrangem. Os painéis do FSx para Windows File Server, do CloudWatch e de outro console da AWS apresentam uma visão rápida do estado do seu ambiente da AWS.

O painel Monitoramento e desempenho do Amazon FSx mostra:

- Avisos atuais e alarmes do CloudWatch
- Um resumo da atividade do sistema de arquivos
- Capacidade e utilização de armazenamento do sistema de arquivos
- Desempenho do servidor de arquivos e do volume de armazenamento
- Alarmes do CloudWatch

O painel do Amazon CloudWatch mostra:

- Alertas e status atual
- Gráficos de alertas e recursos
- Estado de integridade do serviço

Além disso, é possível usar o 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 procure todas as métricas de recursos da AWS.
- Criar e editar alertas para ser notificado sobre problemas.

Para obter mais informações sobre o painel de Monitoramento e performance do Amazon FSx, consulte [Usar métricas do sistema de arquivos](#).

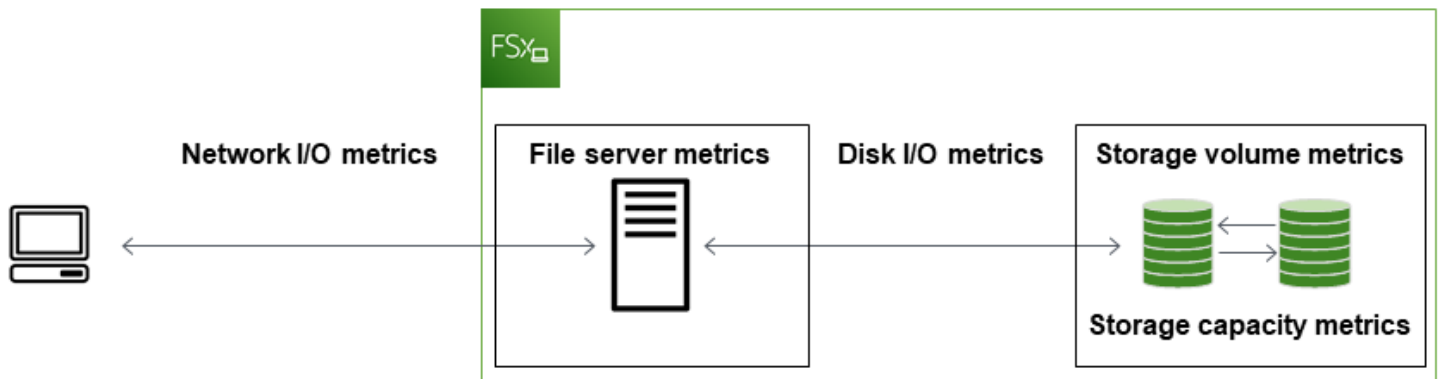
## Monitorar com o Amazon CloudWatch

O Amazon CloudWatch coleta e processa dados brutos do seu FSx para Windows File Server em métricas legíveis e praticamente em tempo real. Essas estatísticas são retidas por um período de 15 meses, proporcionando acesso a informações históricas e ajudando a obter perspectivas sobre o desempenho do seu fluxo de trabalho ou sistema de arquivos.

O FSx para Windows File Server publica métricas do CloudWatch 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 para Windows File Server envia dados de métricas para o CloudWatch em períodos de 1 minuto, com as seguintes exceções que são emitidas em intervalos de 5 minutos:

- FileServerDiskThroughputBalance
- FileServerDiskIopsBalance

Para obter mais informações sobre o CloudWatch, consulte [O que é o Amazon CloudWatch?](#) no Manual do usuário do Amazon CloudWatch.

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 métricas do Amazon FSx CloudWatch são relatadas como Bytes brutos. Os bytes não são arredondados para um múltiplo decimal ou binário da unidade.

## Tópicos

- [Métricas e dimensões do CloudWatch](#)
- [Usar métricas do sistema de arquivos](#)
- [Avisos e recomendações de performance](#)
- [Acesso a métricas de sistema de arquivos](#)
- [Criar alarmes do CloudWatch](#)



## Métricas e dimensões do CloudWatch

O FSx para Windows File Server publica as seguintes métricas no namespace do AWS/FSx no Amazon CloudWatch para todos os sistemas de arquivos:

- DataReadBytes
- DataWriteBytes
- DataReadOperations
- DataWriteOperations
- MetadataOperations
- FreeStorageCapacity

O FSx para Windows File Server publica as métricas descritas nas seções a seguir no namespace do AWS/FSx no Amazon CloudWatch para sistemas de arquivos configurados com uma capacidade de throughput de pelo menos 32 MBps.

### Métricas de E/S de rede

O namespace do AWS/FSx inclui as seguintes métricas de E/S de rede.

| Métrica            | Descrição                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DataReadBytes      | <p>O número de bytes para operações de leitura para clientes que acessam o sistema de arquivos.</p> <p>Unidades: bytes</p> <p>Estatísticas válidas: Sum</p>  |
| DataWriteBytes     | <p>O número de bytes para operações de gravação para clientes que acessam o sistema de arquivos.</p> <p>Unidades: bytes</p> <p>Estatísticas válidas: Sum</p> |
| DataReadOperations | <p>O número de operações de leitura para clientes que acessam o sistema de arquivos.</p>                                                                     |

| Métrica              | Descrição                                                                           |
|----------------------|-------------------------------------------------------------------------------------|
|                      | Unidades: contagem                                                                  |
|                      | Estatísticas válidas: Sum                                                           |
| DataWrite Operations | O número de operações de gravação para clientes que acessam o sistema de arquivos.  |
|                      | Unidades: contagem                                                                  |
|                      | Estatísticas válidas: Sum                                                           |
| MetadataOperations   | O número de operações de metadados para clientes que acessam o sistema de arquivos. |
|                      | Unidades: contagem                                                                  |
|                      | Estatísticas válidas: Sum                                                           |
| ClientConnections    | O número de conexões ativas entre clientes e o servidor de arquivos.                |
|                      | Unidades: contagem                                                                  |

## Métricas do servidor de arquivos

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                                                                                               |

| Métrica                             | Descrição                                                                                                                                                                                                                                                                            |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MemoryUtilization                   | <p>A porcentagem de utilização dos recursos de memória do seu servidor de arquivos.</p> <p>Unidades: percentual</p>                                                                                                                                                                  |
| FileServerDiskThroughputUtilization | <p>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.</p> <p>Unidades: percentual</p>                                                                        |
| FileServerDiskThroughputBalance     | <p>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.</p> <p>Unidades: percentual</p> |
| FileServerDiskIopsUtilization       | <p>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.</p> <p>Unidades: percentual</p>                                                                                |
| FileServerDiskIopsBalance           | <p>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.</p> <p>Unidades: percentual</p>       |

## Métricas de E/S de disco

O namespace do AWS/FSx inclui as seguintes métricas de E/S de disco:

| Métrica             | Descrição                                                                                                                                                           |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskReadBytes       | <p>O número de bytes para operações de leitura que acessam volumes de armazenamento.</p> <p>Unidades: bytes</p> <p>Estatística válida: soma</p>                     |
| DiskWriteBytes      | <p>O número de bytes para operações de gravação que acessam volumes de armazenamento.</p> <p>Unidades: bytes</p> <p>Estatística válida: soma</p>                    |
| DiskReadOperations  | <p>O número de operações de leitura do servidor de arquivos que acessa os volumes de armazenamento.</p> <p>Unidades: contagem</p> <p>Estatísticas válidas: Sum</p>  |
| DiskWriteOperations | <p>O número de operações de gravação do servidor de arquivos que acessa os volumes de armazenamento.</p> <p>Unidades: contagem</p> <p>Estatísticas válidas: Sum</p> |

## 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 | <p>(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.</p> <p>Unidades: percentual</p>  |
| DiskThroughputBalance     | <p>(Somente HDD) A porcentagem de créditos de intermitência disponíveis para o throughput de disco e as IOPS de disco para os volumes de armazenamento.</p> <p>Unidades: percentual</p>                                       |
| DiskIopsUtilization       | <p>(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.</p> <p>Unidades: percentual</p> |

## Métricas da capacidade de armazenamento

O namespace AWS/FSx inclui as seguintes métricas de capacidade de armazenamento.

| Métrica                    | Descrição                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| FreeStorageCapacity        | <p>A quantidade de capacidade de armazenamento disponível.</p> <p>Unidades: bytes</p> <p>Estatísticas válidas: Average, Minimum</p> |
| StorageCapacityUtilization | Capacidade de armazenamento físico usada como porcentagem da capacidade total de armazenamento.                                     |

| Métrica                   | Descrição                                                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | Unidades: percentual                                                                                                                              |
| DeduplicationSavedStorage | A quantidade de espaço de armazenamento economiza da pela eliminação de duplicação dos dados, se ela estiver desabilitada.<br><br>Unidades: bytes |

## Namespace e dimensões para métricas do FSx para Windows File Server

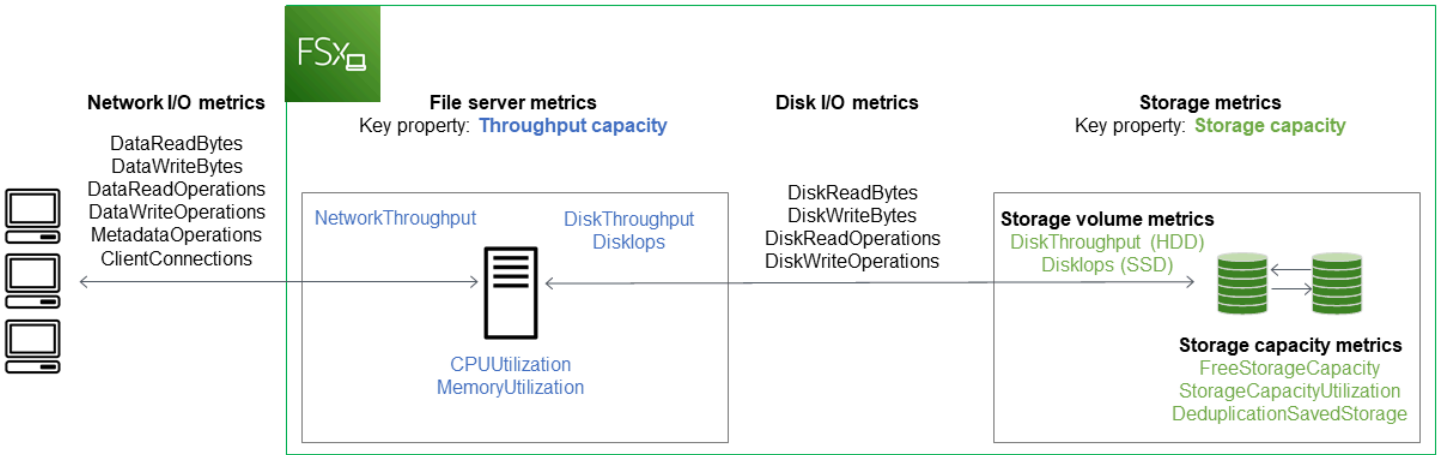
As métricas do FSx para Windows File Server usam o namespace do FSx e fornecem métricas para uma única dimensão, FileSystemId. Você pode encontrar o ID de um sistema de arquivos usando o comando da CLI AWS CLI [describe-file-systems](#) ou o comando da API [DescribeFileSystems](#). O ID do sistema de arquivos possui o formato de *fs-0123456789abcdef0*.

## Usar métricas do sistema de arquivos

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 para Windows File Server relata métricas no CloudWatch que rastreiam a performance 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 do Amazon FSx com seus componentes arquitetônicos e as métricas de performance e recursos do CloudWatch 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 performance no console do Amazon FSx para visualizar as métricas do FSx para Windows File Server CloudWatch 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                          | $\text{SOMA}(\text{DataReadOperations} + \text{DataWriteOperations} + \text{MetadataOperations}) / \text{Período (em segundos)}$ |
|                                       | ...determinar o throughput total do meu sistema de arquivos?                                     | Throughput total                       | $\text{SOMA}(\text{DataReadBytes} + \text{DataWriteBytes}) / \text{Período (em segundos)}$                                       |
|                                       | ...determinar a quantidade da capacidade de armazenamento disponível no meu sistema de arquivos? | Capacidade de armazenamento disponível | FreeStorageCapacity                                                                                                              |

| Painel de monitoramento e performance | Como faço para...                                                                                                                                           | Gráfico                                                            | Métricas relevantes                       |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-------------------------------------------|
|                                       | ...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 <sup>1</sup> |



| 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 <sup>1</sup> |
|                                       | ...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 e as IOPS de operações que acessam volumes de armazenamento em HDD?                       | Equilíbrio de intermitência do throughput do disco (HDD) | DiskThroughputBalance <sup>2</sup>                                                                                                                                 |
|                                       | ...determinar a IOPS para operações que acessam volumes de armazenamento, como uma porcentagem do limite provisionado determinado pela capacidade de armazenamento em HDD?       | Utilização de IOPS do disco (HDD)                        | $\text{SUM}(\text{DiskReadOperations} + \text{DiskWriteOperations}) / \text{Period}$ (em segundos) / (12 * capacidade de armazenamento em HDD provisionada em TiB) |

| Painel de monitoramento e performance | Como faço para...                                                                                                                                                       | Gráfico                           | Métricas relevantes |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|---------------------|
|                                       | ...determinar a IOPS para operações que acessam volumes de armazenamento, como uma porcentagem do limite provisionado determinado pela capacidade de armazenamento SSD? | Utilização de IOPS do disco (SSD) | DiskIopsUtilization |

### Note

<sup>1</sup>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).

<sup>2</sup>Volumes de armazenamento em HDD podem sofrer variações significativas de desempenho, dependendo da workload. Picos repentinos nas IOPS ou no throughput podem levar à degradação do desempenho do disco. Para obter mais informações, consulte [Desempenho da expansão do HDD](#).

## 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 métricas do CloudWatch 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 performance ativos ou recentes do Amazon FSx e todos os alarmes do CloudWatch configurados para o sistema de arquivos que estão em um estado de ALARME aparecem no painel Monitoramento e performance na seção Resumo. O aviso também aparece na seção do painel em que o gráfico de métricas é exibido.

Você pode criar alarmes do CloudWatch para qualquer uma das métricas do Amazon FSx. Para obter mais informações, consulte [Criar alarmes do CloudWatch](#).

## 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                                                   |                                                                                                                  |
| Servidor de arquivos > IOPS de disco: utilização                                 |                                                                                                                  |
| Servidor de arquivos > Throughput de disco: utilização                           | <a href="#">Aumentar a capacidade de throughput</a>                                                              |
| Servidor de arquivos > IOPS de disco - equilíbrio de intermitência               |                                                                                                                  |
| Servidor de arquivos > Throughput de disco: equilíbrio de intermitência          |                                                                                                                  |
| Utilização da capacidade de armazenamento                                        | <a href="#">Aumentar a capacidade de armazenamento</a>                                                           |
| Volume de armazenamento > Throughput de disco: utilização (HDD)                  | <a href="#">Aumentar a capacidade de armazenamento</a> ou <a href="#">mudar para o tipo de armazenamento SDD</a> |
| Volume de armazenamento > Throughput de disco: equilíbrio de intermitência (HDD) |                                                                                                                  |

| Se houver um aviso para essa métrica                      | Faça o seguinte                        |
|-----------------------------------------------------------|----------------------------------------|
| Volume de armazenamento > IOPS de disco: utilização (SSD) | <a href="#">Aumentar a IOPS do SSD</a> |

#### 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 obter mais informações, consulte [Como gerenciar a capacidade de throughput](#).

Para obter mais informações sobre a performance do sistema de arquivos, consulte [desempenho do FSx para Windows File Server](#).

## Acesso a métricas de sistema de arquivos

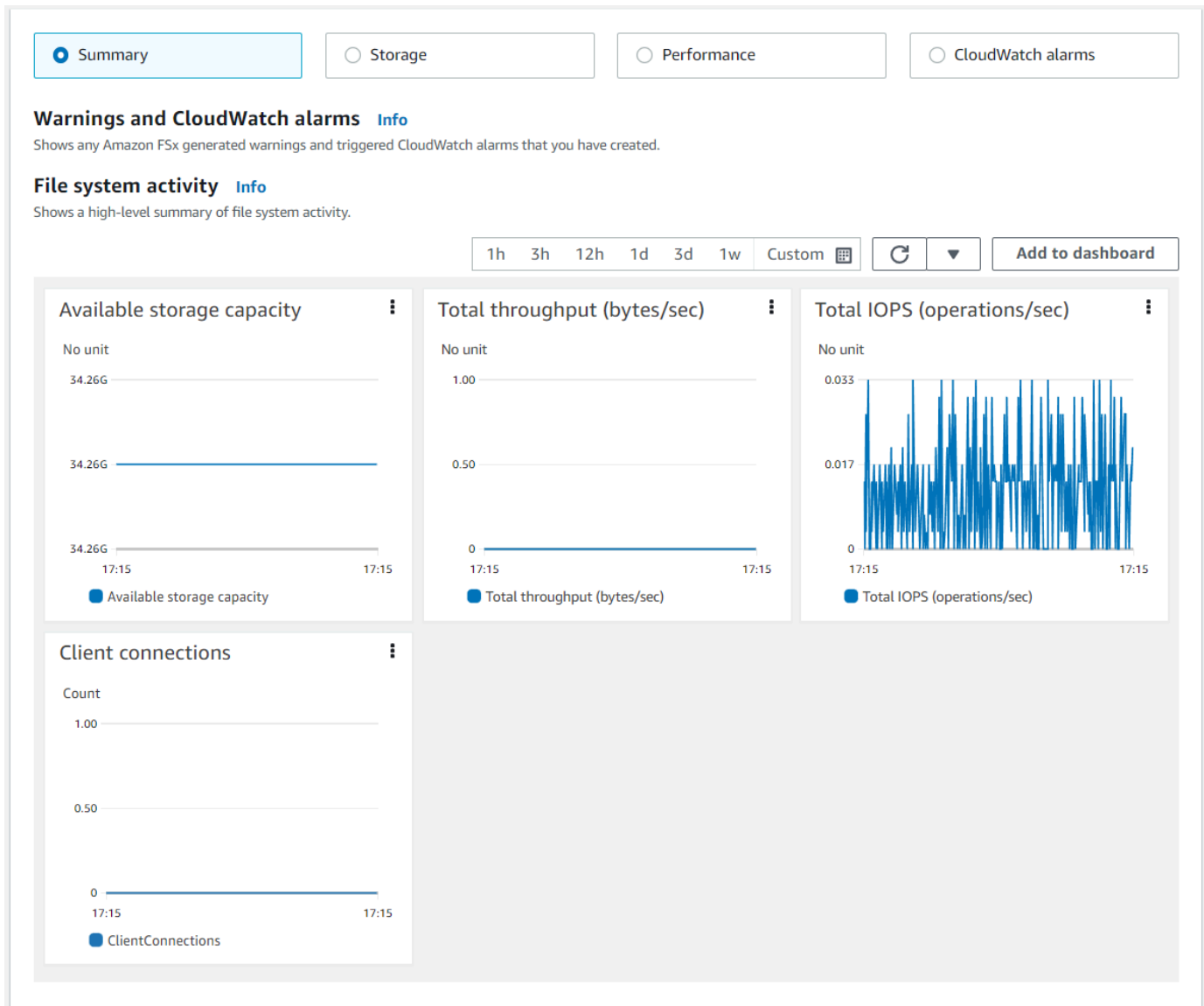
Você pode visualizar as métricas do Amazon FSx para o CloudWatch das seguintes maneiras:

- O console do Amazon FSx
- O console do CloudWatch
- A CLI do CloudWatch
- A API do CloudWatch

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.



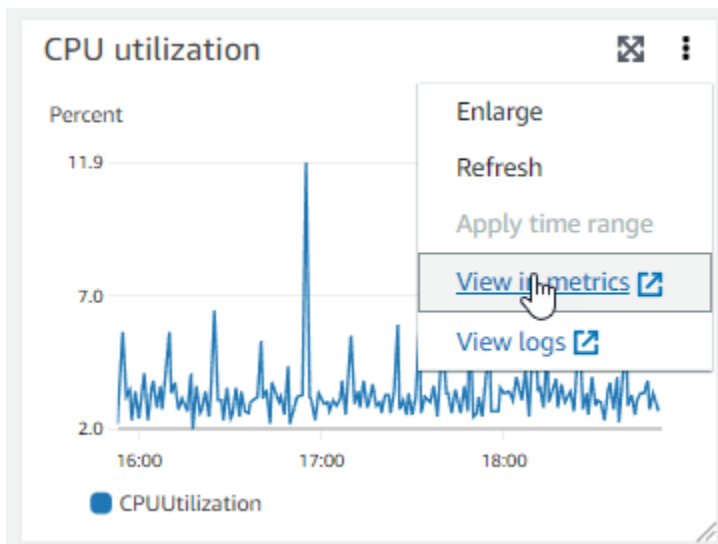
- As métricas de Resumo são exibidas por padrão, mostrando todos os avisos ativos e alarmes do CloudWatch, juntamente com as métricas de Atividade do sistema de arquivos.

- 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.
- Selecione Alarmes do CloudWatch para visualizar gráficos de todos os alarmes configurados para o sistema de arquivos.

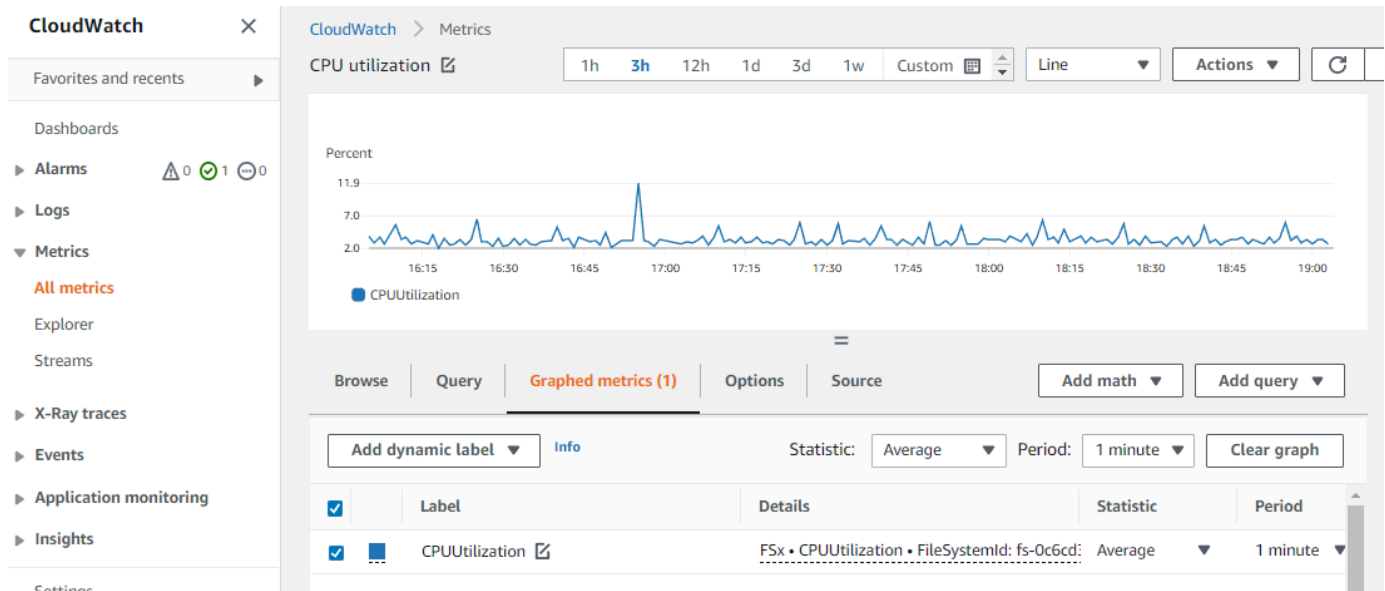
Para obter mais informações, consulte . [Usar métricas do sistema de arquivos](#)

Para exibir métricas no console do CloudWatch

1. Para visualizar uma métrica de sistema de arquivos na página Métricas do console do Amazon CloudWatch, navegue até a métrica no painel Monitoramento e performance do console do 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 console do CloudWatch, mostrando o gráfico de métricas, conforme mostrado na imagem a seguir.



## Adicionar métricas a um painel do CloudWatch

1. Para adicionar um conjunto de métricas do sistema de arquivos do FSx para Windows a um painel no console do CloudWatch, escolha o conjunto de métricas (Resumo, Armazenamento ou Desempenho) no painel Monitoramento e desempenho do console do Amazon FSx.
2. Selecione Adicionar ao painel no canto superior direito do painel, o que abre o console do CloudWatch.
3. Selecione um painel existente do CloudWatch na lista ou crie um novo. Para obter mais informações, consulte [Utilizar painéis do Amazon CloudWatch](#) no Manual do usuário do Amazon CloudWatch.

## Para acessar as métricas a partir da AWS CLI

- Use o comando [list-metrics](#) com o namespace `--namespace "AWS/FSx"`. Para obter mais informações, consulte a [Referência de comandos da AWS CLI](#).

```
$ aws cloudwatch list-metrics --namespace "AWS/FSx"
aws cloudwatch list-metrics --namespace "AWS/FSx"
{
 "Metrics": [
 {
 "Namespace": "AWS/FSx",
 "MetricName": "DataWriteOperationTime",
 "Dimensions": [
```



```

 {
 "Name": "FileSystemId",
 "Value": "fs-09a106ebc3a0bb087"
 }
],
},
{
 "Namespace": "AWS/FSx",
 "MetricName": "CapacityPoolWriteBytes",
 "Dimensions": [
 {
 "Name": "VolumeId",
 "Value": "fsvol-0cb2281509f5db3c2"
 },
 {
 "Name": "FileSystemId",
 "Value": "fs-09a106ebc3a0bb087"
 }
]
},
{
 "Namespace": "AWS/FSx",
 "MetricName": "DiskReadBytes",
 "Dimensions": [
 {
 "Name": "FileSystemId",
 "Value": "fs-09a106ebc3a0bb087"
 }
]
},
{
 "Namespace": "AWS/FSx",
 "MetricName": "CompressionRatio",
 "Dimensions": [
 {
 "Name": "FileSystemId",
 "Value": "fs-0f84c9a176a4d7c92"
 }
]
},
.
.
.
```

```
}
```

## Como usar a API do CloudWatch

### Acessar as métricas com a API do CloudWatch

- Chame [GetMetricStatistics](#). Para obter mais informações, consulte a [Referência da API do Amazon CloudWatch](#).

## Criar alarmes do CloudWatch

Você pode criar um alarme do CloudWatch que envia uma mensagem do Amazon SNS quando o alarme muda de estado. Um alarme observa uma única métrica ao longo de um período especificado por você e realiza uma ou mais ações com base no valor da métrica relativo a um determinado limite ao longo de vários períodos. A ação é uma notificação enviada para um tópico do Amazon SNS ou uma política de Auto Scaling.

Os alertas invocam ações apenas para alterações de estado mantidas. Os alarmes do CloudWatch não invocam ações simplesmente por estarem em um estado específico. O estado deve ter sofrido alteração e deve ter sido mantido por um determinado número de períodos. É possível criar um alarme no console do Amazon FSx ou no console do CloudWatch.

Os procedimentos a seguir descrevem como criar alarmes para o Amazon FSx usando o console, a AWS CLI, e a API.

### Para definir um alarme do CloudWatch (console)

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. Selecione os alarmes do CloudWatch.
6. Escolha Criar alarme do CloudWatch. 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 equivocadas nas condições de alarmes e configurar os alarmes para que sejam resilientes a pontos de dados ausentes, consulte [Configurar como os alarmes do CloudWatch tratam dados ausentes](#) no Guia do usuário do Amazon CloudWatch.

11. Se quiser que o CloudWatch envie a você uma notificação por e-mail ou SNS quando o estado de alarme acionar a ação, selecione um estado de alarme para Sempre que esse estado de alarme ocorrer.

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 alertas usando o console do CloudWatch

1. Faça login no Console de gerenciamento da AWS e abra o console do CloudWatch 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 que o CloudWatch envie um e-mail quando o estado do alarme for atingido, em Sempre que este alarme, escolha Estado ALARM. Em Enviar notificação para, escolha um tópico do SNS existente. Se 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 Criar Alarm.

## Para definir um alarme do CloudWatch (CLI)

- Chame [put-metric-alarm](#). Para obter mais informações, consulte Referência de comandos da [AWS CLI](#).

## Para definir um alarme (API)

- Chame [PutMetricAlarm](#). Para obter mais informações, consulte a [referência de APIs do Amazon CloudWatch](#).

# 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 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 [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 eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especifica. Além disso, é possível configurar outros AWS serviços para melhor analisar e agir de acordo com dados coletados do evento nos logs CloudTrail. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [Serviços e integrações compatíveis com o CloudTrail](#)
- [Configuração 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 às 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 usuário do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

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 Amazon S3 especificado. Os arquivos de log CloudTrail contêm uma ou mais entradas de log.

Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros da solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública, portanto, não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a operação `TagResource` quando uma tag para um sistema de arquivos é criada no console.

```
{
 "eventVersion": "1.05",
 "userIdentity": {
 "type": "Root",
 "principalId": "111122223333",
 "arn": "arn:aws:sts::111122223333:root",
 "accountId": "111122223333",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
 "attributes": {
 "mfaAuthenticated": "false",
 "creationDate": "2018-11-14T22:36:07Z"
 }
 }
 }
}
```

```

 }
 },
 "eventTime": "2018-11-14T22:36:07Z",
 "eventSource": "fsx.amazonaws.com",
 "eventName": "TagResource",
 "awsRegion": "us-east-1",
 "sourceIPAddress": "192.0.2.0",
 "userAgent": "console.amazonaws.com",
 "requestParameters": {
 "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
 },
 "responseElements": null,
 "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
 "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
 "eventType": "AwsApiCall",
 "apiVersion": "2018-03-01",
 "recipientAccountId": "111122223333"
}

```

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `UntagResource` quando uma tag para um sistema de arquivos é excluída do console.

```

{
 "eventVersion": "1.05",
 "userIdentity": {
 "type": "Root",
 "principalId": "111122223333",
 "arn": "arn:aws:sts::111122223333:root",
 "accountId": "111122223333",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
 "attributes": {
 "mfaAuthenticated": "false",
 "creationDate": "2018-11-14T23:40:54Z"
 }
 }
 },
 "eventTime": "2018-11-14T23:40:54Z",
 "eventSource": "fsx.amazonaws.com",
 "eventName": "UntagResource",

```

```
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "console.amazonaws.com",
"requestParameters": {
 "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
},
"responseElements": null,
"requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
"eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
"eventType": "AwsApiCall",
"apiVersion": "2018-03-01",
"recipientAccountId": "111122223333"
}
```



# Segurança na 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 [programas de conformidade da AWS](#). Para saber mais sobre os programas de conformidade que se aplicam ao Amazon FSx para Windows File Server, consulte [AWS Services in Scope by Compliance Program](#).
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa 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 Windows File Server para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Amazon FSx para Windows File Server.

## Tópicos

- [Proteção de dados no Amazon FSx para Windows File Server](#)
- [Controle de acesso em nível de arquivo e pasta usando o Windows ACLs](#)
- [Controle de acesso ao sistema de arquivos com a Amazon VPC](#)
- [Como registrar em log o acesso de usuário final com auditoria de acesso a arquivos](#)
- [Gerenciamento de identidade e acesso para Amazon FSx para Windows File Server](#)
- [Validação de conformidade do Amazon FSx para Windows File Server](#)
- [Amazon FSx para Windows File Server e endpoints da VPC da interface](#)

# Proteção de dados no Amazon FSx para Windows File Server

O [modelo de responsabilidade compartilhada](#) da AWS se aplica à proteção de dados no Amazon FSx para Windows File Server. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Data Privacy FAQ](#). Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and RGPD](#) no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da Conta da AWS e configure as contas de usuário individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure os logs de API e atividade do usuário com AWS CloudTrail. Para obter informações sobre como usar as trilhas do CloudTrail para capturar atividades da AWS, consulte [Working with CloudTrail trails](#) no Guia do usuário do AWS CloudTrail.
- Use as soluções de criptografia AWS, juntamente com todos os controles de segurança padrão em Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar a AWS por meio de uma interface de linha de comandos ou de uma API, use um endpoint do FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-3](#).

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o FSx para Windows File Server ou com outros Serviços da AWS usando o console, a API, a AWS CLI ou os AWS SDKs. Quaisquer dados inseridos em tags ou em

campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

## Criptografia de dados no FSx para Windows File Server

O Amazon FSx para Windows File Server oferece suporte à criptografia de dados em repouso e dados em trânsito. A criptografia de dados em repouso é habilitada automaticamente ao criar um sistema de arquivos do Amazon FSx. A criptografia de dados em trânsito é compatível com compartilhamentos de arquivos mapeados em uma instância de computação que seja compatível com o protocolo SMB 3.0 ou mais recente. 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 seu sistema usando a criptografia de dados em trânsito.

Se sua organização estiver sujeita a políticas corporativas ou regulatórias que exigem criptografia de dados e metadados em repouso, seus dados serão automaticamente criptografados em repouso. É recomendável também que você habilite a criptografia de dados em trânsito montando seu sistema de arquivos com o uso da criptografia de dados em trânsito.

### Criptografia de dados 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 chaves da AWS 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 o AWS KMS

O Amazon FSx integra-se ao AWS KMS para gerenciamento de chaves. O Amazon FSx usa um AWS KMS key para criptografar seu sistema de arquivos. Você escolhe a chave do KMS usada para criptografar e descriptografar 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 [Criar chaves](#) no Guia do desenvolvedor do AWS Key Management Service.

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 [Rotating AWS KMS keys](#) no Guia do desenvolvedor do AWS Key Management Service.

## Políticas de chave do Amazon FSx para o AWS KMS

Políticas de chaves são a principal maneira de controlar o acesso a chaves do KMS. Para obter mais informações sobre as políticas de chaves, consulte [Using key policies in AWS KMS](#) no Guia do desenvolvedor do AWS Key Management Service. A lista a seguir descreve todas as permissões relacionadas ao AWS KMS com suporte do 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 não criptografado 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 do KMS, sem a necessidade de expor o texto simples dos dados no lado do cliente. Primeiro os dados são descriptografados e, depois, recriptografados. Essa permissão está incluída na política de chaves padrão.
- kms:GenerateDataKeyWithoutPlaintext: (obrigatório) retorna uma chave de criptografia de dados criptografada em uma chave do KMS. Essa permissão está incluída na política de chave padrão, em kms:GenerateDataKey\*.
- kms:CreateGrant - (Obrigatório) Adiciona uma concessão a uma chave para especificar quem pode usar a chave e em que condições. Concessões são mecanismos de permissão alternativos para políticas de chaves. Para obter mais informações sobre concessões, consulte [Uso de concessões](#) no Guia do desenvolvedor do AWS Key Management Service. Essa permissão está incluída na política de chaves padrão.
- kms:DescribeKey: (obrigatório) fornece informações detalhadas sobre a chave do KMS especificada. Essa permissão está incluída na política de chaves padrão.
- kms:ListAliases: (opcional) lista todos os aliases de chaves na conta. Quando você usa o console para criar um sistema de arquivos criptografado, essa permissão preenche a lista de chaves do KMS. Recomendamos usar essa permissão para proporcionar a melhor experiência do usuário. Essa permissão está incluída na política de chaves padrão.

## Criptografia de dados em trânsito

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 os dados em trânsito, você pode limitar o acesso ao sistema de arquivos para permitir o acesso apenas a clientes que são compatíveis com a 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.

## Como gerenciar criptografia em trânsito

Você pode usar um conjunto de comandos personalizados do PowerShell para controlar a criptografia dos dados em trânsito entre o sistema de arquivos do FSx para 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 os dados em trânsito sejam sempre criptografados. Quando a imposição é ativada para criptografia de dados em trânsito, 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 de dados em trânsito no nível do compartilhamento de arquivos, em vez de no 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 em trânsito em seu sistema de arquivos usando a CLI do Amazon FSx para gerenciamento remoto no PowerShell. Para saber como usar essa CLI, consulte [Usando a Amazon FSx CLI 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). Na resposta do sistema, você pode escolher a criptografia nas configurações de trânsito do sistema de arquivos com base nos valores das propriedades <code>EncryptData</code> e <code>RejectUnencryptedAccess</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Set-FSxSmbServerConfiguration                         | <p>Esse comando tem duas opções para configurar globalmente a criptografia em trânsito no sistema de arquivos:</p> <ul style="list-style-type: none"> <li>• <code>-EncryptData \$True \$False</code> : defina esse parâmetro como <code>True</code> para ativar a criptografia de dados em trânsito. Defina esse parâmetro como <code>False</code> para desativar a criptografia de dados em trânsito.</li> <li>• <code>-RejectUnencryptedAccess \$True \$False</code> : defina esse parâmetro como <code>True</code> para impedir que clientes não compatíveis com criptografia acessem o sistema de arquivos. Defina esse parâmetro como <code>False</code> para permitir que clientes não compatíveis com criptografia acessem o sistema de arquivos.</li> </ul> |
| Set-FSxSmbShare -name <i>name</i> -EncryptData \$True | Defina esse parâmetro como <code>True</code> para ativar a criptografia de dados em trânsito para o compartilhamento. Defina esse parâmetro como <code>False</code> para desativar a criptografia de dados em trânsito para o 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 `-?`, por exemplo `Get-FSxSmbServerConfiguration -?`.

## Controle de acesso em nível de arquivo e pasta usando o Windows ACLs

O Amazon FSx para Windows File Server oferece suporte à autenticação baseada em identidade pelo 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 na Amazon FSx, consulte [Trabalhar com o Microsoft Active Directory](#).

Suas instâncias computacionais associadas ao domínio podem acessar compartilhamentos de FSx arquivos da Amazon usando as credenciais do Active Directory. Você usa listas de controle de acesso padrão do Windows (ACLs) para um controle de acesso refinado em nível de arquivo e pasta. Os sistemas de FSx arquivos da Amazon verificam automaticamente as credenciais dos usuários que acessam os dados do sistema de arquivos para aplicar esses Windows. ACLs

Todo sistema de FSx arquivos da Amazon vem com um compartilhamento de arquivos padrão do Windows chamado `share`. O Windows ACLs dessa pasta compartilhada está configurado para permitir o read/write acesso 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 o ACLs, você pode mapear o compartilhamento como um usuário que é membro do grupo de administradores delegados.

#### Warning

A Amazon FSx exige que o usuário SYSTEM tenha permissões NTFS ACL de controle total 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 .
- [Etapa 1. Configurar um Active Directory.](#)

## Controle de acesso ao sistema de arquivos com a Amazon VPC

Você acessa seu sistema de FSx arquivos da Amazon 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 FSx arquivos da Amazon por meio do nome Domain Name Service (DNS). 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 Direct Connect ou VPN ou recursos dentro do peering VPCs 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.

FSx para Windows, o File Server oferece suporte ao compartilhamento de VPC, o que permite que você visualize, crie, modifique e exclua recursos em uma sub-rede compartilhada em uma VPC de propriedade de outra conta. AWS Para obter mais informações, consulte Como [trabalhar com o Shared VPCs](#) 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.

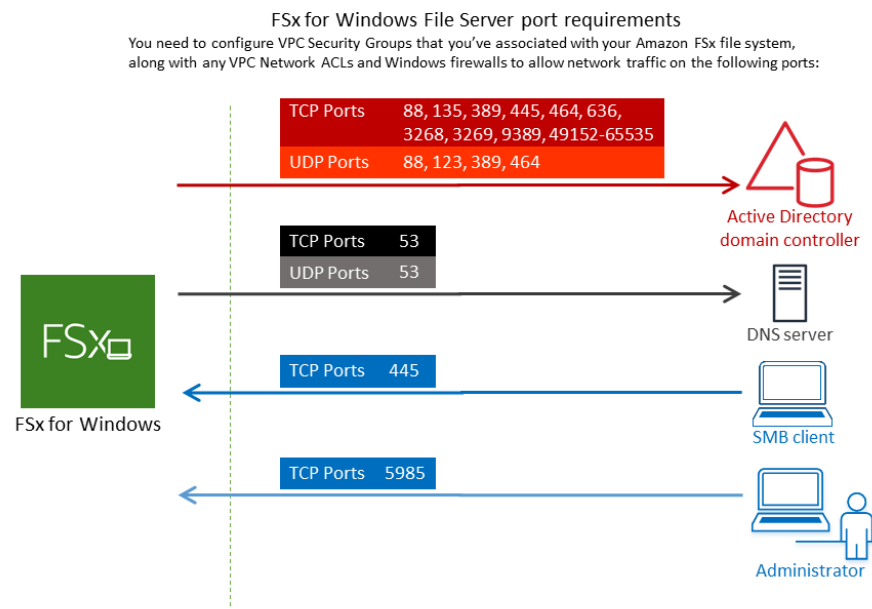
Para usar um grupo de segurança para controlar o acesso ao seu sistema de FSx arquivos da Amazon, adicione regras de entrada e saída. As regras de entrada controlam o tráfego de entrada

e as regras de saída controlam o tráfego de saída do sistema de arquivos. Certifique-se de ter as regras de tráfego de rede corretas em seu grupo de segurança para mapear o compartilhamento de FSx arquivos do sistema de arquivos da Amazon em uma pasta na sua instância computacional compatível.

Para obter mais informações sobre regras de grupos de segurança, consulte [Regras de grupos de segurança](#) no Guia EC2 do usuário da Amazon.

Para criar um grupo de segurança para a Amazon FSx

1. Abra o EC2 console da Amazon 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 a rede VPC da (s) sub-rede ACLs (s) em que você está criando seu sistema de FSx arquivos permitam tráfego nas portas e nas direções mostradas no diagrama a seguir.



A tabela a seguir identifica o perfil de cada porta.

| Protocolo | Portas | Perfil                                                         |
|-----------|--------|----------------------------------------------------------------|
| 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)                                    |
| TCP       | 135    | Distributed Computing Environment/End Point Mapper (DCE/EPMAP) |
| TCP       | 445    | Compartilhamento de arquivos de SMB para serviços de diretório |
| TCP       | 636    | LDAPS TLS/SSL (Lightweight Directory Access Protocol over)     |

| Protocolo | Portas        | Perfil                                                |
|-----------|---------------|-------------------------------------------------------|
| 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, servidores DNS, clientes e administradores do AD. FSx FSx

 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, a maioria dos firewalls do Windows e da rede VPC ACLs exigem que as portas sejam abertas em ambas as direções.

 Note

Se você tiver sites do Active Directory definidos, você deve ter certeza de que as sub-redes na VPC associadas ao seu sistema de arquivos da FSx Amazon estejam definidas em um site do Active Directory e que não existam 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.

 **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 o tráfego do seu sistema de FSx arquivos da Amazon. 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 seu sistema de FSx arquivos Amazon.

Para associar um grupo de segurança ao seu sistema de FSx arquivos da Amazon

1. Abra o FSx console da Amazon 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 proibir temporariamente o acesso de todos os clientes à rede ao seu sistema de arquivos, você pode remover todos os grupos de segurança associados à (s) interface (s) elástica (s) de rede do seu sistema de arquivos e substituí-los por um grupo sem inbound/outbound regras.

## Rede Amazon VPC ACLs

Outra opção para proteger o acesso ao sistema de arquivos em sua VPC é estabelecer listas de controle de acesso à rede (ACLsrede). ACLs As redes são separadas dos grupos de segurança, mas têm funcionalidades semelhantes para adicionar uma camada adicional de segurança aos recursos em sua VPC. Para obter mais informações sobre rede ACLs, consulte [Rede ACLs](#) no Guia do usuário da Amazon VPC.

## Como registrar em log o acesso de usuário final com auditoria de acesso a arquivos

O Amazon FSx para 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 logs de eventos de auditoria de um sistema de arquivos para outros serviços da AWS que oferecem um conjunto avançado de recursos. Isso inclui permitir consultar, processar, armazenar e arquivar logs, emitir notificações e acionar ações para aprimorar 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](#).

### Note

A auditoria de acesso a arquivos é suportada somente em sistemas FSx de arquivos Windows com uma capacidade de taxa de transferência de 32 MBps ou mais. Você pode modificar a capacidade de throughput em sistemas de arquivos existentes. Para obter mais informações, consulte [Como gerenciar a capacidade de throughput](#).

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). Se você já tem 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 Amazon FSx para Windows File Server e migrando seus dados.

A 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, a Amazon FSx suporta o registro de tentativas bem-sucedidas (como um usuário com permissões suficientes acessando com sucesso 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 estiver habilitada. 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](#)
- [Como migrar seus controles de auditoria](#)
- [Como visualizar logs de eventos](#)

- [Como configurar os controles de auditoria de arquivos e pastas](#)
- [Como gerenciar a auditoria de acesso a arquivos](#)

## Destinos dos logs de eventos de auditoria

Ao habilitar a auditoria de acesso a arquivos, você deve configurar um AWS serviço para o qual a 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 registros de eventos de auditoria ao criar seu sistema de arquivos Amazon FSx para Windows File Server ou a qualquer momento ao atualizar um sistema de arquivos existente. Para obter 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 o Amazon Data Firehose se quiser transmitir continuamente eventos 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 análises adicionais.

Por padrão, a Amazon FSx criará e usará um grupo padrão de CloudWatch registros de 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, a Amazon FSx poderá criar e usar um fluxo de registros padrão no grupo de CloudWatch `/aws/fsx/windows` registros de 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 fluxo de entrega do Firehose deve começar com o prefixo `aws-fsx-`. Caso não tenha um fluxo de entrega existente do Firehose, você poderá criar um ao criar ou atualizar seu sistema de arquivos no console.
- O fluxo de entrega do Firehose deve ser configurado para usar `Direct PUT` como sua fonte. Você não pode usar um fluxo de dados existente do Kinesis como fonte de dados para seu fluxo de entrega.
- O destino (o grupo de CloudWatch registros do Logs ou o stream de entrega do Firehose) deve estar na mesma AWS partição e Conta da AWS no sistema de FSx arquivos da Amazon. 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 de logs de eventos de auditoria são entregues aos destinos em minutos, mas, às vezes, podem demorar um pouco. 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 FSx arquivos da Amazon e migrar seus dados para seu novo sistema de arquivos. Recomendamos usar AWS DataSync para transferir dados e os associados SACLs ao seu sistema de FSx arquivos da Amazon. Como solução alternativa, você pode usar o Robocopy (Robust File Copy). Para obter mais informações, consulte [Como migrar o armazenamento de arquivos atual para o Amazon FSx](#).

## Como visualizar logs de eventos

Você pode visualizar os registros de eventos de auditoria depois FSx que a Amazon começar a emití-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 visualizar os logs de eventos de auditoria no Firehose. No entanto, você pode configurar o Firehose para encaminhar os logs para um destino no qual 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 SystemTime refere-se à hora em que o evento foi gerado no sistema e exibido no formato <AAAA-MM-:mm:ss.s>Z. DDThh
- 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).
- AccessList refere-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 |

| Tipo de acesso             | Máscara de acesso | Valor  |
|----------------------------|-------------------|--------|
| 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 write/append dados de um arquivo, que podem ser interpretados a partir de `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;0ICI;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;0ICI;FA;;;SY)
(A;0ICI;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.

## Como configurar os controles de auditoria de arquivos e pastas

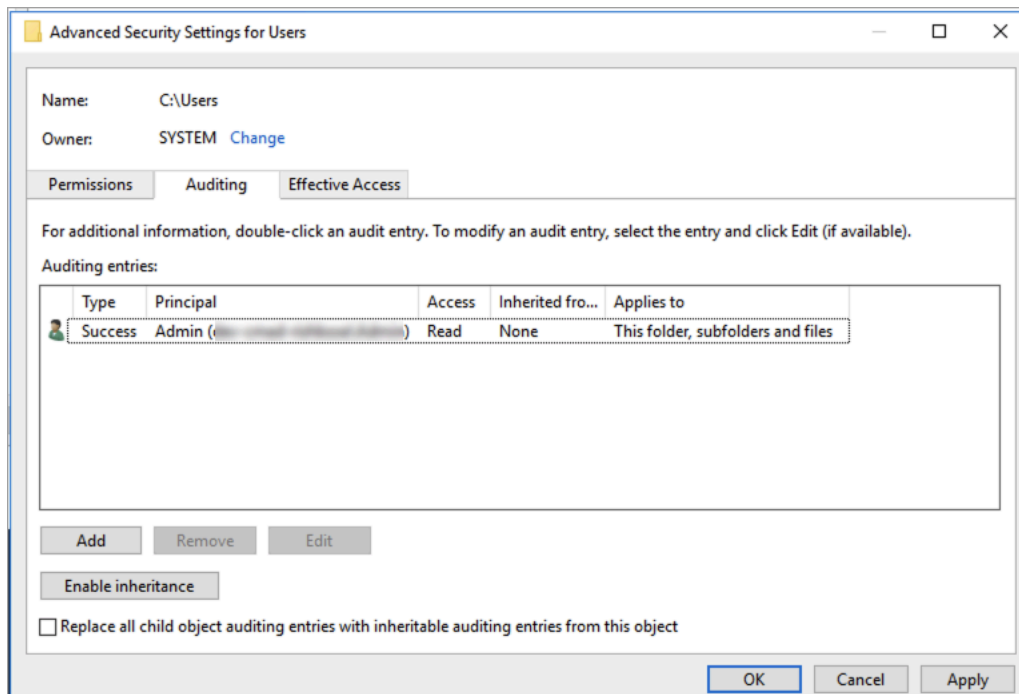
Você precisa definir controles de auditoria nos arquivos e pastas que você deseja auditar quanto a tentativas de acesso do usuário. Os controles de auditoria também são conhecidos como listas de controle de acesso do sistema NTFS (SACLs).

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 ativar a auditoria de acesso a arquivos ao criar um novo sistema de arquivos Amazon FSx para Windows File Server. A auditoria de acesso a arquivos é desativada por padrão quando você cria um sistema de arquivos a partir do FSx console da Amazon.

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 FSx console ou a AWS CLI API da Amazon.

**Note**

A auditoria de acesso a arquivos é suportada somente nos sistemas de arquivos Amazon FSx para Windows File Server com uma capacidade de taxa de transferência de 32 MBps ou mais. Você não pode criar ou atualizar um sistema de arquivos com uma capacidade de transferência inferior a 32 MBps 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 obter 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 FSx console da Amazon em <https://console.aws.amazon.com/fsx/>.
2. Siga o procedimento para a criação de um novo sistema de arquivos descrito na [Etapa 5. Criar 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.

**▼ Auditing - optional**

**Log access to files and folders** [Info](#)  
Once you enable logging here, Windows generates audit logs for files and folders on which you have enabled audit controls (also known as System Access Control Lists or SACLs).

**Info** If you don't already have audit controls configured for your individual files or folders, use the Windows GUI or PowerShell to do so. [See documentation.](#)

☐ Log successful attempts  
☐ Log failed attempts

**Log access to file shares** [Info](#)

☐ Log successful attempts  
☐ Log failed attempts

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 de tentativas and/or 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 de tentativas and/or 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, a Amazon FSx pode criar e usar um fluxo de registros padrão no grupo de CloudWatch /aws/fsx/windows registros de 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.

▼ **Auditing - optional**

Log access to files and folders [Info](#)  
Once you enable logging here, Windows generates audit logs for files and folders on which you have enabled audit controls (also known as System Access Control Lists or SACLs).

❗ If you don't already have audit controls configured for your individual files or folders, use the Windows GUI or PowerShell to do so. [See documentation.](#)

☒ Log successful attempts  
☒ Log failed attempts

Log access to file shares [Info](#)  
☒ Log successful attempts  
☒ Log failed attempts

Choose an audit event log destination

☒ **CloudWatch Logs**  
View and search audit logs in the AWS management console and run queries on logs using CloudWatch Logs Insights

☐ **Kinesis Data Firehose**  
Continuously stream audit events to S3, an Amazon Redshift database, Amazon Elasticsearch, or to partner solutions such as Splunk and Datadog for further analysis

Choose a CloudWatch Logs destination

/aws/fsx/windows ▼

[Create new](#)

Pricing  
Standard Amazon CloudWatch Logs pricing applies based on your usage. [Learn more](#)

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)

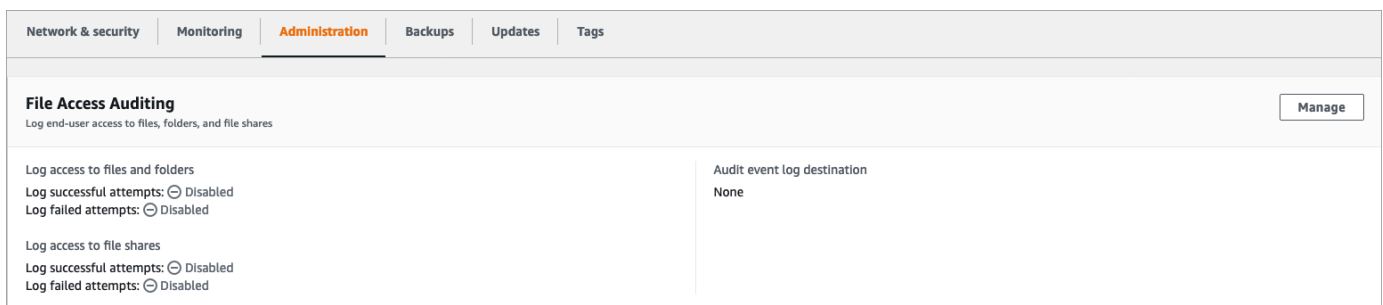
1. Ao criar um novo sistema de arquivos, use a `AuditLogConfiguration` propriedade com a operação da [CreateFileSystem](#) API para habilitar a auditoria de acesso a arquivos para o novo sistema de arquivos.

```
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 FSx console da Amazon 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.

### Manage file access auditing settings

#### Log access to files and folders

Amazon FSx can log successful attempts to access files and folders, failed attempts to access files and folders, neither, or both. Once enabled here, audit logs are generated for files and folders on which audit controls (also known as System Access Control Lists or SACLs) have been configured.

☒ Log successful attempts

☒ Log failed attempts

#### Log access to file shares

Amazon FSx can log successful attempts to access file shares, failed attempts to access file shares, neither, or both.

☒ Log successful attempts

☒ Log failed attempts

#### Choose an audit event log destination

Amazon FSx supports access audit logging to one of the following audit destinations. If you change your audit destination, events will no longer be published to any previous audit destinations.

☒ **CloudWatch Logs**  
View and search audit logs in the AWS management console and run queries on logs using CloudWatch Logs Insights

☐ **Kinesis Data Firehose**  
Continuously stream audit events to S3, an Amazon Redshift database, Amazon Elasticsearch, or to partner solutions such as Splunk and DataDog for further analysis

#### Choose a CloudWatch Logs destination

Use a default CloudWatch Logs log stream created by Amazon FSx, an existing log stream, or create a new log stream.

[Create new](#)

#### Pricing

Standard Amazon CloudWatch Logs pricing applies based on your usage. [Learn more](#)

Cancel

Save

- Em Registrar acesso a arquivos e pastas, selecione o registro de tentativas and/or 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 de tentativas and/or 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"}'
```

## Gerenciamento de identidade e acesso para 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 (tem permissões) FSx para usar os recursos do Windows File Server. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

### Tópicos

- [Público](#)
- [Autenticação com identidades](#)
- [Gerenciar o acesso usando políticas](#)
- [Como o Amazon FSx para Windows File Server funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade FSx para Amazon para Windows File Server](#)
- [AWS políticas gerenciadas para Amazon FSx para Windows File Server](#)
- [Solução de problemas de identidade e acesso ao Amazon FSx para Windows File Server](#)
- [Usando tags com a Amazon FSx](#)
- [Usando funções vinculadas a serviços FSx para Windows File Server](#)

## Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:



- Usuário do serviço: solicite permissões ao administrador caso você não consiga acessar os recursos (consulte [Solução de problemas de identidade e acesso ao Amazon FSx para Windows File Server](#)).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte [Como o Amazon FSx para Windows File Server funciona com o IAM](#)).
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte [Exemplos de políticas baseadas em identidade FSx para Amazon para Windows File Server](#)).

## Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para obter mais informações sobre como fazer login, consulte [Como fazer login na Conta da AWS](#) no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para obter mais informações, consulte [AWS Signature Version 4 para solicitações de API](#) no Guia do usuário do IAM.

### Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Para tarefas que exijam credenciais do usuário-raiz, consulte [Tarefas que exijam credenciais do usuário-raiz](#) no Guia do usuário do IAM.

### Identidade federada

Como prática recomendada, exija que os usuários humanos 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 corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para gerenciamento de acesso centralizado, é recomendável usar o Centro de Identidade do AWS IAM. Para obter mais informações, consulte [O que é o IAM Identity Center?](#) no Guia do usuário do Centro de Identidade do AWS IAM .

## Usuários e grupos do IAM

[Usuário do IAM](#) é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte [Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias](#) no Guia do usuário do IAM.

Um [grupo do IAM](#) especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para obter mais informações, consulte [Casos de uso para usuários do IAM](#) no Guia do usuário do IAM.

## Perfis do IAM

Um [perfil do IAM](#) é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função [mudando de um usuário para uma função do IAM \(console\)](#) ou chamando uma operação de AWS API AWS CLI ou. Para obter mais informações, consulte [Métodos para assumir um perfil](#) no Manual do usuário do IAM.

As funções do IAM são úteis para acesso de usuários federados, permissões temporárias de usuários do IAM, acesso entre contas, acesso entre serviços e aplicativos executados na Amazon. EC2 Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

## Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre documentos de política JSON, consulte [Visão geral das políticas de JSON](#) no Guia do usuário do IAM.

Usando políticas, os administradores especificam quem tem acesso ao quê definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona a funções, que os usuários podem acabar assumindo. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

## Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de política de permissões JSON anexados a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente a uma única identidade) ou políticas gerenciadas (políticas independentes anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do usuário do IAM.

## Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e 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. É necessário [especificar uma entidade principal](#) em uma política baseada em recursos.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

## Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para obter mais informações, consulte [Limites de permissões para entidades do IAM](#) no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para obter mais informações, consulte [Políticas de controle de serviço](#) no Guia do usuário do AWS Organizations .

- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte [Políticas de controle de recursos \(RCPs\)](#) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas passadas como um parâmetro durante a criação de uma sessão temporária para uma função ou um usuário federado. 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 FSx Windows File Server, saiba quais recursos do IAM estão disponíveis para uso com FSx o Windows File Server.

Recursos do IAM que você pode usar com o Amazon FSx para Windows File Server

| Recurso do IAM                                                          | FSx apoio |
|-------------------------------------------------------------------------|-----------|
| <a href="#">Políticas baseadas em identidade</a>                        | Sim       |
| <a href="#">Políticas baseadas em recurso</a>                           | Não       |
| <a href="#">Ações de políticas</a>                                      | Sim       |
| <a href="#">Recursos de políticas</a>                                   | Sim       |
| <a href="#">Chaves de condição de política (específicas do serviço)</a> | Sim       |
| <a href="#">ACLs</a>                                                    | Não       |
| <a href="#">ABAC (tags em políticas)</a>                                | Sim       |
| <a href="#">Credenciais temporárias</a>                                 | Sim       |

| Recurso do IAM                               | FSx apoio |
|----------------------------------------------|-----------|
| <a href="#">Sessões de acesso direto</a>     | Sim       |
| <a href="#">Perfis de serviço</a>            | Não       |
| <a href="#">Perfis vinculados ao serviço</a> | Sim       |

Para ter uma visão de alto nível de como FSx e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte [AWS os serviços que funcionam com o IAM](#) no Guia do usuário do IAM.

## Políticas baseadas em identidade para FSx

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. 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 [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte [Referência de elemento de política JSON do IAM](#) no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para FSx

Para ver exemplos de FSx políticas baseadas em identidade do Windows File Server, consulte. [Exemplos de políticas baseadas em identidade FSx para Amazon para Windows File Server](#)

## Políticas baseadas em recursos dentro FSx

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de 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 atributo ao qual a política está anexada, a política define quais ações uma entidade principal

especificado pode executar nesse atributo e em que condições. É necessário [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, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

## Ações políticas para FSx

Compatível com 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 podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de FSx ações, consulte [Ações definidas pela Amazon FSx para Windows File Server](#) na Referência de Autorização de Serviço.

As ações de política FSx usam o seguinte prefixo antes da ação:

```
fsx
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
 "fsx:action1",
 "fsx:action2"
]
```

Para ver exemplos de FSx políticas baseadas em identidade do Windows File Server, consulte. [Exemplos de políticas baseadas em identidade FSx para Amazon para Windows File Server](#)

## Recursos políticos para FSx

Compatível com 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 de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (\*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"

```

Para ver uma lista dos tipos de FSx recursos e seus ARNs, consulte [Recursos definidos pela Amazon FSx para Windows File Server](#) na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Ações definidas FSx pela Amazon para Windows File Server](#).

Para ver exemplos de FSx políticas baseadas em identidade do Windows File Server, consulte [Exemplos de políticas baseadas em identidade FSx para Amazon para Windows File Server](#)

## Chaves de condição de política para FSx

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem [agentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Para ver uma lista de chaves de FSx condição, consulte [Chaves de condição para Amazon FSx para Windows File Server](#) na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte [Ações definidas pela Amazon FSx para Windows File Server](#).

Para ver exemplos de FSx políticas baseadas em identidade do Windows File Server, consulte [Exemplos de políticas baseadas em identidade FSx para Amazon para Windows File Server](#)

## ACLs in FSx

### Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

### ABAC com FSx

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

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 chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte [Definir permissões com autorização do ABAC](#) no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte [Usar controle de acesso por atributo \(ABAC\)](#) no Guia do usuário do IAM.

### Usando credenciais temporárias com FSx

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte [Credenciais de segurança temporárias no IAM](#) e [Serviços da Serviços da AWS que funcionam com o IAM](#) no Guia do usuário do IAM.

### Sessões de acesso direto para FSx

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim



As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhamento de sessões de acesso](#).

## Funções de serviço para FSx

Compatível com perfis de serviço: não

O perfil de serviço é um [perfil do IAM](#) que um serviço assume para executar 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

Alterar as permissões de uma função de serviço pode interromper FSx a funcionalidade. Edite as funções de serviço somente quando FSx fornecer orientação para fazer isso.

## Funções vinculadas a serviços para FSx

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre a criação ou o gerenciamento FSx de funções vinculadas ao serviço do Windows File Server, consulte. [Usando funções vinculadas a serviços FSx para Windows File Server](#)

## Exemplos de políticas baseadas em identidade FSx para Amazon para Windows File Server

Por padrão, usuários e funções não têm permissão para criar ou modificar FSx recursos do Windows File Server. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte [Criar políticas do IAM \(console\)](#) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por FSx, incluindo o formato de cada um dos tipos de recursos, consulte [Ações, recursos e chaves de condição do Amazon FSx para Windows File Server](#) na Referência de Autorização de Serviço. ARNs

## Tópicos

- [Práticas recomendadas de política](#)
- [Usar o console do FSx](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)

## Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir FSx recursos do Windows File Server em sua conta. Essas ações podem incorrer em custos para sua 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 funções de trabalho](#) no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em 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: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. 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 CloudFormation.

Para obter mais informações, consulte [Elementos da política JSON do IAM: condição](#) no Guia 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 cem verificações de política e recomendações práticas para ajudar 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 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.

## Usar o console do FSx

Para acessar o console do Amazon FSx para Windows File Server, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre FSx os recursos do Windows File Server em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva 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 à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o FSx console, anexe também a política FSx AmazonFSxConsoleReadOnlyAccess AWS gerenciada às entidades. Para obter informações, consulte [Adicionar permissões a um usuário](#) no Guia do usuário do IAM.

## Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui

permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "ViewOwnUserInfo",
 "Effect": "Allow",
 "Action": [
 "iam:GetUserPolicy",
 "iam:ListGroupsForUser",
 "iam:ListAttachedUserPolicies",
 "iam:ListUserPolicies",
 "iam:GetUser"
],
 "Resource": ["arn:aws:iam::*:user/${aws:username}"]
 },
 {
 "Sid": "NavigateInConsole",
 "Effect": "Allow",
 "Action": [
 "iam:GetGroupPolicy",
 "iam:GetPolicyVersion",
 "iam:GetPolicy",
 "iam:ListAttachedGroupPolicies",
 "iam:ListGroupPolicies",
 "iam:ListPolicyVersions",
 "iam:ListPolicies",
 "iam:ListUsers"
],
 "Resource": "*"
 }
]
}
```

## AWS políticas gerenciadas para Amazon FSx para Windows File Server

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 as [políticas gerenciadas pelo cliente](#) que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para mais informações, consulte [Políticas gerenciadas pela AWS](#) no Guia do usuário do IAM.

### Amazon FSx ServiceRolePolicy

Permite que FSx a Amazon gerencie AWS recursos em seu nome. Para saber mais, consulte [Usando funções vinculadas a serviços FSx para Windows File Server](#).

### AWS política gerenciada: Amazon FSx DeleteServiceLinkedRoleAccess

Não é possível anexar a `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 obter mais informações, consulte [Usando funções vinculadas a serviços FSx para Windows File Server](#).

Essa política concede permissões administrativas que permitem FSx à Amazon excluir sua função vinculada ao serviço para acesso ao Amazon S3, usada somente FSx pelo Amazon for Lustre.

#### Detalhes das permissões

Essa política inclui permissões `iam` para permitir que FSx a Amazon visualize, exclua e visualize o status de exclusão das funções vinculadas ao FSx serviço para acesso ao Amazon S3.

Para ver as permissões dessa política, consulte a [Amazon FSx DeleteServiceLinkedRoleAccess](#) no Guia de referência de políticas AWS gerenciadas.

## AWS política gerenciada: Amazon FSx FullAccess

Você pode anexar FSx FullAccess a Amazon às suas entidades do IAM. A Amazon FSx também atribui essa política a uma função de serviço que permite FSx à Amazon realizar ações em seu nome.

Fornecer acesso total à Amazon FSx e acesso aos AWS serviços relacionados.

### Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`— Permite que os diretores tenham acesso total para realizar todas as FSx ações da Amazon, exceto a. `BypassSnaplockEnterpriseRetention`
- `ds`— Permite que os diretores visualizem informações sobre os Directory Service diretórios.
- `ec2`
  - Permite que as entidades principais criem tags sob as condições especificadas.
  - Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança passíveis de uso com uma VPC.
- `iam`— Permite que os princípios criem uma função vinculada ao FSx serviço da Amazon em nome do usuário. Isso é necessário para que a Amazon FSx possa gerenciar AWS recursos em nome do usuário.
- `firehose`: permite que as entidades principais gravem registros em um Amazon Data Firehose. Isso é necessário FSx para que os usuários possam monitorar o acesso ao sistema de arquivos do Windows File Server enviando registros de acesso de auditoria para o Firehose.
- `logs`: permite que as entidades principais criem grupos de logs, fluxos de logs e gravem eventos nos fluxos de logs. Isso é necessário FSx para que os usuários possam monitorar o acesso ao sistema de arquivos do Windows File Server enviando registros de acesso de auditoria para o CloudWatch Logs.

Para ver as permissões dessa política, consulte a [Amazon FSx FullAccess](#) no Guia de referência de políticas AWS gerenciadas.

## AWS política gerenciada: Amazon FSx ConsoleFullAccess

É possível anexar a política `AmazonFSxConsoleFullAccess` às suas identidades do IAM.

Esta política concede permissões administrativas que permitem acesso total à Amazon FSx e acesso a AWS serviços relacionados por meio do Console de gerenciamento da AWS.

### Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`— Permite que os diretores realizem todas as ações no console FSx de gerenciamento da Amazon, exceto `BypassSnaplockEnterpriseRetention`.
- `cloudwatch`— Permite que os diretores visualizem CloudWatch alarmes e métricas no console de FSx gerenciamento da Amazon.
- `ds`— Permite que os diretores listem informações sobre um 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 da Amazon. FSx
  - Permite que entidades principais forneçam validação aprimorada do grupo de segurança de todos os grupos de segurança passíveis de uso com uma VPC.
  - Permite que os diretores visualizem as interfaces de rede elásticas associadas a um sistema de FSx arquivos da Amazon.
- `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).
- `secretsmanager`— Permite que os diretores listem segredos AWS Secrets Manager para selecionar as credenciais da conta de serviço de ingresso no domínio.
- `iam`— Concede permissão para criar uma função vinculada ao serviço que permite FSx à Amazon realizar ações em nome do usuário.

Para ver as permissões dessa política, consulte a [Amazon FSx ConsoleFullAccess](#) no Guia de referência de políticas AWS gerenciadas.

### AWS política gerenciada: Amazon FSx ConsoleReadOnlyAccess

É possível anexar a política `AmazonFSxConsoleReadOnlyAccess` às suas identidades do IAM.

Esta política concede permissões somente de leitura à Amazon FSx e aos AWS serviços relacionados para que os usuários possam visualizar informações sobre esses serviços no Console de gerenciamento da AWS

### Detalhes das permissões

Esta política inclui as seguintes permissões.

- `fsx`— Permite que os diretores visualizem informações sobre os sistemas de FSx arquivos da Amazon, incluindo todas as tags, no Amazon FSx Management Console.
- `cloudwatch`— Permite que os diretores visualizem CloudWatch alarmes e métricas no Amazon FSx Management Console.
- `ds`— Permite que os diretores visualizem informações sobre um 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 FSx sistema de arquivos da Amazon no Amazon Management Console.
  - Permite que entidades principais forneçam validação aprimorada do grupo de segurança de todos os grupos de segurança passíveis de uso com uma VPC.
  - Permite que os diretores visualizem as interfaces de rede elásticas associadas a um sistema de FSx arquivos da Amazon.
- `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 os diretores possam visualizar a configuração de auditoria de acesso a arquivos existente FSx para um sistema de arquivos do Windows File Server.
- `secretsmanager`— Permite que os diretores listem segredos AWS Secrets Manager para selecionar as credenciais da conta de serviço de ingresso no domínio.
- `firehose`: permite que as entidades principais descrevam os fluxos de entrega do Amazon Data Firehose associados à conta que está fazendo a solicitação. Isso é necessário para que os diretores possam visualizar a configuração de auditoria de acesso a arquivos existente FSx para um sistema de arquivos do Windows File Server.



Para ver as permissões dessa política, consulte a [Amazon FSx ConsoleReadOnlyAccess](#) no Guia de referência de políticas AWS gerenciadas.

## AWS política gerenciada: Amazon FSx ReadOnlyAccess

É possível anexar a política `AmazonFSxReadOnlyAccess` às suas identidades do IAM.

- `fsx`— Permite que os diretores visualizem informações sobre os sistemas de FSx arquivos da Amazon, incluindo todas as tags, no Amazon FSx Management Console.
- `ec2`: fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança passíveis de uso com uma VPC.

Para ver as permissões dessa política, consulte a [Amazon FSx ReadOnlyAccess](#) no Guia de referência de políticas AWS gerenciadas.

## FSx Atualizações da Amazon para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas da Amazon FSx desde que esse serviço começou a monitorar essas mudanças. Para receber alertas automáticos sobre alterações nesta página, assine o feed RSS na FSx [Histórico do documento](#) página da Amazon.

| Alteração                                                                                | Descrição                                                                                                                                                                                                                      | Data                  |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente     | A Amazon FSx adicionou uma nova permissão, <code>secretsmanager:ListSecrets</code> que permite que os diretores listem segredos AWS Secrets Manager para selecionar as credenciais da conta de serviço de ingresso no domínio. | 5 de novembro de 2025 |
| <a href="#">Amazon FSx ConsoleReadOnlyAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão, <code>secretsmanager:ListSecrets</code> que permite que os diretores                                                                                                                | 3 de novembro de 2025 |

| Alteração                                                                            | Descrição                                                                                                                                                                                                                                        | Data                |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                                                                      | listem segredos AWS Secrets Manager para selecionar as credenciais da conta de serviço de ingresso no domínio.                                                                                                                                   |                     |
| <a href="#">Amazon FSx ServiceRolePolicy</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão, <code>ec2:AssignIpv6Addresses</code> que permite que os diretores atribuam IPv6 endereços às interfaces de rede do cliente que tenham uma <code>AmazonFSx.FileSystemId</code> tag.                    | 22 de julho de 2025 |
| <a href="#">Amazon FSx ServiceRolePolicy</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão, <code>ec2:UnassignIpv6Addresses</code> que permite que os diretores cancelem a atribuição de IPv6 endereços das interfaces de rede do cliente que tenham uma <code>AmazonFSx.FileSystemId</code> tag. | 22 de julho de 2025 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão, <code>fsx:CreateAndAttachS3AccessPoint</code> que permite que os diretores criem um ponto de acesso S3 e o conectem a um FSx volume.                                                                  | 25 de junho de 2025 |

| Alteração                                                                            | Descrição                                                                                                                                                                                       | Data                |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão, <code>fsx:DescribeS3AccessPointAttachments</code> que permite aos diretores listar todos os pontos de acesso do S3 Conta da AWS em um. Região da AWS | 25 de junho de 2025 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão, <code>fsx:DetachAndDeleteS3AccessPoint</code> que permite que os diretores excluam um ponto de acesso S3.                                            | 25 de junho de 2025 |
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente        | A Amazon FSx adicionou uma nova permissão, <code>fsx:CreateAndAttachS3AccessPoint</code> que permite que os diretores criem um ponto de acesso S3 e o conectem a um FSx volume.                 | 25 de junho de 2025 |
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente        | A Amazon FSx adicionou uma nova permissão, <code>fsx:DescribeS3AccessPointAttachments</code> que permite aos diretores listar todos os pontos de acesso do S3 Conta da AWS em um. Região da AWS | 25 de junho de 2025 |

| Alteração                                                                                | Descrição                                                                                                                                                                                                                               | Data                    |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente            | A Amazon FSx adicionou uma nova permissão, <code>fsx:DetachAndDeleteS3AccessPoint</code> que permite que os diretores excluam um ponto de acesso S3.                                                                                    | 25 de junho de 2025     |
| <a href="#">Amazon FSx ConsoleReadOnlyAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão, <code>ec2:DescribeNetworkInterfaces</code> que permite que os diretores visualizem as interfaces de rede elásticas associadas ao sistema de arquivos.                                        | 25 de fevereiro de 2025 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente     | A Amazon FSx adicionou uma nova permissão, <code>ec2:DescribeNetworkInterfaces</code> que permite que os diretores visualizem as interfaces de rede elásticas associadas ao sistema de arquivos.                                        | 07 de fevereiro de 2025 |
| <a href="#">Amazon FSx ServiceRolePolicy</a> — Atualização de uma política existente     | A Amazon FSx adicionou uma nova permissão, <code>ec2:GetSecurityGroupsForVpc</code> 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                 |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <a href="#">Amazon FSx ReadOnlyAccess</a> — Atualização de uma política existente        | A Amazon FSx adicionou uma nova permissão, <code>ec2:GetSecurityGroupsForVpc</code> 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 |
| <a href="#">Amazon FSx ConsoleReadOnlyAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão, <code>ec2:GetSecurityGroupsForVpc</code> 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 |
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente            | A Amazon FSx adicionou uma nova permissão, <code>ec2:GetSecurityGroupsForVpc</code> 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                   |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão, <code>ec2:GetSecurityGroupsForVpc</code> 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   |
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente        | A Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação de dados entre regiões e entre contas FSx para sistemas de arquivos OpenZFS.                                                              | 20 de dezembro de 2023 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação de dados entre regiões e entre contas FSx para sistemas de arquivos OpenZFS.                                                              | 20 de dezembro de 2023 |
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente        | A Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação sob demanda de volumes FSx para sistemas de arquivos OpenZFS.                                                                             | 26 de novembro de 2023 |

| Alteração                                                                            | Descrição                                                                                                                                                                              | Data                   |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou uma nova permissão para permitir que os usuários realizem a replicação sob demanda de volumes FSx para sistemas de arquivos OpenZFS.                            | 26 de novembro de 2023 |
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente        | A Amazon FSx adicionou novas permissões para permitir que os usuários visualizem, habilitem e desabilitem o suporte compartilhado de VPC FSx para sistemas de arquivos ONTAP Multi-AZ. | 14 de novembro de 2023 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou novas permissões para permitir que os usuários visualizem, habilitem e desabilitem o suporte compartilhado de VPC FSx para sistemas de arquivos ONTAP Multi-AZ. | 14 de novembro de 2023 |
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente        | A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon gerencie configurações de rede FSx para sistemas de arquivos OpenZFS Multi-AZ.                                  | 9 de agosto de 2023    |

| Alteração                                                                                                     | Descrição                                                                                                                                                                                                               | Data                   |
|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <a href="#">AWS política gerenciada: Amazon FSx ServiceRolePolicy</a> — Atualização de uma política existente | A Amazon FSx modificou a <code>cloudwatch:PutMetricData</code> permissão existente para que a Amazon FSx publique CloudWatch métricas no AWS/FSx namespace.                                                             | 24 de julho de 2023    |
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente                                 | A Amazon FSx atualizou a política para remover a <code>fsx:*</code> permissão e adicionar <code>fsx</code> ações específicas.                                                                                           | 13 de julho de 2023    |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente                          | A Amazon FSx atualizou a política para remover a <code>fsx:*</code> permissão e adicionar <code>fsx</code> ações específicas.                                                                                           | 13 de julho de 2023    |
| <a href="#">Amazon FSx ConsoleReadOnlyAccess</a> — Atualização de uma política existente                      | A Amazon FSx adicionou novas permissões para permitir que os usuários visualizem métricas de desempenho aprimoradas e ações recomendadas FSx para sistemas de arquivos do Windows File Server no FSx console da Amazon. | 21 de setembro de 2022 |



| Alteração                                                                                     | Descrição                                                                                                                                                                                                               | Data                   |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente          | A Amazon FSx adicionou novas permissões para permitir que os usuários visualizem métricas de desempenho aprimoradas e ações recomendadas FSx para sistemas de arquivos do Windows File Server no FSx console da Amazon. | 21 de setembro de 2022 |
| <a href="#">Amazon FSx ReadOnlyAccess</a> — Iniciou a política de rastreamento                | Essa política concede acesso somente para leitura a todos os FSx recursos da Amazon e a quaisquer tags associadas a eles.                                                                                               | 4 de fevereiro de 2022 |
| <a href="#">Amazon FSx DeleteServiceLinkedRoleAccess</a> — Iniciou a política de rastreamento | Essa política concede permissões administrativas que permitem FSx à Amazon excluir sua função vinculada ao serviço para acesso ao Amazon S3.                                                                            | 7 de janeiro de 2022   |
| <a href="#">Amazon FSx ServiceRolePolicy</a> — Atualização de uma política existente          | A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon gerencie as configurações de rede dos sistemas de arquivos Amazon FSx for NetApp ONTAP.                                                          | 2 de setembro de 2021  |

| Alteração                                                                            | Descrição                                                                                                                                                                                                                                                                                                                     | Data                  |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente        | A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon crie tags em tabelas de EC2 rotas para chamadas com escopo reduzido.                                                                                                                                                                                   | 2 de setembro de 2021 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon crie sistemas de arquivos Amazon FSx for NetApp ONTAP Multi-AZ.                                                                                                                                                                                        | 2 de setembro de 2021 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente | A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon crie tags em tabelas de EC2 rotas para chamadas com escopo reduzido.                                                                                                                                                                                   | 2 de setembro de 2021 |
| <a href="#">Amazon FSx ServiceRolePolicy</a> — Atualização de uma política existente | <p>A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon descreva e grave nos fluxos de log do CloudWatch Logs.</p> <p>Isso é necessário para que os usuários possam visualizar registros de auditoria de acesso a arquivos FSx para sistemas de arquivos do Windows File Server usando CloudWatch Logs.</p> | 8 de junho de 2021    |

| Alteração                                                                            | Descrição                                                                                                                                                                                                                                                                                                                                                                                              | Data               |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">Amazon FSx ServiceRolePolicy</a> — Atualização de uma política existente | <p>A Amazon FSx adicionou novas permissões para permitir que FSx a Amazon descreva e grave nos fluxos de entrega do Amazon Data Firehose.</p> <p>Isso é necessário para que os usuários possam visualizar os registros de auditoria de acesso aos arquivos de um sistema FSx de arquivos do Windows File Server usando o Amazon Data Firehose.</p>                                                     | 8 de junho de 2021 |
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente        | <p>A Amazon FSx adicionou novas permissões para permitir que os diretores descrevam e criem grupos de CloudWatch registros de registros, fluxos de registros e gravem eventos em fluxos de registros.</p> <p>Isso é necessário para que os diretores possam visualizar os registros de auditoria de acesso a arquivos FSx para sistemas de arquivos do Windows File Server usando CloudWatch Logs.</p> | 8 de junho de 2021 |

| Alteração                                                                            | Descrição                                                                                                                                                                                                                                                                                                                                                                                                  | Data               |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">Amazon FSx FullAccess</a> — Atualização de uma política existente        | <p>A Amazon FSx adicionou novas permissões para permitir que os diretores descrevam e gravem registros em um Amazon Data Firehose.</p> <p>Isso é necessário para que os usuários possam visualizar os registros de auditoria de acesso aos arquivos de um sistema FSx de arquivos do Windows File Server usando o Amazon Data Firehose.</p>                                                                | 8 de junho de 2021 |
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente | <p>A 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.</p> <p>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 FSx para um sistema de arquivos do Windows File Server.</p> | 8 de junho de 2021 |

| Alteração                                                                                | Descrição                                                                                                                                                                                                                                                                                                                                                                                       | Data               |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">Amazon FSx ConsoleFullAccess</a> — Atualização de uma política existente     | <p>A 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.</p> <p>Isso é necessário para que os diretores possam escolher um stream de entrega existente do Firehose ao configurar a auditoria de acesso a arquivos para FSx um sistema de arquivos do Windows File Server.</p> | 8 de junho de 2021 |
| <a href="#">Amazon FSx ConsoleReadOnlyAccess</a> — Atualização de uma política existente | <p>A 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.</p> <p>Isso é necessário para que os diretores possam visualizar a configuração de auditoria de acesso a arquivos existente FSx para um sistema de arquivos do Windows File Server.</p>                                | 8 de junho de 2021 |

| Alteração                                                                                 | Descrição                                                                                                                                                                                                                                                                                                                                                          | Data               |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">Amazon FSx ConsoleRe adOnlyAccess</a> — Atualização de uma política existente | <p>A 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.</p> <p>Isso é necessário para que os diretores possam visualizar a configuração de auditoria de acesso a arquivos existente FSx para um sistema de arquivos do Windows File Server.</p> | 8 de junho de 2021 |
| A Amazon FSx começou a monitorar as mudanças                                              | A Amazon FSx começou a monitorar as mudanças em suas políticas AWS gerenciadas.                                                                                                                                                                                                                                                                                    | 8 de junho de 2021 |

## Solução de problemas de identidade e acesso ao Amazon FSx para Windows File Server

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com FSx o Windows File Server e o IAM.

### Tópicos

- [Não estou autorizado a realizar uma ação em FSx](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha Conta da AWS acessem meus FSx recursos](#)

## Não estou autorizado a realizar uma ação em FSx

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo `my-example-widget` fictício, mas não tem as permissões `fsx:GetWidget` fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
fsx:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso `my-example-widget` usando a ação `fsx:GetWidget`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função FSx para o Windows File Server.

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 exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no FSx Windows File Server. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Quero permitir que pessoas fora da minha Conta da AWS acessem meus FSx recursos

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se FSx o Windows File Server 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 perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

## Usando tags com a Amazon FSx

Você pode usar tags para controlar o acesso aos FSx recursos da Amazon e implementar o controle de acesso baseado em atributos (ABAC). Os usuários precisam ter permissão para aplicar tags aos FSx recursos da Amazon durante a criação.

### Conceder permissão para marcar recursos durante a criação

Algumas ações de criação de recursos FSx para a API do Windows File Server 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 a marcação de FSx recursos da Amazon, consulte [Marcação de seus recursos do Amazon FSx](#). Para obter mais informações sobre o uso de tags para controlar o acesso aos FSx recursos, consulte [Usando tags para controlar o acesso aos seus FSx recursos da Amazon](#).

## Usando tags para controlar o acesso aos seus FSx recursos da Amazon

Para controlar o acesso aos FSx recursos e ações da Amazon, 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 FSx recursos da Amazon 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 a marcação de FSx recursos da Amazon no momento da criação, consulte [Conceder permissão para marcar recursos durante a criação](#). Para obter mais informações sobre como marcar recursos, consulte [Marcação de seus recursos do Amazon FSx](#).

### Como controlar o acesso com base em tags em um recurso

Para controlar quais ações um usuário ou função pode realizar em um FSx recurso da Amazon, 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 — Crie backups somente dos sistemas de FSx arquivos da Amazon 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 `Department=Finance`.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "fsx:CreateBackup"
],
 "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
 "Condition": {
 "StringEquals": {
 "aws:ResourceTag/Department": "Finance"
 }
 }
 }
]
}
```

```

 },
 {
 "Effect": "Allow",
 "Action": [
 "fsx:TagResource",
 "fsx:CreateBackup"
],
 "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
 "Condition": {
 "StringEquals": {
 "aws:RequestTag/Department": "Finance"
 }
 }
 }
]
}

```

Exemplo 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.

JSON

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "fsx:CreateFileSystemFromBackup",
 "fsx:TagResource"
],
 "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
 "Condition": {
 "StringEquals": {
 "aws:ResourceTag/Department": "Finance"
 }
 }
 }
],
}

```

```

 {
 "Effect": "Allow",
 "Action": [
 "fsx:CreateFileSystemFromBackup",
 "fsx:TagResource"
],
 "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
 "Condition": {
 "StringEquals": {
 "aws:ResourceTag/Department": "Finance"
 }
 }
 }
]
}

```

Exemplo 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.

JSON

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "fsx:DeleteFileSystem"
],
 "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
 "Condition": {
 "StringEquals": {
 "aws:ResourceTag/Department": "Finance"
 }
 }
 },
 {
 "Effect": "Allow",

```

```
 "Action": [
 "fsx:TagResource"
],
 "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
 "Condition": {
 "StringEquals": {
 "aws:RequestTag/Department": "Finance"
 }
 }
 }
}
```

## Usando funções vinculadas a serviços FSx para Windows File Server

O Amazon FSx para Windows File Server usa funções [vinculadas a serviços AWS Identity and Access Management](#) (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao FSx Windows File Server. As funções vinculadas ao serviço são predefinidas FSx pelo Windows File Server e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração FSx do Windows File Server porque você não precisa adicionar manualmente as permissões necessárias. FSx para o Windows File Server define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente FSx o Windows File Server pode assumir suas funções. 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 FSx recursos do Windows File Server porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados a serviços, consulte [Serviços da AWS compatíveis com o IAM](#) e procure os serviços que contenham Sim na coluna Service-Linked Role. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

## Permissões de função vinculadas ao serviço FSx para Windows File Server

FSx para Windows File Server usa a função vinculada ao serviço chamada `AWSServiceRoleForAmazonFSx` — que executa determinadas ações em sua conta, como criar interfaces de rede elásticas para seus sistemas de arquivos em sua VPC.

A política de permissões de função permite que FSx o Windows File Server conclua as seguintes ações em todos os AWS recursos aplicáveis:

Você não pode vincular `FSx ServiceRolePolicy` a Amazon às suas entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite FSx gerenciar AWS recursos em seu nome. Para obter mais informações, consulte [Usando funções vinculadas a serviços FSx para Windows File Server](#).

Para obter atualizações dessa política, consulte [Amazon FSx ServiceRolePolicy](#).

Essa política concede permissões administrativas que FSx permitem gerenciar AWS recursos em nome do usuário.

### Detalhes das permissões

As permissões de `FSx ServiceRolePolicy` função da Amazon são definidas pela política `FSx ServiceRolePolicy` AWS gerenciada da Amazon. A `Amazon FSx ServiceRolePolicy` tem as seguintes permissões:

#### Note

`FSxServiceRolePolicy` A Amazon é usada por todos os tipos de sistemas de FSx arquivos da Amazon; algumas das permissões listadas podem não se aplicar ao FSx Windows.

- `ds`— Permite FSx visualizar, autorizar e desautorizar aplicativos em seu diretório. Directory Service
- `ec2`— Permite FSx fazer o seguinte:
  - Visualize, crie e desassocie interfaces de rede associadas a um sistema de FSx arquivos da Amazon.
  - Visualize um ou mais endereços IP elásticos associados a um sistema de FSx arquivos da Amazon.

- Veja a Amazon VPCs, os grupos de segurança e as sub-redes associadas a um sistema de FSx arquivos da Amazon.
- Atribua IPv6 endereços às interfaces de rede do cliente que tenham uma `AmazonFSx.FileSystemId` tag.
- Cancele a atribuição de IPv6 endereços das interfaces de rede do cliente que tenham uma `AmazonFSx.FileSystemId` tag.
- Fornecer validação aprimorada do grupo de segurança de todos os grupos de segurança passíveis de uso com uma VPC.
- Crie uma permissão para que um usuário AWS autorizado realize determinadas operações em uma interface de rede.
- `cloudwatch`— Permite FSx publicar pontos de dados métricos CloudWatch abaixo do FSx namespace `AWS/`.
- `route53`— Permite FSx associar uma Amazon VPC a uma zona hospedada privada.
- `logs`— Permite FSx descrever e gravar em fluxos de log de CloudWatch registros. Isso é para que os usuários possam enviar registros de auditoria de acesso a arquivos de um FSx sistema de arquivos do Windows File Server para um stream de CloudWatch registros.
- `firehose`— Permite FSx descrever e gravar 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 FSx de arquivos do Windows File Server em um stream de distribuição do Amazon Data Firehose.

## JSON

```
{
 "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 [FSx Atualizações da Amazon para políticas AWS 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 a serviço. Para mais informações, consulte [Permissões de perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Criando uma função vinculada ao serviço FSx para o Windows File Server

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 Windows File Server cria a função vinculada ao serviço FSx para você. Console de gerenciamento da AWS

### 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, FSx o Windows File Server cria a função vinculada ao serviço para você novamente.

## Editando uma função vinculada ao serviço FSx para Windows File Server

FSx para Windows File Server não permite que você edite a função vinculada 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 do perfil usando o IAM. Para obter mais informações, consulte [Editar uma função vinculada a serviço](#) no Guia do usuário do IAM.

## Excluindo uma função vinculada ao serviço FSx para Windows File Server

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 FSx para Windows File Server estiver usando a função 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 suportadas FSx para funções vinculadas ao serviço do Windows File Server

FSx para Windows File Server oferece suporte ao uso de funções vinculadas 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 no escopo de programas de conformidade específicos, consulte [Serviços da AWS no escopo por programa de conformidade](#) e escolha o

programa de conformidade desejado. Para obter informações gerais, consulte [Programas de Conformidade da AWS](#).

É possível baixar relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte [Baixar relatórios no AWS Artifact](#).

Sua responsabilidade de conformidade ao usar os Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. Para ter mais informações sobre sua responsabilidade pela conformidade ao usar Serviços da AWS, consulte a [documentação da AWS sobre segurança](#).

## 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 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. O Amazon FSx é compatível com endpoints VPC configurados com tipos de endereço IP somente IPv4 e de pilha dupla (IPv4 e IPv6). Para obter mais informações, consulte [Como criar um endpoint da VPC da interface](#) no Guia do usuário da Amazon VPC.

## 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 mais informações, consulte [Controlar o acesso a serviços com VPC endpoints](#) no Guia do usuário da Amazon VPC.

## Como trabalhar com outros serviços do

Além da Amazon CloudWatch,, e AWS Identity and Access Management AWS CloudTrail, FSx para Windows AWS DataSync, o File Server também se integra com o seguinte: Serviços da AWS

- Amazon WorkSpaces Applications — WorkSpaces Applications é um serviço de streaming de aplicativos totalmente gerenciado que fornece aos usuários acesso instantâneo aos seus aplicativos de desktop de qualquer lugar. WorkSpaces Os aplicativos gerenciam AWS os recursos necessários para hospedar e executar seus aplicativos, escalam automaticamente e fornecem acesso aos usuários sob demanda. Aprenda a criar armazenamento persistente para usuários individuais e compartilhar o armazenamento entre vários usuários em seus sistemas FSx de arquivos do Windows File Server usando WorkSpaces aplicativos. Para obter mais informações, consulte [Usando a Amazon FSx com WorkSpaces aplicativos da Amazon](#).
- Amazon Kendra: o Amazon Kendra é um serviço de pesquisa inteligente que usa processamento de linguagem natural e algoritmos avançados de machine learning para retornar respostas específicas às perguntas de pesquisa de seus dados. Com o Amazon Kendra, você poderá criar uma experiência de pesquisa unificada conectando vários repositórios de dados a um índice e ingerindo e fazendo crawling em documentos. Para obter mais informações sobre o uso do Amazon Kendra FSx com o Windows File Server, consulte. [Usando o FSx Windows File Server com o Amazon Kendra](#)

### Tópicos

- [Usando a Amazon FSx com WorkSpaces aplicativos da Amazon](#)
- [Usando o FSx Windows File Server com o Amazon Kendra](#)

## Usando a Amazon FSx com WorkSpaces aplicativos da Amazon

Ao oferecer suporte ao protocolo Server Message Block (SMB), o Amazon FSx for Windows File Server suporta o acesso ao seu sistema de arquivos a partir das instâncias Amazon EC2, VMware Cloud on AWS WorkSpaces, Amazon e Amazon WorkSpaces Applications. WorkSpaces O Applications é um serviço de streaming de aplicativos totalmente gerenciado. Você gerencia centralmente seus aplicativos de desktop em WorkSpaces Aplicativos e os entrega com segurança a um navegador em qualquer computador. Para obter mais informações sobre WorkSpaces aplicativos, consulte o [Guia de administração de WorkSpaces aplicativos da Amazon](#). Para obter instruções sobre como você pode simplificar o gerenciamento de suas imagens e frotas de



WorkSpaces aplicativos da Amazon, consulte a postagem do AWS blog [Crie automaticamente imagens AppStream 2.0 personalizadas do Windows](#).

Os procedimentos a seguir mostram como usar a Amazon FSx com WorkSpaces aplicativos para fornecer armazenamento pessoal persistente para cada usuário e fornecer uma pasta compartilhada para que vários usuários possam acessar arquivos comuns.

## Como fornecer armazenamento pessoal Persistent para cada usuário

Você pode usar FSx a Amazon para fornecer a cada usuário da sua organização uma unidade de armazenamento exclusiva nas sessões de streaming de WorkSpaces aplicativos. 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.

Para criar pastas pessoais para usuários de domínio usando a Amazon FSx

1. Crie um sistema de FSx arquivos da Amazon. 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 de WorkSpaces aplicativos de domínio em seu sistema de FSx arquivos da Amazon. 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 [Criar, atualizar e remover compartilhamentos de arquivos](#).

Para iniciar um construtor de imagens de aplicativos associado ao domínio WorkSpaces

1. Faça login no console de WorkSpaces aplicativos: <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 [Usando o Active Directory com WorkSpaces aplicativos](#) no Amazon WorkSpaces Applications Administration Guide.
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 FSx arquivos da Amazon. Certifique-se de associar o construtor de imagens ao mesmo AWS Managed Microsoft AD diretório ao qual seu sistema de FSx arquivos da Amazon está associado. Os grupos de segurança da VPC que você associa ao criador de imagens devem permitir o acesso ao seu sistema de FSx arquivos da Amazon.
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.

Para vincular compartilhamentos FSx de arquivos da Amazon com WorkSpaces aplicativos

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 da unidade para mapear a pasta compartilhada no sistema de FSx arquivos da Amazon. Você usa o nome DNS do seu sistema de FSx arquivos da Amazon ou um alias DNS associado ao sistema de arquivos neste script, que pode ser obtido na visualização de detalhes do sistema de arquivos no console da 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 PowerShell prompt 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 de WorkSpaces aplicativos. Certifique-se de também unir a frota de WorkSpaces aplicativos ao mesmo domínio do Active Directory que você usou para o criador de imagens. Inicie a frota na mesma VPC usada pelo seu sistema de FSx arquivos da Amazon. Os grupos de segurança da VPC que você associa à frota devem fornecer acesso ao seu sistema de FSx arquivos da Amazon.
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 [Acesso de login único ao AppStream 2.0 usando o SAML 2.0 no](#) Guia de administração de WorkSpaces aplicativos da Amazon.
9. Seu compartilhamento de FSx arquivos da Amazon é mapeado para a letra S: na sessão de streaming.

## Como fornecer uma pasta compartilhada entre os usuários

Você pode usar FSx a Amazon para fornecer uma pasta compartilhada aos usuários da 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.

Para criar uma pasta compartilhada usando a Amazon FSx

1. Crie um sistema de FSx arquivos da Amazon. Para obter mais informações, consulte [Introdução ao Amazon FSx para Windows File Server](#).
2. Cada sistema de FSx arquivos da Amazon inclui uma pasta compartilhada por padrão que você pode acessar usando o endereço `\\file-system-DNS-name\share` ou `\\fqdn-DNS-alias\share` se estiver usando aliases de DNS. Você pode usar o compartilhamento padrão ou criar uma pasta compartilhada diferente. Para obter mais informações, consulte [Criar, atualizar e remover compartilhamentos de arquivos](#).

## Para iniciar um construtor WorkSpaces de imagens de aplicativos

1. No console de WorkSpaces aplicativos, inicie um novo criador de imagens ou conecte-se a um criador de imagens existente. Inicie o construtor de imagens na mesma VPC usada pelo seu sistema de FSx arquivos da Amazon. Os grupos de segurança da VPC que você associa ao criador de imagens devem permitir o acesso ao seu sistema de FSx arquivos da Amazon.
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.

## Para vincular a pasta compartilhada aos WorkSpaces aplicativos

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 você pode obter na visualização de detalhes do sistema de arquivos no Amazon FSx Console) 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.

# Usando o FSx Windows File Server com o Amazon Kendra

O Amazon Kendra é um serviço de busca altamente preciso e inteligente. FSx para Windows, os sistemas de arquivos do 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 em seu 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 seu sistema de arquivos como uma fonte de dados do Amazon Kendra, [consulte Introdução a uma fonte de dados da FSx Amazon \(console\) no Guia](#) do desenvolvedor do Amazon Kendra.
- Para obter informações da visão geral sobre o Amazon Kendra, consulte o [site do Amazon Kendra](#).
- Para obter uma explicação sobre como pesquisar seu sistema de arquivos usando o Amazon Kendra, [consulte Pesquisar com segurança dados não estruturados em sistemas de arquivos Windows com o conector Amazon Kendra para Amazon for Windows File Server no blog do Machine Learning](#). FSx AWS

## desempenho do sistema de arquivos

Quando você adiciona um sistema de arquivos 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 FSx desempenho da Amazon, consulte [desempenho do FSx para Windows File Server](#).

# Cotas

A seguir, você poderá entender sobre cotas quando trabalhar com o Amazon FSx para Windows File Server.

## Tópicos

- [Cotas que podem ser aumentadas](#)
- [Cotas de recursos para cada sistema de arquivos](#)
- [Considerações adicionais](#)
- [Cotas específicas para o Microsoft Windows](#)

## 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 | 524288 | 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 | 524288  | 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 mil | 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 [Solicitar 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 mil GiB                      |
| Capacidade máxima de armazenamento, SSD e HDD                                                             | 64 TiB                         |
| IOPS de SSD mínima                                                                                        | 96                             |
| IOPS de SSD máxima                                                                                        | 400 mil                        |
| Capacidade de throughput mínima                                                                           | 8 MBps                         |
| Capacidade de throughput máxima                                                                           | 12.288 MBps                    |
| Número máximo de compartilhamentos de arquivos                                                            | 100 mil                        |

## 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 da Amazon FSx

Use as seções a seguir para ajudar a solucionar problemas que você tem com a Amazon FSx.

Se você encontrar problemas não listados a seguir ao usar a Amazon FSx, tente fazer uma pergunta no [FSx fórum da Amazon](#).

## Tópicos

- [Não é possível acessar o sistema de arquivos](#)
- [Falha na criação de um novo sistema FSx de arquivos da Amazon](#)
- [O sistema de arquivos está em um estado de configuração incorreta](#)
- [Não é possível configurar a DFS-R em um sistema de arquivos multi-AZ ou single-AZ 2](#)
- [Falha nas atualizações da capacidade de armazenamento ou capacidade de throughput](#)

## 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

- [A interface de rede elástica do sistema de arquivos foi modificada ou excluída](#)
- [O endereço IP elástico anexado à interface de rede elástica do sistema de arquivos foi excluído](#)
- [O grupo de segurança do sistema de arquivos não possui as regras de entrada ou saída necessárias.](#)
- [O grupo de segurança da instância de computação não tem as regras de saída necessárias](#)
- [Instância de computação não associada a um Active Directory](#)
- [O compartilhamento de arquivos não existe](#)
- [O usuário do Active Directory não possui as permissões necessárias](#)
- [Remoção do Permitir controle total de permissões de NTFS ACL](#)
- [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 nem exclua a interface de rede FSx elástica da Amazon. Para obter 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

A Amazon FSx não oferece suporte ao acesso a sistemas de arquivos da Internet pública. A Amazon separa FSx 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 obter mais informações, consulte [Acessar seus dados](#).

## 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 obter mais informações, consulte [Como usar o Amazon FSx com o 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 [Criar, atualizar e remover compartilhamentos de arquivos](#).

## 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 do Windows (ACLs) para a pasta compartilhada permitam 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 obter mais informações, consulte [Criar, atualizar e remover compartilhamentos de arquivos](#). 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 FSx arquivos da Amazon a partir do uso local Direct Connect ou de uma VPN e está usando um intervalo de endereços IP não privado para o cliente local.

A Amazon FSx só oferece suporte ao acesso de clientes locais com endereços IP não privados em sistemas de arquivos criados após 17 de dezembro de 2020.

Se precisar acessar o FSx sistema de arquivos do 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 obter mais informações, consulte [Proteger seus dados com backups](#).

## O novo sistema de arquivos não está registrado no DNS

Para sistemas de arquivos associados a um Active Directory autogerenciado, a Amazon FSx não registrou o DNS do sistema de arquivos quando ele foi criado porque a rede do cliente não usa o Microsoft DNS.

FSx A Amazon não registra sistemas de arquivos no DNS se sua rede usa um serviço DNS de terceiros em vez do Microsoft DNS. Você deve configurar manualmente as entradas de DNS A para seus sistemas de FSx arquivos da Amazon. 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. No <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 na Amazon EC2 .
    - O endereço IP do sistema de arquivos Single-AZ 1 a ser usado é mostrado na coluna IPv4 IP 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 na Amazon EC2 .
- O endereço IP da sub-rede preferencial a ser usada é mostrado na coluna IPv4 IP privado secundário.
- No painel de sub-rede Amazon FSx Standby, escolha a interface de rede elástica mostrada em Interface de rede para abrir a página Interfaces de rede no console da Amazon EC2 .
- O endereço IP usado pela sub-rede em espera é mostrado na coluna IPv4 IP 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. Usando o FSx console da Amazon — 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 da [describe-file-system-aliases](#) CLI ou a operação da [DescribeFileSystemAliases](#) API 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 obter 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:
  - Nomes principais de serviço criados (SPNs) correspondentes ao alias de DNS no objeto de computador do Active Directory do seu sistema de FSx arquivos Amazon.

Para obter mais informações, consulte [Configurar nomes de entidade principal de serviço \(SPNs\) para o Kerberos](#).

- Criou um registro DNS CNAME para o alias DNS que é resolvido para o nome DNS padrão do sistema de arquivos da Amazon. FSx

Para obter mais informações, consulte [Atualizar ou criar um registro CNAME de DNS](#).

4. Se você criou um registro DNS SPNs CNAME válido, verifique se o DNS do cliente tem 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 FSx arquivos da Amazon e o cliente ainda não conseguir acessar o sistema de arquivos, consulte as etapas adicionais de solução [Não é possível acessar o sistema de arquivos](#) 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 DNS do sistema de arquivos e quaisquer aliases de DNS associados no [FSx console da Amazon](#) escolhendo Windows File Server, Network & security. Ou você pode encontrá-lo na resposta do [CreateFileSystem](#) ou na operação da API [DescribeFileSystems](#). 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 FSx de arquivos da Amazon

Há várias causas possíveis para a falha de uma solicitação de criação de sistema de arquivos, conforme descrito na seção a seguir.

## Tópicos

- [Grupo de segurança e rede VPC configurados incorretamente ACLs](#)
- [Nomes duplicados de grupo de administradores de sistemas de arquivos](#)
- [Servidores de DNS ou controladores de domínio inacessíveis](#)
- [Credenciais inválidos da conta de serviço](#)
- [A Amazon não FSx pode acessar as credenciais da sua conta de serviço do Active Directory em AWS Secrets Manager](#)
- [Permissões insuficientes da conta de serviço](#)
- [Capacidade excedida da conta de serviço](#)
- [A Amazon não FSx pode acessar a unidade organizacional \(OU\)](#)
- [A conta de serviço não consegue acessar o grupo de administradores](#)
- [A Amazon FSx perdeu a conectividade no domínio](#)
- [A conta de serviço não tem permissões corretas](#)
- [Caracteres Unicode usados em parâmetros de criação](#)
- [Falha ao mudar o tipo de armazenamento para HDD durante a restauração de um backup](#)

## Grupo de segurança e rede VPC configurados incorretamente ACLs

Certifique-se de que os grupos de segurança e a rede da VPC ACLs estejam configurados usando a configuração recomendada do grupo de segurança. Para obter mais informações, consulte [Criar grupos de segurança](#).

## Nomes duplicados de grupo de administradores de sistemas de arquivos

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.
```

A 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, a Amazon FSx tentará usar o valor padrão “Administradores de domínio” como grupo de administradores. A solicitação falhará se houver mais de um grupo usando o nome padrão “Administradores de domínio”.

Reproduza as etapas a seguir para solucionar o problema.

1. Analise os [pré-requisitos](#) para associar o 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 para Windows File Server associado a um Active Directory autogerenciado.
3. Crie um novo sistema de arquivos usando o Console de gerenciamento da AWS ou AWS CLI. Para obter mais informações, consulte [Unindo um sistema de FSx arquivos da Amazon a um domínio autogerenciado do Microsoft Active Directory](#).
4. Dê um nome ao grupo de administradores do sistema de arquivos que seja exclusivo no domínio do Active Directory autogerenciado.

## Servidores de 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 conectividade e roteamento de rede entre a sub-rede em que você está criando um sistema de FSx arquivos da Amazon e seu Active Directory autogerenciado. Para obter mais informações, consulte [Pré-requisitos](#).

Use a [ferramenta de validação do Amazon FSx Active Directory](#) para testar e verificar essas configurações de rede.

 **Note**

Se você tiver vários sites do Active Directory definidos, certifique-se de que as sub-redes na VPC associadas ao seu sistema de FSx arquivos da Amazon estejam definidas em um site do Active Directory e que não existam conflitos de IP 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.

2. Verifique se você configurou os grupos de segurança da VPC que você associou ao seu sistema de FSx arquivos da Amazon, junto com qualquer rede VPC ACLs, para permitir o tráfego de saída da rede 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 Active Directory permitam o tráfego do seu sistema de FSx arquivos da Amazon. Para obter mais informações, consulte a [Documentação do Microsoft Active Directory](#).

## Credenciais inválidas da conta de serviço

Falha na criação de um sistema de arquivos associado ao Active Directory autogerenciado 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.

Caso 1: Se você estiver usando um AWS Secrets Manager segredo para armazenar suas credenciais do Active Directory

1. Consulte [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#).
2. no ARN secreto está correto e segue o formato adequado:  
`arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`.
3. Verifique se o segredo contém os dois campos obrigatórios com valores não vazios:
  - CUSTOMER\_MANAGED\_ACTIVE\_DIRECTORY\_USERNAME: seu nome de usuário da conta de serviço do AD.
  - CUSTOMER\_MANAGED\_ACTIVE\_DIRECTORY\_PASSWORD: a senha da sua conta de serviço do AD.
4. Verifique se o segredo e a chave têm uma política baseada em recursos que concede ao principal FSx serviço da Amazon `fsx.amazonaws.com` com permissão para recuperar o valor secreto.

Caso 2: se você estiver usando credenciais de texto não criptografado para ingressar no seu Active Directory

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 [Conta de FSx serviço da Amazon](#).

## A Amazon não FSx pode acessar as credenciais da sua conta de serviço do Active Directory em AWS Secrets Manager

As seções a seguir descrevem problemas comuns e como resolvê-los.

A associação a um sistema de arquivos do seu Active Directory autogerenciado gera uma falha com a seguinte mensagem de erro:

```
You can't provide both username/password and a domain join service account secret to connect to your Active Directory. Provide only one set of credentials.
```

Para resolver esse problema

1. Defina se prefere fornecer credenciais armazenadas em um segredo do Secrets Manager ou em texto não criptografado.
2. Ao ingressar em um Active Directory, forneça apenas um desses parâmetros e não ambos.

A associação a um sistema de arquivos do seu Active Directory autogerenciado gera uma falha com a seguinte mensagem de erro:

```
The domain join service account secret ARN format you entered isn't valid. Use the format: arn:partition:secretsmanager:region:account-id:secret:secret-name-6chars
```

Para resolver esse problema

1. Consulte [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#).
2. Verifique se o formato do ARN que você está inserindo está correto.  
Um exemplo de formato correto é `arn:aws:secretsmanager:us-east-1:123456789012:secret:MyDatabaseSecret-Ab3d5f`.

A associação a um sistema de arquivos do seu Active Directory autogerenciado gera uma falha com a seguinte mensagem de erro:

```
Amazon FSx can't access the domain join service account secret [ARN]. Add a resource permission to the secret that grants the FSx service principal (fsx.amazonaws.com) permission to access it.
```

Para resolver esse problema

1. Consulte [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#).
2. Verifique se o segredo do Secrets Manager que você está fornecendo tem as políticas corretas que permitem que FSx a Amazon use o segredo.

A associação a um sistema de arquivos do seu Active Directory autogerenciado gera uma falha com a seguinte mensagem de erro:

You don't have permission to access the domain join service account secret [ARN]. A resource permission needs to be added to the secret to grant you access.

Para resolver esse problema

- O proprietário ou administrador do segredo do Secrets Manager precisa dar acesso à sua conta para usar esse segredo. Para obter mais informações, consulte [Políticas baseadas em identidade](#).

A associação a um sistema de arquivos do seu Active Directory autogerenciado gera uma falha com a seguinte mensagem de erro:

```
The domain join service account secret format or content isn't valid. Make
sure the secret includes both CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME
and CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD fields with non-empty
values.
```

Para resolver esse problema

1. Consulte [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#).
2. Verifique se o segredo do Secrets Manager que você está fornecendo tem os dois campos obrigatórios.

## 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 [Conta de FSx serviço da Amazon](#).

## Capacidade excedida 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 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 obter mais informações, consulte [Conta de FSx serviço da Amazon](#).

## A Amazon não FSx 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 [Conta de FSx serviço da Amazon](#).

## 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= FSx Admins, 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 forneceu um parâmetro de grupo de administradores, a Amazon FSx tentará usar o `Builtin Domain Admins` grupo 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.

## A 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, a Amazon FSx conseguiu acessar os servidores DNS e controladores de domínio do seu domínio do Active Directory e unir o sistema de arquivos com sucesso ao seu domínio do Active Directory. No entanto, ao concluir a criação do sistema de arquivos, a Amazon FSx perdeu a conectividade ou a associação ao seu domínio. Use as etapas a seguir para solucionar o problema.

1. Garanta que a conectividade de rede continue existindo entre o sistema de FSx arquivos da Amazon e o Active Directory. E garanta que o tráfego de rede continue sendo permitido entre eles usando regras de roteamento, regras de grupo de segurança VPC, ACLs rede VPC e regras de firewall do controlador de domínio.
2. Certifique-se de que os objetos de computador criados pela Amazon FSx para seus sistemas de arquivos em seu 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 [Conta de FSx serviço da Amazon](#).

## Caracteres Unicode usados em 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.
```

A Amazon FSx não oferece suporte a 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.

## 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 SSD. Para obter mais informações, consulte [Como monitorar os aumentos da capacidade de armazenamento](#).
2. Faça um backup do sistema de arquivos iniciado pelo usuário. Para obter 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 obter mais informações, consulte [Restaurar backups em um novo sistema de arquivos](#).

## O sistema de arquivos está em um estado de configuração incorreta

Um sistema FSx de arquivos do 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 configurado incorretamente inclui uma mensagem de erro e uma ação corretiva recomendada que você pode acessar usando o FSx console, a API ou a Amazon. 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.

 Important

Não mova objetos de computador que a Amazon FSx cria na OU após a criação do sistema de arquivos. Isso fará com que o sistema de arquivos fique configurado incorretamente.

(Para obter a lista completa dos requisitos do Active Directory, consulte [Pré-requisitos](#). Você também pode validar se seu ambiente do Active Directory está configurado adequadamente para atender a esses requisitos usando a [ferramenta de validação do Amazon FSx Active Directory](#).)

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 FSx console da Amazon, da API ou AWS CLI 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 Tentativa de recuperação ao lado do status de configuração incorreta no FSx console da Amazon ou use o `StartMisconfiguredStateRecovery` comando no FSx console da Amazon, na API ou AWS CLI.

## Tópicos

- [Sistema de arquivos configurado incorretamente: a Amazon não FSx consegue acessar os servidores DNS nem os controladores de domínio do seu domínio.](#)
- [Sistema de arquivos com configuração incorreta: as credenciais da conta de serviço são inválidas](#)
- [Sistema de arquivos configurado incorretamente: a chave AWS Secrets Manager secreta ou KMS não está configurada corretamente](#)
- [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 configurado incorretamente: a Amazon não FSx consegue acessar os servidores DNS nem os controladores de domínio do seu domínio.

Um sistema de arquivos entrará em um Misconfigured estado em que a Amazon não FSx poderá 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 Amazon FSx Active Directory](#) para testar e verificar as configurações de rede do seu Active Directory autogerenciado. Para obter mais informações, consulte [Usar um Microsoft Active Directory autogerenciado](#).
3. Analise a configuração autogerenciada do Active Directory do sistema de arquivos no FSx console da Amazon.
4. Para atualizar a configuração autogerenciada do Active Directory do sistema de arquivos, você pode usar o FSx console da Amazon.
  - 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 da Amazon FSx CLI ou a operação da API. [UpdateFileSystem](#)

## Sistema de arquivos com configuração incorreta: as credenciais da conta de serviço são inválidas

A Amazon não FSx pode 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 obter mais informações, consulte [Usar um 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 correta ou as credenciais da conta usando o FSx console da Amazon.
  - 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.

Você também pode usar a operação de FSx API da Amazon `update-file-system`. Para saber mais, consulte [UpdateFileSystem](#) na Amazon FSx API Reference.

## Sistema de arquivos configurado incorretamente: a chave AWS Secrets Manager secreta ou KMS não está configurada corretamente

A Amazon não FSx pode estabelecer uma conexão com seu controlador ou controladores de domínio do Microsoft Active Directory. Isso ocorre porque seu AWS Secrets Manager segredo ou não AWS KMS key está configurado corretamente. Para obter mais informações, consulte [Armazenando credenciais do Active Directory usando AWS Secrets Manager](#).

Para resolver a configuração incorreta, faça o seguinte:

1. Verifique se o ARN secreto está correto e segue o formato adequado:  
`arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`.
2. Verifique se o segredo contém os dois campos obrigatórios com valores não vazios:
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`: seu nome de usuário da conta de serviço do AD.
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`: a senha da sua conta de serviço do AD.
  - Verifique se o segredo e a chave têm uma política baseada em recursos que concede ao principal FSx serviço da Amazon `fsx.amazonaws.com` com permissão para recuperar o valor secreto.

## Sistema de arquivos com configuração incorreta: a conta de serviço fornecida não tem permissão para associar o sistema de arquivos ao domínio

A Amazon não FSx pode 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 FSx serviço da Amazon ou crie uma nova conta de serviço com as permissões necessárias. Para obter mais informações sobre como fazer isso, consulte [Conta de FSx serviço da Amazon](#).
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 FSx console da Amazon.
  - 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 a operação de FSx API da Amazon `update-file-system`. Para saber mais, consulte [UpdateFileSystem](#) na Amazon FSx API Reference.

## Sistema de arquivos com configuração incorreta: a conta de serviço não consegue associar mais computadores ao domínio

A Amazon não FSx pode 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 autogerenciada do Active Directory do sistema de arquivos com as novas credenciais da conta de serviço usando o console da 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 a operação de FSx API da Amazon `update-file-system`. Para saber mais, consulte [UpdateFileSystem](#) na Amazon FSx API Reference.

## Sistema de arquivos com configuração incorreta: a conta de serviço não tem acesso à UO

A Amazon não FSx pode estabelecer uma conexão com seus controladores de domínio do Microsoft Active Directory porque a conta de serviço fornecida não tem acesso à OU 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.

Você também pode usar a operação de FSx API da Amazon `update-file-system`. Para saber mais, consulte [UpdateFileSystem](#) na Amazon FSx API Reference.

## Não é possível configurar a 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 obter 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 a Amazon não FSx consegue acessar o sistema de arquivos AWS KMS key

Uma solicitação de aumento da capacidade de armazenamento falhou porque a Amazon não FSx conseguiu acessar a chave KMS usada para criptografar o sistema de arquivos.

Você precisa garantir que a Amazon FSx tenha acesso à chave KMS usada para criptografar o sistema de arquivos 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, o sistema de arquivos e qualquer um de seus backups que use a chave do KMS excluída não serão passíveis de recuperação. Para obter mais informações, consulte [Excluindo AWS KMS keys](#) no Guia do AWS Key Management Service desenvolvedor.
- Se a chave do KMS estiver desabilitada e for uma chave gerenciada pelo cliente, será necessário habilitá-la e tentar novamente a solicitação de aumento da capacidade de armazenamento. Para obter mais informações, consulte [Ativação e desativação de chaves](#) no Guia do AWS Key Management Service desenvolvedor.
- Se a chave for inválida por exclusão pendente, você deverá [cancelar a exclusão da chave](#) enquanto ela ainda estiver em um estado PendingDeletion. Você poderá repetir a solicitação quando a chave do KMS estiver Enabled.
- 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 AWS Key Management Service desenvolvedor. 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 MBps.

Aumente a capacidade de taxa de transferência do sistema de arquivos para um mínimo de 16 e, em seguida MBps, repita a solicitação. Para obter mais informações, consulte [Como gerenciar a capacidade de throughput](#).

## A atualização da capacidade de taxa de transferência para 8 falhas MBps

Uma solicitação para modificar a capacidade de taxa de transferência de um sistema de arquivos para 8 MBps falhou.

Isso pode ocorrer quando uma solicitação de aumento da capacidade de armazenamento está pendente ou em andamento. Os aumentos da capacidade de armazenamento exigem uma taxa de transferência mínima de 16 MBps. 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.

# Histórico do documento

- Versão da API: 1/3/2018
- Última atualização da documentação: 30 de setembro de 2025

A tabela a seguir descreve mudanças importantes no Guia do usuário do Amazon FSx Windows. Para receber notificações sobre atualizações da documentação, inscreva-se no feed RSS.

| Alteração                                                                            | Descrição                                                                                                                                                                                                                                                                                                                               | Data                   |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <a href="#">Support adicionado para AWS Secrets Manager integração</a>               | A Amazon FSx agora se integra ao gerenciamento AWS Secrets Manager aprimorado das credenciais do Active Directory. Para obter mais informações, consulte <a href="#">Armazenando credenciais do Active Directory usando AWS Secrets Manager</a> .                                                                                       | 5 de novembro de 2025  |
| <a href="#">Amazon FSx ConsoleFullAccess — Atualização de uma política existente</a> | A Amazon FSx adicionou uma nova permissão, <code>secretsmanager:ListSecrets</code> , que permite que os diretores listem segredos AWS Secrets Manager para selecionar as credenciais da conta de serviço de adesão ao domínio. Para obter mais informações, consulte a <a href="#">política AWS gerenciada: Amazon FSx FullAccess</a> . | 5 de novembro de 2025  |
| <a href="#">Support adicionado para o Internet Protocol versão 6 (IPv6)</a>          | FSx para Windows File Server, os sistemas de arquivos agora oferecem                                                                                                                                                                                                                                                                    | 30 de setembro de 2025 |

suporte a duas opções de tipo de rede: IPv4 -only e dual-stack (para ambos e). IPv4 IPv6 Especifique uma dessas opções ao criar o sistema de arquivos. Você pode alterar o tipo de rede de um sistema FSx de arquivos existente do Windows File Server a qualquer momento. Para obter mais informações, consulte [Como gerenciar o tipo de rede](#).

[A Amazon FSx atualizou a política FSx ServiceRolePolicy AWS gerenciada da Amazon](#)

A Amazon FSx adicionou as `ec2:UnassignIpv6Addresses` permissões `ec2:AssignIpv6Addresses` e à Amazon FSxServiceRolePolicy. Para obter mais informações, consulte [Amazon FSx ServiceRolePolicy](#).

22 de julho de 2025

[A Amazon FSx atualizou a política FSx FullAccess AWS gerenciada da Amazon](#)

A política FSx FullAccess gerenciada da [Amazon](#) foi atualizada para adicionar as `fsx:DetachAndDeleteS3AccessPoint` permissões `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments`, e.

25 de junho de 2025

[A Amazon FSx atualizou a política FSx ConsoleFullAccess AWS gerenciada da Amazon](#)

A política FSx ConsoleFullAccess gerenciada da [Amazon](#) foi atualizada para adicionar as fsx:DetachAndDeleteS3AccessPoint permissões fsx:CreateAndAttachS3AccessPoint fsx:DescribeS3AccessPointAttachments , e.

25 de junho de 2025

[A Amazon FSx atualizou a política FSx ConsoleReadOnlyAccess AWS gerenciada da Amazon](#)

A Amazon FSx atualizou a FSx ConsoleReadOnlyAccess política da Amazon para adicionar a ec2:DescribeNetworkInterfaces permissão. Para obter mais informações, consulte a FSx ConsoleReadOnlyAccess política [da Amazon](#).

25 de fevereiro de 2025

[Support adicionado para endpoints de interface VPC de pilha dupla para Amazon FSx](#)

Agora você pode criar endpoints de interface VPC de pilha dupla para a FSx Amazon com endereços IP IPv4 IPv6 e nomes DNS. Para obter mais informações, consulte [FSx Windows File Server e interface VPC endpoints](#).

7 de fevereiro de 2025

[Adição de suporte para endpoints da API de pilha dupla](#)

A API FSx de serviços da Amazon para criar e gerenciar sistemas de arquivos tem novos endpoints de pilha dupla. Para obter mais informações, consulte os [endpoints da API](#) na Amazon FSx API Reference.

7 de fevereiro de 2025

[A Amazon FSx atualizou a política FSx ConsoleFullAccess AWS gerenciada da Amazon](#)

A Amazon FSx atualizou a FSx ConsoleFullAccess política da Amazon para adicionar a `ec2:DescribeNetworkInterfaces` permissão. Para obter mais informações, consulte a FSx ConsoleFullAccess política [da Amazon](#).

7 de fevereiro de 2025

[Versão atualizada da ferramenta de validação do Active Directory FSx para Windows File Server](#)

Uma versão atualizada da ferramenta de validação do Active Directory FSx para Windows File Server está disponível. Para obter mais informações, consulte [Validando sua configuração do Active Directory](#)

6 de novembro de 2024

[Support adicionado para níveis mais altos de IOPS em sistemas de arquivos com capacidades de taxa de transferência de 4 ou mais GBps](#)

FSx para Windows, o File Server está aumentando o IOPS máximo de 130 K para 150 K para sistemas de arquivos com 4 GBps de capacidade de taxa de transferência ou mais, de 175 K para 200 K para sistemas de arquivos com 6 de capacidade e de taxa GBps de transferência ou superior, de 260 K para 300 K para sistemas de arquivos com 9 de capacidade e de taxa de transferência ou superior e de 350 K para 400 K para sistemas GBps de arquivos com 12 de capacidade e de taxa de transferência ou superior. GBps Para obter mais informações, consulte sobre [FSx o desempenho do Windows File Server](#).

17 de janeiro de 2024



[A Amazon FSx FSx FullAccess atualizou as políticas FSx ServiceRolePolicy AWS gerenciadas da Amazon FSx ConsoleFullAccess FSx ReadOnlyAccess FSxConsoleReadOnlyAccess, Amazon, Amazon e Amazon](#)

A Amazon FSx atualizou as FSx ServiceRolePolicy políticas da Amazon FSx FullAccess FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon, Amazon FSxConsoleReadOnlyAccess, Amazon e Amazon para adicionar a `ec2:GetSecurityGroupsForVpc` permissão. Para obter mais informações, consulte as [FSx atualizações da Amazon para políticas AWS gerenciadas](#).

9 de janeiro de 2024

[A Amazon FSx atualizou a Amazon FSx FullAccess e as políticas FSx ConsoleFullAccess AWS gerenciadas pela Amazon](#)

A Amazon FSx atualizou as FSx ConsoleFullAccess políticas da Amazon FSx FullAccess e da Amazon para adicionar a `ManageCrossAccountDataReplication` ação. Para obter mais informações, consulte as [FSx atualizações da Amazon para políticas AWS gerenciadas](#).

20 de dezembro de 2023

[A Amazon FSx atualizou a Amazon FSx FullAccess e as políticas FSx ConsoleFullAccess AWS gerenciadas pela Amazon](#)

A Amazon FSx atualizou as FSx ConsoleFullAccess políticas da Amazon FSx FullAccess e da Amazon para adicionar a `fsx:CopySnapshotAndUpdateVolume` permissão. Para obter mais informações, consulte as [FSx atualizações da Amazon para políticas AWS gerenciadas](#).

26 de novembro de 2023

[A Amazon FSx atualizou a Amazon FSx FullAccess e as políticas FSx ConsoleFullAccess AWS gerenciadas pela Amazon](#)

A Amazon FSx atualizou as FSx ConsoleFullAccess políticas da Amazon FSx FullAccess e da Amazon para adicionar as `fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` permissões e. Para obter mais informações, consulte as [FSx atualizações da Amazon para políticas AWS gerenciadas](#).

14 de novembro de 2023

[Suporte adicionado para atualizar o tipo de armazenamento do sistema de arquivos](#)

FSx para sistemas de arquivos do Windows File Server agora oferecem suporte à 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](#)

FSx para Windows File Server, os sistemas de arquivos agora oferecem suporte a até 12 capacidades de taxa de GBps transferência. Para obter mais informações, consulte sobre [FSx o desempenho do Windows File Server](#).

9 de agosto de 2023

[Suporte adicionado para provisionamento de IOPS de SSD](#)

FSx para sistemas de arquivos do Windows File Server agora oferecem suporte ao provisionamento de IOPS SSD, independentemente da capacidade de armazenamento, até um máximo de 350.000 IOPS. Para obter mais informações, consulte [Managing SSD IOPS](#).

9 de agosto de 2023

[A Amazon FSx atualizou a política FSx ServiceRolePolicy AWS gerenciada da Amazon](#)

A Amazon FSx atualizou a `cloudwatch:PutMetricData` permissão na Amazon FSxServiceRolePolicy. Para obter mais informações, consulte [Amazon FSx ServiceRolePolicy](#).

24 de julho de 2023

[A Amazon FSx atualizou a política FSx FullAccess AWS gerenciada da Amazon](#)

A Amazon FSx atualizou a FSx FullAccess política da Amazon para remover a `fsx:*` permissão e adicionar `fsx` ações específicas. Para obter mais informações, consulte a FSx FullAccess política [da Amazon](#).

13 de julho de 2023

[A Amazon FSx atualizou a política FSx ConsoleFullAccess AWS gerenciada da Amazon](#)

A Amazon FSx atualizou a FSx ConsoleFullAccess política da Amazon para remover a fsx : \* permissão e adicionar fsx ações específicas. Para obter mais informações, consulte a FSx ConsoleFullAccess política [da Amazon](#).

13 de julho de 2023

[Support adicionado para novas CloudWatch métricas do Amazon FSx for Windows File Server](#)

FSx para Windows File Server agora fornece CloudWatch métricas 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](#)

A Amazon FSx agora fornece avisos na janela 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 FSx console Amazon FSx para sistemas de arquivos do Windows File Server inclui novas seções de resumo, armazenamento e desempenho. 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 você pode usar endpoints VPC de interface para acessar a FSx API da Amazon a partir da sua VPC sem enviar tráfego pela Internet. Para obter mais informações, consulte [Amazon FSx e a interface de VPC endpoints](#).

5 de abril de 2022

### [Suporte adicionado para o Amazon Kendra](#)

Agora você pode usar seu FSx sistema de arquivos do Windows File Server como fonte de dados para o Amazon Kendra, permitindo indexar e pesquisar informações contidas em documentos armazenados em seu sistema de arquivos. Para obter mais informações, consulte [Usando o FSx Windows File Server com o 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 FSx a Amazon 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 CloudFormation modelo personalizável AWS desenvolvido para aumentar automaticamente a capacidade e 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 FSx os sistemas de arquivos do Windows File Server com clientes locais usando endereços IP não privados. Para obter mais informações, consulte [Supported environments.](#) Você pode associar o sistema FSx de arquivos do Windows File Server a um Microsoft Active Directory autogerenciado com servidores DNS e controladores de domínio AD que usam endereços IP não privados. Para obter mais informações, consulte [Usando a Amazon FSx com seu Microsoft Active Directory autogerenciado.](#)

17 de dezembro de 2020

### [Suporte adicionado para usar aliases de DNS](#)

Agora você pode associar aliases de DNS aos seus sistemas FSx de arquivos do 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 Windows File Server com o Amazon ECS. Para obter mais informações, consulte [Supported Clients.](#)

9 de novembro de 2020

### [A Amazon agora FSx está integrada com AWS Backup](#)

Agora você pode usar AWS Backup para fazer backup e restaurar seus sistemas de FSx arquivos, além de usar FSx backups nativos da Amazon. Para obter mais informações, consulte [Usando AWS Backup com a Amazon FSx.](#)

9 de novembro de 2020



[Suporte adicionado para a escalabilidade da capacidade de throughput](#)

Agora você pode modificar a capacidade de taxa de transferência dos sistemas de arquivos do Windows File Server existentes FSx à medida que seus requisitos de taxa de transferência 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 Windows File Server existentes FSx 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 desempenho ao ser usado FSx no Windows File Server. Para obter mais informações, consulte [Otimizando custos com a 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 FSx para o seu servidor de arquivos do Windows. 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, deduplicação de dados, cotas de armazenamento e criptografia em trânsito para seus compartilhamentos de arquivos usando a Amazon FSx CLI 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 ao Multi-AZ](#)

Você pode usar a implantação Multi-AZ 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 de Pastas Compartilhadas nativa do Microsoft Windows para gerenciar sessões de usuários e abrir arquivos em seus FSx sistemas de arquivos do 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 você pode configurar as cópias de sombra do Windows em seus sistemas FSx de arquivos do 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 ao Microsoft Active Directory](#)

Agora você pode unir FSx os sistemas de arquivos do Windows File Server a AWS Managed Microsoft AD 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 ao Microsoft Active Directory](#)

Agora você pode unir FSx os sistemas de arquivos do Windows File Server aos seus domínios autogerenciados do Microsoft Active Directory, no local ou na nuvem. Para obter mais informações, consulte [Active Directory Support](#).

24 de junho de 2019

[A Amazon FSx está em conformidade com a certificação SOC](#)

FSx A Amazon foi avaliada para estar em 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 Direct Connect suporte à conexão de emparelhamento de VPC entre regiões](#)

Os sistemas de FSx arquivos da Amazon criados após 22 de fevereiro de 2019 podem ser acessados usando Direct Connect VPN e emparelhamento de VPC entre regiões. Para obter mais informações, consulte [Supported Access Methods](#).

25 de fevereiro de 2019

[Suporte adicionado ao 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 a partir de recursos locais e de recursos em uma Amazon Conta da AWS VPC diferente ou. Para obter mais informações, consulte [Supported Access Methods](#).

22 de fevereiro de 2019

[A Amazon agora FSx está disponível ao público em geral](#)

O Amazon FSx para Windows File Server fornece servidores de arquivos Microsoft Windows que são totalmente gerenciados, apoiados por um sistema de arquivos Windows totalmente nativo. O Amazon FSx para Windows File Server fornece os recursos, o desempenho e a compatibilidade para os quais é fácil migrar e migrar aplicativos corporativos 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.