



Windows-Benutzerhandbuch

# Amazon FSx für Windows File Server



# Amazon FSx für Windows File Server: Windows-Benutzerhandbuch

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

---

# Table of Contents

Was ist FSx for Windows File Server? .....	1
Amazon FSx-Ressourcen .....	1
Zugreifen auf Dateifreigaben .....	2
Sicherheit und Datenschutz .....	2
Verfügbarkeit und Beständigkeit .....	3
Verwalten von Dateisystemen .....	3
Flexibilität bei Preis und Leistung .....	3
Preise für Amazon FSx .....	4
Annahmen .....	4
Voraussetzungen .....	5
Foren für Amazon FSx for Windows File Server .....	5
Sind Sie ein Erstbenutzer von Amazon FSx? .....	6
Bewährte Methoden für FSx für Windows .....	7
Allgemeine bewährte Methoden .....	7
Testen Sie Ihre Workloads, bevor Sie zur Produktion übergehen .....	7
Erstellen eines Überwachungsplans .....	7
Stellen Sie sicher, dass Ihre Dateisysteme über ausreichende Ressourcen verfügen .....	8
Erstellen Sie regelmäßig Backups Ihrer Dateisysteme .....	8
Bewährte Methoden für die Gewährleistung der Sicherheit .....	8
Netzwerksicherheit .....	8
Active Directory .....	9
Konfiguration und Anpassung der Größe Ihres Dateisystems .....	11
Auswahl eines Bereitstellungstyps .....	11
Auswahl eines Speichertyps .....	11
Auswahl einer Durchsatzkapazität .....	12
Erhöhen Sie Ihre Speicherkapazität und Durchsatzkapazität .....	12
Änderung der Durchsatzkapazität in Leerlaufphasen .....	13
Erste Schritte .....	14
Richten Sie Ihr ein AWS-Konto .....	14
.....	15
Erstellen Sie Ihr Dateisystem .....	16
Ordnen Sie Ihre Dateifreigabe einer EC2-Instance zu, auf der Windows Server ausgeführt wird .....	23
Schreiben Sie Daten in Ihre Dateifreigabe .....	24

Erstellen Sie ein Backup Ihres Dateisystems .....	24
Bereinigen von -Ressourcen .....	25
Status des Amazon FSx-Dateisystems .....	27
Unterstützte Clients, Zugriffsmethoden und Umgebungen .....	29
Unterstützte Clients .....	29
Unterstützte Zugriffsmethoden .....	30
Zugriff auf Dateisysteme mit ihren Standard-DNS-Namen .....	30
Zugreifen auf Dateisysteme mithilfe von DNS-Aliasen .....	31
Arbeiten mit FSx for Windows File Server Dateisysteme und DFS-Namespaces .....	32
Unterstützte Umgebungen .....	32
Zugriff auf FSx von lokalen .....	34
Zugriff auf FSx for Windows File Server Dateisysteme von einer anderen VPC,AWS- Region .....	34
Verfügbarkeit und Beständigkeit .....	36
Wählen Sie die Single-AZ- oder Multi-AZ-Dateisystembereitstellung .....	36
Funktionsunterstützung nach Bereitstellungstyp .....	37
Failover-Prozess für FSx for Windows File Server .....	38
Failover-Erfahrung auf Windows-Clients .....	38
Failover-Erfahrung auf Linux-Clients .....	39
Testen des Failovers auf einem Dateisystem .....	39
Arbeiten mit Single- und Multi-AZ-Dateisystemressourcen .....	39
Subnetze .....	39
Elastische Netzwerkschnittstellen für Dateisysteme .....	40
Kostenoptimierung mit Amazon FSx .....	42
Flexibilität, Speicher und Durchsatz unabhängig voneinander zu wählen .....	42
Optimierung der Speicherkosten .....	43
Kostenoptimierung mithilfe von Speichertypen .....	43
Optimierung der Speicherkosten mithilfe von Datendeduplizierung .....	43
Nutzung und Abrechnung überprüfen .....	43
Arbeiten mit Active Directory .....	45
Benutzen AWS Managed Microsoft AD .....	46
Voraussetzungen für das Netzwerk .....	47
Verwenden Sie ein Modell zur Isolierung von Ressourcengesamtstrukturen .....	52
Testen Sie Ihre Active Directory-Konfiguration .....	52
Verwendung AWS Managed Microsoft AD in einer anderen VPC oder einem anderen Konto .....	53

Überprüfen der Konnektivität zu Ihren Active Directory-Domänencontrollern .....	54
Verwenden eines selbstverwalteten Active Directory .....	57
Voraussetzungen für selbstverwaltetes Active Directory .....	60
Bewährte Methoden für selbstverwaltetes Active Directory .....	66
Überprüfen Sie Ihre Active Directory-Konfiguration .....	70
Verbinden von FSx mit einem selbstverwalteten Active Directory .....	74
Abrufen der richtigen Dateisystem-IP-Adressen zur Verwendung für DNS .....	84
Aktualisieren Sie die selbstverwaltete Active Directory-Konfiguration .....	85
Verwenden von Microsoft Windows-Dateifreigaben .....	90
Zugreifen auf Dateifreigaben .....	90
Zuordnen einer Dateifreigabe auf einer Amazon EC2 EC2-Windows-Instance .....	90
Mounten einer Dateifreigabe auf einer Amazon EC2 Mac-Instance .....	93
Mounten einer Dateifreigabe auf einer Amazon EC2 EC2-Linux-Instance .....	96
Automatisches Mounten von Dateifreigaben auf einer Amazon Linux EC2-Instance, die nicht mit Ihrem Active Directory verknüpft ist .....	102
Migration zu Amazon FSx .....	106
Migrieren von Dateien zu FSx for Windows File Server .....	106
Bewährte Methoden für die Migration .....	107
Migrieren von Dateien mit AWS DataSync .....	107
Migrieren von Dateien mit Robocopy .....	111
Migration von Dateifreigabekonfigurationen .....	115
Migration der DNS-Konfiguration zur Verwendung von Amazon FSx .....	117
Umstellung auf Amazon FSx .....	120
Vorbereitung der Umstellung auf Amazon FSx .....	121
Konfigurieren Sie SPNs für die Kerberos-Authentifizierung .....	121
Aktualisieren Sie die DNS-CNAME-Einträge für das Amazon FSx-Dateisystem .....	125
Verwenden von FSx for Windows File Server mit Microsoft SQL Server mit Microsoft SQL Server .....	127
Amazon FSx für aktive SQL Server-Datendateien verwenden .....	127
Eine kontinuierlich verfügbare Aktie erstellen .....	128
SMB-Timeout-Einstellungen konfigurieren .....	128
Amazon FSx als SMB File Share Witness verwenden .....	128
Verwenden von FSx for Windows File Server mit Amazon Kendra .....	129
Dateisystemleistung .....	129
Schützen Sie Ihre Daten .....	130
Arbeiten mit Backups .....	130

Arbeiten mit automatischen täglichen Backups .....	131
Arbeiten mit vom Benutzer initiierten Backups .....	132
Verwenden von AWS Backup mit Amazon FSx .....	133
Kopieren eines Backups .....	134
Wiederherstellen von Sicherungen .....	138
Löschen eines Backups .....	139
Größe der Backups .....	140
Arbeiten Sie mit Schattenkopien .....	140
Bewährte Methoden .....	142
Schattenkopien einrichten .....	143
Konfigurieren Sie Schattenkopien so, dass sie die Standardeinstellungen verwenden .....	146
Einzelne Dateien und Ordner wiederherstellen .....	148
Einstellung der maximalen Speichermenge für Schattenkopien .....	149
Ihren Schattenkopie-Speicher anzeigen .....	151
Löschen des Schattenkopie-Speichers, des Zeitplans und aller Schattenkopien .....	152
Einen benutzerdefinierten Zeitplan für Schattenkopien erstellen .....	153
Ihren Schattenkopie-Zeitplan anzeigen .....	155
Löschen eines Schattenkopie-Zeitplans .....	155
Eine Schattenkopie erstellen .....	155
Vorhandene Schattenkopien anzeigen .....	156
Löschen von Schattenkopien .....	156
Geplante Replikation .....	158
Verwaltung von Dateisystemen .....	159
Verwenden des Amazon FSx Custom PowerShell .....	159
Starten einer Amazon FSx-Remotesitzung PowerShell .....	161
DNS-Aliase .....	162
DNS-Aliasstatus .....	164
Verwendung von DNS-Aliassen mit Kerberos .....	165
Bestehende DNS-Aliase anzeigen .....	165
DNS-Aliase mit Dateisystemen verknüpfen .....	166
Verwaltung von DNS-Aliassen auf vorhandenen Dateisystemen .....	168
Verwaltung von Dateifreigaben .....	171
Dateifreigaben verwalten (GUI) .....	172
Dateifreigaben verwalten mit PowerShell .....	174
Prüfung des Dateizugriffs .....	177
Überprüfen Sie die Ziele des Ereignisprotokolls .....	178

Migrieren Sie Ihre Auditkontrollen .....	180
Ereignisprotokolle anzeigen .....	180
Einstellungen für die Überwachung von Dateien und Ordnern einrichten .....	188
Verwaltung der Dateizugriffsüberwachung .....	190
Benutzersitzungen und geöffnete Dateien .....	195
Verwenden der GUI zur Verwaltung von Benutzern und Sitzungen .....	195
Wird PowerShell zur Verwaltung von Benutzersitzungen und zum Öffnen von Dateien verwendet .....	199
Datendeduplizierung .....	199
Bewährte Methoden .....	201
Verwaltung der Datendeduplizierung .....	201
Datendeduplizierung aktivieren .....	203
Erstellen eines Zeitplans für die Datendeduplizierung .....	203
Ändern eines Zeitplans für die Datendeduplizierung .....	204
Die Menge des gespeicherten Speicherplatzes anzeigen .....	205
Problembehandlung bei der Datendeduplizierung .....	205
Speicherkontingente .....	208
Verwaltung von Benutzerspeicherkontingenten .....	209
Verwaltung der Verschlüsselung bei der Übertragung .....	209
Verwaltung der Speicherkonfiguration .....	211
Verwaltung der Speicherkapazität .....	211
Speichertyp verwalten .....	227
Verwalten von SSD-IOPS .....	231
Verwaltung der Durchsatzkapazität .....	236
Wann muss die Durchsatzkapazität geändert werden .....	237
So ändern Sie die Durchsatzkapazität .....	238
Überwachung von Änderungen der Durchsatzkapazität .....	240
Markieren Ihrer -Ressourcen mit Tags (Markierungen) .....	243
Grundlagen zu Tags (Markierungen) .....	243
Markieren Ihrer -Ressourcen .....	244
Tag (Markierung)-Einschränkungen .....	245
Berechtigungen und Tag .....	246
Wartungsfenster .....	246
Bewährte Methoden .....	247
Einmalige administrative Einrichtungsaufgaben .....	248
Laufende Verwaltungsaufgaben zur Überwachung Ihres Dateisystems .....	250

Gruppieren von Dateisystemen mit DFS-Namespaces .....	252
Einrichtung von DFS-Namespaces für die Gruppierung mehrerer Dateisysteme .....	252
Überwachung von FSx für Windows .....	255
Überwachungstools .....	255
Automatisierte Tools .....	255
Manuelle Überwachungstools .....	256
Überwachung von Metriken mit CloudWatch .....	257
FSx-Metriken CloudWatch .....	259
So verwenden Sie FSx for Windows File Server Server-Metriken .....	264
Leistungswarnungen und Empfehlungen .....	268
Zugreifen auf FSx for Windows File Server-Metriken .....	270
Erstellen von Alarmen .....	274
CloudTrail aufzeichnen .....	277
Amazon FSx Informationen in CloudTrail .....	277
Erläuterungen der Amazon FSx Einträge .....	278
Leistung .....	281
Leistung des Dateisystems .....	281
Zusätzliche Überlegungen zur Leistung .....	282
Latency .....	283
Durchsatz und IOPS .....	283
Leistung eines einzelnen Clients .....	283
Leistungssteigerung .....	283
Durchsatzkapazität und Leistung .....	284
Wahl der Durchsatzkapazität .....	287
Speicherkonfiguration und Leistung .....	288
Burst-Leistung von Festplatten .....	288
Beispiel: Speicherkapazität und Durchsatzkapazität .....	289
Messung der Leistung anhand von Metriken CloudWatch .....	290
Behebung von Leistungsproblemen .....	290
Anleitungen .....	291
Exemplarische Vorgehensweise 1: Voraussetzungen für die ersten Schritte .....	291
Schritt 1: Einrichten von Active Directory .....	291
Schritt 2: Starten Sie eine Windows-Instance in der Amazon EC2 EC2-Konsole .....	293
Schritt 3: Herstellen einer Verbindung zu Ihrer Instance .....	295
Schritt 4: Treten Sie Ihrer Instanz zu IhremAWS Directory ServiceVerzeichnis .....	297
Exemplarische Vorgehensweise 2: Erstellen eines Dateisystems aus einer Sicherung .....	299



Exemplarische Vorgehensweise 3: Aktualisieren Sie ein vorhandenes -Dateisystem .....	301
Komplettlösung 4: Verwenden von Amazon FSx mit Amazon AppStream 2.0 .....	302
Bereitstellung von persönlichem persistentem Speicher für jeden Benutzer .....	303
Bereitstellung eines gemeinsam genutzten Ordners für alle Benutzer .....	305
Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisystem .....	307
Schritt 1: Verknüpfen Sie DNS-Aliase mit Ihrem Amazon FSx-Dateisystem .....	307
Schritt 2: Konfigurieren Sie Service Principal Names (SPNs) für Kerberos .....	309
Schritt 3: Aktualisieren oder erstellen Sie einen DNS-CNAME-Eintrag für das Dateisystem ..	313
Erzwingen der Kerberos-Authentifizierung mithilfe von GPOs .....	315
Exemplarische Vorgehensweise 6: Skalierung der Leistung mit Shards .....	316
Einrichtung von DFS-Namespaces für Scale-Out-Leistung .....	316
Exemplarische Vorgehensweise 7: Kopieren einer Sicherung in ein anderesAWS-Region .....	319
Sicherheit .....	320
Datenverschlüsselung .....	321
Verwendung von Verschlüsselung .....	321
Verschlüsselung im Ruhezustand .....	321
Verschlüsselung während der Übertragung .....	323
Windows-ACLs .....	324
Weiterführende Links .....	325
Dateisystem-Zugriffskontrolle mit Amazon VPC .....	325
Amazon VPC-Sicherheitsgruppen .....	326
Amazon VPC-Netzwerk-ACLs .....	330
Identitäts- und Zugriffsverwaltung .....	330
Zielgruppe .....	331
Authentifizierung mit Identitäten .....	332
Verwalten des Zugriffs mit Richtlinien .....	336
Funktionsweise von Amazon FSx for Windows File Server mit IAM .....	338
Beispiele für identitätsbasierte Richtlinien .....	346
AWS Von verwaltete Richtlinien .....	349
Fehlerbehebung .....	365
Verwenden von Tags mit Amazon FSx .....	367
Verwenden von serviceverknüpften Rollen .....	372
Compliance-Validierung .....	378
Schnittstellen-VPC-Endpunkte .....	380
Überlegungen zu Amazon FSx Schnittstellen-VPC-Endpunkten .....	380

Erstellen eines Schnittstellen-VPC-Endpunkts für die Amazon FSx API .....	381
Erstellen einer VPC-Endpunktrichtlinie für Amazon FSx .....	381
Kontingente .....	383
Kontingente, die Sie erhöhen können .....	383
Ressourcenkontingente für jedes Dateisystem .....	385
Weitere Überlegungen .....	385
Kontingente für Microsoft Windows .....	386
Fehlerbehebung .....	387
Sie können nicht auf Ihr Dateisystem zugreifen .....	387
Die elastic network interface des Dateisystems wurde geändert oder gelöscht .....	388
Die Elastic IP-Adresse, die an die elastic network interface des Dateisystems angehängt ist, wurde gelöscht. ....	388
Der Sicherheitsgruppe des Dateisystems fehlen die erforderlichen Regeln für eingehenden oder ausgehenden Datenverkehr. ....	388
In der Sicherheitsgruppe der Compute-Instanz fehlen die erforderlichen Regeln für ausgehenden Datenverkehr .....	389
Die Compute-Instanz ist nicht mit einem Active Directory verbunden .....	389
Die Dateifreigabe ist nicht vorhanden .....	389
Dem Active Directory-Benutzer fehlen die erforderlichen Berechtigungen .....	389
Vollzugriff zulassen: NTFS-ACL-Berechtigungen wurden entfernt .....	390
Mit einem lokalen Client kann nicht auf ein Dateisystem zugegriffen werden .....	390
Das neue Dateisystem ist nicht im DNS registriert .....	390
Mit einem DNS-Alias kann nicht auf das Dateisystem zugegriffen werden .....	391
Über eine IP-Adresse kann nicht auf das Dateisystem zugegriffen werden .....	393
Das Erstellen des Dateisystems schlägt fehl .....	393
Dateisysteme, die mit AWS Managed Active Directory verknüpft sind .....	393
Das Erstellen eines Dateisystems, das mit einem selbstverwalteten Active Directory verknüpft ist, schlägt fehl .....	394
Das Dateisystem befindet sich in einem falsch konfigurierten Zustand .....	403
Falsch konfiguriertes Dateisystem: Amazon FSx kann weder die DNS-Server noch die Domain-Controller für Ihre Domain erreichen. ....	404
Falsch konfiguriertes Dateisystem: Die Anmeldeinformationen für das Dienstkonto sind ungültig .....	405
Falsch konfiguriertes Dateisystem: Das angegebene Servicekonto ist nicht berechtigt, das Dateisystem mit der Domain zu verbinden .....	406

Falsch konfiguriertes Dateisystem: Das Servicekonto kann keine weiteren Computer zur Domäne hinzufügen .....	407
Falsch konfiguriertes Dateisystem: Das Servicekonto hat keinen Zugriff auf die Organisationseinheit .....	407
Problembehandlung mit Remote Power Shell auf FSx for Windows File Server .....	408
Der Befehl New-F schlägt bei unidirektionaler Vertrauensstellung fehl SxSmbShare .....	408
Sie können mit Remote nicht auf Ihr Dateisystem zugreifen PowerShell .....	409
Sie können DFS-R nicht auf einem Multi-AZ- oder Single-AZ 2-Dateisystem konfigurieren .....	410
Aktualisierungen der Speicher- oder Durchsatzkapazität schlagen fehl .....	410
Die Erhöhung der Speicherkapazität schlägt fehl, weil Amazon FSx nicht auf den KMS-Verschlüsselungsschlüssel des Dateisystems zugreifen kann .....	410
Die Aktualisierung der Speicher- oder Durchsatzkapazität schlägt fehl, weil das selbstverwaltete Active Directory falsch konfiguriert ist .....	411
Die Erhöhung der Speicherkapazität schlägt aufgrund unzureichender Durchsatzkapazität fehl .....	411
Die Aktualisierung der Durchsatzkapazität auf 8 MB/s schlägt fehl .....	412
Das Umschalten des Speichertyps auf Festplatte während der Wiederherstellung eines Backups schlägt fehl .....	412
Problembehandlung bei Schattenkopien .....	413
Die ältesten Schattenkopien fehlen .....	413
Alle meine Schattenkopien fehlen .....	413
Auf einem kürzlich wiederhergestellten oder aktualisierten Dateisystem können keine Amazon FSx-Backups erstellt oder auf Schattenkopien zugegriffen werden .....	414
Fehlerbehebung bei der Leistung .....	414
Ermitteln Sie den Durchsatz und die IOPS-Grenzwerte für das Dateisystem .....	415
Was ist Netzwerk-I/O im Vergleich zu Festplatten-I/O? Warum unterscheiden sie sich? .....	415
Warum ist die CPU- oder Speicherauslastung hoch, wenn die Netzwerk-I/O niedrig ist? .....	416
Was ist Bursting? Wie viel Bursting verwendet mein Dateisystem? Was passiert, wenn das Burst-Guthaben aufgebraucht ist? .....	416
Auf der Seite Überwachung und Leistung wird eine Warnung angezeigt. Muss ich die Konfiguration meines Dateisystems ändern? .....	417
Meine Messwerte fehlten vorübergehend, sollte ich mir Sorgen machen? .....	418
Zusätzliche Informationen .....	419
Einen benutzerdefinierten Backup-Zeitplan einrichten .....	419
Übersicht über die Architektur .....	420
AWS CloudFormation Vorlage .....	421

---

Automatisierte Bereitstellung .....	421
Zusätzliche Optionen .....	423
Verwenden der DFS-Replikation .....	424
Einrichtung der DFS-Replikation .....	425
DFS-Namespaces für Failover einrichten .....	428
Arbeiten mit Maintenance Windows und FSx Multi-AZ .....	432
Dokumentverlauf .....	433
.....	cdxlvii

# Was ist FSx for Windows File Server?

Amazon FSx for Windows File Server bietet vollständig verwaltete Microsoft-Windows-Dateiserver, die von einem vollständig nativen Windows-Dateisystem unterstützt werden. FSx for Windows File Server bietet die Funktionen, die Leistung und die Kompatibilität, um Unternehmensanwendungen auf einfache Weise zu erweitern und zu verlagern. AWS Cloud

Amazon FSx unterstützt eine breite Palette von Windows-Workloads im Unternehmen mit vollständig verwaltetem Dateispeicher, der auf Microsoft Windows Server basiert. Amazon FSx bietet native Unterstützung für Windows-Dateisystemfunktionen und für das branchenübliche SMB-Protokoll (Server Message Block) für den Zugriff auf Dateispeicher über ein Netzwerk. Amazon FSx ist für Unternehmensanwendungen in der optimiert und bietet native Windows-Kompatibilität AWS Cloud, Unternehmensleistung und Funktionen sowie konsistente Latenzen unter einer Millisekunde.

Windows-Developer können ihre Arbeit mit dem Code, den Anwendungen und Tools, die heute gängig sind, mit dem Dateispeicher auf Amazon FSx unverändert fortsetzen. Zu den für Amazon FSx idealen Windows-Anwendungen und -Workloads gehören Geschäftsanwendungen, Basisverzeichnisse, Webserver, Inhaltsverwaltung, Datenanalyse, Software-Build-Setups und Workloads zur Medienverarbeitung.

Mit FSx for Windows File Server als vollständig verwaltetem Service entfällt der Verwaltungsaufwand, den die Einrichtung und Bereitstellung von Dateiservern und Speichervolumen mit sich bringt. Darüber hinaus hält Amazon FSx die Windows-Software auf dem neuesten Stand, erkennt und behebt Hardwarefehler und führt Backups durch. Es bietet auch eine umfassende Integration mit anderen AWS Diensten wie [AWS IAM](#), [AWS Directory Service for Microsoft Active Directory](#), [WorkSpaces](#), [AWS Key Management Service](#), [Amazon](#) und [AWS CloudTrail](#).

## Ressourcen für FSx for Windows File Server: Dateisysteme, Backups und Dateifreigaben

Die Hauptressourcen in Amazon FSx sind Dateisysteme und Backups. In einem Dateisystem speichern Sie Ihre Dateien und Ordner und greifen darauf zu. Ein Dateisystem besteht aus einem oder mehreren Windows-Dateiservern und Speichervolumen. Wenn Sie ein Dateisystem erstellen, geben Sie eine Menge an Speicherkapazität (in GiB), SSD-IOPS und Durchsatzkapazität (in MB/s) an. Sie können diese Eigenschaften an Ihre Bedürfnisse anpassen, nachdem Sie das Dateisystem erstellt haben. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#), [Verwalten von SSD-IOPS](#) und [Verwaltung der Durchsatzkapazität](#).

FSx for Windows File Server-Backups sind file-system-consistent äußerst robust und inkrementell. Um die Konsistenz des Dateisystems sicherzustellen, verwendet Amazon FSx den Volume Shadow Copy Service (VSS) in Microsoft Windows. Automatische tägliche Backups sind standardmäßig aktiviert, wenn Sie ein Dateisystem erstellen. Sie können auch jederzeit zusätzliche manuelle Backups erstellen. Weitere Informationen finden Sie unter [Arbeiten mit Backups](#).

Eine Windows-Dateifreigabe ist ein bestimmter Ordner (und seine Unterordner) in Ihrem Dateisystem, den Sie Ihren Recheninstanzen mit SMB zugänglich machen. Ihr Dateisystem verfügt bereits über eine standardmäßige Windows-Dateifreigabe namens `\share`. Mithilfe der grafischen Benutzeroberfläche (GUI) für gemeinsame Ordner unter Windows können Sie beliebig viele andere Windows-Dateifreigaben erstellen und verwalten. Weitere Informationen finden Sie unter [Verwenden von Microsoft Windows-Dateifreigaben](#).

Auf Dateifreigaben wird entweder über den DNS-Namen des Dateisystems oder über DNS-Aliase zugegriffen, die Sie dem Dateisystem zuordnen. Weitere Informationen finden Sie unter [DNS-Aliase verwalten](#).

## Zugreifen auf Dateifreigaben

Auf Amazon FSx kann über Compute-Instances mit dem SMB-Protokoll zugegriffen werden (unterstützt die Versionen 2.0 bis 3.1.1). Sie können von allen Windows-Versionen ab Windows Server 2008 und Windows 7 sowie von aktuellen Linux-Versionen aus auf Ihre Shares zugreifen. Sie können Ihre Amazon FSx-Dateifreigaben auf Amazon Elastic Compute Cloud (Amazon EC2) - Instances und auf WorkSpaces Instances, Amazon AppStream 2.0-Instances und VMware Cloud auf AWS VMs zuordnen.

Sie können von lokalen Compute-Instances aus mit oder auf Ihre Dateifreigaben zugreifen. AWS Direct Connect AWS VPN Neben dem Zugriff auf Dateifreigaben, die sich in derselben VPC, demselben AWS Konto und derselben AWS Region wie das Dateisystem befinden, können Sie auch auf Ihre Freigaben auf Compute-Instances zugreifen, die sich in einer anderen Amazon VPC, einem anderen Konto oder einer anderen Region von Amazon befinden. Sie tun dies mithilfe von VPC-Peering oder Transit-Gateways. Weitere Informationen finden Sie unter [Unterstützte Zugriffsmethoden](#).

## Sicherheit und Datenschutz

Amazon FSx bietet mehrere Sicherheits- und Compliance-Stufen, um sicherzustellen, dass Ihre Daten geschützt sind. Es verschlüsselt automatisch Daten im Ruhezustand (sowohl für Dateisysteme als auch für Backups) mithilfe von Schlüsseln, die Sie in AWS Key Management Service (AWS

KMS) verwalten. Daten während der Übertragung werden ebenfalls automatisch mit SMB-Kerberos-Sitzungsschlüsseln verschlüsselt. Es wurde auf die Einhaltung der ISO-, PCI-DSS- und SOC-Zertifizierungen geprüft und ist HIPAA-fähig.

Amazon FSx bietet Zugriffskontrolle auf Datei- und Ordner Ebene mit Windows-Zugriffskontrolllisten (ACLs). Es bietet Zugriffskontrolle auf Dateisystemebene mithilfe von Amazon Virtual Private Cloud (Amazon VPC) -Sicherheitsgruppen. Darüber hinaus bietet es Zugriffskontrolle auf API-Ebene mithilfe von AWS Identity and Access Management (IAM) -Zugriffsrichtlinien. Benutzer, die auf Dateisysteme zugreifen, werden mit Microsoft Active Directory authentifiziert. Amazon FSx lässt sich integrieren AWS CloudTrail, um Ihre API-Aufrufe zu überwachen und zu protokollieren, sodass Sie sehen können, welche Aktionen Benutzer auf Ihren Amazon FSx-Ressourcen ausgeführt haben.

Darüber hinaus schützt es Ihre Daten, indem es täglich automatisch hochbelastbare Backups Ihres Dateisystems erstellt und es Ihnen ermöglicht, jederzeit zusätzliche Backups zu erstellen. Weitere Informationen finden Sie unter [Sicherheit in Amazon FSx](#).

## Verfügbarkeit und Beständigkeit

FSx for Windows File Server bietet Dateisysteme mit zwei Verfügbarkeits- und Haltbarkeitsstufen. Single-AZ-Dateien gewährleisten eine hohe Verfügbarkeit innerhalb einer einzigen Availability Zone (AZ), indem sie Komponentenausfälle automatisch erkennen und beheben. Darüber hinaus bieten Multi-AZ-Dateisysteme Hochverfügbarkeit und Failover-Unterstützung in mehreren Availability Zones, indem sie einen Standby-Dateiserver in einer separaten Availability Zone innerhalb einer Region bereitstellen und verwalten. AWS Weitere Informationen zu Single-AZ- und Multi-AZ-Dateisystembereitstellungen finden Sie unter [Verfügbarkeit und Haltbarkeit: Single-AZ- und Multi-AZ-Dateisysteme](#)

## Verwalten von Dateisystemen

Sie können Ihre FSx for Windows File Server Server-Dateisysteme mit benutzerdefinierten PowerShell Fernverwaltungsbefehlen oder in einigen Fällen mit der Windows-eigenen GUI verwalten. Weitere Informationen zur Verwaltung von Amazon FSx-Dateisystemen finden Sie unter [Verwaltung von Dateisystemen](#).

## Flexibilität bei Preis und Leistung

FSx for Windows File Server bietet Ihnen Flexibilität in Bezug auf Preis und Leistung, da es sowohl Solid State Drive (SSD) als auch Hard Disk Drive (HDD) Speichertypen anbietet. Festplattenspeicher

sind für ein breites Spektrum an Workloads konzipiert, darunter Home-Verzeichnisse, Benutzer- und Abteilungsfreigaben sowie Content-Management-Systeme. SSD-Speicher sind für die leistungsstärksten und latenzempfindlichsten Workloads konzipiert, darunter Datenbanken, Medienverarbeitungs-Workloads und Datenanalyseanwendungen.

Mit FSx for Windows File Server können Sie Dateisystemspeicher, SSD-IOPS und Durchsatz unabhängig voneinander bereitstellen, um die richtige Mischung aus Kosten und Leistung zu erzielen. Sie können den Speicher, die SSD-IOPS und die Durchsatzkapazitäten Ihres Dateisystems an sich ändernde Workload-Anforderungen anpassen, sodass Sie nur für das bezahlen, was Sie benötigen. Weitere Informationen finden Sie unter [Kostenoptimierung mit Amazon FSx](#).

## Preise für Amazon FSx

Bei Amazon FSx fallen keine Hardware- oder Softwarekosten im Voraus an. Sie zahlen nur für die genutzten Ressourcen, ohne Mindestverpflichtungen, Einrichtungskosten oder zusätzliche Gebühren. Informationen zu den Preisen und Gebühren im Zusammenhang mit dem Service finden Sie unter [Amazon FSx for Windows File Server — Preise](#).

## Annahmen

Um Amazon FSx verwenden zu können, benötigen Sie ein AWS Konto mit einer Amazon EC2 EC2-Instance, WorkSpaces -Instance, AppStream 2.0-Instance oder VM, die in VMware Cloud in AWS Umgebungen des unterstützten Typs ausgeführt wird.

In diesem Leitfaden gehen wir von den folgenden Annahmen aus:

- Wenn Sie Amazon EC2 verwenden, gehen wir davon aus, dass Sie mit Amazon EC2 vertraut sind. Weitere Informationen zur Verwendung von Amazon EC2 finden Sie in der [Dokumentation zu Amazon Elastic Compute Cloud](#).
- Wenn Sie verwenden WorkSpaces, gehen wir davon aus, dass Sie mit WorkSpaces vertraut sind. Weitere Informationen zur Verwendung WorkSpaces finden Sie im [WorkSpaces Amazon-Benutzerhandbuch](#).
- Wenn Sie VMware Cloud on verwenden AWS, gehen wir davon aus, dass Sie damit vertraut sind. Weitere Informationen finden Sie unter [VMware Cloud on AWS](#).
- Wir gehen davon aus, dass Sie mit den Konzepten von Microsoft Active Directory vertraut sind.



## Voraussetzungen

Um ein Amazon FSx-Dateisystem zu erstellen, benötigen Sie Folgendes:

- Ein AWS Konto mit den erforderlichen Berechtigungen, um ein Amazon FSx-Dateisystem und eine Amazon EC2 EC2-Instance zu erstellen. Weitere Informationen finden Sie unter [Richten Sie Ihr ein AWS-Konto](#).
- Eine Amazon EC2 EC2-Instance, auf der Microsoft Windows Server in der Virtual Private Cloud (VPC) ausgeführt wird, die auf dem Amazon VPC-Service basiert, den Sie mit Ihrem Amazon FSx-Dateisystem verknüpfen möchten. Informationen zur Erstellung einer Instance finden Sie unter [Getting Started with Amazon EC2 Windows Instances](#) im Amazon EC2 EC2-Benutzerhandbuch.
- Amazon FSx arbeitet mit Microsoft Active Directory zusammen, um Benutzerauthentifizierung und Zugriffskontrolle durchzuführen. Sie verbinden Ihr Amazon FSx-Dateisystem bei der Erstellung mit einem Microsoft Active Directory. Weitere Informationen finden Sie unter [Arbeiten mit Microsoft Active Directory in FSx for Windows File Server](#).
- In diesem Handbuch wird davon ausgegangen, dass Sie die Regeln für die Standardsicherheitsgruppe für Ihre VPC, die auf dem Amazon VPC-Service basiert, nicht geändert haben. Falls ja, müssen Sie sicherstellen, dass Sie die erforderlichen Regeln hinzufügen, um Netzwerkverkehr von Ihrer Amazon EC2 EC2-Instance zu Ihrem Amazon FSx-Dateisystem zuzulassen. Weitere Details finden Sie unter [Sicherheit in Amazon FSx](#).
- Installieren und konfigurieren Sie das AWS Command Line Interface (AWS CLI). Unterstützte Versionen sind 1.9.12 und neuer. Weitere Informationen finden Sie unter [Installation, Aktualisierung und Deinstallation von AWS CLI im AWS Command Line Interface Benutzerhandbuch](#).

### Note

Sie können die Version von, die AWS CLI Sie verwenden, mit dem `aws --version` Befehl überprüfen.

## Foren für Amazon FSx for Windows File Server

Wenn Sie bei der Verwendung von Amazon FSx auf Probleme stoßen, verwenden Sie die [Foren](#).

## Sind Sie ein Erstbenutzer von Amazon FSx?

Wenn Sie Amazon FSx zum ersten Mal verwenden, empfehlen wir Ihnen, die folgenden Abschnitte der Reihe nach zu lesen:

1. Wenn Sie bereit sind, Ihr erstes Amazon FSx-Dateisystem zu erstellen, versuchen Sie es mit dem [Erste Schritte mit Amazon FSx for Windows File Server](#).
2. Informationen zur Leistung finden Sie unter [Leistung von FSx for Windows File Server](#).
3. Sicherheitsinformationen zu Amazon FSx finden Sie unter [Sicherheit in Amazon FSx](#).
4. Informationen zur Amazon FSx API finden Sie unter [Amazon FSx API Reference](#).

# Bewährte Methoden für FSx for Windows File Server

Wir empfehlen Ihnen, diese bewährten Methoden zu befolgen, wenn Sie mit Amazon FSx for Windows File Server arbeiten. Folgen Sie den Links unten, um mehr über die besprochenen Themen zu erfahren.

Themen

- [Allgemeine bewährte Methoden](#)
- [Bewährte Methoden für die Gewährleistung der Sicherheit](#)
- [Konfiguration und Anpassung der Größe Ihres Dateisystems](#)

## Allgemeine bewährte Methoden

### Testen Sie Ihre Workloads, bevor Sie zur Produktion übergehen

Wir empfehlen, zum Testen Ihrer Workloads eine Staging-Umgebung mit derselben Konfiguration wie Ihre Produktionsumgebung zu verwenden. Verwenden Sie beispielsweise dieselben Active Directory (AD) und Netzwerkkonfigurationen, dieselbe Größe und Konfiguration des Dateisystems sowie dieselben Windows-Funktionen wie Datendeduplizierung und Schattenkopien. Das Ausführen von Test-Workloads in einer Staging-Umgebung, die Ihren gewünschten Produktionsdatenverkehr simuliert, trägt dazu bei, dass der Prozess reibungslos abläuft.

Wir empfehlen außerdem, das Verfügbarkeitsmodell für Ihr Dateisystem zu überprüfen und sicherzustellen, dass Ihr Workload dem erwarteten Wiederherstellungsverhalten für Ihren Dateisystemtyp bei Ereignissen wie der Dateisystemwartung, Änderungen der Durchsatzkapazität und ungeplanten Betriebsunterbrechungen standhält. Weitere Informationen finden Sie unter [Verfügbarkeit und Haltbarkeit: Single-AZ- und Multi-AZ-Dateisysteme](#).

## Erstellen eines Überwachungsplans

Sie können Dateisystem-Metriken verwenden, um Ihre Speicher- und Leistungsnutzung zu überwachen, Ihre Nutzungsmuster zu verstehen und Benachrichtigungen auszulösen, wenn Ihre Nutzung die Speicher- oder Leistungsgrenzen Ihres Dateisystems erreicht. Durch die Überwachung Ihrer Amazon FSx-Dateisysteme zusammen mit dem Rest Ihrer Anwendungsumgebung können Sie Probleme, die sich auf die Leistung auswirken könnten, schnell debuggen.

## Stellen Sie sicher, dass Ihre Dateisysteme über ausreichende Ressourcen verfügen

Unzureichende Ressourcen können zu erhöhter Latenz und Warteschlangen für I/O-Anfragen führen, was als vollständige oder teilweise Nichtverfügbarkeit Ihres Dateisystems erscheinen kann. Weitere Informationen zur Leistungsüberwachung und zum Zugriff auf Leistungswarnungen und Empfehlungen finden Sie unter [Überwachung von FSx for Windows File Server](#)

## Erstellen Sie regelmäßig Backups Ihrer Dateisysteme

Regelmäßige Backups ermöglichen es Ihnen, Ihre Anforderungen an Datenarchivierung, Geschäftstätigkeiten und Compliance zu erfüllen. Wir empfehlen, die automatischen täglichen Backups zu verwenden, die standardmäßig für Ihr Dateisystem aktiviert sind, und sie als zentrale Backup-Lösung AWS Backup für alle zu verwenden AWS-Services. AWS Backup ermöglicht es Ihnen, zusätzliche Backup-Pläne mit unterschiedlichen Intervallen (z. B. mehrmals täglich, täglich oder wöchentlich) und Aufbewahrungsfristen zu konfigurieren.

## Bewährte Methoden für die Gewährleistung der Sicherheit

Wir empfehlen Ihnen, diese bewährten Methoden zur Verwaltung der Sicherheits- und Zugriffskontrollen Ihres Dateisystems zu befolgen. Weitere Informationen zur Konfiguration von Amazon FSx zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele finden Sie unter [Sicherheit in Amazon FSx](#).

### Netzwerksicherheit

Ändern oder löschen Sie die ENI, die mit Ihrem Dateisystem verknüpft ist, nicht

Auf Ihr Amazon FSx-Dateisystem wird über ein elastic network interface (ENI) zugegriffen, das sich in der Virtual Private Cloud (VPC) befindet, die mit Ihrem Dateisystem verknüpft ist. Das Ändern oder Löschen der Netzwerkschnittstelle kann zu einem dauerhaften Verbindungsverlust zwischen Ihrer VPC und Ihrem Dateisystem führen.

### Verwenden von Sicherheitsgruppen und Netzwerk-ACLs

Sie können Sicherheitsgruppen und Network Access Control Lists (ACLs) verwenden, um den Zugriff auf Ihre Dateisysteme zu beschränken. Für VPC-Sicherheitsgruppen wurde die Standardsicherheitsgruppe bereits zu Ihrem Dateisystem in der Konsole hinzugefügt. Stellen Sie

sicher, dass die Sicherheitsgruppe und die Netzwerk-ACLs für die Subnetze, in denen Sie Ihr Dateisystem erstellen, den Datenverkehr über die Ports zulassen. Weitere Informationen finden Sie unter [Amazon VPC-Sicherheitsgruppen](#).

## Active Directory

Wenn Sie ein Amazon FSx-Dateisystem erstellen, können Sie es mit Ihrer Microsoft AD-Domain verbinden, um Benutzerauthentifizierung und Autorisierung für Zugriffskontrolle auf Freigabe-, Datei- und Ordner Ebene bereitzustellen. Ihre Benutzer können ihre vorhandenen AD-Konten verwenden, um eine Verbindung zu Dateifreigaben herzustellen und auf die darin enthaltenen Dateien und Ordner zuzugreifen. Darüber hinaus können Sie die bestehende Sicherheits-ACL-Konfiguration ohne Änderungen auf Amazon FSx migrieren. Amazon FSx bietet Ihnen zwei Optionen für Active Directory: AWS verwaltetes Microsoft AD oder selbstverwaltetes Microsoft AD.

Wenn Sie ein AWS verwaltetes Microsoft AD verwenden, empfehlen wir, die Standardeinstellungen Ihrer AD-Sicherheitsgruppe beizubehalten. Wenn Sie diese Einstellungen ändern, stellen Sie sicher, dass Sie eine Netzwerkkonfiguration beibehalten, die den Netzwerkanforderungen entspricht. Weitere Informationen finden Sie unter [Voraussetzungen für das Netzwerk](#).

Wenn Sie ein selbstverwaltetes Microsoft AD verwenden, haben Sie zusätzliche Optionen für die Konfiguration Ihres Dateisystems. Wir empfehlen die folgenden bewährten Methoden für die Erstkonfiguration, wenn Sie Amazon FSx mit Ihrem selbstverwaltetem Microsoft AD verwenden:

- Weisen Sie Subnetze einem einzelnen AD-Standort zu: Wenn Ihre AD-Umgebung über eine große Anzahl von Domain-Controllern verfügt, verwenden Sie Active Directory-Standorte und -Dienste, um die von Ihren Amazon FSx-Dateisystemen verwendeten Subnetze einem einzigen AD-Standort mit höchster Verfügbarkeit und Zuverlässigkeit zuzuweisen. Stellen Sie sicher, dass die VPC-Sicherheitsgruppe, die VPC-Netzwerk-ACL, die Windows-Firewallregeln auf Ihren DCs und alle anderen Netzwerk-Routing-Kontrollen, die Sie in Ihrer AD-Infrastruktur haben, die Kommunikation von Amazon FSx über die erforderlichen Ports zulassen. Auf diese Weise kann Windows zu anderen DCs zurückkehren, wenn es die zugewiesene AD-Site nicht verwenden kann. Weitere Informationen finden Sie unter [Dateisystem-Zugriffskontrolle mit Amazon VPC](#).
- Verwenden Sie eine separate Organisationseinheit (OU): Verwenden Sie eine Organisationseinheit für Ihre Amazon FSx-Dateisysteme, die von allen anderen Organisationseinheiten, die Sie möglicherweise haben, getrennt ist.
- Konfigurieren Sie Ihr Servicekonto mit den erforderlichen Mindestberechtigungen: Konfigurieren oder delegieren Sie das Servicekonto, das Sie Amazon FSx zur Verfügung stellen, mit den erforderlichen Mindestberechtigungen. Weitere Informationen finden Sie unter [Voraussetzungen](#)

[für die Verwendung eines selbstverwalteten Microsoft Active Directory](#) und [Delegieren von Berechtigungen an Ihr Amazon-FSx-Servicekonto](#) .

- Kontinuierliche Überprüfung Ihrer AD-Konfiguration: Führen Sie das [Amazon FSx Active Directory-Validierungstool](#) anhand Ihrer AD-Konfiguration aus, bevor Sie Ihr Amazon FSx-Dateisystem erstellen, um zu überprüfen, ob Ihre Konfiguration für die Verwendung mit Amazon FSx gültig ist, und um alle Warnungen und Fehler zu entdecken, die das Tool möglicherweise aufdeckt.

## Vermeiden Sie den Verlust der Verfügbarkeit aufgrund einer AD-Fehlkonfiguration

Wenn Sie Amazon FSx mit Ihrem selbstverwalteten Microsoft AD verwenden, ist es wichtig, dass Sie nicht nur bei der Erstellung Ihres Dateisystems, sondern auch für den laufenden Betrieb und die Verfügbarkeit über eine gültige AD-Konfiguration verfügen. Bei der Wiederherstellung nach einem Ausfall, bei routinemäßigen Wartungsereignissen und bei Aktionen zur Aktualisierung der Durchsatzkapazität verknüpft Amazon FSx die Dateiserverressourcen wieder mit Ihrem Active Directory. Wenn die AD-Konfiguration während eines Ereignisses nicht gültig ist, wechselt Ihr Dateisystem in den Status Falsch konfiguriert und es besteht die Gefahr, dass es nicht mehr verfügbar ist. Im Folgenden finden Sie einige Möglichkeiten, wie Sie den Verlust der Verfügbarkeit vermeiden können:

- Halten Sie Ihre AD-Konfiguration mit Amazon FSx auf dem neuesten Stand: Wenn Sie Änderungen vornehmen, z. B. das Passwort Ihres Dienstkontos zurücksetzen, stellen Sie sicher, dass Sie die Konfiguration für alle Dateisysteme aktualisieren, die dieses Dienstkonto verwenden.
- Achten Sie auf AD-Fehlkonfigurationen: Richten Sie selbst Statusbenachrichtigungen für falsch konfigurierte Konfigurationen ein, sodass Sie bei Bedarf die AD-Konfiguration Ihres Dateisystems zurücksetzen können. Ein Beispiel, das eine Lambda-basierte Lösung verwendet, um dies zu erreichen, finden Sie unter [Überwachung des Zustands von Amazon FSx-Dateisystemen mithilfe von Amazon](#) und EventBridge AWS Lambda
- Überprüfen Sie Ihre AD-Konfiguration regelmäßig: Wenn Sie AD-Fehlkonfigurationen proaktiv erkennen möchten, empfehlen wir Ihnen, das Active Directory-Validierungstool fortlaufend anhand Ihrer AD-Konfiguration auszuführen. Wenn Sie beim Ausführen des Validierungstools Warnungen oder Fehler erhalten, bedeutet dies, dass Ihr Dateisystem Gefahr läuft, falsch konfiguriert zu werden.
- Verschieben oder ändern Sie keine Computerobjekte, die von FSx erstellt wurden: Amazon FSx erstellt und verwaltet Computerobjekte in Ihrem AD unter Verwendung des von Ihnen angegebenen Dienstkontos und der von Ihnen bereitgestellten Berechtigungen. Das Verschieben oder Ändern dieser Computerobjekte kann dazu führen, dass Ihr Dateisystem falsch konfiguriert wird.

## Windows-ACLs

Mit Amazon FSx verwenden Sie standardmäßige Windows-Zugriffskontrolllisten (ACLs) für eine detaillierte Zugriffskontrolle auf Freigabe-, Datei- und Ordnebene. Amazon FSx-Dateisysteme überprüfen automatisch die Anmeldeinformationen von Benutzern, die auf Dateisystemdaten zugreifen, um diese Windows-ACLs durchzusetzen.

- Ändern Sie nicht die NTFS-ACL-Berechtigungen für den SYSTEM-Benutzer: Amazon FSx verlangt, dass der SYSTEM-Benutzer volle Kontrolle über NTFS-ACL-Berechtigungen für alle Ordner in Ihrem Dateisystem hat. Eine Änderung der NTFS-ACL-Berechtigungen für den SYSTEM-Benutzer kann dazu führen, dass auf Ihr Dateisystem nicht mehr zugegriffen werden kann und future Dateisystemsicherungen möglicherweise unbrauchbar werden.

## Konfiguration und Anpassung der Größe Ihres Dateisystems

### Auswahl eines Bereitstellungstyps

Amazon FSx bietet zwei Bereitstellungsoptionen: Single-AZ und Multi-AZ. Wir empfehlen die Verwendung von Multi-AZ-Dateisystemen für die meisten Produktionsworkloads, die eine hohe Verfügbarkeit gemeinsam genutzter Windows-Dateidaten erfordern. Weitere Informationen finden Sie unter [Verfügbarkeit und Haltbarkeit: Single-AZ- und Multi-AZ-Dateisysteme](#).

### Auswahl eines Speichertyps

SSD-Speicher eignet sich für die meisten Produktionsworkloads mit hohen Leistungsanforderungen und Latenzempfindlichkeit. Zu diesen Workloads gehören beispielsweise Datenbanken, Datenanalysen, Medienverarbeitung und Geschäftsanwendungen. Wir empfehlen SSD auch für Anwendungsfälle mit einer großen Anzahl von Endbenutzern, einem hohen I/O-Aufwand oder Datensätzen mit einer großen Anzahl kleiner Dateien. Schließlich empfehlen wir die Verwendung von SSD-Speicher, wenn Sie Schattenkopien aktivieren möchten. Sie können SSD-IOPS für Dateisysteme mit SSD-Speicher, aber nicht mit HDD-Speicher konfigurieren und skalieren.

Wenn Sie sich für die Verwendung von Festplattenspeicher entscheiden, testen Sie Ihr Dateisystem, um sicherzustellen, dass es Ihren Leistungsanforderungen entspricht. HDD-Speicher ist im Vergleich zu SSD-Speichern kostengünstiger, weist jedoch höhere Latenzen und einen geringeren Festplattendurchsatz und Festplatten-IOPS pro Speichereinheit auf. Es eignet sich möglicherweise für allgemeine Benutzerfreigaben und Basisverzeichnisse mit geringen I/O-Anforderungen, für große Content-Management-Systeme (CMS), bei denen Daten selten abgerufen werden, oder

für Datensätze mit einer geringen Anzahl großer Dateien. Weitere Informationen finden Sie unter [Speicherkonfiguration und Leistung](#).

Sie können Ihren Speichertyp jederzeit von HDD auf SSD aktualisieren, indem Sie die Amazon FSx-Konsole oder die Amazon FSx-API verwenden. Weitere Informationen finden Sie unter [Speichertyp verwalten](#).

## Auswahl einer Durchsatzkapazität

Konfigurieren Sie Ihr Dateisystem mit ausreichender Durchsatzkapazität, um nicht nur den erwarteten Datenverkehr Ihrer Arbeitslast zu bewältigen, sondern auch zusätzliche Leistungsressourcen, die zur Unterstützung der Funktionen erforderlich sind, die Sie in Ihrem Dateisystem aktivieren möchten. Wenn Sie beispielsweise eine Datendeduplizierung ausführen, muss die von Ihnen gewählte Durchsatzkapazität ausreichend Arbeitsspeicher bereitstellen, um die Deduplizierung auf der Grundlage des verfügbaren Speichers ausführen zu können. Wenn Sie Schattenkopien verwenden, erhöhen Sie die Durchsatzkapazität auf einen Wert, der mindestens dem Dreifachen des Werts entspricht, der voraussichtlich von Ihrer Arbeitslast bestimmt wird, um zu verhindern, dass Windows Server Ihre Schattenkopien löscht. Weitere Informationen finden Sie unter [Auswirkung der Durchsatzkapazität auf die Leistung](#).

## Erhöhen Sie Ihre Speicherkapazität und Durchsatzkapazität

Erhöhen Sie die Speicherkapazität Ihres Dateisystems, wenn der freie Speicherplatz knapp wird oder wenn Sie erwarten, dass Ihr Speicherbedarf über dem aktuellen Speicherlimit liegt. Wir empfehlen, jederzeit mindestens 10% der freien Speicherkapazität in Ihrem Dateisystem beizubehalten. Wir empfehlen außerdem, die Speicherkapazität vor der Speicherskalierung um mindestens 20% zu erhöhen, da Sie sie während des laufenden Prozesses nicht erhöhen können. Mithilfe der FreeStorage CloudWatch Kapazitätsmetrik können Sie die Menge des verfügbaren freien Speichers überwachen und deren Entwicklung nachvollziehen. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#).

Sie sollten auch die Durchsatzkapazität Ihres Dateisystems erhöhen, wenn Ihre Arbeitslast durch die aktuellen Leistungsgrenzen eingeschränkt ist. Sie können die Seite Überwachung und Leistung auf der FSx-Konsole verwenden, um zu sehen, wann die Workload-Anforderungen Leistungsgrenzen erreicht oder überschritten haben, um festzustellen, ob Ihr Dateisystem für Ihren Workload nicht ausreichend bereitgestellt ist.

Um die Dauer der Speicherskalierung zu minimieren und eine Verringerung der Schreibleistung zu vermeiden, empfehlen wir, die Durchsatzkapazität Ihres Dateisystems zu erhöhen, bevor Sie die



Speicherkapazität erhöhen, und dann die Durchsatzkapazität wieder herunterzufahren, nachdem die Speicherkapazitätserhöhung abgeschlossen ist. Bei den meisten Workloads kommt es bei der Speicherskalierung nur zu minimalen Leistungseinbußen. Bei schreibintensiven Anwendungen mit großen aktiven Datensätzen kann die Schreibleistung jedoch vorübergehend um bis zu der Hälfte reduziert werden.

## Änderung der Durchsatzkapazität in Leerlaufphasen

Die Aktualisierung der Durchsatzkapazität unterbricht die Verfügbarkeit für Single-AZ-Dateisysteme für einige Minuten und führt bei Multi-AZ-Dateisystemen zu Failover und Failback. Bei Multi-AZ-Dateisystemen müssen alle Datenänderungen, die während dieser Zeit vorgenommen werden, zwischen den Dateiservern synchronisiert werden, wenn während des Failovers und Failbacks andauernder Datenverkehr stattfindet. Die Datensynchronisierung kann bei schreib- und IOPS-intensiven Workloads bis zu mehrere Stunden dauern. Obwohl Ihr Dateisystem während dieser Zeit weiterhin verfügbar sein wird, empfehlen wir, Wartungsfenster einzuplanen und Durchsatzkapazitätsaktualisierungen während Leerlaufzeiten durchzuführen, wenn Ihr Dateisystem nur minimal belastet wird, um die Dauer der Datensynchronisierung zu verkürzen. Weitere Informationen hierzu finden Sie unter [Verwaltung der Durchsatzkapazität](#).

# Erste Schritte mit Amazon FSx for Windows File Server

Im Folgenden erfahren Sie, wie Sie mit FSx for Windows File Server beginnen können. Diese Übung für den Einstieg umfasst die folgenden Schritte.

1. Melden Sie sich für ein Konto an AWS-Konto und erstellen Sie einen Administratorbenutzer.
2. Erstellen Sie ein AWS verwaltetes Microsoft AD Active Directory mit dem AWS Directory Service. Sie fügen Ihr Dateisystem und Ihre Recheninstanz dem Active Directory hinzu.
3. Erstellen Sie eine Amazon Elastic Compute Cloud-Recheninstanz, auf der Microsoft Windows Server ausgeführt wird. Sie werden diese Instance verwenden, um auf Ihr Dateisystem zuzugreifen.
4. Erstellen Sie mit der Amazon FSx-Konsole ein Dateisystem von Amazon FSx für Windows File Server.
5. Ordnen Sie Ihr Dateisystem Ihrer EC2-Instance zu
6. Schreiben Sie Daten in Ihr Dateisystem.
7. Erstellen Sie eine Sicherungskopie Ihres Dateisystems.
8. Bereinigen Sie die -Ressourcen, die Sie erstellt haben.

## Themen

- [Richten Sie Ihr ein AWS-Konto](#)
- [Erstellen Sie Ihr Dateisystem](#)
- [Ordnen Sie Ihre Dateifreigabe einer EC2-Instance zu, auf der Windows Server ausgeführt wird](#)
- [Schreiben Sie Daten in Ihre Dateifreigabe](#)
- [Erstellen Sie ein Backup Ihres Dateisystems](#)
- [Bereinigen von -Ressourcen](#)
- [Status des Amazon FSx-Dateisystems](#)

## Richten Sie Ihr ein AWS-Konto

Bevor Sie Amazon FSx zum ersten Mal verwenden, führen Sie die folgenden Aufgaben aus:

1. [Melden Sie sich an für ein AWS-Konto](#)
2. [Erstellen Sie einen Benutzer mit Administratorzugriff](#)

## Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/signup>.
2. Folgen Sie den Online-Anweisungen.

Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontos wird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um [Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich](#) ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu <https://aws.amazon.com/> auf und klicken Sie auf Mein Konto.

## Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich [AWS Management Console](#) als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Anmelden als Root-Benutzer](#) im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

Anweisungen finden Sie unter [Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer \(Konsole\)](#) im IAM-Benutzerhandbuch.

## Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden [Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis](#) im AWS IAM Identity Center Benutzerhandbuch.

## Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie [im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal](#).

## Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

Anweisungen finden Sie im Benutzerhandbuch unter [Einen Berechtigungssatz erstellen](#).AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

Anweisungen finden [Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen](#).

## Erstellen Sie Ihr Dateisystem

Um Ihr Amazon FSx-Dateisystem zu erstellen, müssen Sie Ihre Windows Amazon Elastic Compute Cloud (Amazon EC2) -Instance und das AWS Directory Service Verzeichnis erstellen. Falls

Sie das noch nicht eingerichtet haben, finden Sie weitere Informationen unter [Exemplarische Vorgehensweise 1: Voraussetzungen für die ersten Schritte](#)

So erstellen Sie Ihr Dateisystem (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Klicken Sie auf dem Dashboard auf Create file system (Dateisystem erstellen), um den Erstellungsassistenten für Dateisysteme zu starten.
3. Wählen Sie auf der Seite Wählen Sie den Dateisystemtyp FSx for Windows File Server und wählen Sie dann Weiter aus. Die Seite Create file system (Dateisystem erstellen) wird angezeigt.
4. Wählen Sie als Erstellungsmethode Standard create aus.

Einzelheiten zum Dateisystem

1. Geben Sie im Abschnitt Details zum Dateisystem einen Namen für Ihr Dateisystem an. Es ist einfacher, Ihre Dateisysteme zu finden und zu verwalten, wenn Sie sie benennen. Sie können maximal 256 Unicode-Buchstaben, Leerzeichen und Zahlen sowie die Sonderzeichen + - = verwenden. \_:/
2. Wählen Sie als Bereitstellungstyp Multi-AZ oder Single-AZ.
  - Wählen Sie Multi-AZ, um ein Dateisystem bereitzustellen, das die Nichtverfügbarkeit der Availability Zone toleriert. Diese Option unterstützt SSD- und HDD-Speicher.
  - Wählen Sie Single-AZ, um ein Dateisystem bereitzustellen, das in einer einzigen Availability Zone bereitgestellt wird. Single-AZ 2 ist die neueste Generation einzelner Availability Zone-Dateisysteme und unterstützt SSD- und HDD-Speicher.

Weitere Informationen finden Sie unter [Verfügbarkeit und Haltbarkeit: Single-AZ- und Multi-AZ-Dateisysteme](#).

3. Als Speichertyp können Sie entweder SSD oder HDD wählen.


FSx for Windows File Server bietet Speichertypen wie Solid State Drive (SSD) und Hard Disk Drive (HDD). SSD-Speicher wurde für die leistungsstärksten und latenzempfindlichsten Workloads konzipiert, darunter Datenbanken, Workloads zur Medienverarbeitung und Datenanalyseanwendungen. Festplattenspeicher sind für ein breites Spektrum an Workloads konzipiert, darunter Home-Verzeichnisse, Dateifreigaben von Benutzern und Abteilungen sowie

Content-Management-Systeme. Weitere Informationen finden Sie unter [Kostenoptimierung mithilfe von Speichertypen](#).

4. Für bereitgestellte SSD-IOPS können Sie entweder den automatischen Modus oder den vom Benutzer bereitgestellten Modus wählen.

Wenn Sie den automatischen Modus wählen, skaliert FSx for Windows File Server Ihre SSD-IOPS automatisch, um 3 SSD-IOPS pro GiB Speicherkapazität aufrechtzuerhalten. Wenn Sie den vom Benutzer bereitgestellten Modus wählen, geben Sie eine beliebige ganze Zahl im Bereich von 96-400.000 ein. Die Skalierung von SSD-IOPS über 80.000 ist in den Regionen USA Ost (Nord-Virginia), USA West (Oregon), USA Ost (Ohio), Europa (Irland), Asien-Pazifik (Tokio) und Asien-Pazifik (Singapur) verfügbar. Weitere Informationen finden Sie unter [Verwalten von SSD-IOPS](#).

5. Geben Sie unter Speicherkapazität die Speicherkapazität Ihres Dateisystems in GiB ein. Wenn Sie SSD-Speicher verwenden, geben Sie eine ganze Zahl im Bereich von 32 bis 65.536 ein. Wenn Sie Festplattenspeicher verwenden, geben Sie eine ganze Zahl im Bereich von 2.000 bis 65.536 ein. Sie können die Speicherkapazität jederzeit nach der Erstellung des Dateisystems nach Bedarf erhöhen. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#).
6. Behalten Sie die Durchsatzkapazität auf ihrer Standardeinstellung. Die Durchsatzkapazität ist die konstante Geschwindigkeit, mit der der Dateiserver, der Ihr Dateisystem hostet, Daten bereitstellen kann. Die Einstellung Empfohlene Durchsatzkapazität basiert auf der ausgewählten Speicherkapazität. Wenn Sie mehr als die empfohlene Durchsatzkapazität benötigen, wählen Sie Durchsatzkapazität angeben und wählen Sie dann einen Wert aus. Weitere Informationen finden Sie unter [Leistung von FSx for Windows File Server](#).

 Note

Wenn Sie die Dateizugriffsüberwachung aktivieren möchten, müssen Sie eine Durchsatzkapazität von 32 MB/s oder mehr wählen. Weitere Informationen finden Sie unter [Prüfung des Dateizugriffs](#).

Sie können die Durchsatzkapazität jederzeit nach der Erstellung des Dateisystems nach Bedarf ändern. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

## Netzwerk und Sicherheit

1. Wählen Sie im Bereich Netzwerk und Sicherheit die Amazon VPC aus, die Sie mit Ihrem Dateisystem verknüpfen möchten. Wählen Sie für diese Übung „Erste Schritte“ dieselbe Amazon VPC aus, die Sie für Ihr AWS Directory Service Verzeichnis und Ihre Amazon EC2 EC2-Instance ausgewählt haben.
2. Für VPC-Sicherheitsgruppen wurde die Standardsicherheitsgruppe für Ihre standardmäßige Amazon-VPC bereits zu Ihrem Dateisystem in der Konsole hinzugefügt. Wenn Sie nicht die Standardsicherheitsgruppe verwenden, stellen Sie sicher, dass sich die von Ihnen gewählte Sicherheitsgruppe in Ihrem AWS-Region Dateisystem befindet. Um sicherzustellen, dass Sie eine EC2-Instance mit Ihrem Dateisystem verbinden können, müssen Sie der ausgewählten Sicherheitsgruppe die folgenden Regeln hinzufügen:
  - a. Fügen Sie die folgenden Regeln für eingehenden und ausgehenden Datenverkehr hinzu, um die folgenden Ports zuzulassen.

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

Fügen Sie von und zu IP-Adressen oder Sicherheitsgruppen-IDs hinzu, die den Client-Compute-Instances zugeordnet sind, von denen aus Sie auf Ihr Dateisystem zugreifen möchten.

- b. Fügen Sie Regeln für ausgehenden Datenverkehr hinzu, um den gesamten Datenverkehr zum Active Directory zuzulassen, mit dem Sie Ihr Dateisystem verbinden. Führen Sie dazu einen der folgenden Schritte aus:
  - Lassen Sie ausgehenden Datenverkehr zu der Sicherheitsgruppen-ID zu, die Ihrem AWS Managed AD-Verzeichnis zugeordnet ist.
  - Lassen Sie ausgehenden Datenverkehr zu den IP-Adressen zu, die Ihren selbstverwalteten Active Directory-Domänencontrollern zugeordnet sind.

**Note**

In einigen Fällen haben Sie möglicherweise die Standardeinstellungen für die Regeln Ihrer AWS Managed Microsoft AD Sicherheitsgruppe geändert. Falls ja, stellen Sie sicher, dass diese Sicherheitsgruppe über die erforderlichen Regeln für eingehenden Datenverkehr aus Ihrem Amazon FSx-Dateisystem verfügt. Weitere Informationen zu den erforderlichen Regeln für eingehenden Datenverkehr finden Sie unter [AWS Managed Microsoft AD Voraussetzungen im AWS Directory Service Administratorhandbuch](#).

Weitere Informationen finden Sie unter [Dateisystem-Zugriffskontrolle mit Amazon VPC](#).

3. Multi-AZ-Dateisysteme verfügen über einen primären und einen Standby-Dateiserver, die sich jeweils in einer eigenen Availability Zone und einem eigenen Subnetz befinden. Wenn Sie ein Multi-AZ-Dateisystem erstellen (siehe Schritt 5), wählen Sie einen Wert für das bevorzugte Subnetz für den primären Dateiserver und einen Wert für das Standby-Subnetz für den Standby-Dateiserver.

Wenn Sie ein Single-AZ-Dateisystem erstellen, wählen Sie das Subnetz für Ihr Dateisystem aus.

## Windows-Authentifizierung


- Für die Windows-Authentifizierung haben Sie die folgenden Optionen:

Wählen Sie AWS Managed Microsoft Active Directory, wenn Sie Ihr Dateisystem mit einer Microsoft Active Directory-Domäne verbinden möchten, die von verwaltet wird AWS, und wählen Sie dann Ihr AWS Directory Service Verzeichnis aus der Liste aus. Weitere Informationen finden Sie unter [Arbeiten mit Microsoft Active Directory in FSx for Windows File Server](#).

Wählen Sie Selbstverwaltetes Microsoft Active Directory, wenn Sie Ihr Dateisystem mit einer selbstverwalteten Microsoft Active Directory-Domäne verbinden möchten, und geben Sie die folgenden Details für Ihr Active Directory an. Weitere Informationen finden Sie unter [Verwenden von Amazon FSx mit Ihrem selbstverwalteten Microsoft Active Directory](#).


- Der vollqualifizierte Domänenname Ihres Active Directory.



 **Important**

Für Single-AZ 2- und alle Multi-AZ-Dateisysteme darf der Active Directory-Domänenname 47 Zeichen nicht überschreiten. Diese Einschränkung gilt sowohl AWS Directory Service für selbstverwaltete Active Directory-Domännennamen. Amazon FSx benötigt eine direkte Verbindung für internen Datenverkehr zu Ihrer DNS-IP-Adresse. Eine Verbindung über ein Internet-Gateway wird nicht unterstützt. Verwenden Sie AWS Virtual Private Network stattdessen VPC-Peering oder AWS Direct Connect AWS Transit Gateway Assoziation.

- IP-Adressen der DNS-Server — Die IPv4-Adressen der DNS-Server für Ihre Domain

 **Note**

Auf Ihrem DNS-Server muss EDNS (Extension Mechanisms for DNS) aktiviert sein. Wenn EDNS deaktiviert ist, kann Ihr Dateisystem möglicherweise keine Erstellung durchführen.

- Benutzername des Dienstkontos — der Benutzername des Dienstkontos in Ihrem vorhandenen Active Directory. Geben Sie kein Domänenpräfix oder -suffix an.
- Passwort für das Dienstkonto — das Passwort für das Dienstkonto.
- (Optional) Organizational Unit (OU) — der definierte Pfadname der Organisationseinheit, der Sie Ihrem Dateisystem beitreten möchten.
- (Optional) Gruppe delegierter Dateisystemadministratoren — der Name der Gruppe in Ihrem Active Directory, die Ihr Dateisystem verwalten kann. Die Standardgruppe ist „Domain-Admins“. Weitere Informationen finden Sie unter [Delegieren von Berechtigungen an Ihr Amazon-FSx-Servicekonto](#).

## Verschlüsselung, Überwachung und Zugriff (DNS-Aliase)

1. Wählen Sie für Verschlüsselung den AWS KMS key Verschlüsselungsschlüssel aus, mit dem die Daten in Ihrem Dateisystem im Ruhezustand verschlüsselt werden. Sie können den standardmäßigen aws/fsx (Standard), der von verwaltet wird AWS KMS, einen vorhandenen Schlüssel oder einen vom Kunden verwalteten Schlüssel wählen, indem Sie den ARN für den Schlüssel angeben. Weitere Informationen finden Sie unter [Verschlüsselung im Ruhezustand](#).

2. Für Auditing — optional ist die Dateizugriffsprüfung standardmäßig deaktiviert. Informationen zur Aktivierung und Konfiguration der Dateizugriffsüberwachung finden Sie unter [Um die Dateizugriffsüberwachung beim Erstellen eines Dateisystems \(Konsole\) zu aktivieren](#).
3. Geben Sie unter Zugriff — optional alle DNS-Aliase ein, die Sie dem Dateisystem zuordnen möchten. Jeder Aliasname muss als vollqualifizierter Domänenname (FQDN) formatiert sein. Weitere Informationen finden Sie unter [DNS-Aliase verwalten](#).

## Backup und Wartung

Weitere Informationen zu automatischen täglichen Backups und den Einstellungen in diesem Abschnitt finden Sie unter [Arbeiten mit Backups](#).

1. Für tägliche automatische Backups ist diese Option standardmäßig aktiviert. Sie können diese Einstellung deaktivieren, wenn Sie nicht möchten, dass Amazon FSx täglich automatisch Backups Ihres Dateisystems erstellt.
2. Wenn automatische Backups aktiviert sind, erfolgen sie innerhalb eines Zeitraums, der als Backup-Fenster bezeichnet wird. Sie können das Standardfenster verwenden oder eine Startzeit für das automatische Backup-Fenster wählen.
3. Für den Aufbewahrungszeitraum für automatische Backups können Sie die Standardeinstellung von 30 Tagen verwenden oder einen Wert zwischen 1 und 90 Tagen festlegen, für den Amazon FSx automatische tägliche Backups Ihres Dateisystems aufbewahrt. Diese Einstellung gilt nicht für vom Benutzer initiierte Backups oder Backups von AWS Backup.
4. Geben Sie unter Tags — optional einen Schlüssel und einen Wert ein, um Ihrem Dateisystem Tags hinzuzufügen. Ein Tag ist ein Schlüssel-Wert-Paar, bei dem die Groß- und Kleinschreibung beachtet wird. Es hilft Ihnen dabei, Ihr Dateisystem zu verwalten, zu filtern und danach zu suchen. Weitere Informationen finden Sie unter [Markieren Ihrer Amazon FSx-Ressourcen mit Tags](#).

Wählen Sie Weiter.

Überprüfen Sie Ihre Konfiguration und erstellen Sie

1. Prüfen Sie die Dateisystemkonfiguration, die auf der Seite Create File System (Dateisystem erstellen) angezeigt wird. Zu Ihrer Information können Sie sehen, welche Dateisystemeinstellungen Sie nach der Erstellung des Dateisystems ändern können und welche nicht. Wählen Sie Create file system (Dateisystem erstellen) aus.

2. Nachdem Amazon FSx das Dateisystem erstellt hat, wählen Sie die Dateisystem-ID aus der Liste im Dateisystem-Dashboard aus, um die Details anzuzeigen. Wählen Sie Anhängen und notieren Sie sich den DNS-Namen für Ihr Dateisystem auf der Registerkarte Netzwerk und Sicherheit. Sie benötigen ihn im folgenden Verfahren, um einen Share einer EC2-Instance zuzuordnen.

## Ordnen Sie Ihre Dateifreigabe einer EC2-Instance zu, auf der Windows Server ausgeführt wird

Sie können jetzt Ihr Amazon FSx-Dateisystem auf Ihrer Microsoft Windows-basierten Amazon EC2 EC2-Instance mounten, die mit Ihrem Verzeichnis verbunden ist. AWS Directory Service Der Name Ihrer Dateifreigabe ist nicht identisch mit dem Namen Ihres Dateisystems.

So ordnen Sie eine Dateifreigabe auf einer Amazon EC2 EC2-Windows-Instance mithilfe der GUI zu

1. Bevor Sie eine Dateifreigabe auf einer Windows-Instance mounten können, müssen Sie die EC2-Instance starten und sie mit einer verbinden. AWS Directory Service for Microsoft Active Directory Um diese Aktion auszuführen, wählen Sie eines der folgenden Verfahren aus dem AWS Directory Service Administratorhandbuch:
  - [Nahtlose Anbindung an eine Windows EC2-Instance](#)
  - [Manuelle Anbindung an eine Windows-Instance](#)
2. Verbinden Sie sich mit der Instance. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Wenn Sie verbunden sind, öffnen Sie den Datei-Explorer.
4. Öffnen Sie im Navigationsbereich das Kontextmenü (Rechtsklick) für Netzwerk und wählen Sie Netzlaufwerk zuordnen aus.
5. Wählen Sie einen beliebigen Laufwerksbuchstaben für Drive aus.
6. Sie können Ihr Dateisystem entweder mit dem von Amazon FSx zugewiesenen Standard-DNS-Namen oder mit einem DNS-Alias Ihrer Wahl zuordnen. Dieses Verfahren beschreibt die Zuordnung einer Dateifreigabe unter Verwendung des Standard-DNS-Namens. Informationen zum Zuordnen einer Dateifreigabe mithilfe eines DNS-Alias finden Sie unter [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisystem](#).

Geben Sie unter Ordner den DNS-Namen und den Freigabenamen des Dateisystems ein. Die standardmäßige Amazon FSx-Aktie wird aufgerufen `\share`. Sie finden den DNS-Namen in der Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>, Windows File Server >

Network & Security oder in der Antwort auf unseren CreateFileSystem DescribeFileSystems API-Befehl.

- Für ein Single-AZ-Dateisystem, das mit einem AWS verwalteten Microsoft Active Directory verknüpft ist, sieht der DNS-Name wie folgt aus.

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

- Für ein Single-AZ-Dateisystem, das mit einem selbstverwalteten Active Directory verbunden ist, und für jedes Multi-AZ-Dateisystem sieht der DNS-Name wie folgt aus.

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

Geben Sie z. B. ei `\\fs-0123456789abcdef0.ad-domain.com\share`.

7. Wählen Sie aus, ob die Dateifreigabe bei der Anmeldung erneut verbunden werden soll, und klicken Sie dann auf Fertig stellen.

## Schreiben Sie Daten in Ihre Dateifreigabe

Nachdem Sie Ihre Dateifreigabe Ihrer Instanz zugeordnet haben, können Sie Ihre Dateifreigabe wie jedes andere Verzeichnis in Ihrer Windows-Umgebung verwenden.

Um Daten in Ihre Dateifreigabe zu schreiben

1. Öffnen Sie den Notepad-Texteditor.
2. Schreiben Sie einige Inhalte in den Texteditor. Zum Beispiel: *Hello, World!*
3. Speichern Sie die Datei unter dem Laufwerksbuchstaben Ihrer Dateifreigabe.
4. Navigieren Sie mit dem Datei-Explorer zu Ihrer Dateifreigabe und suchen Sie die Textdatei, die Sie gerade gespeichert haben.

## Erstellen Sie ein Backup Ihres Dateisystems

Nachdem Sie nun die Möglichkeit hatten, Ihr Amazon FSx-Dateisystem und seine Dateifreigaben zu verwenden, können Sie es sichern. Standardmäßig werden tägliche Backups automatisch während des 30-minütigen Backup-Fensters Ihres Dateisystems erstellt. Sie können jedoch jederzeit ein vom

Benutzer initiiertes Backup erstellen. Backups sind mit zusätzlichen Kosten verbunden. Weitere Informationen zu den Backup-Preisen finden Sie unter [Preise](#).

Um ein Backup Ihres Dateisystems von der Konsole aus zu erstellen

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Konsolen-Dashboard den Namen des Dateisystems aus, das Sie für diese Übung erstellt haben.
3. Wählen Sie auf der Registerkarte „Übersicht“ für Ihr Dateisystem die Option Backup erstellen aus.
4. Geben Sie im sich öffnenden Dialogfeld „Backup erstellen“ einen Namen für Ihr Backup ein. Dieser Name kann maximal 256 Unicode-Buchstaben enthalten und Leerzeichen, Zahlen und die folgenden Sonderzeichen enthalten: + - =. \_:/
5. Wählen Sie Create backup (Backup erstellen).
6. Um alle Ihre Backups in einer Liste anzuzeigen, sodass Sie Ihr Dateisystem wiederherstellen oder das Backup löschen können, wählen Sie Backups.

Wenn Sie ein neues Backup erstellen, wird sein Status während der Erstellung auf CREATING gesetzt. Dies kann einige Minuten dauern. Wenn das Backup zur Verwendung verfügbar ist, ändert sich sein Status auf VERFÜGBAR.

## Bereinigen von -Ressourcen

Nachdem Sie diese Übung abgeschlossen haben, sollten Sie die folgenden Schritte ausführen, um Ihre Ressourcen zu bereinigen und Ihr AWS Konto zu schützen.

So bereinigen Sie Ressourcen

1. Beenden Sie Ihre Instance auf der Amazon EC2 EC2-Konsole. Weitere Informationen finden Sie unter [Terminate Your Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
2. Löschen Sie auf der Amazon FSx-Konsole Ihr Dateisystem. Alle automatischen Backups werden automatisch gelöscht. Sie müssen die manuell erstellten Backups jedoch weiterhin löschen. In den folgenden Schritten wird dieser Vorgang beschrieben:
  - a. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
  - b. Wählen Sie im Konsolen-Dashboard den Namen des Dateisystems aus, das Sie für diese Übung erstellt haben.

- c. Klicken Sie bei Aktionen auf Dateisystem löschen.
- d. Entscheiden Sie im sich öffnenden Dialogfeld „Dateisystem löschen“, ob Sie eine endgültige Sicherung erstellen möchten. Geben Sie in diesem Fall einen Namen für die endgültige Sicherung ein. Alle automatisch erstellten Backups werden ebenfalls gelöscht.

 **Important**

Neue Dateisysteme können aus Backups erstellt werden. Als bewährte Methode empfehlen wir Ihnen, ein abschließendes Backup zu erstellen. Wenn Sie feststellen, dass Sie es nach einer bestimmten Zeit nicht mehr benötigen, können Sie dieses und andere manuell erstellte Backups löschen.

- e. Geben Sie die ID des Dateisystems, das Sie löschen möchten, in das Feld Dateisystem-ID ein.
- f. Wählen Sie Dateisystem löschen.
- g. Das Dateisystem wird jetzt gelöscht und sein Status im Dashboard ändert sich auf LÖSCHEN. Wenn das Dateisystem gelöscht wurde, wird es nicht mehr im Dashboard angezeigt.
- h. Jetzt können Sie alle manuell erstellten Backups für Ihr Dateisystem löschen. Wählen Sie in der linken Navigationsleiste Backups aus.
- i. Wählen Sie im Dashboard alle Backups aus, die dieselbe Dateisystem-ID haben wie das Dateisystem, das Sie gelöscht haben, und wählen Sie Backup löschen.
- j. Das Dialogfeld „Backups löschen“ wird geöffnet. Lassen Sie das Kontrollkästchen für die ID des ausgewählten Backups aktiviert und wählen Sie Backups löschen.

Ihr Amazon FSx-Dateisystem und die zugehörigen automatischen Backups sind jetzt gelöscht.

3. Wenn Sie für diese Übung in ein AWS Directory Service Verzeichnis erstellt haben [Exemplarische Vorgehensweise 1: Voraussetzungen für die ersten Schritte](#), können Sie es jetzt löschen. Weitere Informationen finden Sie im AWS Directory Service Administratorhandbuch unter [Löschen Ihres Verzeichnisses](#).

## Status des Amazon FSx-Dateisystems

Sie können den Status eines Amazon FSx-Dateisystems anzeigen, indem Sie die Amazon FSx-Konsole, den AWS CLI Befehl `describe-file-systems` oder die API-Betriebssysteme verwenden.

### DescribeFile

Status des Dateisystems	Beschreibung
VERFÜGBAR	Das Dateisystem befindet sich in einem fehlerfreien Zustand und ist erreichbar und kann verwendet werden.
WIRD ERSTELLT	Amazon FSx erstellt ein neues Dateisystem.
WIRD GELÖSCHT	Amazon FSx löscht ein vorhandenes Dateisystem.
WIRD AKTUALISIERT	Das Dateisystem wird derzeit einem vom Kunden initiierten Update unterzogen.
FALSCH KONFIGURIERT	Das Dateisystem befindet sich aufgrund einer Änderung in Ihrer Active Directory-Umgebung in einem beeinträchtigten Zustand. Ihr Dateisystem ist entweder derzeit nicht verfügbar oder es besteht die Gefahr, dass die Verfügbarkeit verloren geht, und Backups sind möglicherweise nicht erfolgreich. Informationen zur Wiederherstellung der Verfügbarkeit finden Sie unter <a href="#">Das Dateisystem befindet sich in einem falsch konfigurierten Zustand</a> .
MISCONFIGURED_UNAVAILABLE	Das Dateisystem ist derzeit aufgrund einer Änderung in Ihrer Active Directory-Umgebung nicht verfügbar. Informationen zur Wiederherstellung der Verfügbarkeit finden Sie unter <a href="#">Das Dateisystem befindet sich in einem falsch konfigurierten Zustand</a> .

Status des Dateisystems	Beschreibung
FEHLGESCHLAGEN	<ul style="list-style-type: none"><li>• Beim Erstellen eines neuen Dateisystems konnte Amazon FSx das neue Dateisystem nicht erstellen.</li><li>• Das Dateisystem ist nicht verfügbar.</li><li>• Das Dateisystem ist ausgefallen und Amazon FSx kann es nicht wiederherstellen.</li><li>• Amazon FSx kann keine Backups erstellen.</li></ul>



# Unterstützte Clients, Zugriffsmethoden und Umgebungen für Amazon FSx for Windows File Server

Sie können mit einer Vielzahl unterstützter Clients und Methoden von beiden auf Ihre Amazon FSx-Dateisysteme zugreifenAWSund On-Premise-Umgebungen.

Themen

- [Unterstützte Clients](#)
- [Unterstützte Zugriffsmethoden](#)
- [Unterstützte Umgebungen](#)

## Unterstützte Clients

Amazon FSx unterstützt die Verbindung zu Ihrem Dateisystem von einer Vielzahl von Compute-Instances und Betriebssystemen aus. Dies geschieht durch Unterstützung des Zugriffs über das Server Message Block (SMB) -Protokoll, Versionen 2.0 bis 3.1.1.

Die folgendenAWSCompute-Instances werden für die Verwendung mit Amazon FSx unterstützt:

- Amazon Elastic Compute Cloud (Amazon EC2) -Instances, einschließlich Microsoft Windows-, Amazon Linux- und Amazon Linux 2-Instances Weitere Informationen finden Sie unter [Zugreifen auf Dateifreigaben](#).
- Amazon Elastic Container Service (Amazon ECS) -Container Weitere Informationen finden Sie unter [FSx for Windows File Server Volumes](#) in der Amazon Elastic Container Service Entwicklerhandbuch.
- WorkSpaces -Instances — Weitere Informationen hierzu finden Sie unterAWSBlogbeitrag [Verwenden von FSx for Windows File Server WorkSpaces](#).
- Amazon AppStream 2.0-Instances — Weitere Informationen hierzu finden Sie unterAWSBlogbeitrag [Verwenden von Amazon FSx mit Amazon AppStream 2.0](#).
- VMs, die in VMware Cloud ausgeführt werdenAWS-Umgebungen — Weitere Informationen hierzu finden Sie unterAWSBlogbeitrag [Speichern und Freigeben von Dateien mit FSx for Windows File Server in einer VMware Cloud aufAWSUmgebung](#).

Die folgenden Betriebssysteme werden für die Verwendung mit Amazon FSx unterstützt:

- Windows Server 2008, Windows Server 2008 Server 2012, Windows Server 2012
- Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 (einschließlich der Windows 7- und Windows 10-Desktop-Erfahrungen von WorkSpaces) und Windows 11.
- Linux, unter Verwendung der `cifs-utils`-Werkzeug.
- macOS

## Unterstützte Zugriffsmethoden

Sie können die folgenden Zugriffsmethoden und -Methoden mit Amazon FSx verwenden.

### Zugriff auf Dateisysteme mit ihren Standard-DNS-Namen

FSx for Windows File Server stellt für jedes Dateisystem einen DNS-Namen (Domain Name System) bereit. Sie greifen auf Ihr FSx for Windows File Server Server-Dateisystem zu, indem Sie unter Verwendung dieses DNS-Namens einen Laufwerksbuchstaben auf Ihrer Compute-Instance Ihrer Amazon FSx-Dateifreigabe zuordnen. Weitere Informationen hierzu finden Sie unter [Verwenden von Microsoft Windows-Dateifreigaben](#).

#### Important

Amazon FSx registriert DNS-Einträge für ein Dateisystem nur, wenn Sie Microsoft DNS als Standard-DNS verwenden. Wenn Sie ein DNS eines Drittanbieters verwenden, müssen Sie DNS-Einträge für Ihre Amazon FSx-Dateisysteme manuell einrichten. Informationen zur Auswahl der richtigen IP-Adressen für das Dateisystem [Abrufen der richtigen Dateisystem-IP-Adressen zur Verwendung für DNS](#).

So finden Sie den DNS-Namen:

- Wählen Sie in der Amazon FSx Konsole `Dateisysteme` und dann `wähle-Details`. Zeigen Sie den DNS-Namen in der `Netzwerk & Sicherheit`-Abschnitt.
- Oder sehen Sie es sich in der Antwort des `CreateFileSystem` oder `DescribeFileSystems` API-Befehl.

Für alle Single-AZ-Dateisysteme, die mit einem AWS-Verwaltetes Microsoft Active Directory, der DNS-Name sieht wie folgt aus: `fs-0123456789abcdef0.ad-dns-domain-name`

Für alle Single-AZ-Dateisysteme, die mit einem selbstverwalteten Active Directory verbunden sind, und für jedes Multi-AZ-Dateisystem sieht der DNS-Name wie folgt aus: `amznfsxaa11bb22.ad-domain.com`

## Verwenden von DNS-Namen mit Kerberos-Authentifizierung

Wir empfehlen die Verwendung von Kerberos-basierter Authentifizierung und Verschlüsselung bei der Übertragung mit Amazon FSx. Kerberos bietet die sicherste Authentifizierung für Clients, die auf Ihr Dateisystem zugreifen. Um die Kerberos-basierte Authentifizierung und Verschlüsselung von Daten während der Übertragung für Ihre SMB-Sitzungen zu aktivieren, verwenden Sie den von Amazon FSx bereitgestellten DNS-Namen des Dateisystems für den Zugriff auf Ihr Dateisystem.

Wenn Sie eine externe Vertrauensstellung zwischen Ihrem konfiguriert haben AWS Verwaltetes Microsoft Active Directory und Ihr lokales Active Directory zur Verwendung von Amazon FSx Remote PowerShell. Bei der Kerberos-Authentifizierung müssen Sie auf dem Client eine lokale Gruppenrichtlinie für die Suchreihenfolge der Gesamtstruktur konfigurieren. Weitere Informationen finden Sie unter [Kerberos Forest-Suchreihenfolge \(KFSO\) konfigurieren](#) in der Microsoft-Dokumentation.

## Zugreifen auf Dateisysteme mithilfe von DNS-Aliassen

FSx for Windows File Server bietet einen DNS-Namen für jedes Dateisystem, das Sie für den Zugriff auf Ihre Dateifreigaben verwenden können. Sie können den Zugriff auf Amazon FSx auch über andere DNS-Namen als den standardmäßigen DNS-Namen aktivieren, den Amazon FSx erstellt, indem Sie Aliase für Ihre FSx for Windows File Server Server-Dateisysteme registrieren.

Mithilfe von DNS-Aliasnamen können Sie Ihre Windows-Dateifreigabedaten nach Amazon FSx verschieben und weiterhin Ihre vorhandenen DNS-Namen verwenden, um auf Daten auf Amazon FSx zuzugreifen. Mit DNS-Aliasnamen können Sie auch aussagekräftige Namen verwenden, die die Verwaltung von Tools und Anwendungen für die Verbindung mit Ihren Amazon FSx-Dateisystemen erleichtern. Weitere Informationen finden Sie unter [DNS-Aliase verwalten](#).

## Verwenden von DNS-Aliasnamen mit Kerberos-Authentifizierung

Wir empfehlen die Verwendung von Kerberos-basierter Authentifizierung und Verschlüsselung bei der Übertragung mit Amazon FSx. Kerberos bietet die sicherste Authentifizierung für Clients, die auf Ihr Dateisystem zugreifen. Um die Kerberos-Authentifizierung für Clients zu aktivieren, die über einen DNS-Alias auf Amazon FSx zugreifen, müssen Sie Dienstprinzipalnamen (SPNs) hinzufügen, die dem DNS-Alias auf dem Active Directory-Computerobjekt Ihres Amazon FSx-Dateisystems entsprechen.

Optional können Sie Clients, die über einen DNS-Alias auf das Dateisystem zugreifen, die Kerberos-Authentifizierung und -Verschlüsselung erzwingen, indem Sie die folgenden Gruppenrichtlinienobjekte (GPOs) in Ihrem Active Directory festlegen:

- **Beschränken von NTLM: Ausgehender NTLM-Verkehr zu Remoteservern-** Verwenden Sie diese Richtlinieneinstellung, um ausgehenden NTLM-Datenverkehr von einem Computer zu einem Remote-Server, auf dem das Windows-Betriebssystem ausgeführt wird, zu verweigern oder zu überwachen.
- **Beschränken von NTLM: Hinzufügen von Remote-Server-Ausnahmen für die NTLM-Authentifizierung-** Verwenden Sie diese Richtlinieneinstellung, um eine Ausnahmeliste von Remoteservern zu erstellen, für die Clientgeräte die NTLM-Authentifizierung verwenden dürfen, wenn **Netzwerk-Sicherheit: Beschränken von NTLM: Ausgehender NTLM-Verkehr zu Remoteservern** Richtlinieneinstellung ist konfiguriert.

Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisystem](#).

## Arbeiten mit FSx for Windows File Server Dateisysteme und DFS-Namespaces

FSx for Windows File Server unterstützt die Verwendung von Microsoft Distributed File System (DFS) -Namespaces. Mit DFS-Namespaces können Sie Dateifreigaben auf mehreren Dateisystemen in einer gemeinsamen Ordnerstruktur (einem Namespace) organisieren, die Sie für den Zugriff auf das gesamte Datei-Dataset verwenden. Sie können einen Namen in Ihrem DFS-Namespace verwenden, um auf Ihr Amazon FSx-Dateisystem zuzugreifen, indem Sie dessen Linkziel als DNS-Name des Dateisystems konfigurieren. Weitere Informationen finden Sie unter [Gruppierung mehrerer Dateisysteme mit DFS-Namespaces](#).

## Unterstützte Umgebungen

Sie können über Ressourcen, die sich in derselben VPC wie Ihr Dateisystem befinden, auf Ihr Dateisystem zugreifen. Weitere Informationen und eine detaillierte Anleitung finden Sie unter [Exemplarische Vorgehensweise 1: Voraussetzungen für die ersten Schritte](#).

Sie können auch auf Dateisysteme zugreifen, die nach dem 22. Februar 2019 erstellt wurden, aus lokalen Ressourcen und aus Ressourcen, die sich in einer anderen VPC befinden. AWS-Konto, oder AWS Region. Die folgende Tabelle zeigt die Umgebungen, aus denen Amazon FSx den Zugriff

von Clients in jeder der unterstützten Umgebungen unterstützt, je nachdem, wann das Dateisystem erstellt wurde.

Kunden mit Sitz in...	Zugriff auf Dateisysteme, die vor dem 22. Februar 2019 erstellt wurden	Zugriff auf Dateisysteme, die vor dem 17. Dezember 2020 erstellt wurden	Zugriff auf Dateisysteme, die nach dem 17. Dezember 2020 erstellt wurden
Subnetze, in denen das Dateisystem erstellt wird	✓	✓	✓
Primäre CIDR-Blöcke der VPC, in der das Dateisystem erstellt wurde	✓	✓	✓
Sekundäre CIDRs der VPC, in der das Dateisystem erstellt wurde		Clients mit IP-Adressen in einem <a href="#">RFC 1918</a> privater IP-Adressbereich:	Clients mit IP-Adressen außerhalb des folgenden CIDR-Blockbereichs: 198.19.0.0/16
Andere CIDRs oder Peered-Netzwerke		<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>	

### Note

In einigen Fällen möchten Sie möglicherweise lokal über einen nicht privaten IP-Adressbereich auf ein Dateisystem zugreifen, das vor dem 17. Dezember 2020 erstellt wurde. Erstellen Sie dazu ein neues Dateisystem aus einer Sicherung des Dateisystems. Weitere Informationen finden Sie unter [Arbeiten mit Backups](#).

Im Folgenden finden Sie Informationen darüber, wie Sie lokal und von verschiedenen VPCs auf Ihre FSx for Windows File Server Server-Dateisysteme zugreifen können. AWS-Konten, oder AWS-Regionen.

## Zugriff auf FSx for Windows File Server Dateisysteme von On-Premise-Standorten

FSx for Windows File Server AWS Direct Connect oder AWS VPN um von Ihren lokalen Compute-Instanzen aus auf Ihre Dateisysteme zuzugreifen. Mit Unterstützung für AWS Direct Connect ermöglicht Ihnen FSx for Windows File Server den Zugriff auf Ihr Dateisystem über eine dedizierte Netzwerkverbindung von Ihrer lokalen Umgebung aus. Mit Unterstützung für AWS VPN ermöglicht Ihnen FSx for Windows File Server den Zugriff auf Ihr Dateisystem von Ihren lokalen Geräten über einen sicheren und privaten Tunnel.

Nachdem Sie Ihre lokale Umgebung mit der VPC verbunden haben, die Ihrem Amazon FSx-Dateisystem zugeordnet ist, können Sie über den DNS-Namen oder einen DNS-Alias auf Ihr Dateisystem zugreifen. Sie tun dies genauso wie bei Compute-Instances innerhalb der VPC. Weitere Informationen zu AWS Direct Connect finden Sie im [AWS Direct Connect-Benutzerhandbuch](#). Weitere Informationen zur Einrichtung AWS VPN-Verbindungen, siehe [VPN-Verbindungen](#) in der Amazon VPC User Guide.

FSx for Windows File Server unterstützt auch die Verwendung von Amazon FSx File Gateway, um einen nahtlosen Zugriff auf Ihre In-Cloud-Dateifreigaben von FSx für Windows aus Ihren lokalen Rechnerinstanzen zu ermöglichen. Weitere Informationen finden Sie hier: [Amazon FSx File Gateway-Benutzerhandbuch](#).

## Zugriff auf FSx for Windows File Server Dateisysteme von einer anderen VPC, AWS-Region

Sie können auf Ihr FSx for Windows File Server Dateisystem von Compute-Instances in einer anderen VPC AWS-Konto, oder AWS-Region aus dieser Region, die mit Ihrem Dateisystem verknüpft ist. Dazu können Sie VPC-Peering oder Transit-Gateways verwenden. Wenn Sie eine VPC-Peering-Verbindung oder ein Transit-Gateway zum Verbinden von VPCs verwenden, können Compute-Instances, die sich in einer VPC befinden, auf Amazon FSx-Dateisysteme in einer anderen VPC zugreifen. Dieser Zugriff ist auch dann möglich, wenn die VPCs zu verschiedenen Konten gehören und selbst wenn sich die VPCs in verschiedenen AWS-Regionen.

Ein VPC-Peering-Verbindungs ist eine Netzwerkverbindung zwischen zwei VPCs. Sie ermöglicht die Weiterleitung des Datenverkehrs zwischen den VPCs mithilfe privater IPv4- oder IPv6-Adressen. Sie können VPC-Peering verwenden, um VPCs innerhalb derselben zu verbinden AWS-Region oder zwischen AWS-Regionen. Weitere Informationen über VPC Peering finden Sie unter [Was ist VPC Peering?](#) in der Amazon VPC Peering Guide.

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und lokale Netzwerke miteinander verbinden können. Weitere Informationen zur Verwendung von VPC Transit-Gateways finden Sie unter [Erste Schritte mit Transit-Gateways](#) in der Amazon VPC Transit Gateways.

Nachdem Sie eine VPC-Peering- oder Transit-Gateway-Verbindung eingerichtet haben, können Sie über den DNS-Namen auf Ihr Dateisystem zugreifen. Sie tun dies genauso wie bei Compute-Instances innerhalb der zugehörigen VPC.

# Verfügbarkeit und Haltbarkeit: Single-AZ- und Multi-AZ-Dateisysteme

Amazon FSx for Windows File Server bietet zwei Arten der Dateisystembereitstellung: Single-AZ und Multi-AZ. Die folgenden Abschnitte enthalten Informationen, die Ihnen bei der Auswahl des richtigen Bereitstellungstyps für Ihre Workloads helfen sollen. Informationen zum Verfügbarkeits-SLA (Service Level Agreement) des Services finden Sie unter [Amazon FSx Service Level Agreement](#).

Single-AZ-Dateisysteme bestehen aus einer einzelnen Windows-Dateiserverinstanz und einer Reihe von Speichervolumen innerhalb einer einzigen Availability Zone (AZ). Bei Single-AZ-Dateisystemen werden Daten in den meisten Fällen automatisch repliziert, um sie vor dem Ausfall einer einzelnen Komponente zu schützen. Amazon FSx überwacht kontinuierlich Hardwarefehler und stellt die Wiederherstellung nach Ausfällen automatisch wieder her, indem die ausgefallene Infrastrukturkomponente ersetzt wird. Single-AZ-Dateisysteme sind während dieser Ausfallwiederherstellungsereignisse und während der geplanten Dateisystemwartung innerhalb des Wartungsfensters, das Sie für Ihr Dateisystem konfigurieren, in der Regel für weniger als 20 Minuten offline. Bei Single-AZ-Dateisystemen kann ein Dateisystemausfall in seltenen Fällen nicht behoben werden, z. B. aufgrund von Ausfällen mehrerer Komponenten oder aufgrund eines fehlerhaften Fehlers eines einzelnen Dateiservers, der das Dateisystem in einem inkonsistenten Zustand zurücklässt. In diesem Fall können Sie Ihr Dateisystem aus der letzten Sicherung wiederherstellen.

Multi-AZ-Dateisysteme bestehen aus einem Hochverfügbarkeitscluster von Windows-Dateiservern, die auf zwei AZs (eine bevorzugte AZ und eine Standby-AZ) verteilt sind und die Windows Server Failover Clustering (WSFC) -Technologie und eine Reihe von Speichervolumen auf jeder der beiden AZs nutzen. Die Daten werden innerhalb jeder einzelnen AZ und zwischen den beiden AZs synchron repliziert. Im Vergleich zur Single-AZ-Bereitstellung bieten Multi-AZ-Bereitstellungen eine längere Lebensdauer, da Daten zwischen AZs weiter repliziert werden, und eine höhere Verfügbarkeit bei geplanten Systemwartungen und ungeplanten Betriebsunterbrechungen durch automatisches Failover auf die Standby-AZ. Auf diese Weise können Sie weiterhin auf Ihre Daten zugreifen und Ihre Daten vor Instance-Ausfällen und AZ-Störungen schützen.

## Wählen Sie die Single-AZ- oder Multi-AZ-Dateisystembereitstellung

Wir empfehlen die Verwendung von Multi-AZ-Dateisystemen für die meisten Produktionsworkloads aufgrund des damit verbundenen Hochverfügbarkeits- und Haltbarkeitsmodells. Die Single-AZ-Bereitstellung ist als kosteneffiziente Lösung für Test- und Entwicklungsworkloads, für



bestimmte Produktionsworkloads, bei denen die Replikation in die Anwendungsebene integriert ist und für die keine zusätzliche Redundanz auf Speicherebene erforderlich ist, sowie für Produktionsworkloads konzipiert, für die weniger Verfügbarkeit und RPO-Anforderungen (Recovery Point Objective) gelten. Workloads mit lockeren Verfügbarkeitsanforderungen können im Fall einer geplanten Dateisystemwartung oder ungeplanten Serviceunterbrechung einen vorübergehenden Verfügbarkeitsverlust von bis zu 20 Minuten tolerieren, und Workloads mit gelockerten RPO-Anforderungen können in seltenen Fällen den Verlust von Datenaktualisierungen seit dem letzten Backup tolerieren.

## Funktionsunterstützung nach Bereitstellungstyp

In der folgenden Tabelle sind die Funktionen zusammengefasst, die von den Dateisystem-Bereitstellungstypen FSx for Windows File Server unterstützt werden:

Deployment type (Bereitstellungstyp)	SSD-Speicher	HDD-Speicher	DFS-Namespaces	DFS-Replikation	Benutzerdefinierte DNS-Namen	CA-Aktionen
Single-AZ 1	✓		✓	✓	✓	
Einzel-AZ 2	✓	✓	✓		✓	✓*
Multi-AZ	✓	✓	✓		✓	✓*

### Note

\* Sie können zwar kontinuierlich verfügbare Freigaben (CA) auf Single-AZ 2-Dateisystemen erstellen, aber Sie sollten CA-Freigaben auf Multi-AZ-Dateisystemen für SQL Server-HA-Bereitstellungen verwenden.

## Failover-Prozess für FSx for Windows File Server

Multi-AZ-Dateisysteme führen automatisch ein Failover vom bevorzugten Dateiserver zum Standby-Dateiserver durch, wenn eine der folgenden Bedingungen eintritt:

- Es tritt ein Ausfall der Availability Zone auf.
- Der bevorzugte Dateiserver ist nicht mehr verfügbar.
- Der bevorzugte Dateiserver wird planmäßig gewartet.

Beim Failover von einem Dateiserver auf einen anderen beginnt der neue aktive Dateiserver automatisch, alle Lese- und Schreibanforderungen des Dateisystems zu bearbeiten. Wenn die Ressourcen im bevorzugten Subnetz verfügbar sind, kehrt Amazon FSx automatisch zum bevorzugten Dateiserver im bevorzugten Subnetz zurück. Ein Failover dauert in der Regel weniger als 30 Sekunden von der Erkennung des Fehlers auf dem aktiven Dateiserver bis zur Heraufstufung des Standby-Dateiservers in den aktiven Status. Das Failback zur ursprünglichen Multi-AZ-Konfiguration ist ebenfalls in weniger als 30 Sekunden abgeschlossen und erfolgt erst, wenn der Dateiserver im bevorzugten Subnetz vollständig wiederhergestellt ist.

Während des kurzen Zeitraums, in dem Ihr Dateisystem einen Failover und ein Failback durchführt, kann es sein, dass I/O angehalten wird und CloudWatch Amazon-Metriken vorübergehend nicht verfügbar sind.

Bei Multi-AZ-Dateisystemen müssen alle während dieser Zeit vorgenommenen Datenänderungen zwischen den Dateiservern synchronisiert werden, wenn während des Failovers und des Failbacks fortlaufender Datenverkehr besteht. Dieser Vorgang kann bei schreib- und IOPS-intensiven Workloads bis zu mehreren Stunden dauern. Wir empfehlen, die Auswirkungen von Failovers auf Ihre Anwendung zu testen, während Ihr Dateisystem geringer ausgelastet ist.

## Failover-Erfahrung auf Windows-Clients

Beim Failover von einem Dateiserver auf einen anderen beginnt der neue aktive Dateiserver automatisch, alle Lese- und Schreibanforderungen des Dateisystems zu bearbeiten. Sobald die Ressourcen im bevorzugten Subnetz verfügbar sind, kehrt Amazon FSx automatisch zum bevorzugten Dateiserver im bevorzugten Subnetz zurück. Da der DNS-Name des Dateisystems derselbe bleibt, sind Failover für Windows-Anwendungen transparent, die den Dateisystembetrieb ohne manuelles Eingreifen wieder aufnehmen. Ein Failover dauert in der Regel weniger als 30 Sekunden von der Erkennung des Fehlers auf dem aktiven Dateiserver bis zur Heraufstufung des

Standby-Dateiservers in den aktiven Status. Das Failback zur ursprünglichen Multi-AZ-Konfiguration ist ebenfalls in weniger als 30 Sekunden abgeschlossen und erfolgt erst, nachdem der Dateiserver im bevorzugten Subnetz vollständig wiederhergestellt ist.

## Failover-Erfahrung auf Linux-Clients

Linux-Clients unterstützen kein automatisches DNS-basiertes Failover. Daher stellen sie während eines Failovers nicht automatisch eine Verbindung zum Standby-Dateiserver her. Sie nehmen den Dateisystembetrieb automatisch wieder auf, nachdem das Multi-AZ-Dateisystem einen Failback auf den Dateiserver im bevorzugten Subnetz ausgeführt hat.

## Testen des Failovers auf einem Dateisystem

Sie können das Failover Ihres Multi-AZ-Dateisystems testen, indem Sie dessen Durchsatzkapazität ändern. Wenn Sie die Durchsatzkapazität Ihres Dateisystems ändern, schaltet Amazon FSx den Dateiserver des Dateisystems aus. Multi-AZ-Dateisysteme schalten automatisch auf den sekundären Server um, während Amazon FSx zuerst den bevorzugten Server-Dateiserver ersetzt. Dann kehrt das Dateisystem automatisch auf den neuen Primärserver zurück und Amazon FSx ersetzt den sekundären Dateiserver.

Sie können den Fortschritt der Anfrage zur Aktualisierung der Durchsatzkapazität in der Amazon FSx-Konsole, der CLI und der API überwachen. Sobald das Update erfolgreich abgeschlossen wurde, wurde für Ihr Dateisystem ein Failover auf den Sekundärserver und ein Failback auf den Primärserver durchgeführt. Weitere Informationen zur Änderung der Durchsatzkapazität Ihres Dateisystems und zur Überwachung des Fortschritts der Anfrage finden Sie unter [Verwaltung der Durchsatzkapazität](#).

## Arbeiten mit Single- und Multi-AZ-Dateisystemressourcen

### Subnetze

Wenn Sie eine VPC erstellen, erstreckt sie sich über alle Availability Zones (AZs) in der Region. Availability Zones sind unabhängige Standorte, die so aufgebaut sind, dass sie von Fehlern in anderen Availability Zones nicht betroffen sind. Nach dem Erstellen einer VPC können Sie in jeder Availability Zone ein oder mehrere Subnetze hinzufügen. Die Standard-VPC hat in jeder Availability Zone ein Subnetz. Jedes Subnetz muss sich vollständig innerhalb einer Availability Zone befinden und darf nicht mehrere Zonen umfassen. Wenn Sie ein Single-AZ-Amazon FSx-Dateisystem erstellen, geben Sie ein einzelnes Subnetz für das Dateisystem an. Das von Ihnen gewählte Subnetz definiert die Availability Zone, in der das Dateisystem erstellt wird.

Wenn Sie ein Multi-AZ-Dateisystem erstellen, geben Sie zwei Subnetze an, eines für den bevorzugten Dateiserver und eines für den Standby-Dateiserver. Die beiden ausgewählten Subnetze müssen sich in unterschiedlichen Availability Zones innerhalb derselben Region befinden. AWS

Für AWS In-Applications empfehlen wir, dass Sie Ihre Clients in derselben Availability Zone wie Ihr bevorzugter Dateiserver starten, um die Latenz zu minimieren.

## Elastische Netzwerkschnittstellen für Dateisysteme

Wenn Sie ein Amazon FSx-Dateisystem erstellen, stellt Amazon FSx eine oder mehrere [elastische Netzwerkschnittstellen](#) in der [Amazon Virtual Private Cloud \(VPC\)](#) bereit, die Sie Ihrem Dateisystem zuordnen. Die Netzwerkschnittstelle ermöglicht Ihrem Client die Kommunikation mit dem Dateisystem FSx for Windows File Server. Es wird davon ausgegangen, dass die Netzwerkschnittstelle zum Serviceumfang von Amazon FSx gehört, obwohl sie Teil der VPC Ihres Kontos ist. Multi-AZ-Dateisysteme verfügen über zwei elastische Netzwerkschnittstellen, eine für jeden Dateiserver. Single-AZ-Dateisysteme verfügen über eine elastic network interface.

### Warning

Sie dürfen die mit Ihrem Dateisystem verknüpften Elastic Network-Schnittstellen nicht ändern oder löschen. Das Ändern oder Löschen der Netzwerkschnittstelle kann zu einem dauerhaften Verbindungsverlust zwischen Ihrer VPC und Ihrem Dateisystem führen.

In der folgenden Tabelle sind die Subnetz-, elastic network interface- und IP-Adressressourcen für die Bereitstellungstypen des Dateisystems FSx for Windows File Server zusammengefasst:

Bereitstellungstyp des Dateisystems	Anzahl der Subnetze	Anzahl der elastischen Netzwerkschnittstellen	Anzahl der IP-Adressen
Single-AZ 2	1	1	2
Einzel-AZ 1	1	1	1
Multi-AZ	2	2	4

Sobald ein Dateisystem erstellt wurde, ändern sich seine IP-Adressen erst, wenn das Dateisystem gelöscht wird.

 **Important**

Amazon FSx unterstützt nicht den Zugriff auf Dateisysteme aus dem öffentlichen Internet oder die Offenlegung von Dateisystemen im öffentlichen Internet. Wenn eine Elastic IP-Adresse, bei der es sich um eine öffentliche IP-Adresse handelt, die über das Internet erreichbar ist, an die elastic network interface eines Dateisystems angehängt wird, trennt Amazon FSx sie automatisch.

# Kostenoptimierung mit Amazon FSx

FSx für Windows File Server bietet verschiedene Funktionen, mit denen Sie Ihre Gesamtbetriebskosten (TCO) auf der Grundlage Ihrer Anwendungsanforderungen optimieren können. Sie können den Speichertyp (HDD oder SSD) wählen, um das richtige Gleichgewicht zwischen Kosten und Leistungsanforderungen für Ihre Anwendung zu erreichen. Sie haben die Flexibilität, die Durchsatzkapazität getrennt von der Menge der Speicherkapazität auszuwählen, um Ihre Kosten zu optimieren. Und Sie können Datendeduplizierung nutzen, um die Speicherkosten zu optimieren, indem Sie redundante Daten in Ihrem Dateisystem eliminieren.

## Themen

- [Flexibilität, Speicher und Durchsatz unabhängig voneinander zu wählen](#)
- [Optimierung der Speicherkosten](#)
- [Nutzung und Abrechnung überprüfen](#)

## Flexibilität, Speicher und Durchsatz unabhängig voneinander zu wählen

Mit FSx für Windows File Server können Sie den Speicher, die SSD-IOPS und die Durchsatzkapazitäten Ihres Dateisystems unabhängig voneinander konfigurieren. Dies gibt Ihnen die Flexibilität, um die richtige Mischung aus Kosten und Leistung zu erzielen. Sie können sich beispielsweise für eine große Speichermenge mit einer relativ geringen Durchsatzkapazität für kalte (in der Regel inaktive) Workloads entscheiden, um unnötige Durchsatzkosten zu sparen. Oder, als weiteres Beispiel, Sie könnten sich für eine große Durchsatzkapazität für eine relativ geringe Speicherkapazität entscheiden. Eine höhere Durchsatzkapazität geht mit einer höheren Speichermenge für das Caching auf dem Dateiserver einher. Sie können das schnelle Caching auf dem Dateiserver nutzen, um die Leistung für aktiv abgerufene Daten zu optimieren. Weitere Informationen finden Sie unter [Leistung von FSx for Windows File Server](#).

Sie können die Speicherkapazität jederzeit erhöhen, nachdem Sie ein Dateisystem erstellt haben. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#). Sie können SSD-IOPS jederzeit unabhängig von der Speicherkapazität skalieren, nachdem Sie ein Dateisystem erstellt haben. Weitere Informationen finden Sie unter [Verwalten von SSD-IOPS](#). Sie können die Durchsatzkapazität jederzeit erhöhen oder verringern, sodass Sie flexibel auf sich ändernde

Leistungsanforderungen reagieren können. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

## Optimierung der Speicherkosten

Sie können Ihre Speicherkosten mit Amazon FSx auf verschiedene Arten optimieren, die im Folgenden beschrieben werden.

### Kostenoptimierung mithilfe von Speichertypen

FSx für Windows File Server bietet zwei Speichertypen — Festplattenlaufwerke (HDD) und Solid-State-Laufwerke (SSD) —, sodass Sie das Kosten-/Leistungsverhältnis optimieren können, um Ihre Workload-Anforderungen zu erfüllen. HDD-Speicher sind für ein breites Spektrum an Workloads konzipiert, darunter Home-Verzeichnisse, Benutzer- und Abteilungsfreigaben sowie Content-Management-Systeme. SSD-Speicher wurden für die leistungsstärksten und latenzempfindlichsten Workloads entwickelt, einschließlich Datenbanken, Workloads zur Medienverarbeitung und Datenanalyseanwendungen. Weitere Informationen finden Sie unter [Latency](#) und [Preise für Amazon FSx für Windows-Dateiserver](#).

### Optimierung der Speicherkosten mithilfe von Datendeduplizierung

Große Datensätze enthalten oft redundante Daten, was die Datenspeicherkosten erhöht. Beispielsweise können Benutzerdateifreigaben mehrere Kopien derselben Datei enthalten, die von mehreren Benutzern gespeichert werden. Softwareentwicklungsaktien können viele Binärdateien enthalten, die von Build zu Build unverändert bleiben. Sie können Ihre Datenspeicherkosten senken, indem Sie Folgendes aktivieren: **Datendeduplizierung** für Ihr Dateisystem. Wenn sie aktiviert ist, reduziert oder entfernt die Datendeduplizierung automatisch redundante Daten, indem duplizierte Teile des Datensatzes nur einmal gespeichert werden. Weitere Informationen zur Datendeduplizierung und wie Sie sie einfach für Ihr Amazon FSx-Dateisystem aktivieren können, finden Sie unter [Datendeduplizierung](#).

## Nutzung und Abrechnung überprüfen

Sie können die Nutzung Ihres Dateisystems, einschließlich Ihrer Speicherkapazität, Durchsatzkapazität, Sicherung und Datenübertragung, überprüfen, indem Sie den **AWS Billing Armaturenbrett** oder das **AWS Cost Explorer**. Mit diesen Tools können Sie die Nutzung Ihrer Ressourcen überprüfen und nach Nutzungsart, Region und anderen relevanten Kriterien filtern

und gruppieren. Beachten Sie, dass Sie, um die Nutzung eines einzelnen Dateisystems oder eines einzelnen Dateisystem-Backups einsehen zu können, Tags für diese spezifische Ressource aktivieren und tagbasierte Abrechnungsberichte aktivieren müssen. Weitere Informationen finden Sie unter [BenutzenAWSTags für die Kostenzuweisung](#) in der AWS Billing Benutzeranleitung.



# Arbeiten mit Microsoft Active Directory in FSx for Windows File Server

Amazon FSx arbeitet mit Microsoft Active Directory zusammen, um es in Ihre bestehenden Microsoft Windows-Umgebungen zu integrieren. Active Directory ist der Verzeichnisdienst von Microsoft, der verwendet wird, um Informationen über Objekte im Netzwerk zu speichern und Administratoren und Benutzern das Auffinden und Verwenden dieser Informationen zu erleichtern. Zu diesen Objekten gehören in der Regel gemeinsam genutzte Ressourcen wie Dateiserver und Netzwerkbenutzer- und Computerkonten.

Wenn Sie ein Dateisystem mit Amazon FSx erstellen, fügen Sie es Ihrer Active Directory-Domain hinzu, um Benutzerauthentifizierung und Zugriffskontrolle auf Datei- und Orderebene zu ermöglichen. Ihre Benutzer können dann ihre bestehenden Benutzeridentitäten in Active Directory verwenden, um sich zu authentifizieren und auf das Amazon FSx-Dateisystem zuzugreifen. Benutzer können auch ihre vorhandenen Identitäten verwenden, um den Zugriff auf einzelne Dateien und Ordner zu kontrollieren. Darüber hinaus können Sie Ihre vorhandenen Dateien und Ordner sowie die Konfiguration der Sicherheitszugriffskontrollliste (ACL) dieser Elemente ohne Änderungen auf Amazon FSx migrieren.

Amazon FSx bietet Ihnen zwei Optionen für die Verwendung Ihres Dateisystems FSx for Windows File Server mit Active Directory: [Verwenden von Amazon FSx mit AWS Directory Service for Microsoft Active Directory](#) und [Verwenden von Amazon FSx mit Ihrem selbstverwalteten Microsoft Active Directory](#)

## Note

Amazon FSx unterstützt [Microsoft Azure Active Directory Domain Services](#), die Sie mit einem [Microsoft Azure Active Directory](#) verbinden können.


Nachdem Sie eine verknüpfte Active Directory-Konfiguration für ein Dateisystem erstellt haben, können Sie nur die folgenden Eigenschaften aktualisieren:

- Benutzeranmeldeinformationen für den Dienst
- IP-Adressen von DNS-Servern

Sie können die folgenden Eigenschaften für Ihr verbundenes Microsoft AD nicht ändern, nachdem Sie das Dateisystem erstellt haben:

- DomainName
- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

Sie können jedoch aus einer Sicherung ein neues Dateisystem erstellen und diese Eigenschaften in der Microsoft Active Directory-Integrationskonfiguration für das neue Dateisystem ändern. Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 2: Erstellen eines Dateisystems aus einer Sicherung](#).

 Note

Amazon FSx unterstützt [Active Directory Connector](#) und [Simple Active Directory](#) nicht.

Ihr FSx for Windows File Server wird möglicherweise falsch konfiguriert, wenn es eine Änderung in Ihrer Active Directory-Konfiguration gibt, die die Verbindung zu Ihrem Dateisystem unterbricht. Um Ihr Dateisystem wieder in den Status Verfügbar zu versetzen, wählen Sie in der Amazon FSx-Konsole die Schaltfläche „Wiederherstellung versuchen“ oder verwenden Sie den `StartMisconfiguredStateRecovery` Befehl in der Amazon FSx-API oder -Konsole. Weitere Informationen finden Sie unter [Das Dateisystem befindet sich in einem falsch konfigurierten Zustand](#).

#### Themen

- [Verwenden von Amazon FSx mit AWS Directory Service for Microsoft Active Directory](#)
- [Verwenden von Amazon FSx mit Ihrem selbstverwalteten Microsoft Active Directory](#)

## Verwenden von Amazon FSx mit AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) bietet vollständig verwaltete, hochverfügbare, aktuelle Active Directory-Verzeichnisse in der Cloud. Sie können diese Active Directory-Verzeichnisse in Ihrer Workload-Bereitstellung verwenden.

Wenn Ihr Unternehmen Identitäten und Geräte verwaltet, empfehlen wir Ihnen, Ihr Amazon FSx-Dateisystem mit zu integrieren. AWS Managed Microsoft AD AWS Managed Microsoft AD Auf diese Weise erhalten Sie eine schlüsselfertige Lösung mit Amazon FSx mit. AWS Managed Microsoft AD AWS kümmert sich um die Bereitstellung, den Betrieb, die hohe Verfügbarkeit, Zuverlässigkeit, Sicherheit und die nahtlose Integration der beiden Dienste, sodass Sie sich auf den effektiven Betrieb Ihrer eigenen Workloads konzentrieren können.

Um Amazon FSx mit Ihrem AWS Managed Microsoft AD Setup zu verwenden, können Sie die Amazon FSx-Konsole verwenden. Wenn Sie in der Konsole ein neues Dateisystem FSx for Windows File Server erstellen, wählen Sie im Abschnitt Windows-Authentifizierung die Option AWS Managed Active Directory aus. Sie wählen auch das spezifische Verzeichnis aus, das Sie verwenden möchten. Weitere Informationen finden Sie unter [Erstellen Sie Ihr Dateisystem](#).

Ihre Organisation verwaltet möglicherweise Identitäten und Geräte in einer selbstverwalteten Active Directory-Domäne (lokal oder in der Cloud). Falls ja, können Sie Ihr Amazon FSx-Dateisystem direkt mit Ihrer bestehenden, selbstverwalteten Active Directory-Domain verbinden. Weitere Informationen finden Sie unter [Verwenden von Amazon FSx mit Ihrem selbstverwalteten Microsoft Active Directory](#).

Darüber hinaus können Sie Ihr System auch so einrichten, dass es von einem Modell zur Isolierung von Ressourcengesamtstrukturen profitiert. In diesem Modell isolieren Sie Ihre Ressourcen, einschließlich Ihrer Amazon FSx-Dateisysteme, in einer anderen Active Directory-Gesamtstruktur als der, in der sich Ihre Benutzer befinden.

#### Important

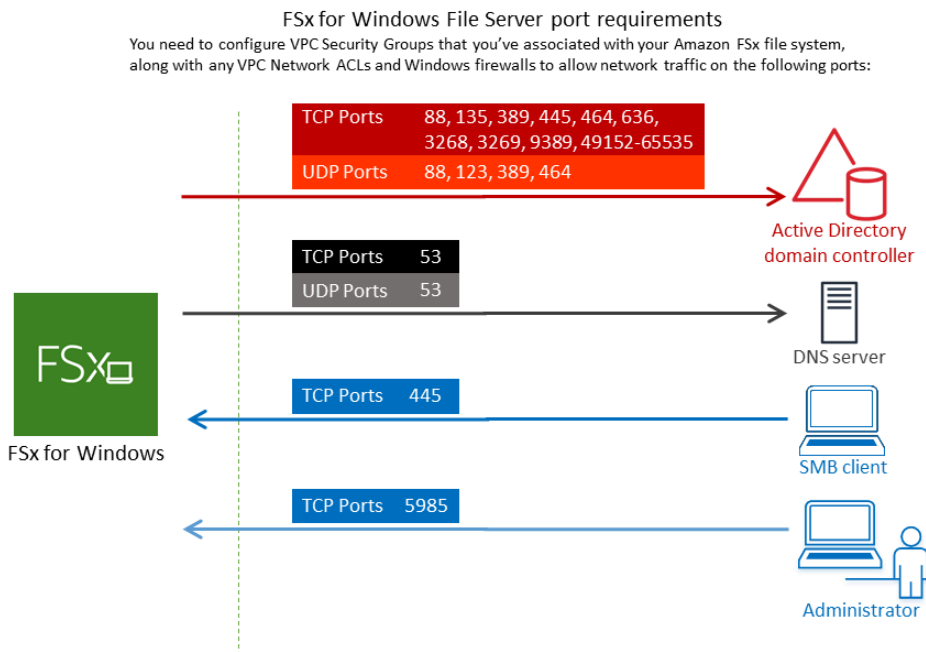
Für Single-AZ 2- und alle Multi-AZ-Dateisysteme darf der Active Directory-Domänenname 47 Zeichen nicht überschreiten.

## Voraussetzungen für das Netzwerk

Bevor Sie ein FSx for Windows File Server Server-Dateisystem erstellen, das mit Ihrer AWS Microsoft Managed Active Directory-Domäne verknüpft ist, stellen Sie sicher, dass Sie die folgenden Netzwerkkonfigurationen erstellt und eingerichtet haben:

- Für VPC-Sicherheitsgruppen ist die Standardsicherheitsgruppe für Ihre standardmäßige Amazon-VPC bereits zu Ihrem Dateisystem in der Konsole hinzugefügt. Bitte stellen Sie sicher, dass die Sicherheitsgruppe und die VPC-Netzwerk-ACLs für die Subnetze, in denen Sie Ihr FSx-

Dateisystem erstellen, Datenverkehr auf den Ports und in den in der folgenden Abbildung gezeigten Anweisungen zulassen.



In der folgenden Tabelle ist die Rolle der einzelnen Ports aufgeführt.

Protokoll	Ports	Rolle
TCP/UDP	53	Doma Name System (DNS)
TCP/UDP	88	Kerbe Auth izierun
TCP/UDP	464	Passw änder fe stlege

Protokoll	Ports	Rolle
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)
UDP	123	Network Time Protocol (NTP)
TCP	135	Distributed Component Environment / End Point Mapper (DCE EPMA)
TCP	445	Direct - Service - SMB-Dateifreigabe

Protokoll	Ports	Rolle
TCP	636	Lightweight Directory Access Protocol über TLS/SSL (LDAP)
TCP	3268	Global Catalog Microsoft - Katalo
TCP	3269	Microsoft Global Catalog über SSL
TCP	5985	WinRM 2.0 (Microsoft Windows Fernverwaltung)

Protokoll	Ports	Rolle
TCP	9389	Microsoft Active Directory, Webdienste, PowerShell
TCP	49152–65535	Flüchtige Ports für RPC

#### Important

Für Single-AZ 2- und alle Multi-AZ-Dateisystembereitstellungen ist es erforderlich, ausgehenden Verkehr auf TCP-Port 9389 zuzulassen.

#### Note

Wenn Sie VPC-Netzwerk-ACLs verwenden, müssen Sie auch ausgehenden Datenverkehr auf dynamischen Ports (49152-65535) aus Ihrem FSx-Dateisystem zulassen.

- Wenn Sie Ihr Amazon FSx-Dateisystem mit einem AWS Managed Microsoft Active Directory in einer anderen VPC oder einem anderen Konto verbinden, stellen Sie die Konnektivität zwischen dieser VPC und der Amazon VPC sicher, auf der Sie das Dateisystem erstellen möchten. Weitere Informationen finden Sie unter [Amazon FSx AWS Managed Microsoft AD in einer anderen VPC oder einem anderen Konto verwenden](#).

**⚠ Important**

Während Amazon VPC-Sicherheitsgruppen verlangen, dass Ports nur in der Richtung geöffnet werden, in der der Netzwerkverkehr initiiert wird, erfordern VPC-Netzwerk-ACLs, dass Ports in beide Richtungen geöffnet sind.

Verwenden Sie das [Amazon FSx Network Validation Tool](#), um die Konnektivität zu Ihren Active Directory-Domain-Controllern zu überprüfen.

## Verwenden Sie ein Modell zur Isolierung von Ressourcengesamtstrukturen

Sie verbinden Ihr Dateisystem mit einem AWS Managed Microsoft AD Setup. Anschließend richten Sie eine unidirektionale Gesamtstruktur-Vertrauensstellung zwischen einer von Ihnen erstellten AWS Managed Microsoft AD Domäne und Ihrer vorhandenen selbstverwalteten Active Directory-Domäne ein. Für die Windows-Authentifizierung in Amazon FSx benötigen Sie nur eine unidirektionale Gesamtstrukturvertrauensstellung, bei der die AWS verwaltete Gesamtstruktur der Unternehmensdomänengesamtstruktur vertraut.

Ihre Unternehmensdomäne übernimmt die Rolle der vertrauenswürdigen Domäne, und die AWS Directory Service verwaltete Domäne übernimmt die Rolle der vertrauenswürdigen Domäne. Validierte Authentifizierungsanfragen werden zwischen den Domänen nur in eine Richtung übertragen, sodass sich Konten in Ihrer Unternehmensdomäne anhand von Ressourcen authentifizieren können, die in der verwalteten Domäne gemeinsam genutzt werden. In diesem Fall interagiert Amazon FSx nur mit der verwalteten Domain. Die verwaltete Domain leitet dann die Authentifizierungsanfragen an Ihre Unternehmensdomain weiter.

## Testen Sie Ihre Active Directory-Konfiguration

Bevor Sie Ihr Amazon FSx-Dateisystem erstellen, empfehlen wir Ihnen, die Konnektivität zu Ihren Active Directory-Domain-Controllern mit dem Amazon FSx Network Validation Tool zu überprüfen. Weitere Informationen finden Sie unter [Überprüfen der Konnektivität zu Ihren Active Directory-Domänencontrollern](#).

Die folgenden verwandten Ressourcen können Ihnen bei der Verwendung AWS Directory Service for Microsoft Active Directory von FSx for Windows File Server helfen:

- [Was ist der AWS Directory Service](#) im AWS Directory Service Administratorhandbuch



- [Erstellen Sie Ihr AWS verwaltetes Active Directory](#) im AWS Directory Service Administratorhandbuch
- [Wann sollte im AWS Directory Service Administratorhandbuch eine Vertrauensbeziehung eingerichtet werden](#)
- [Exemplarische Vorgehensweise 1: Voraussetzungen für die ersten Schritte](#)

## Amazon FSx AWS Managed Microsoft AD in einer anderen VPC oder einem anderen Konto verwenden

Sie können Ihr Dateisystem FSx for Windows File Server mit einem AWS Managed Microsoft AD Verzeichnis verbinden, das sich in einer anderen VPC innerhalb desselben Kontos befindet, indem Sie VPC-Peering verwenden. Sie können Ihr Dateisystem auch mit einem AWS Managed Microsoft AD Verzeichnis verknüpfen, das sich in einem anderen AWS Konto befindet, indem Sie die Verzeichnisfreigabe verwenden.

### Note

Sie können nur eine auswählen, die sich AWS Managed Microsoft AD innerhalb AWS-Region Ihres Dateisystems befindet. Wenn Sie ein regionsübergreifendes VPC-Peering-Setup verwenden möchten, sollten Sie ein selbstverwaltetes Microsoft Active Directory verwenden. Weitere Informationen finden Sie unter [Verwenden von Amazon FSx mit Ihrem selbstverwaltetem Microsoft Active Directory](#).

Der Workflow für das Verbinden Ihres Dateisystems mit einem Dateisystem AWS Managed Microsoft AD , das sich in einer anderen VPC befindet, umfasst die folgenden Schritte:

1. Richten Sie Ihre Netzwerkumgebung ein.
2. Geben Sie Ihr Verzeichnis frei.
3. Fügen Sie Ihr Dateisystem dem gemeinsamen Verzeichnis hinzu.

Weitere Informationen finden Sie im AWS Directory Service Administratorhandbuch unter [Verzeichnis teilen](#).

Um Ihre Netzwerkumgebung einzurichten, können Sie Amazon VPC verwenden AWS Transit Gateway und eine VPC-Peering-Verbindung herstellen. Stellen Sie außerdem sicher, dass Netzwerkverkehr zwischen den beiden VPCs zulässig ist.

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und On-Premises-Netzwerke miteinander verbinden können. Weitere Informationen zur Verwendung von VPC-Transit Gateways finden Sie unter [Erste Schritte mit Transit Gateways](#) im Amazon VPC-Gateways-Handbuch.

Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs. Diese Verbindung ermöglicht es Ihnen, den Verkehr zwischen ihnen mithilfe von privaten Internet Protocol Version 4 (IPv4) - oder Internet Protocol Version 6 (IPv6) -Adressen weiterzuleiten. Sie können VPC-Peering verwenden, um VPCs innerhalb derselben AWS Region oder zwischen Regionen zu verbinden. AWS Weitere Informationen zu VPC-Peering finden Sie unter [Was ist VPC-Peering?](#) im Amazon VPC Peering Guide.

Es gibt noch eine weitere Voraussetzung, wenn Sie Ihr Dateisystem mit einem AWS Managed Microsoft AD Verzeichnis verknüpfen, das sich in einem anderen Konto als dem Ihres Dateisystems befindet. Sie müssen auch Ihr Microsoft Active Directory mit dem anderen Konto teilen. Zu diesem Zweck können Sie die Verzeichnisfreigabefunktion von AWS Managed Microsoft Active Directory verwenden. Weitere Informationen finden Sie im AWS Directory Service Administratorhandbuch unter [Verzeichnis teilen](#).

## Überprüfen der Konnektivität zu Ihren Active Directory-Domänencontrollern

Bevor Sie ein FSx for Windows File Server Server-Dateisystem erstellen, das mit Ihrem Active Directory verknüpft ist, verwenden Sie das Amazon FSx Active Directory Validation Tool, um die Konnektivität zu Ihrer Active Directory-Domain zu überprüfen. Sie können diesen Test unabhängig davon verwenden, ob Sie FSx for Windows File Server mit AWS verwaltetem Microsoft Active Directory oder mit einer selbstverwalteten Active Directory-Konfiguration verwenden. Der Netzwerkverbindungstest für den Domänencontroller (Test-FsxADControllerConnection) führt nicht die gesamte Suite von Netzwerkkonnektivitätsprüfungen für jeden Domänencontroller in der Domäne durch. Verwenden Sie diesen Test stattdessen, um die Netzwerkkonnektivität anhand einer bestimmten Gruppe von Domänencontrollern zu überprüfen.

Um die Konnektivität zu Ihren Active Directory-Domänencontrollern zu überprüfen

1. Starten Sie eine Amazon EC2 Windows-Instance im selben Subnetz und mit denselben Amazon VPC-Sicherheitsgruppen, die Sie für Ihr FSx for Windows File Server Server-Dateisystem

verwendet werden. Verwenden Sie für Multi-AZ-Bereitstellungstypen das Subnetz für den bevorzugten aktiven Dateiserver.

2. Verbinden Sie Ihre EC2-Windows-Instance mit Ihrem Active Directory. Weitere Informationen finden Sie unter [Manuelles Beitreten zu einer Windows-Instance](#) im AWS Directory Service Administratorhandbuch.
3. Stellen Sie eine Verbindung zu Ihrer EC2- Instance her. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
4. Öffnen Sie ein PowerShell Windows-Fenster (mit „Als Administrator ausführen“) auf der EC2-Instance.

Verwenden Sie den folgenden Testbefehl, um zu testen, ob das erforderliche Active Directory-Modul für Windows installiert PowerShell ist.

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

Wenn oben ein Fehler zurückgegeben wird, installieren Sie es mit dem folgenden Befehl.

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

5. Laden Sie das Netzwerkvalidierungstool mit dem folgenden Befehl herunter.

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

6. Erweitern Sie die ZIP-Datei mit dem folgenden Befehl.

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

7. Fügen Sie das AmazonFSxADValidation-Modul zur aktuellen Sitzung hinzu.

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

8. Legen Sie den Wert für die IP-Adresse des Active Directory-Domänencontrollers fest und führen Sie den Konnektivitätstest mit den folgenden Befehlen aus:

```
$ADControllerIp = '10.0.75.243'
```

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

9. Das folgende Beispiel zeigt das Abrufen der Testausgabe mit den Ergebnissen eines erfolgreichen Konnektivitätstests.

```
PS C:\AmazonFSxADValidation> $Result
```

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

Das folgende Beispiel zeigt, wie der Test ausgeführt wird und ein fehlgeschlagenes Ergebnis angezeigt wird.

```
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>

## Verwenden von Amazon FSx mit Ihrem selbstverwalteten Microsoft Active Directory

Wenn Ihre Organisation Identitäten und Geräte in einem selbstverwalteten Active Directory vor Ort oder in der Cloud verwaltet, können Sie Ihr Amazon FSx-Dateisystem direkt mit Ihrer bestehenden selbstverwalteten Active Directory-Domain verbinden. Um Amazon FSx mit zu verwenden AWS Managed Microsoft AD, können Sie die Amazon FSx-Konsole verwenden. Wenn Sie in der Konsole ein neues Dateisystem FSx for Windows File Server erstellen, wählen Sie unter Windows-Authentifizierung die Option Selbstveraltetes Microsoft Active Directory aus. Geben Sie die folgenden Details für Ihr selbstveraltetes Active Directory an:

- Ein vollqualifizierter Domänenname für Ihr selbstveraltetes Verzeichnis

**Note**

Der Domainname darf nicht im Format Single Label Domain (SLD) vorliegen. Amazon FSx unterstützt derzeit keine SLD-Domains.

**Note**

Bei Single-AZ 2- und Multi-AZ-Dateisystemen darf der Active Directory-Domainname 47 Zeichen nicht überschreiten.

- DNS-Server-IP-Adressen für Ihre Domain

Die IP-Adressen des DNS-Servers, die IP-Adressen der Active Directory-Domänencontroller und das Client-Netzwerk müssen die folgenden Anforderungen erfüllen:

Für Dateisysteme, die vor dem 17. Dezember 2020 erstellt wurden

IP-Adressen müssen sich in einem privaten IP-Adressbereich nach [RFC 1918](#) befinden:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Für Dateisysteme, die nach dem 17. Dezember 2020 erstellt wurden

IP-Adressen können in einem beliebigen Bereich liegen, mit Ausnahme von:

- IP-Adressen, die mit den IP-Adressen von Amazon Web Services in dieser AWS Region in Konflikt stehen. Eine Liste der AWS eigenen IP-Adressen nach Regionen finden Sie unter [AWS IP-Adressbereiche](#).
- IP-Adressen im folgenden CIDR-Blockbereich: 198.19.0.0/16

**Note**

Ihre Active Directory-Domänencontroller müssen beschreibbar sein.

- Benutzername und Passwort für ein Dienstkonto in Ihrer Active Directory-Domain, das Amazon FSx verwenden kann, um das Dateisystem mit Ihrer Active Directory-Domain zu verbinden

- (Optional) Die Organisationseinheit (OU) in Ihrer Domain, der Sie Ihr Dateisystem hinzufügen möchten
- (Optional) Die Domänengruppe, an die Sie die Befugnis zur Durchführung administrativer Aktionen in Ihrem Dateisystem delegieren möchten. Diese Domänengruppe kann beispielsweise Windows-Dateifreigaben verwalten, Zugriffssteuerungslisten (ACLs) im Stammordner des Dateisystems verwalten, den Besitz von Dateien und Ordnern übernehmen usw. Wenn Sie diese Gruppe nicht angeben, delegiert Amazon FSx diese Autorität standardmäßig an die Gruppe Domain-Admins in Ihrer Active Directory-Domain.

#### Note

Der von Ihnen angegebene Domänengruppenname muss in Ihrem Active Directory eindeutig sein. FSx for Windows File Server erstellt die Domänengruppe unter den folgenden Umständen nicht:

- Wenn bereits eine Gruppe mit dem von Ihnen angegebenen Namen existiert
- Wenn Sie keinen Namen angeben und eine Gruppe mit dem Namen „Domain-Admins“ bereits in Ihrem Active Directory existiert.

Weitere Informationen finden Sie unter [Verbinden eines Amazon-FSx-Dateisystems mit einer selbstverwalteten Microsoft-Active-Directory-Domain](#).

#### Important

Amazon FSx registriert DNS-Einträge für ein Dateisystem nur, wenn Sie Microsoft DNS als Standard-DNS-Service verwenden. Wenn Sie DNS eines Drittanbieters verwenden, müssen Sie DNS-Einträge für Ihre Amazon FSx-Dateisysteme manuell einrichten, nachdem Sie sie erstellt haben.

Wenn Sie Ihr Dateisystem direkt mit Ihrem selbstverwalteten Active Directory verbinden, befindet sich Ihr FSx for Windows File Server in derselben Active Directory-Gesamtstruktur (dem obersten logischen Container in einer Active Directory-Konfiguration, die Domänen, Benutzer und Computer enthält) und in derselben Active Directory-Domäne wie Ihre Benutzer und vorhandenen Ressourcen (einschließlich vorhandener Dateiserver).

**Note**

Sie können Ihre Ressourcen — einschließlich Ihrer Amazon FSx-Dateisysteme — in einer anderen Active Directory-Gesamtstruktur isolieren als die, in der sich Ihre Benutzer befinden. Fügen Sie dazu Ihr Dateisystem einem AWS verwalteten Active Directory hinzu und richten Sie eine unidirektionale Gesamtvertrauensstellung zwischen einem von Ihnen erstellten verwalteten Active Directory und Ihrem vorhandenen AWS selbstverwalteten Active Directory ein.

## Themen

- [Voraussetzungen für die Verwendung eines selbstverwalteten Microsoft Active Directory](#)
- [Bewährte Methoden für die Verbindung von FSx for Windows File Server-Dateisystemen mit einer selbstverwalteten Microsoft Active Directory-Domain](#)
- [Überprüfen Sie Ihre Active Directory-Konfiguration](#)
- [Verbinden eines Amazon-FSx-Dateisystems mit einer selbstverwalteten Microsoft-Active-Directory-Domain](#)
- [Abrufen der richtigen Dateisystem-IP-Adressen zur Verwendung für DNS](#)
- [Aktualisierung der selbstverwalteten Active Directory-Konfiguration](#)

## Voraussetzungen für die Verwendung eines selbstverwalteten Microsoft Active Directory

Bevor Sie ein Amazon FSx-Dateisystem erstellen, das mit Ihrer selbstverwalteten Microsoft Active Directory-Domain verknüpft ist, überprüfen Sie die folgenden Voraussetzungen.

## Themen

- [Lokale Konfigurationen](#)
- [Netzwerkkonfigurationen](#)
- [Berechtigungen für das Dienstkonto](#)



## Lokale Konfigurationen

Stellen Sie sicher, dass Sie über ein lokales oder ein anderes selbstverwaltetes Microsoft Active Directory verfügen, mit dem Sie das Amazon FSx-Dateisystem verbinden können. Ihr lokales Active Directory sollte die folgende Konfiguration haben:

- Ihr Active Directory-Domänencontroller hat eine Domänenfunktionsebene auf Windows Server 2008 R2 oder höher.
- Je nachdem, wann Ihr Dateisystem erstellt wurde, lauten die IP-Adressen des DNS-Servers und des Active Directory-Domänencontrollers wie folgt:

Für Dateisysteme, die vor dem 17. Dezember 2020 erstellt wurden

IP-Adressen müssen sich in einem privaten IP-Adressbereich nach [RFC 1918](#) befinden:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Für Dateisysteme, die nach dem 17. Dezember 2020 erstellt wurden

IP-Adressen können in einem beliebigen Bereich liegen, mit Ausnahme von:

- IP-Adressen, die mit den IP-Adressen von Amazon Web Services in dieser AWS Region in Konflikt stehen. Eine Liste der AWS eigenen IP-Adressen nach Regionen finden Sie unter [AWS IP-Adressbereiche](#).
- IP-Adressen im folgenden CIDR-Blockbereich: 198.19.0.0/16

Wenn Sie auf ein Dateisystem FSx for Windows File Server zugreifen müssen, das vor dem 17. Dezember 2020 mit einem nicht privaten IP-Adressbereich erstellt wurde, können Sie ein neues Dateisystem erstellen, indem Sie eine Sicherungskopie des Dateisystems wiederherstellen. Weitere Informationen finden Sie unter [Arbeiten mit Backups](#).

- Ein Domainname, der nicht im Single Label Domain (SLD) -Format vorliegt. Amazon FSx unterstützt keine SLD-Domains.
- Für Single-AZ 2- und alle Multi-AZ-Dateisysteme darf der Active Directory-Domänenname 47 Zeichen nicht überschreiten.
- Wenn Sie Active Directory-Standorte definiert haben, müssen die Subnetze in der VPC, die Ihrem Amazon FSx-Dateisystem zugeordnet ist, an einem Active Directory-Standort definiert werden,

und es dürfen keine Konflikte zwischen den Subnetzen in Ihrer VPC und den Subnetzen an Ihren anderen Standorten bestehen.

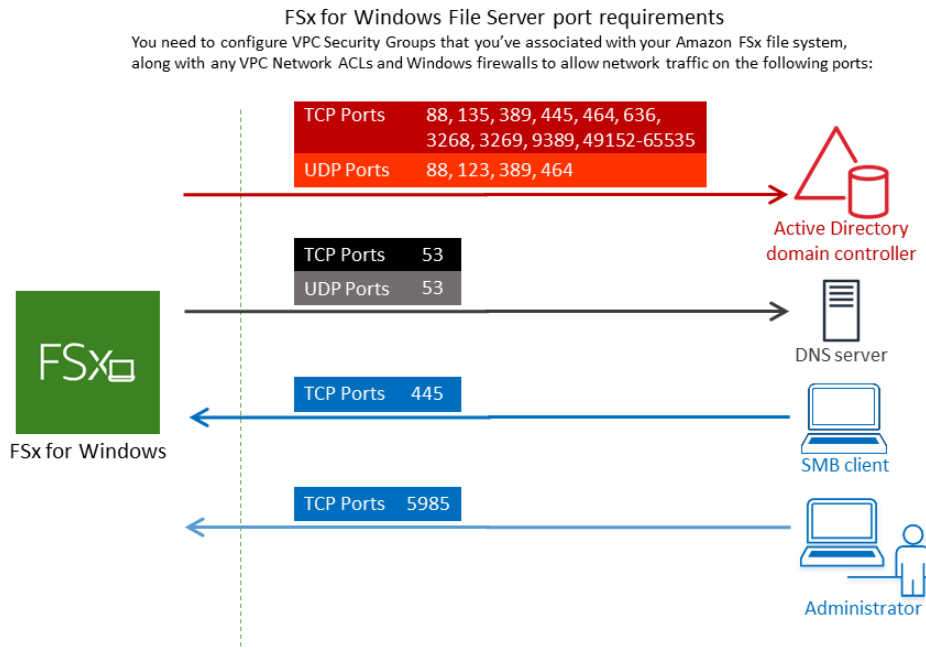
- Möglicherweise müssen Sie Ihrer Firewall Regeln hinzufügen, um ICMP-Traffic zwischen Ihren Active Directory-Domain-Controllern und Amazon FSx zuzulassen.

## Netzwerkkonfigurationen

In diesem Abschnitt werden die Netzwerkkonfigurationen beschrieben, die für den Beitritt eines Dateisystems zu Ihrem selbstverwalteten Active Directory erforderlich sind.

Wir empfehlen Ihnen, das [Amazon FSx Active Directory-Validierungstool](#) zu verwenden, um Ihre Netzwerkeinstellungen zu testen, bevor Sie versuchen, Ihr Dateisystem mit Ihrem selbstverwalteten Active Directory zu verbinden.

- Die Konnektivität zwischen der Amazon VPC, auf der Sie das Dateisystem erstellen möchten, und Ihrem selbstverwalteten Active Directory muss konfiguriert werden. Sie können diese Konnektivität mithilfe von AWS Direct Connect, [AWS Virtual Private Network](#), [VPC-Peering](#) oder [AWS Transit Gateway](#) einrichten.
- Für VPC-Sicherheitsgruppen muss die Standardsicherheitsgruppe für Ihre standardmäßige Amazon-VPC Ihrem Dateisystem in der Konsole hinzugefügt werden. Stellen Sie sicher, dass die Sicherheitsgruppe und die VPC-Netzwerk-ACLs für die Subnetze, in denen Sie Ihr FSx-Dateisystem erstellen, Datenverkehr auf den Ports und in den in der folgenden Abbildung gezeigten Anweisungen zulassen.




In der folgenden Tabelle ist die Rolle der einzelnen Ports aufgeführt.


| Protokoll | Ports | Rolle                                                  |
|-----------|-------|--------------------------------------------------------|
| TCP/UDP   | 53    | Domain Name System (DNS)                               |
| TCP/UDP   | 88    | Kerberos-Authentifizierung                             |
| TCP/UDP   | 464   | Passwort ändern/einrichten                             |
| TCP/UDP   | 389   | Lightweight Directory Access Protocol (LDAP)           |
| UDP       | 123   | Network Time Protocol (NTP)                            |
| TCP       | 135   | Verteilte Computerumgebung/Endpunktmapper (DCE/ EPMAP) |
| TCP       | 445   | Directory-Services-SMB-Dateifreigabe                   |

| Protokoll | Ports       | Rolle                                                      |
|-----------|-------------|------------------------------------------------------------|
| TCP       | 636         | Lightweight Directory Access Protocol über TLS/SSL (LDAPS) |
| TCP       | 3268        | Globaler Microsoft-Katalog                                 |
| TCP       | 3269        | Microsoft Global Catalog über SSL                          |
| TCP       | 5985        | WinRM 2.0 (Microsoft Windows-Fernverwaltung)               |
| TCP       | 9389        | Microsoft Active Directory DS-Webdienste, PowerShell       |
| TCP       | 49152–65535 | Flüchtige Ports für RPC                                    |


Stellen Sie sicher, dass diese Verkehrsregeln auch auf den Firewalls widergespiegelt werden, die für jeden der Active Directory-Domänencontroller, DNS-Server, FSx-Clients und FSx-Administratoren gelten.

 **Important**

Für Single-AZ 2- und Multi-AZ-Dateisystembereitstellungen ist es erforderlich, ausgehenden Verkehr auf TCP-Port 9389 zuzulassen.

 **Note**

Wenn Sie VPC-Netzwerk-ACLs verwenden, müssen Sie auch ausgehenden Datenverkehr auf dynamischen Ports (49152-65535) aus Ihrem FSx-Dateisystem zulassen.

 **Important**

Während Amazon VPC-Sicherheitsgruppen verlangen, dass Ports nur in der Richtung geöffnet werden, in der der Netzwerkverkehr initiiert wird, erfordern die meisten Windows-Firewalls und VPC-Netzwerk-ACLs, dass Ports in beide Richtungen geöffnet sind.

## Berechtigungen für das Dienstkonto

Stellen Sie sicher, dass Sie in Ihrem selbstverwalteten Microsoft Active Directory über ein Dienstkonto mit delegierten Berechtigungen zum Hinzufügen von Computern zur Domäne verfügen. Ein Dienstkonto ist ein Benutzerkonto in Ihrem selbstverwalteten Microsoft Active Directory, dem bestimmte Aufgaben delegiert wurden.

Dem Dienstkonto müssen mindestens die folgenden Berechtigungen in der Organisationseinheit, der Sie dem Dateisystem beitreten, delegiert werden:

- Fähigkeit, Passwörter zurückzusetzen
- Möglichkeit, Konten am Lesen und Schreiben von Daten zu hindern
- Überprüfte Fähigkeit zum Schreiben in den DNS-Hostnamen
- Überprüfte Fähigkeit zum Schreiben in den Prinzipalnamen des Service
- Fähigkeit (kann delegiert werden), Computerobjekte zu erstellen und zu löschen
- Bestätigte Fähigkeit zum Lesen und Schreiben von Kontoeinschränkungen
- Fähigkeit, Berechtigungen zu ändern


Dies sind die Mindestberechtigungen, die erforderlich sind, um Computerobjekte mit Ihrem Active Directory zu verknüpfen. Weitere Informationen finden Sie in der Microsoft Windows Server-Dokumentation zum Thema [Fehler: Zugriff wird verweigert, wenn Benutzer ohne Administratorrechte, denen die Steuerung delegiert wurde, versuchen, Computer mit einem Domänencontroller zu verbinden](#).

Weitere Informationen zum Erstellen eines Dienstkontos mit den richtigen Berechtigungen finden Sie unter [Delegieren von Berechtigungen an Ihr Amazon-FSx-Servicekonto](#)

Amazon FSx benötigt während der gesamten Lebensdauer Ihres Amazon FSx-Dateisystems ein gültiges Servicekonto. Amazon FSx muss in der Lage sein, das Dateisystem vollständig zu verwalten und Aufgaben auszuführen, die das Trennen und Wiederverbinden mit Ihrer Active Directory-Domain über das Servicekonto erfordern. Zu diesen Aufgaben gehören das Ersetzen eines ausgefallenen Dateiservers oder das Patchen der Windows Server-Software. Es ist unbedingt erforderlich, dass Sie Ihre Active Directory-Konfiguration, einschließlich der Anmeldeinformationen für das Dienstkonto, mit Amazon FSx auf dem neuesten Stand halten. Weitere Informationen finden Sie unter [Aktualisieren Ihrer Active-Directory-Konfiguration](#).

Amazon FSx erfordert Konnektivität zu allen Domain-Controllern in Ihrer Active Directory-Umgebung. Wenn Sie über mehrere Domain-Controller verfügen, stellen Sie sicher, dass alle die oben genannten Anforderungen erfüllen, und stellen Sie sicher, dass alle Änderungen an Ihrem Servicekonto auf alle Domain-Controller übertragen werden.

Mit dem [Amazon FSx Active Directory Validation Tool](#) können Sie Ihre Active Directory-Konfiguration validieren, einschließlich des Testens der Konnektivität mehrerer Domain-Controller. Um die Anzahl der Domain-Controller zu begrenzen, die Konnektivität benötigen, können Sie auch eine Vertrauensbeziehung zwischen Ihren lokalen Domain-Controllern und aufbauen. AWS Managed Microsoft AD Weitere Informationen finden Sie unter [Verwenden Sie ein Modell zur Isolierung von Ressourcengesamtstrukturen](#).

 **Important**

Verschieben Sie keine Computerobjekte, die Amazon FSx in der Organisationseinheit erstellt, nachdem Ihr Dateisystem erstellt wurde. Andernfalls wird Ihr Dateisystem falsch konfiguriert.

## Bewährte Methoden für die Verbindung von FSx for Windows File Server-Dateisystemen mit einer selbstverwalteten Microsoft Active Directory-Domain

Wir empfehlen diese bewährten Methoden, wenn Sie Amazon FSx for Windows File Server-Dateisysteme mit Ihrem selbstverwalteten Microsoft Active Directory verbinden.

### Delegieren von Berechtigungen an Ihr Amazon-FSx-Servicekonto

Stellen Sie sicher, dass Sie das Servicekonto, das Sie Amazon FSx zur Verfügung stellen, mit den erforderlichen Mindestberechtigungen konfigurieren. Trennen Sie außerdem die Organisationseinheit (OU) von anderen Domain-Controller-Belangen.

Um Amazon-FSx-Dateisysteme mit Ihrer Domain zu verbinden, stellen Sie sicher, dass das Servicekonto über delegierte Berechtigungen verfügt. Mitglieder der Domain-Admins-Gruppe verfügen über ausreichende Berechtigungen, um diese Aufgabe auszuführen. Verwenden Sie jedoch als bewährte Methode ein Servicekonto, das nur über die erforderlichen Mindestberechtigungen verfügt. Die folgenden Verfahren zeigen, wie Sie nur die Berechtigungen delegieren, die zum Verbinden von Amazon-FSx-Dateisystemen mit Ihrer Domain erforderlich sind.

Sie verwenden entweder Delegierte Kontrolle oder Erweiterte Funktionen im MMC-Snap-In für Active Directory-Benutzer und Computer, um diese Berechtigungen zuzuweisen.

Führen Sie eines dieser Verfahren auf einem Computer durch, der mit Ihrem aktiven Verzeichnis verbunden ist und auf dem das Active Directory User and Computers MMC Snap-In installiert ist.

So weisen Sie einem Servicekonto oder einer Gruppe mithilfe von Delegierungskontrolle Berechtigungen zu

1. Melden Sie sich bei Ihrem System als Domänenadministrator für Ihre Active-Directory-Domäne an.
2. Öffnen Sie das MMC-Snap-in Active Directory User und Computer.
3. Erweitern Sie im Aufgabenbereich den Domänenknoten.
4. Suchen und öffnen Sie das Kontextmenü (rechte Maustaste) für die Organisationseinheit, die Sie ändern möchten, und wählen Sie dann Kontrolle delegieren aus.
5. Wählen Sie auf der Seite Assistent für die Delegation der Kontrolle die Option Weiter aus.
6. Wählen Sie Hinzufügen, um den Namen Ihres Amazon-FSx-Servicekontos oder Ihrer Amazon-FSx-Servicegruppe hinzuzufügen, und wählen Sie dann Weiter aus.
7. Wählen Sie auf der Seite Zu delegierende Aufgabe die Option Eine zu delegierende benutzerdefinierte Aufgabe erstellen aus und klicken Sie auf Weiter.
8. Wählen Sie im Ordner Nur die folgenden Objekte und dann Computerobjekte aus.
9. Wählen Sie Ausgewählte Objekte in diesem Ordner erstellen und Ausgewählte Objekte in diesem Ordner löschen aus. Wählen Sie anschließend Weiter.
10. Wählen Sie für Berechtigungen Folgendes aus:
  - Passwort zurücksetzen
  - Kontobeschränkungen lesen und schreiben
  - Validiertes Schreiben in den DNS-Hostnamen
  - Überprüfter Schreibvorgang in den Service-Prinzipalnamen
11. Wählen Sie Next (Weiter) und danach Finish (Beenden).
12. Schließen Sie das MMC-Snap-In Active Directory User und Computer.

## So weisen Sie Berechtigungen mit erweiterten Funktionen zu

1. Melden Sie sich bei Ihrem System als Domänenadministrator für Ihre Active-Directory-Domäne an.
2. Öffnen Sie das MMC-Snap-in Active Directory User und Computer.
3. Wählen Sie in der Menüleiste Ansicht aus und stellen Sie sicher, dass erweiterte Funktionen aktiviert sind (daneben wird ein Häkchen angezeigt, wenn die Funktion aktiviert ist).
4. Erweitern Sie im Aufgabenbereich den Domänenknoten.
5. Suchen und öffnen Sie das Kontextmenü für die OU, die Sie ändern möchten, und wählen Sie dann Eigenschaften aus (rechte Maustaste).
6. Wählen Sie im Bereich OU Properties die Registerkarte Security aus.
7. Wählen Sie auf der Registerkarte Sicherheit die Option Erweitert aus. Wählen Sie dann Hinzufügen aus.
8. Wählen Sie auf der Seite Berechtigungseintrag die Option Prinzipal auswählen aus und geben Sie den Namen Ihres Amazon-FSx-Servicekontos oder Ihrer Gruppe ein. Wählen Sie für Gilt für: die Option Objekte des untergeordneten Computers aus. Stellen Sie sicher, dass Folgendes ausgewählt ist:
  - Ändern von Berechtigungen
  - Computerobjekte erstellen
  - Löschen von Computerobjekten
9. Wählen Sie Anwenden und dann OK aus.
10. Schließen Sie das MMC-Snap-In für Active-Directory-Benutzer und Computer.

### Important

Verschieben Sie keine Computerobjekte, die Amazon FSx in der OU erstellt, nachdem Ihr Dateisystem erstellt wurde. Dadurch wird Ihr Dateisystem falsch konfiguriert. Wenn Sie Ihr Dateisystem mit einem neuen Servicekonto aktualisieren, stellen Sie sicher, dass das neue Servicekonto über Vollzugriffsberechtigungen für die vorhandenen Computerobjekte verfügt, die dem Dateisystem zugeordnet sind.



## Aktualisieren Ihrer Active-Directory-Konfiguration

Um eine kontinuierliche, unterbrechungsfreie Verfügbarkeit Ihres Amazon-FSx-Dateisystems sicherzustellen, müssen Sie die Active-Directory-Konfiguration des Dateisystems jedes Mal aktualisieren, wenn Sie Änderungen an Ihrer selbstverwalteten Active-Directory-Einrichtung vornehmen.

Wenn Ihr Active Directory beispielsweise eine zeitbasierte Richtlinie zum Zurücksetzen des Passworts verwendet, sobald das Passwort zurückgesetzt wurde, stellen Sie sicher, dass Sie das Servicekonto-Passwort mit Amazon FSx aktualisieren. Wenn sich die IP-Adressen des DNS-Servers für Ihre Active-Directory-Domain ändern, aktualisieren Sie die IP-Adressen des DNS-Servers mit Amazon FSx. Weitere Informationen finden Sie unter [Aktualisierung der selbstverwalteten Active Directory-Konfiguration](#).

Wenn Sie die selbstverwaltete Active-Directory-Konfiguration für Ihr Amazon-FSx-Dateisystem aktualisieren, wechselt der Status Ihres Dateisystems von Verfügbar auf Aktualisieren, während das Update angewendet wird. Stellen Sie sicher, dass der Status nach dem Anwenden des Updates wieder auf Verfügbar wechselt. Beachten Sie, dass das Update einige Minuten dauern kann. Weitere Informationen finden Sie unter [Überwachung von selbstverwalteten Active Directory-Updates](#).

Wenn es ein Problem mit der aktualisierten selbstverwalteten Active-Directory-Konfiguration gibt, wechselt der Dateisystemstatus zu Fehlkonfiguriert. Dieser Status zeigt eine Fehlermeldung und empfohlene Korrekturmaßnahmen neben der Dateisystembeschreibung in der Konsole, API und CLI an. Nachdem Sie die empfohlenen Korrekturmaßnahmen ergriffen haben, überprüfen Sie, ob sich der Status Ihres Dateisystems schließlich in Verfügbar ändert.

Weitere Informationen zur Behebung möglicher selbstverwalteter Active-Directory-Fehlkonfigurationen finden Sie unter [Das Dateisystem befindet sich in einem falsch konfigurierten Zustand](#).

## Verwenden von Sicherheitsgruppen zur Begrenzung des Datenverkehrs innerhalb Ihrer VPC

Um den Netzwerkverkehr in Ihrer Virtual Private Cloud (VPC) einzuschränken, können Sie das Prinzip der geringsten Berechtigung in Ihrer VPC implementieren. Mit anderen Worten, Sie können Berechtigungen auf die mindestens erforderlichen beschränken. Verwenden Sie dazu Sicherheitsgruppenregeln. Weitere Informationen hierzu finden Sie unter [Amazon VPC-Sicherheitsgruppen](#).

## Erstellen ausgehender Sicherheitsgruppenregeln für die Netzwerkschnittstelle Ihres Dateisystems

Für mehr Sicherheit sollten Sie eine Sicherheitsgruppe mit Regeln für ausgehenden Datenverkehr konfigurieren. Diese Regeln sollten ausgehenden Datenverkehr nur zu Ihren selbstverwalteten Microsoft Active Directory-Domain-Controllern oder innerhalb des Subnetzes oder der Sicherheitsgruppe zulassen. Wenden Sie diese Sicherheitsgruppe auf die VPC an, die der Elastic Network-Schnittstelle Ihres Amazon FSx-Dateisystems zugeordnet ist. Weitere Informationen hierzu finden Sie unter [Dateisystem-Zugriffskontrolle mit Amazon VPC](#).

## Überprüfen Sie Ihre Active Directory-Konfiguration

Bevor Sie ein FSx for Windows File Server Server-Dateisystem erstellen, das mit Ihrem Active Directory verknüpft ist, empfehlen wir Ihnen, Ihre Active Directory-Konfiguration mit dem Amazon FSx Active Directory Validation Tool zu überprüfen. Beachten Sie, dass eine ausgehende Internetverbindung erforderlich ist, um die Active Directory-Konfiguration erfolgreich zu validieren.

Um Ihre Active Directory-Konfiguration zu überprüfen

1. Starten Sie eine Amazon EC2 Windows-Instance im selben Subnetz und mit denselben Amazon VPC-Sicherheitsgruppen, die Sie für Ihr FSx for Windows File Server Server-Dateisystem verwenden. Stellen Sie sicher, dass Ihre EC2-Instance über die erforderlichen IAM-Berechtigungen verfügt. AmazonEC2ReadOnlyAccess Sie können die Rollenberechtigungen für EC2-Instances mithilfe des IAM-Richtliniensimulators überprüfen. Weitere Informationen finden Sie unter [Testen von IAM-Richtlinien mit dem IAM-Richtliniensimulator](#) im IAM-Benutzerhandbuch.
2. Verbinden Sie Ihre EC2-Windows-Instance mit Ihrem Active Directory. Weitere Informationen finden Sie unter [Manuelles Beitreten zu einer Windows-Instance](#) im AWS Directory Service Administratorhandbuch.
3. Stellen Sie eine Verbindung zu Ihrer EC2-Instance her. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
4. Öffnen Sie ein PowerShell Windows-Fenster (mit „Als Administrator ausführen“) auf der EC2-Instance.

Verwenden Sie den folgenden Testbefehl, um zu testen, ob das erforderliche Active Directory-Modul für Windows installiert PowerShell ist.

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

Wenn oben ein Fehler zurückgegeben wird, installieren Sie es mit dem folgenden Befehl.

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

5. Laden Sie das Netzwerkvalidierungstool mit dem folgenden Befehl herunter.

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

6. Erweitern Sie die ZIP-Datei mit dem folgenden Befehl.

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

7. Fügen Sie das AmazonFSxADValidation Modul zur aktuellen Sitzung hinzu.

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

8. Stellen Sie die erforderlichen Parameter ein, indem Sie den folgenden Befehl durch Ihr ersetzen:

- *Active Directory-Domänenname (DOMAINNAME.COM)*
- Bereiten Sie das `$Credential` Objekt mit einer der folgenden Optionen für das Dienstkontokennwort vor.
  - Verwenden Sie den folgenden Befehl, um das Anmeldeinformationsobjekt interaktiv zu generieren.

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

- Verwenden Sie den folgenden Befehl, um das Anmeldeinformationsobjekt mithilfe einer AWS Secrets Manager Ressource zu generieren.

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

- *IP-Adressen des DNS-Servers (IP\_ADDRESS\_1, IP\_ADDRESS\_2)*
- Subnetz-ID (s) für Subnetze, in denen Sie Ihr Amazon FSx-Dateisystem erstellen möchten (z. B. *SUBNET\_1, 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. (Optional) Legen Sie die Organisationseinheit und die Gruppe der delegierten Administratoren fest und aktivieren Sie die Überprüfung der Dienstkontoberechtigungen DomainControllersMaxCount, indem Sie die Anweisungen in der mitgelieferten Datei befolgen, bevor Sie das Validierungstool ausführen. README.md

#### Note

Die Domain Admins Gruppe hat einen anderen Namen, wenn das Betriebssystem nicht auf Englisch ist. Die Gruppe ist beispielsweise Administrateurs du domaine in der französischen Betriebssystemversion benannt. Wenn Sie keinen Wert angeben, wird der Domain Admins Standardgruppenname verwendet und die Erstellung des Dateisystems schlägt fehl.

10. Führen Sie das Überprüfungstool mit diesem Befehl aus.

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

11. Im Folgenden finden Sie ein Beispiel für ein erfolgreiches Testergebnis.

```
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

```

Das Folgende ist ein Beispiel für ein Testergebnis mit Fehlern.

```

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

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

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

```

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

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

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

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

Wenn Sie beim Ausführen des Validierungstools Warnungen oder Fehler erhalten, finden Sie weitere Informationen in der Anleitung zur Fehlerbehebung, die im Validierungstoolpaket enthalten ist (TROUBLESHOOTING.md) und [Problemebehebung bei Amazon FSx](#).

## Verbinden eines Amazon-FSx-Dateisystems mit einer selbstverwalteten Microsoft-Active-Directory-Domain

Wenn Sie ein neues FSx for Windows File Server-Dateisystem erstellen, können Sie die Microsoft Active Directory-Integration so konfigurieren, dass sie mit Ihrer selbstverwalteten Microsoft Active Directory-Domain verbunden wird. Geben Sie dazu die folgenden Informationen für Ihr Microsoft Active Directory an:

- Der vollqualifizierte Domänenname Ihres lokalen Microsoft Active Directory-Verzeichnisses.

### Note

Amazon FSx unterstützt derzeit keine Single Label Domain (SLD)-Domains.

- Die IP-Adressen der DNS-Server für Ihre Domain.

- Anmeldeinformationen für ein Servicekonto in Ihrer lokalen Microsoft Active Directory-Domain. Amazon FSx verwendet diese Anmeldeinformationen, um sich mit Ihrem selbstverwalteten Active Directory zu verbinden.

Optional können Sie auch Folgendes spezifizieren:

- Eine bestimmte Organisationseinheit (OU) innerhalb der Domain, der Ihr Amazon-FSx-Dateisystem beitreten soll.
- Der Name der Domänengruppe, deren Mitgliedern Administratorrechte für das Amazon-FSx-Dateisystem gewährt werden.

#### Note

Der von Ihnen angegebene Domänengruppenname muss in Ihrem Active Directory eindeutig sein. FSx for Windows File Server erstellt die Domänengruppe unter den folgenden Umständen nicht:

- Wenn bereits eine Gruppe mit dem von Ihnen angegebenen Namen vorhanden ist
- Wenn Sie keinen Namen angeben und bereits eine Gruppe mit dem Namen „Domain Admins“ in Ihrem Active Directory vorhanden ist.

Nachdem Sie diese Informationen angegeben haben, verbindet Amazon FSx Ihr neues Dateisystem mit Ihrer selbstverwalteten Active-Directory-Domain mithilfe des von Ihnen angegebenen Servicekontos.

#### Important

Amazon FSx registriert DNS-Datensätze für ein Dateisystem nur, wenn die Active-Directory-Domain, der Sie beitreten, Microsoft DNS als Standard-DNS verwendet. Wenn Sie ein DNS eines Drittanbieters verwenden, müssen Sie DNS-Einträge für Ihre Amazon-FSx-Dateisysteme manuell einrichten, nachdem Sie Ihr Dateisystem erstellt haben. Weitere Informationen zur Auswahl der richtigen IP-Adressen für das Dateisystem finden Sie unter [Abrufen der richtigen Dateisystem-IP-Adressen zur Verwendung für DNS](#).

## Bevor Sie beginnen

Stellen Sie sicher, dass Sie die [Voraussetzungen für die Verwendung eines selbstverwalteten Microsoft Active Directory](#) unter beschriebenen Schritte abgeschlossen haben [Verwenden von Amazon FSx mit Ihrem selbstverwalteten Microsoft Active Directory](#).

So erstellen Sie ein FSx for Windows File Server-Dateisystem, das mit einem selbstverwalteten Active Directory (Konsole) verbunden ist

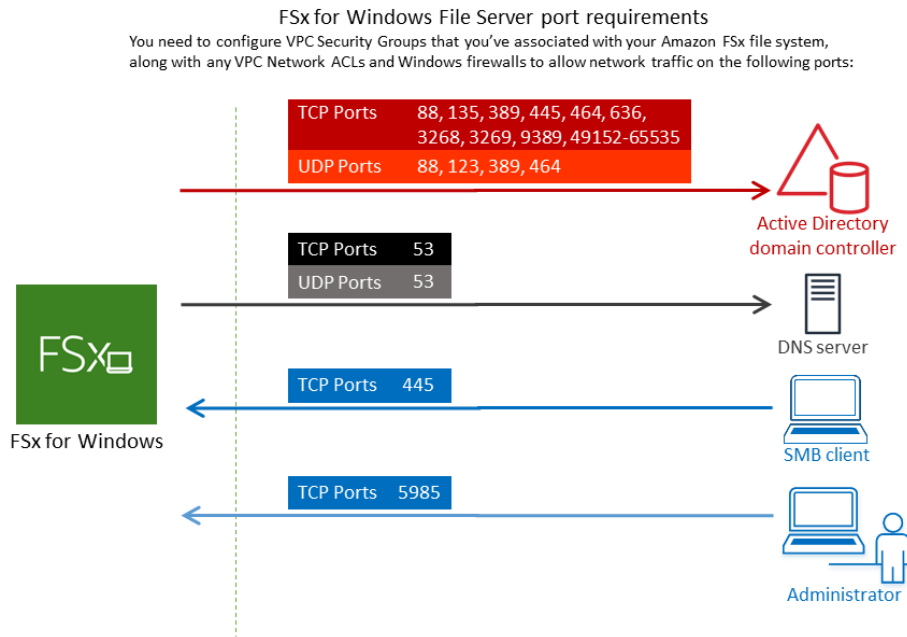
1. Öffnen Sie die Amazon-FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Klicken Sie auf dem Dashboard auf Create file system (Dateisystem erstellen), um den Erstellungsassistenten für Dateisysteme zu starten.
3. Wählen Sie FSx für Windows File Server und dann Weiter aus. Die Seite Create file system (Dateisystem erstellen) wird angezeigt.
4. Geben Sie einen Namen für Ihr Dateisystem an. Sie können maximal 256 Unicode-Buchstaben, Leerzeichen und Zahlen sowie die Sonderzeichen + - = . \_ : / verwenden.
5. Geben Sie für Speicherkapazität die Speicherkapazität Ihres Dateisystems in GiB ein. Wenn Sie SSD-Speicher verwenden, geben Sie eine ganze Zahl im Bereich von 32 bis 65 536 ein. Wenn Sie HDD-Speicher verwenden, geben Sie eine beliebige Ganzzahl im Bereich von 2.000 bis 65.536 ein. Sie können die Speicherkapazität jederzeit nach Bedarf erhöhen, nachdem Sie das Dateisystem erstellt haben. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#).
6. Behalten Sie die Durchsatzkapazität auf ihrer Standardeinstellung. Die Durchsatzkapazität ist die anhaltende Geschwindigkeit, mit der der Dateiserver, der Ihr Dateisystem hostet, Daten bereitstellen kann. Die Einstellung Empfohlene Durchsatzkapazität basiert auf der von Ihnen gewählten Speicherkapazität. Wenn Sie mehr als die empfohlene Durchsatzkapazität benötigen, wählen Sie Durchsatzkapazität angeben und wählen Sie dann einen Wert aus. Weitere Informationen finden Sie unter [Leistung von FSx for Windows File Server](#).

Sie können die Durchsatzkapazität jederzeit nach Bedarf ändern, nachdem Sie das Dateisystem erstellt haben. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

7. Wählen Sie die VPC aus, die Sie Ihrem Dateisystem zuordnen möchten. Wählen Sie für die Zwecke dieser Übung „Erste Schritte“ dieselbe VPC wie für Ihr AWS Directory Service Verzeichnis und Ihre Amazon EC2 aus.
8. Wählen Sie einen beliebigen Wert für Availability Zones und Subnetz aus.



- Für VPC-Sicherheitsgruppen ist die Standardsicherheitsgruppe für Ihre standardmäßige Amazon VPC bereits in der Konsole zu Ihrem Dateisystem hinzugefügt. Bitte stellen Sie sicher, dass die Sicherheitsgruppe und die VPC-Netzwerk-ACLs für das/die Subnetz(e), in dem/denen Sie Ihr FSx-Dateisystem erstellen, Datenverkehr an den Ports und in den im folgenden Diagramm gezeigten Richtungen zulassen.




In der folgenden Tabelle ist die Rolle der einzelnen Ports aufgeführt.

| Protokoll | Ports | Rolle                           |
|-----------|-------|---------------------------------|
| TCP/UDP   | 53    | Doma<br>Name<br>System<br>(DNS) |
| TCP/UDP   | 88    | Kerbe<br>Auth<br>izieru         |


| Protokoll | Ports | Rolle                                                          |
|-----------|-------|----------------------------------------------------------------|
| TCP/UDP   | 464   | Passwörter ändern, Benutzerprofile erstellen                   |
| TCP/UDP   | 389   | Lightweight Directory Access Protocol (LDAP)                   |
| UDP       | 123   | Network Time Protocol (NTP)                                    |
| TCP       | 135   | Distributed Component Environment / Endpoint Mapper (DCE/EPMA) |
| TCP       | 445   | Direct - Service - SMB - Dateifreigabe                         |

| Protokoll | Ports | Rolle                                                     |
|-----------|-------|-----------------------------------------------------------|
| TCP       | 636   | Lightweight Directory Access Protocol über TLS/SSL (LDAP) |
| TCP       | 3268  | Global Catalog - Katalo                                   |
| TCP       | 3269  | Microsoft Global Catalog über SSL                         |
| TCP       | 5985  | WinRM 2.0 (Microsoft Windows Remote Management)           |

| Protokoll | Ports       | Rolle                                                           |
|-----------|-------------|-----------------------------------------------------------------|
| TCP       | 9389        | Micros<br>Active<br>Direct<br>DS<br>Web<br>Servic<br>Power<br>I |
| TCP       | 49152–65535 | Flücht<br>Ports<br>für<br>RPC                                   |

 **Important**

Für Single-AZ 2 und alle Multi-AZ-Dateisystembereitstellungen ist das Zulassen von ausgehendem Datenverkehr auf TCP-Port 9389 erforderlich.


 **Note**

Wenn Sie VPC-Netzwerk-ACLs verwenden, müssen Sie auch ausgehenden Datenverkehr auf dynamischen Ports (49152-65535) von Ihrem FSx-Dateisystem zulassen.

- Ausgehende Regeln, um den gesamten Datenverkehr zu den IP-Adressen zuzulassen, die den DNS-Servern und Domain-Controllern für Ihre selbstverwaltete Microsoft Active Directory-Domain zugeordnet sind. Weitere Informationen finden Sie [in der Microsoft-Dokumentation zur Konfiguration Ihrer Firewall für die Active-Directory-Kommunikation](#).
- Stellen Sie sicher, dass diese Datenverkehrsregeln auch in den Firewalls gespiegelt werden, die für jeden der Active-Directory-Domain-Controller, DNS-Server, FSx-Clients und FSx-Administratoren gelten.


 Note

Wenn Sie Active-Directory-Standorte definiert haben, müssen Sie sicherstellen, dass das/die Subnetz(e) in der VPC, die Ihrem Amazon-FSx-Dateisystem zugeordnet sind, an einem Active-Directory-Standort definiert sind und dass keine Konflikte zwischen dem/den Subnetz(en) in Ihrer VPC und den Subnetzen an Ihren anderen Standorten bestehen. Sie können diese Einstellungen mithilfe des MMC-Snap-Ins für Active Directory-Standorte und -Services anzeigen und ändern.

 Important

Während Amazon-VPC-Sicherheitsgruppen verlangen, dass Ports nur in der Richtung geöffnet werden, in der der Netzwerkverkehr initiiert wird, erfordern die meisten Windows-Firewalls und VPC-Netzwerk-ACLs, dass Ports in beide Richtungen geöffnet sind.

10. Wählen Sie für Windows-Authentifizierung die Option Selbstverwaltetes Microsoft Active Directory aus.
11. Geben Sie einen Wert für Vollständig qualifizierter Domänenname für das selbstverwaltete Microsoft Active Directory-Verzeichnis ein.

 Note

Der Domänenname darf nicht im SLD-Format (Single Label Domain) vorliegen. Amazon FSx unterstützt derzeit keine SLD-Domänen.

 Important

Für Single-AZ 2 und alle Multi-AZ-Dateisysteme darf der Active-Directory-Domainname 47 Zeichen nicht überschreiten.

12. Geben Sie einen Wert für Organisationseinheit für das selbstverwaltete Microsoft Active Directory-Verzeichnis ein.

 Note


Stellen Sie sicher, dass das von Ihnen angegebene Servicekonto über Berechtigungen verfügt, die an die OU delegiert sind, die Sie hier angeben, oder an die Standard-OU, wenn Sie keine angeben.

13. Geben Sie mindestens einen und nicht mehr als zwei Werte für DNS-Server-IP-Adressen für das selbstverwaltete Microsoft Active Directory-Verzeichnis ein.
14. Geben Sie einen Zeichenfolgenwert für den Benutzernamen des Servicekontos für das Konto in Ihrer selbstverwalteten Active-Directory-Domain ein, z. B. `ServiceAcct`. Amazon FSx verwendet diesen Benutzernamen, um Ihrer Microsoft Active Directory-Domain beizutreten.

 Important

Geben Sie bei der Eingabe des Benutzernamens des Servicekontos kein Domänenpräfix (`corp.com\ServiceAcct`) oder Domänensuffix (`ServiceAcct@corp.com`) an. Verwenden Sie NICHT den Distinguished Name (DN), wenn Sie den Benutzernamen des Servicekontos () eingeben `CN=ServiceAcct,OU=example,DC=corp,DC=com`.

15. Geben Sie einen Wert für das Servicekontopasswort für das Konto in Ihrer selbstverwalteten Active-Directory-Domain ein. Amazon FSx verwendet dieses Passwort, um Ihrer Microsoft Active Directory-Domain beizutreten.
16. Geben Sie das Passwort erneut ein, um es unter Passwort bestätigen zu bestätigen.
17. Geben Sie für Delegierte Dateisystemadministratorengruppe die `Domain Admins` Gruppe oder eine benutzerdefinierte delegierte Dateisystemadministratorengruppe an (falls Sie eine erstellt haben). Die von Ihnen angegebene Gruppe sollte über die delegierte Autorität verfügen, administrative Aufgaben in Ihrem Dateisystem auszuführen. Wenn Sie keinen Wert angeben, verwendet Amazon FSx die integrierte `Domain Admins` Gruppe. Beachten Sie, dass Amazon FSx keine unterstützt, wenn sich ein `Delegated file system administrators group` (entweder die von Ihnen angegebene `Domain Admins` Gruppe oder eine benutzerdefinierte Gruppe) im integrierten Container befindet.

 Important

Wenn Sie keine delegierte Dateisystemadministratorengruppe angeben, versucht Amazon FSx standardmäßig, die integrierte `Domain Admins` Gruppe in Ihrer Active-

Directory-Domain zu verwenden. Wenn der Name dieser integrierten Gruppe geändert wurde oder Sie eine andere Gruppe für die Domänenverwaltung verwenden, müssen Sie diesen Namen für die Gruppe hier angeben.

**⚠ Important**

Fügen Sie beim Angeben des Gruppennamensparameters NICHT ein Domänenpräfix (corp.com\F SxAdmins) oder ein Domänensuffix (F SxAdmins@corp.com) ein. Verwenden Sie NICHT den Distinguished Name (DN) für die Gruppe. Ein Beispiel für einen definierten Namen ist CN=FSxAdmins, OU=example,DC=corp,DC=com.

So erstellen Sie ein FSx for Windows File Server-Dateisystem, das mit einem selbstverwalteten Active Directory (AWS CLI) verbunden ist

Im folgenden Beispiel wird ein FSx for Windows File Server-Dateisystem mit einem SelfManagedActiveDirectoryConfiguration in der us-east-2 Availability Zone erstellt.

```
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**

Verschieben Sie keine Computerobjekte, die Amazon FSx nach der Erstellung Ihres Dateisystems in der OU erstellt. Dies führt dazu, dass Ihr Dateisystem falsch konfiguriert wird.

## Abrufen der richtigen Dateisystem-IP-Adressen zur Verwendung für DNS

Amazon FSx registriert DNS-Einträge für ein Dateisystem nur, wenn Sie Microsoft DNS als Standard-DNS-Service verwenden. Wenn Sie DNS eines Drittanbieters verwenden, müssen Sie DNS-Einträge für Ihre Amazon FSx-Dateisysteme manuell einrichten. In diesem Abschnitt wird beschrieben, wie Sie die richtigen Dateisystem-IP-Adressen erhalten, die Sie verwenden können, wenn Sie das Dateisystem manuell zu Ihrem DNS hinzufügen müssen. Beachten Sie, dass sich die IP-Adressen eines einmal erstellten Dateisystems erst ändern, wenn das Dateisystem gelöscht wird.

Wie erhält man Dateisystem-IP-Adressen, die für DNS-A-Einträge verwendet werden können

1. Wählen Sie [unter `https://console.aws.amazon.com/fsx/`](https://console.aws.amazon.com/fsx/) das Dateisystem aus, dessen IP-Adresse Sie abrufen möchten, um die Seite mit den Dateisystemdetails anzuzeigen.
2. Führen Sie auf der Registerkarte Netzwerk und Sicherheit einen der folgenden Schritte aus:
  - Für Single-AZ 1-Dateisysteme:
    - Wählen Sie im Bereich Subnet die elastic network interface aus, die unter Netzwerkschnittstelle angezeigt wird, um die Seite Netzwerkschnittstellen in der Amazon EC2 EC2-Konsole zu öffnen.
    - Die IP-Adresse für das zu verwendende Single-AZ 1-Dateisystem wird in der Spalte Primäre private IPv4-IP angezeigt.
  - Für Single-AZ 2- oder Multi-AZ-Dateisysteme:
    - Wählen Sie im Bereich Bevorzugtes Subnetz die elastic network interface aus, die unter Netzwerkschnittstelle angezeigt wird, um die Seite Netzwerkschnittstellen in der Amazon EC2 EC2-Konsole zu öffnen.
    - Die IP-Adresse für das bevorzugte zu verwendende Subnetz wird in der Spalte Sekundäre private IPv4-IP angezeigt.
    - Wählen Sie im Amazon FSx Standby-Subnetz-Panel die Elastic Network-Schnittstelle aus, die unter Netzwerkschnittstelle angezeigt wird, um die Seite Netzwerkschnittstellen in der Amazon EC2 EC2-Konsole zu öffnen.
    - Die IP-Adresse für das zu verwendende Standby-Subnetz wird in der Spalte Sekundäre private IPv4-IP angezeigt.



**Note**

Wenn Sie DNS-Einträge für Ihren Windows Remote PowerShell Endpoint für Single-AZ 2- oder Multi-AZ-Dateisysteme einrichten müssen, sollten Sie die primäre private IPv4-Adresse für die elastic network interface für Ihr bevorzugtes Subnetz verwenden. Weitere Informationen finden Sie unter [Verwenden der Amazon FSx CLI für PowerShell](#).

## Aktualisierung der selbstverwalteten Active Directory-Konfiguration

Sie können die AWS Management Console Amazon FSx-API oder verwenden, AWS CLI um den Benutzernamen und das Passwort des Dienstkontos sowie die DNS-Server-IP-Adressen der selbstverwalteten Active Directory-Konfiguration eines Dateisystems zu aktualisieren. Sie können den Fortschritt eines selbstverwalteten Active Directory-Konfigurationsupdates jederzeit mithilfe von CLI und API verfolgen. AWS Management Console Weitere Informationen finden Sie unter [Überwachung von selbstverwalteten Active Directory-Updates](#).

So aktualisieren Sie die selbstverwaltete Active Directory-Konfiguration (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Windows-Dateisystem aus, für das Sie die selbstverwaltete Active Directory-Konfiguration aktualisieren möchten.
3. Wählen Sie dann auf der Registerkarte Netzwerk und Sicherheit die Option Update für die IP-Adressen des DNS-Servers oder für den Benutzernamen des Dienstkontos aus, je nachdem, welche Active Directory-Eigenschaften Sie aktualisieren.
4. Geben Sie die neuen DNS-Server-IP-Adressen oder die neuen Anmeldeinformationen für das Dienstkonto in das angezeigte Dialogfeld ein.
5. Wählen Sie Update, um das Active Directory-Konfigurationsupdate zu starten.

Sie können [den Aktualisierungsfortschritt mit dem AWS Management Console oder dem überwachen](#) AWS CLI.

So aktualisieren Sie die selbstverwaltete Active Directory-Konfiguration (CLI)

- [Verwenden Sie den AWS CLI Befehl update-file-system, um die selbstverwaltete Active Directory-Konfiguration eines Dateisystems vom Typ FSx für Windows File Server zu aktualisieren](#). Legen Sie die folgenden Parameter fest:

- `--file-system-id` auf die ID des Dateisystems, das Sie aktualisieren.
- `UserName` der neue Benutzername für das selbstverwaltete Active Directory-Dienstkonto.
- `Password` das neue Passwort für das selbstverwaltete Active Directory-Dienstkonto.
- `DnsIps` die IP-Adressen für die selbstverwalteten Active Directory-DNS-Server.

```
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]}'
```

Wenn die Aktualisierungsaktion erfolgreich ist, sendet der Dienst eine HTTP 200-Antwort zurück. Das `AdministrativeActions` Objekt in der Antwort beschreibt die Anfrage und ihren Status.

## Überwachung von selbstverwalteten Active Directory-Updates

Wenn Sie die selbstverwaltete Active Directory-Konfiguration Ihres Dateisystems aktualisieren, wechselt der Status des Dateisystems während der Installation des Updates von Verfügbar zu Aktualisierung. Sobald das Update abgeschlossen ist, wechselt der Status wieder zu Verfügbar. Beachten Sie, dass es mehrere Minuten dauern kann, bis das Update abgeschlossen ist.

Sie können den Fortschritt eines selbstverwalteten Active Directory-Konfigurationsupdates mithilfe der AWS Management Console, der API oder der, wie in den folgenden Abschnitten beschrieben AWS CLI, überwachen.

### Updates in der Konsole überwachen

Auf der Registerkarte Updates im Fenster Dateisystemdetails können Sie die 10 neuesten Updates für jeden Updatetyp einsehen.

| Updates (10) <span style="float: right;">↻</span>                                            |                |             |              |                           |
|----------------------------------------------------------------------------------------------|----------------|-------------|--------------|---------------------------|
| <input type="text" value="Filter updates"/> <span style="float: right;">&lt; 1 &gt; ⚙</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 |

Für selbstverwaltete Active Directory-Updates können Sie die folgenden Informationen einsehen.

### Art des Updates

Folgende Typen werden unterstützt:

- IP-Adresse des DNS-Servers
- Anmeldeinformationen für das Dienstkonto

### Zielwert

Der gewünschte Wert, auf den die Dateisystemeigenschaft aktualisiert werden soll. Bei Aktualisierungen der Anmeldeinformationen für Dienstkonten wird nur der Benutzername angezeigt. Kennwörter für Dienstkonten sind in diesem Feld nie enthalten.

### Status

Der aktuelle Status des Updates. Für selbstverwaltete Active Directory-Updates sind die folgenden Werte möglich:

- Ausstehend — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.
- In Bearbeitung — Amazon FSx verarbeitet die Aktualisierungsanfrage.
- Abgeschlossen — Das Dateisystem-Update wurde erfolgreich abgeschlossen.
- Fehlgeschlagen — Das Dateisystem-Update ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Details zum Fehler zu sehen.

## Fortschritt%

Zeigt den Fortschritt der Dateisystemaktualisierung in Prozent an.

## Uhrzeit der Anfrage

Der Zeitpunkt, zu dem Amazon FSx die Anfrage zur Aktualisierungsaktion erhalten hat.

## Überwachung von Updates mithilfe der AWS CLI AND-API

[Mithilfe des AWS CLI Befehls `describe-file-systems` und der Systems-API-Aktion können Sie laufende Aktualisierungsanforderungen für das Dateisystem anzeigen und überwachen. `DescribeFile`](#)

Das `AdministrativeActions` Array listet die 10 neuesten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf.

Das folgende Beispiel zeigt einen Auszug aus der Antwort auf den `describe-file-systems` CLI-Befehl `show two self-managed Active Directory-Dateisystemupdates`.

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

# Verwenden von Microsoft Windows-Dateifreigaben

Eine Microsoft Windows-Dateifreigabe ist ein bestimmter Ordner in Ihrem Dateisystem. Sie umfasst die Unterordner dieses Ordners, auf die Sie Ihren Recheninstanzen mit dem Server Message Block (SMB) -Protokoll Zugriff gewähren. Ihr Dateisystem verfügt über eine standardmäßige Windows-Dateifreigabe mit dem Namen `share` Mithilfe des Windows-Tools für die grafische Benutzeroberfläche (GUI) namens Shared Folders können Sie beliebig viele andere Windows-Dateifreigaben erstellen und verwalten.

## Zugreifen auf Dateifreigaben

Um auf Ihre Dateifreigaben zuzugreifen, verwenden Sie die Windows Map Network Drive-Funktion, um Ihrer Amazon FSx-Dateifreigabe einen Laufwerksbuchstaben auf Ihrer Compute-Instance zuzuordnen. Das Zuordnen einer Dateifreigabe zu einem Laufwerk auf Ihrer Compute-Instance wird unter Linux als Mounthen einer Dateifreigabe bezeichnet. Dieser Vorgang unterscheidet sich je nach Art der Recheninstanz und dem Betriebssystem. Nachdem Ihre Dateifreigabe zugeordnet wurde, können Ihre Anwendungen und Benutzer auf Dateien und Ordner in Ihrer Dateifreigabe zugreifen, als ob es sich um lokale Dateien und Ordner handeln würde.

Im Folgenden finden Sie Verfahren zum Zuordnen einer Dateifreigabe auf den verschiedenen unterstützten Recheninstanzen.

### Themen


- [Zuordnen einer Dateifreigabe auf einer Amazon EC2 EC2-Windows-Instance](#)
- [Mounthen einer Dateifreigabe auf einer Amazon EC2 Mac-Instance](#)
- [Mounthen einer Dateifreigabe auf einer Amazon EC2 EC2-Linux-Instance](#)
- [Automatisches Mounthen von Dateifreigaben auf einer Amazon Linux EC2-Instance, die nicht mit Ihrem Active Directory verknüpft ist](#)

## Zuordnen einer Dateifreigabe auf einer Amazon EC2 EC2-Windows-Instance

Sie können eine Dateifreigabe auf einer EC2-Windows-Instance zuordnen, indem Sie den Windows-Datei-Explorer oder die Befehlszeile verwenden.

So ordnen Sie eine Dateifreigabe auf einer Amazon EC2 EC2-Windows-Instance (Konsole) zu

1. Starten Sie die EC2-Windows-Instance und verbinden Sie sie mit dem Microsoft Active Directory, mit dem Sie Ihr Amazon FSx-Dateisystem verknüpft haben. Wählen Sie dazu eines der folgenden Verfahren aus dem AWS Directory Service Administratorhandbuch aus:
  - [Schließen Sie sich nahtlos einer Windows EC2-Instanz an](#)
  - [Manuell einer Windows-Instanz beitreten](#)
2. Stellen Sie eine Verbindung mit Ihrer Windows-Instance her. Weitere Informationen finden Sie unter [Herstellen einer Verbindung zu Ihrer Windows-Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Nachdem Sie die Verbindung hergestellt haben, öffnen Sie den Datei-Explorer.
4. Öffnen Sie im Navigationsbereich das Kontextmenü (Rechtsklick) für Netzwerk und wählen Sie Netzlaufwerk zuordnen aus.
5. Wählen Sie für Drive einen Laufwerksbuchstaben aus.
6. Geben Sie unter Ordner entweder den DNS-Namen des Dateisystems oder einen mit dem Dateisystem verknüpften DNS-Alias und den Freigabenamen ein.

 **Important**

Die Verwendung einer IP-Adresse anstelle des DNS-Namens könnte dazu führen, dass das Multi-AZ-Dateisystem während des Failover-Prozesses nicht verfügbar ist. Außerdem sind DNS-Namen oder zugehörige DNS-Aliase für die Kerberos-basierte Authentifizierung in Multi-AZ- und Single-AZ-Dateisystemen erforderlich.

Sie finden den DNS-Namen des Dateisystems und alle zugehörigen DNS-Aliase auf der [Amazon FSx-Konsole](#), indem Sie Windows File Server, Network & Security wählen. Sie können sie auch in der Antwort auf die [CreateFileSystem-](#) oder [DescribeFileSystem-API-Operation](#) finden. Weitere Hinweise zur Verwendung von DNS-Aliassen finden Sie unter [DNS-Aliase verwalten](#).

- Für ein Single-AZ-Dateisystem, das mit einem AWS verwalteten Microsoft Active Directory verknüpft ist, sieht der DNS-Name wie folgt aus.

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

- Für ein Single-AZ-Dateisystem, das mit einem selbstverwalteten Active Directory verbunden ist, und für jedes Multi-AZ-Dateisystem sieht der DNS-Name wie folgt aus.

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

Um beispielsweise den DNS-Namen eines Single-AZ-Dateisystems zu verwenden, geben Sie Folgendes für Ordner ein.

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

Um den DNS-Namen eines Multi-AZ-Dateisystems zu verwenden, geben Sie Folgendes für Ordner ein.

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

Um einen DNS-Alias zu verwenden, der dem Dateisystem zugeordnet ist, geben Sie Folgendes für Ordner ein.

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

7. Wählen Sie eine Option für Bei Anmeldung erneut verbinden aus, die angibt, ob die Dateifreigabe bei der Anmeldung erneut verbunden werden soll, und klicken Sie dann auf Fertig stellen.

Um eine Dateifreigabe auf einer Amazon EC2 EC2-Windows-Instance zuzuordnen (Eingabeaufforderung)

1. Starten Sie die EC2-Windows-Instance und verbinden Sie sie mit dem Microsoft Active Directory, mit dem Sie Ihr Amazon FSx-Dateisystem verknüpft haben. Wählen Sie dazu eines der folgenden Verfahren aus dem AWS Directory Service Administratorhandbuch aus:
  - [Schließen Sie sich nahtlos einer Windows EC2-Instanz an](#)
  - [Manuell einer Windows-Instanz beitreten](#)
2. Stellen Sie als Benutzer in Ihrem AWS Managed Microsoft AD Verzeichnis eine Connect zu Ihrer EC2-Windows-Instance her. Weitere Informationen finden Sie unter [Herstellen einer Verbindung zu Ihrer Windows-Instanz](#) im Amazon EC2 EC2-Benutzerhandbuch.



3. Nachdem Sie die Verbindung hergestellt haben, öffnen Sie ein Befehlszeilenfenster.
4. Mounten Sie die Dateifreigabe mit einem Laufwerksbuchstaben Ihrer Wahl, dem DNS-Namen des Dateisystems und dem Freigabennamen. Sie können den DNS-Namen mithilfe der [Amazon FSx-Konsole](#) finden, indem Sie Windows File Server, Network & Security wählen. Sie können sie auch in der Antwort auf die Operation `CreateFileSystem` oder der `DescribeFileSystems` API finden.
  - Für ein Single-AZ-Dateisystem, das mit einem AWS verwalteten Microsoft Active Directory verknüpft ist, sieht der DNS-Name wie folgt aus.

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

- Für ein Single-AZ-Dateisystem, das mit einem selbstverwalteten Active Directory verbunden ist, und für jedes Multi-AZ-Dateisystem sieht der DNS-Name wie folgt aus.

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

Im Folgenden finden Sie einen Beispielbefehl zum Mounten der Dateifreigabe.

```
$ net use H: \\amznfsxaa11bb22.ad-domain.com\share /persistent:yes
```

Anstelle des `net use` Befehls können Sie auch jeden unterstützten PowerShell Befehl verwenden, um eine Dateifreigabe zu mounten.

## Mounten einer Dateifreigabe auf einer Amazon EC2 Mac-Instance

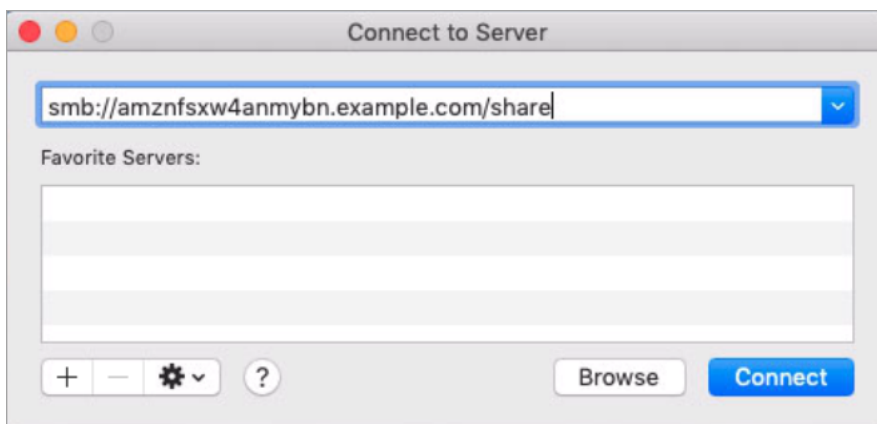
Sie können eine Dateifreigabe auf einer Amazon EC2 Mac-Instance mounten, die entweder mit Ihrem Active Directory verbunden ist oder nicht. Wenn die Instance nicht mit Ihrem Active Directory verbunden ist, stellen Sie sicher, dass Sie die DHCP-Optionen für die Amazon Virtual Private Cloud (Amazon VPC), in der sich die Instance befindet, so aktualisieren, dass sie die DNS-Nameserver für Ihre Active Directory-Domain enthalten. Starten Sie dann die Instance neu.

So mounten Sie eine Dateifreigabe auf einer Amazon EC2 Mac-Instance (GUI)

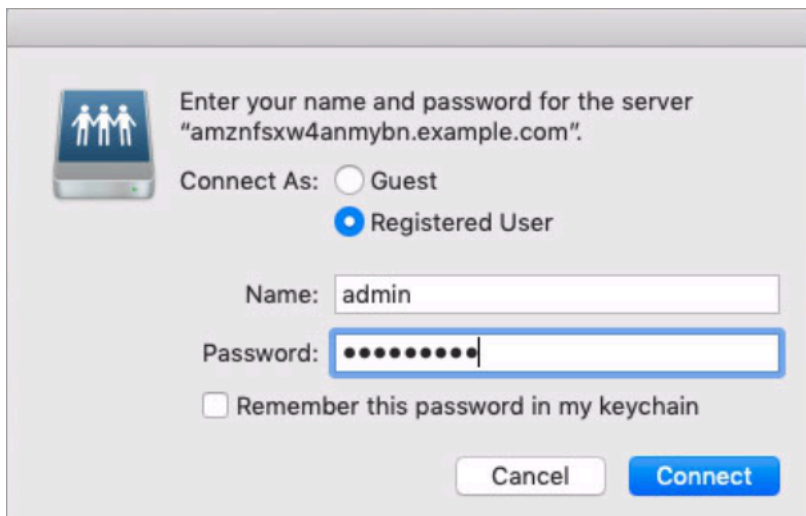
1. Starten Sie die EC2 Mac-Instance. Wählen Sie dazu eines der folgenden Verfahren aus dem Amazon EC2 EC2-Benutzerhandbuch:

- [Starten Sie eine Mac-Instance mit der Konsole](#)
  - [Starten Sie eine Mac-Instanz mit dem AWS CLI](#)
2. Stellen Sie mithilfe von Virtual Network Computing (VNC) eine Connect zu Ihrer EC2-Mac-Instance her. Weitere Informationen finden Sie unter [Connect zu Ihrer Instance mithilfe von VNC](#) herstellen im Amazon EC2 EC2-Benutzerhandbuch.
  3. Stellen Sie auf Ihrer EC2-Mac-Instance wie folgt eine Verbindung zu Ihrer Amazon FSx-Dateifreigabe her:
    - a. Öffnen Sie den Finder, wählen Sie „Los“ und anschließend „Mit Server verbinden“.
    - b. Geben Sie im Dialogfeld Mit Server verbinden entweder den DNS-Namen des Dateisystems oder einen mit dem Dateisystem verknüpften DNS-Alias und den Freigabennamen ein. Wählen Sie dann Verbinden aus.

Sie finden den DNS-Namen des Dateisystems und alle zugehörigen DNS-Aliase auf der [Amazon FSx-Konsole](#), indem Sie Windows File Server, Network & Security wählen. Sie können sie auch in der Antwort auf die [CreateFileSystem- oder DescribeFileSystem-API-Operation](#) finden. Weitere Hinweise zur Verwendung von DNS-Aliassen finden Sie unter [DNS-Aliase verwalten](#).



- c. Wählen Sie auf dem nächsten Bildschirm Connect, um fortzufahren.
- d. Geben Sie Ihre Microsoft Active Directory (AD) -Anmeldeinformationen für das Amazon FSx-Servicekonto ein, wie im folgenden Beispiel gezeigt. Wählen Sie dann Verbinden aus.



- e. Wenn die Verbindung erfolgreich ist, können Sie die Amazon FSx-Freigabe unter Standorte in Ihrem Finder-Fenster sehen.

So mounten Sie eine Dateifreigabe auf einer Amazon EC2 Mac-Instance (Befehlszeile)

1. Starten Sie die EC2 Mac-Instance. Wählen Sie dazu eines der folgenden Verfahren aus dem Amazon EC2 EC2-Benutzerhandbuch:
  - [Starten Sie eine Mac-Instance mit der Konsole](#)
  - [Starten Sie eine Mac-Instanz mit dem AWS CLI](#)
2. Stellen Sie mithilfe von Virtual Network Computing (VNC) eine Connect zu Ihrer EC2-Mac-Instance her. Weitere Informationen finden Sie unter [Connect zu Ihrer Instance mithilfe von VNC](#) herstellen im Amazon EC2 EC2-Benutzerhandbuch.
3. Mounten Sie die Dateifreigabe mit dem folgenden Befehl.

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

Sie finden den DNS-Namen auf der [Amazon FSx-Konsole](#), indem Sie Windows File Server, Network & Security wählen. Sie können sie auch in der Antwort auf die Operation `CreateFileSystem` oder der `DescribeFileSystems` API finden.

- Für ein Single-AZ-Dateisystem, das mit einem AWS verwalteten Microsoft Active Directory verknüpft ist, sieht der DNS-Name wie folgt aus.

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

- Für ein Single-AZ-Dateisystem, das mit einem selbstverwalteten Active Directory verbunden ist, und für jedes Multi-AZ-Dateisystem sieht der DNS-Name wie folgt aus.

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

Der in diesem Verfahren verwendete Mount-Befehl führt an den angegebenen Stellen Folgendes aus:

- `//file_system_dns_name/file_share`— Gibt den DNS-Namen und die gemeinsame Nutzung des Dateisystems an, das gemountet werden soll.
- `mount_point` — Das Verzeichnis auf der EC2-Instance, in das Sie das Dateisystem mounten.

## Mounten einer Dateifreigabe auf einer Amazon EC2 EC2-Linux-Instance

Sie können eine FSx for Windows File Server Server-Dateifreigabe auf einer Amazon EC2 EC2-Linux-Instance mounten, die entweder mit Ihrem Active Directory verbunden ist oder nicht.

### Note

- Die folgenden Befehle geben Parameter wie SMB-Protokoll, Caching und Lese- und Schreibpuffergröße nur als Beispiele an. Die Parameterauswahl für den `cifs` Linux-Befehl sowie die verwendete Linux-Kernelversion können sich auf den Durchsatz und die Latenz bei Netzwerkoperationen zwischen dem Client und dem Amazon FSx-Dateisystem auswirken. Weitere Informationen finden Sie in der `cifs` Dokumentation für die von Ihnen verwendete Linux-Umgebung.
- Linux-Clients unterstützen kein automatisches DNS-basiertes Failover. Weitere Informationen finden Sie unter [Failover-Erfahrung auf Linux-Clients](#).

So mounten Sie eine Dateifreigabe auf einer Amazon EC2 EC2-Linux-Instance, die mit Ihrem Active Directory verbunden ist

1. Wenn Sie noch keine laufende EC2-Linux-Instance haben, die mit Ihrem Microsoft Active Directory verbunden ist, finden Sie [entsprechende Anweisungen unter Manuelles Beitreten zu einer Linux-Instance](#) im AWS Directory Service Administratorhandbuch.
2. Connect zu Ihrer EC2-Linux-Instance her. Weitere Informationen finden Sie unter [Connect to your Linux Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Zur Installation des `cifs-utils` Pakets führen Sie den folgenden Befehl aus: Dieses Paket wird verwendet, um Netzwerkdateisysteme wie Amazon FSx unter Linux zu mounten.

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

4. Erstellen Sie das Mount-Point-Verzeichnis `/mnt/fsx`. Hier werden Sie das Amazon FSx-Dateisystem mounten.

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

5. Authentifizieren Sie sich mit dem folgenden Befehl mit Kerberos.

```
$ kinit
```

6. Mounten Sie die Dateifreigabe mit dem folgenden Befehl.

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

Sie finden den DNS-Namen auf der [Amazon FSx-Konsole](#), indem Sie Windows File Server, Network & Security wählen. Sie können sie auch in der Antwort auf unsere DescribeFileSystems API-Operation finden. CreateFileSystem

- Für ein Single-AZ-Dateisystem, das mit einem AWS verwalteten Microsoft Active Directory verknüpft ist, sieht der DNS-Name wie folgt aus.

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

- Für ein Single-AZ-Dateisystem, das mit einem selbstverwalteten Active Directory verbunden ist, und für jedes Multi-AZ-Dateisystem sieht der DNS-Name wie folgt aus.

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

Ersetzen Sie ihn *CIFSMaxBufSize* durch den größten Wert, den Ihr Kernel zulässt. Führen Sie den folgenden Befehl aus, um diesen Wert zu erhalten.

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

Die Ausgabe zeigt, dass die maximale Puffergröße 130048 beträgt.

7. Stellen Sie sicher, dass das Dateisystem bereitgestellt ist, indem Sie den folgenden Befehl ausführen, der nur Dateisysteme vom Typ Common Internet File System (CIFS) zurückgibt.

```
$ 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
```

Der in diesem Verfahren verwendete Mount-Befehl führt an den angegebenen Punkten Folgendes aus:

- *//file\_system\_dns\_name/file\_share*— Gibt den DNS-Namen und die gemeinsame Nutzung des Dateisystems an, das gemountet werden soll.
- *mount\_point* — Das Verzeichnis auf der EC2-Instance, in das Sie das Dateisystem mounten.
- *-t cifs vers=SMB\_version*— Gibt den Typ des Dateisystems als CIFS und die SMB-Protokollversion an. Amazon FSx for Windows File Server unterstützt die SMB-Versionen 2.0 bis 3.1.1.
- *sec=krb5*— Legt fest, dass Kerberos Version 5 für die Authentifizierung verwendet werden soll.
- *cache=cache\_mode*— Legt den Cache-Modus fest. Diese Option für den CIFS-Cache kann sich auf die Leistung auswirken. Sie sollten testen, welche Einstellungen für Ihren Kernel und Ihren Workload am besten funktionieren (und die Linux-Dokumentation lesen). Die Optionen *strict* und *none* werden empfohlen, da sie aufgrund der lockereren Protokollsemantik zu Dateninkonsistenzen führen *loose* können.
- *cuid=ad\_user*— Legt die UID des Besitzers des Credentials-Caches auf den AD-Verzeichnisadministrator fest.

- `/mnt/fsx`— Gibt den Bereitstellungspunkt für die Amazon FSx-Dateifreigabe auf Ihrer EC2-Instance an.
- `rsize=CIFSMaxBufSize, wsize=CIFSMaxBufSize`— Gibt die Größe des Lese- und Schreibpuffers als die vom CIFS-Protokoll zulässige Höchstgröße an. `CIFSMaxBufSize` Ersetzen Sie durch den größten Wert, den Ihr Kernel zulässt. Ermitteln Sie den, `CIFSMaxBufSize` indem Sie den folgenden Befehl ausführen.

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

Die Ausgabe zeigt, dass die maximale Puffergröße 130048 beträgt.

- `ip=preferred-file-server-IP`— Setzt die Ziel-IP-Adresse auf die des bevorzugten Dateiservers des Dateisystems.

Sie können die bevorzugte Dateiserver-IP-Adresse des Dateisystems wie folgt abrufen:

- Verwenden Sie die Amazon FSx-Konsole auf der Registerkarte Netzwerk und Sicherheit auf der Seite mit den Dateisystemdetails.
- In der Antwort auf den `describe-file-systems` CLI-Befehl oder den entsprechenden [DescribeFileSystems](#) API-Befehl.

So mounten Sie eine Dateifreigabe auf einer Amazon EC2 EC2-Linux-Instance, die nicht mit Ihrem Active Directory verknüpft ist

Mit dem folgenden Verfahren wird eine Amazon FSx-Dateifreigabe in eine Amazon EC2 EC2-Linux-Instance eingebunden, die nicht mit Ihrem Active Directory (AD) verbunden ist. Für eine EC2-Linux-Instance, die nicht mit Ihrem AD verbunden ist, können Sie eine FSx for Windows File Server Server-Dateifreigabe nur mithilfe ihrer privaten IP-Adresse mounten. Sie können die private IP-Adresse des Dateisystems mithilfe der [Amazon FSx-Konsole](#) auf der Registerkarte Netzwerk und Sicherheit unter Bevorzugte Dateiserver-IP-Adresse abrufen.

In diesem Beispiel wird die NTLM-Authentifizierung verwendet. Dazu mounten Sie das Dateisystem als Benutzer, der Mitglied der Microsoft Active Directory-Domäne ist, zu der das Dateisystem FSx for Windows File Server gehört. Die Anmeldeinformationen für das Benutzerkonto werden in einer Textdatei bereitgestellt, die Sie auf Ihrer EC2-Instance erstellen. `creds.txt` Diese Datei enthält den Benutzernamen, das Passwort und die Domäne für den Benutzer.

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

So starten und konfigurieren Sie die Amazon Linux EC2-Instance

1. Starten Sie eine Amazon Linux EC2-Instance mit der [Amazon EC2 EC2-Konsole](#). Weitere Informationen finden Sie unter [Launch an Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
2. Connect zu Ihrer Amazon Linux EC2-Instance her. Weitere Informationen finden Sie unter [Connect to your Linux Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Zur Installation des `cifs-utils` Pakets führen Sie den folgenden Befehl aus: Dieses Paket wird verwendet, um Netzwerkdateisysteme wie Amazon FSx unter Linux zu mounten.

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

4. Erstellen Sie den Bereitstellungspunkt `/mnt/fsxx`, an dem Sie das Amazon FSx-Dateisystem mounten möchten.

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

5. Erstellen Sie die `creds.txt` Anmeldeinformationsdatei im `/home/ec2-user` Verzeichnis und verwenden Sie dabei das zuvor gezeigte Format.
6. Stellen Sie die `creds.txt` Dateiberechtigungen so ein, dass nur Sie (der Besitzer) die Datei lesen und in sie schreiben können, indem Sie den folgenden Befehl ausführen.

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

So mounten Sie das Dateisystem

1. Sie stellen eine Dateifreigabe, die nicht mit Ihrem Active Directory verknüpft ist, mithilfe ihrer privaten IP-Adresse bereit. Sie können die private IP-Adresse des Dateisystems mithilfe der [Amazon FSx-Konsole](#) auf der Registerkarte Netzwerk und Sicherheit unter Bevorzugte Dateiserver-IP-Adresse abrufen.
2. Hängen Sie das Dateisystem mit dem folgenden Befehl ein:



```
$ 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
```

*CIFSMaxBufSize* Ersetzen Sie es durch den größten Wert, den Ihr Kernel zulässt. Führen Sie den folgenden Befehl aus, um diesen Wert zu erhalten.

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

Die Ausgabe zeigt, dass die maximale Puffergröße 130048 beträgt.

3. Stellen Sie sicher, dass das Dateisystem bereitgestellt ist, indem Sie den folgenden Befehl ausführen, der nur CIFS-Dateisysteme zurückgibt.

```
$ 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
```

Der in diesem Verfahren verwendete Mount-Befehl führt an den angegebenen Punkten Folgendes aus:

- *//file-system-IP-address/file\_share*— Gibt die IP-Adresse und die gemeinsame Nutzung des Dateisystems an, das Sie mounten.
- *-t cifs vers=SMB\_version*— Gibt den Typ des Dateisystems als CIFS und die SMB-Protokollversion an. Amazon FSx for Windows File Server unterstützt die SMB-Versionen 2.0 bis 3.1.1.
- *sec=ntlmsspi*— Gibt an, dass NT LAN Manager Security Support Provider Interface (NTLMSSPI) für die Authentifizierung verwendet werden soll.
- *cache=cache\_mode*— Legt den Cachemodus fest. Diese Option für den CIFS-Cache kann sich auf die Leistung auswirken. Sie sollten testen, welche Einstellungen für Ihren Kernel und Ihren Workload am besten funktionieren (und die Linux-Dokumentation lesen). Die Optionen *strict* und *none* werden empfohlen, da sie aufgrund der lockereren Protokollsemantik zu Dateninkonsistenzen führen *loose* können.

- `cred=/home/ec2-user/creds.txt`— Gibt an, wo die Benutzeranmeldedaten abgerufen werden sollen.
- `/mnt/fsx`— Gibt den Bereitstellungspunkt für die Amazon FSx-Dateifreigabe auf Ihrer EC2-Instance an.
- `rsize=CIFSMaxBufSize, wsize=CIFSMaxBufSize`— Gibt die Größe des Lese- und Schreibpuffers als die vom CIFS-Protokoll zulässige Höchstgröße an. `CIFSMaxBufSize` Ersetzen Sie durch den größten Wert, den Ihr Kernel zulässt. Ermitteln Sie den, `CIFSMaxBufSize` indem Sie den folgenden Befehl ausführen.

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

## Automatisches Mounten von Dateifreigaben auf einer Amazon Linux EC2-Instance, die nicht mit Ihrem Active Directory verknüpft ist

Sie können Ihre FSx for Windows File Server Server-Dateifreigabe automatisch mounten, wenn die Amazon EC2 EC2-Linux-Instance, auf der sie bereitgestellt wurde, neu gestartet wird. Fügen Sie dazu der `/etc/fstab` Datei auf der EC2-Instance einen Eintrag hinzu. Die `/etc/fstab`-Datei enthält Informationen zu Dateisystemen. Der Befehl `mount -a`, der beim Start der Instanz ausgeführt wird, mountet die in der Datei aufgelisteten Dateisysteme. `/etc/fstab`

Für eine Amazon EC2 EC2-Linux-Instance, die nicht mit Ihrem Active Directory verknüpft ist, können Sie eine FSx for Windows File Server Server-Dateifreigabe nur mithilfe ihrer privaten IP-Adresse mounten. Sie können die private IP-Adresse des Dateisystems mithilfe der [Amazon FSx-Konsole](#) auf der Registerkarte Netzwerk und Sicherheit unter Bevorzugte Dateiserver-IP-Adresse abrufen.

Das folgende Verfahren verwendet die Microsoft NTLM-Authentifizierung. Sie mounten das Dateisystem als Benutzer, der Mitglied der Microsoft Active Directory-Domäne ist, zu der das Dateisystem FSx for Windows File Server gehört. Die Anmeldeinformationen für das Benutzerkonto werden in der Textdatei `creds.txt` bereitgestellt. Diese Datei enthält den Benutzernamen, das Passwort und die Domäne für den Benutzer.

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

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

Automatisches Mounten einer Dateifreigabe auf einer Amazon Linux EC2-Instance, die nicht mit Ihrem Active Directory verknüpft ist

So starten und konfigurieren Sie die Amazon Linux EC2-Instance

1. Starten Sie eine Amazon Linux EC2-Instance mit der [Amazon EC2 EC2-Konsole](#). Weitere Informationen finden Sie unter [Launch an Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
2. Verbinden Sie sich mit der Instance. Weitere Informationen finden Sie unter [Connect to your Linux Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Zur Installation des `cifs-utils` Pakets führen Sie den folgenden Befehl aus: Dieses Paket wird verwendet, um Netzwerkdateisysteme wie Amazon FSx unter Linux zu mounten.

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

4. Erstellen des `/mnt/fsx` Verzeichnisses. Hier werden Sie das Amazon FSx-Dateisystem mounten.

```
$ sudo mkdir /mnt/fsx
```

5. Erstellen Sie die Datei mit den `creds.txt` Anmeldeinformationen im `/home/ec2-user` Verzeichnis.
6. Stellen Sie die Dateiberechtigungen so ein, dass nur Sie (der Besitzer) die Datei lesen können, indem Sie den folgenden Befehl ausführen.

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

Um das Dateisystem automatisch zu mounten

1. Sie hängen eine Dateifreigabe, die nicht mit Ihrem Active Directory verknüpft ist, automatisch mithilfe ihrer privaten IP-Adresse ein. Sie können die private IP-Adresse des Dateisystems mithilfe der [Amazon FSx-Konsole](#) auf der Registerkarte Netzwerk und Sicherheit unter Bevorzugte Dateiserver-IP-Adresse abrufen.
2. Um die Dateifreigabe mithilfe ihrer privaten IP-Adresse automatisch zu mounten, fügen Sie der `/etc/fstab` Datei die folgende Zeile hinzu.

```
//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
```

*CIFSMaxBufSize* Ersetzen Sie durch den größten Wert, den Ihr Kernel zulässt. Führen Sie den folgenden Befehl aus, um diesen Wert zu erhalten.

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

Die Ausgabe zeigt, dass die maximale Puffergröße 130048 beträgt.

3. Testen Sie den `fstab` Eintrag, indem Sie den `mount` Befehl mit der Option `'fake'` in Verbindung mit den Optionen `'all'` und `'verbose'` verwenden.

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

4. Um die Dateifreigabe zu mounten, starten Sie die Amazon EC2 EC2-Instance neu.
5. Wenn die Instance wieder verfügbar ist, stellen Sie sicher, dass das Dateisystem bereitgestellt ist, indem Sie den folgenden Befehl ausführen.

```
$ 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
```

Die Zeile, die der `/etc/fstab` Datei in diesem Verfahren hinzugefügt wird, bewirkt an den angegebenen Stellen Folgendes:

- *//file-system-IP-address/file\_share*— Gibt die IP-Adresse und die gemeinsame Nutzung des Amazon FSx-Dateisystems an, das Sie mounten.
- `/mnt/fsx`— Gibt den Bereitstellungspunkt für das Amazon FSx-Dateisystem auf Ihrer EC2-Instance an.
- `cifs vers=SMB_version`— Gibt den Typ des Dateisystems als CIFS und die SMB-Protokollversion an. Amazon FSx for Windows File Server unterstützt die SMB-Versionen 2.0 bis 3.1.1.

- `sec=ntlmssp`— Gibt an, dass NT LAN Manager Security Support Provider Interface verwendet wird, um die NTLM-Challenge-Response-Authentifizierung zu erleichtern.
- `cache=cache_mode`— Legt den Cachemodus fest. Diese Option für den CIFS-Cache kann sich auf die Leistung auswirken. Sie sollten testen, welche Einstellungen für Ihren Kernel und Ihren Workload am besten funktionieren (und die Linux-Dokumentation lesen). Die Optionen `strict` und `none` werden empfohlen, da sie aufgrund der lockereren Protokollsemantik zu Dateninkonsistenzen führen können.
- `cred=/home/ec2-user/creds.txt`— Gibt an, wo die Benutzeranmeldedaten abgerufen werden sollen.
- `_netdev`— Teilt dem Betriebssystem mit, dass sich das Dateisystem auf einem Gerät befindet, das Netzwerkzugriff benötigt. Mit dieser Option wird verhindert, dass die Instanz das Dateisystem mountet, bis der Netzwerkdienst auf dem Client aktiviert ist.
- `0`— Gibt an, dass das Dateisystem mit `gesichert` werden soll, falls es sich um einen Wert ungleich Null handelt. Für Amazon FSx sollte dieser Wert sein. `0`
- `0`— Gibt die Reihenfolge an, in der Dateisysteme beim Booten `fsck` überprüft werden. Für Amazon FSx-Dateisysteme sollte dieser Wert angeben, dass `0` sie beim Start nicht ausgeführt werden sollen.

# Migration von vorhandenem Dateispeicher zu Amazon FSx

FSx for Windows File Server bietet die Funktionen, die Leistung und die Kompatibilität, mit denen Sie Unternehmensanwendungen problemlos in die Amazon Web Services Cloud verlagern und verlagern können. Die Migration zu FSx for Windows File Server umfasst die folgenden Schritte:

1. Migrieren Sie Ihre Dateien zu FSx for Windows File Server. Weitere Informationen finden Sie unter [Migration von vorhandenem Dateispeicher zu FSx for Windows File Server](#).
2. Migrieren Sie Ihre Dateifreigabekonfiguration auf FSx for Windows File Server. Weitere Informationen finden Sie unter [Migration von Dateifreigabekonfigurationen zu Amazon FSx](#).
3. Ordnen Sie Ihren vorhandenen DNS-Namen als DNS-Alias für Ihr Amazon FSx-Dateisystem zu. Weitere Informationen finden Sie unter [Einen DNS-Alias mit Amazon FSx verknüpfen](#).
4. Wechseln Sie zu FSx for Windows File Server. Weitere Informationen finden Sie unter [Umstellung auf Amazon FSx](#).

Die Einzelheiten zu den einzelnen Prozessschritten finden Sie in den folgenden Abschnitten.

## Themen

- [Migration von vorhandenem Dateispeicher zu FSx for Windows File Server](#)
- [Migration von Dateifreigabekonfigurationen zu Amazon FSx](#)
- [Migration der DNS-Konfiguration zur Verwendung von Amazon FSx](#)
- [Umstellung auf Amazon FSx](#)

## Migration von vorhandenem Dateispeicher zu FSx for Windows File Server

Um Ihre vorhandenen Dateien auf FSx for Windows File Server Server-Dateisysteme zu migrieren, empfehlen wir die Verwendung AWS DataSync eines Online-Datenübertragungsdienstes, der das Kopieren großer Datenmengen zu und von AWS Speicherdiensten vereinfacht, automatisiert und beschleunigt. DataSync kopiert Daten über das Internet oder AWS Direct Connect. Da es sich um einen vollständig verwalteten Dienst handelt, fällt ein Großteil der Notwendigkeit, Anwendungen zu ändern, Skripts zu entwickeln oder die Infrastruktur zu verwalten. Weitere Informationen finden Sie unter [Migrieren vorhandener Dateien zu FSx for Windows File Server mit AWS DataSync](#).

Als alternative Lösung können Sie Robust File Copy oder Robocopy verwenden. Dabei handelt es sich um einen Befehlssatz für Befehlszeilenverzeichnis und Dateireplikation für Microsoft Windows. Ausführliche Verfahren zur Verwendung von Robocopy zur Migration von Dateispeichern auf FSx for Windows File Server finden Sie unter [Migrieren vorhandener Dateien zu FSx for Windows File Server mit Robocopy](#)

## Bewährte Methoden für die Migration von vorhandenem Dateispeicher zu FSx for Windows File Server

Um große Datenmengen so schnell wie möglich auf FSx for Windows File Server zu migrieren, verwenden Sie Amazon FSx-Dateisysteme, die mit Solid-State-Drive-Speicher (SSD) konfiguriert sind. Nach Abschluss der Migration können Sie die Daten mithilfe von Festplattenspeicher (HDD) in Amazon FSx-Dateisysteme verschieben, wenn dies die beste Lösung für Ihre Anwendung ist.

Um Daten von einem Amazon FSx-Dateisystem mithilfe von SSD-Speicher auf HDD-Speicher zu verschieben, können Sie die folgenden Schritte ausführen. (Beachten Sie, dass HDD-Dateisysteme über eine Mindestspeicherkapazität von 2 TB verfügen und Sie die Speicherkapazität bei der Wiederherstellung aus einem Backup nicht ändern können.)

1. Erstellen Sie eine Sicherungskopie Ihres SSD-Dateisystems. Weitere Informationen finden Sie unter [Erstellen von vom Benutzer initiierten Backups](#).
2. Stellen Sie das Backup mithilfe von Festplattenspeicher in einem Dateisystem wieder her. Weitere Informationen finden Sie unter [Wiederherstellen von Sicherungen](#).

## Migrieren vorhandener Dateien zu FSx for Windows File Server mit AWS DataSync

Wir empfehlen AWS DataSync die Verwendung zur Übertragung von Daten zwischen FSx for Windows File Server Server-Dateisystemen. DataSync ist ein Datenübertragungsdienst, der das Verschieben und Replizieren von Daten zwischen lokalen Speichersystemen und anderen AWS Speicherdiensten über das Internet vereinfacht, automatisiert und beschleunigt. AWS Direct Connect DataSync kann Ihre Dateisystemdaten und Metadaten wie Eigentum, Zeitstempel und Zugriffsberechtigungen übertragen.

DataSync unterstützt das Kopieren von NTFS-Zugriffskontrolllisten (ACLs) und unterstützt auch das Kopieren von Dateiüberwachungsinformationen, auch bekannt als NTFS-Systemzugriffskontrolllisten

(SACLs), die von Administratoren verwendet werden, um die Auditprotokollierung von Benutzerzugriffsversuchen zu kontrollieren.

Sie können DataSync verwenden, um Dateien zwischen zwei FSx for Windows File Server Server-Dateisystemen zu übertragen und auch Daten in ein Dateisystem in einer anderen AWS-Region in ein AWS OR-Konto zu verschieben. Sie können Dateisysteme DataSync mit FSx for Windows File Server für andere Aufgaben verwenden. Sie können beispielsweise einmalige Datenmigrationen durchführen, regelmäßig Daten für verteilte Workloads aufnehmen und die Replikation für Datenschutz und Wiederherstellung planen.

In AWS DataSync ist ein Speicherort für FSx for Windows File Server ein Endpunkt für einen FSx for Windows File Server. Sie können Dateien zwischen einem Speicherort für FSx for Windows File Server und einem Speicherort für andere Dateisysteme übertragen. Weitere Informationen finden Sie im AWS DataSync Benutzerhandbuch unter [Arbeiten mit Speicherorten](#).

DataSync greift über das Server Message Block (SMB) -Protokoll auf Ihren FSx for Windows File Server zu. Es authentifiziert sich mit dem Benutzernamen und dem Passwort, die Sie in der Konsole oder konfigurieren. AWS DataSync AWS CLI

## Voraussetzungen

Um Daten in Ihr Amazon FSx for Windows File Server-Setup zu migrieren, benötigen Sie einen Server und ein Netzwerk, die die DataSync Anforderungen erfüllen. Weitere Informationen finden Sie unter [Anforderungen für DataSync](#) im AWS DataSync Benutzerhandbuch.

Wenn Sie eine große Datenmigration oder eine Migration mit vielen kleinen Dateien durchführen, empfehlen wir die Verwendung eines Amazon FSx-Dateisystems mit SSD-Speichertyp. Dies liegt daran, dass DataSync Aufgaben das Scannen von Dateimetadaten beinhalten, wodurch die Festplatten-IOPS-Grenzwerte von HDD-Dateisystemen ausgeschöpft werden können, was zu lang andauernden Migrationen und einer Beeinträchtigung der Dateisystemleistung führen kann. Weitere Informationen finden Sie unter: [Bewährte Methoden für die Migration von vorhandenem Dateispeicher zu FSx for Windows File Server](#).

Wenn Ihr Datensatz hauptsächlich aus kleinen Dateien besteht, die Anzahl der Dateien in die Millionen geht oder wenn Sie mehr Netzwerkbandbreite zur Verfügung haben, als eine einzelne DataSync Aufgabe verbraucht, können Sie Ihre Datenübertragungen auch mit einer Scale-Out-Architektur beschleunigen. Weitere Informationen finden Sie unter: [So beschleunigen Sie Ihre Datenübertragungen mit AWS DataSync Scale-Out-Architekturen](#).



Sie können die Festplatten-I/O-Auslastung Ihres Dateisystems mithilfe von [FSx-Leistungsmetriken](#) überwachen.

## Grundlegende Schritte für die Migration von Dateien mit DataSync

Gehen Sie wie folgt vor, um Dateien von einem Quellverzeichnis an ein Zielverzeichnis mit DataSync zu übertragen:

- Laden Sie einen Agent herunter, stellen Sie ihn in Ihrer Umgebung bereit, und aktivieren Sie ihn.
- Erstellen und konfigurieren Sie einen Quell- und Zielspeicherort.
- Erstellen und konfigurieren Sie eine Aufgabe.
- Führen Sie die Aufgabe aus, um Dateien von der Quelle zum Ziel zu übertragen.

Informationen zum Übertragen von Dateien von einem vorhandenen lokalen Dateisystem auf Ihren FSx for Windows File Server finden Sie unter [Datenübertragung zwischen selbstverwaltetem Speicher und AWS, Erstellen eines Speicherorts für SMB](#) und [Erstellen eines Speicherorts für Amazon FSx for Windows File Server](#) im Benutzerhandbuch.AWS DataSync

Informationen zum Übertragen von Dateien von einem vorhandenen In-Cloud-Dateisystem auf Ihren FSx for Windows File Server finden Sie unter [Deploy your agent as Amazon EC2 EC2-Instance](#) im AWS DataSync Benutzerhandbuch.

## Migration zwischen zwei Amazon FSx-Dateisystemen

Sie können DataSync verwenden, um Daten zwischen zwei Amazon FSx-Dateisystemen zu migrieren. Dies kann hilfreich sein, wenn Sie Ihre Arbeitslast von einem vorhandenen Dateisystem auf ein neues Dateisystem mit einer anderen Konfiguration verschieben müssen, z. B. von einer Single-AZ- auf eine Multi-AZ-Konfiguration. Sie können es auch verwenden DataSync , um Ihre Arbeitslast auf zwei Dateisysteme aufzuteilen.

Hier ist ein Beispiel für einen Überblick über den Migrationsprozess:

1. Erstellen Sie DataSync Speicherorte für die Quell- und Zieldateisysteme. Beachten Sie, dass Quelle und Ziel derselben Active Directory-Domäne (AD) angehören müssen oder dass zwischen ihren Domänen eine AD-Vertrauensstellung besteht.
2. Erstellen und konfigurieren Sie eine DataSync Aufgabe zur Übertragung von Daten von der Quelle zum Ziel. Sie können die Aufgabe als einmalige Instanz ausführen oder die Aufgabe so einrichten, dass sie automatisch nach einem von Ihnen konfigurierten Zeitplan ausgeführt wird.

3. Nach erfolgreichem Abschluss der Aufgabe sind die Daten in Ihrem Zielsystem eine exakte Kopie Ihrer Quelle. Beachten Sie, dass Sie alle Schreibaktivitäten oder Dateiaktualisierungen in Ihrem Quellsystem vorübergehend unterbrechen müssen, um die Aufgabe abzuschließen. Sie können dann zu Ihrem Zielsystem wechseln und das Quellsystem löschen.

Vor der Migration von Ihrem Produktionsdateisystem können Sie den Migrationsprozess auf einem Dateisystem testen, das aus einer aktuellen Sicherung wiederhergestellt wurde. Auf diese Weise können Sie abschätzen, wie lange der Datenübertragungsprozess dauert, und DataSync Fehler im Voraus beheben.

Um die Umstellungszeit zu minimieren, können Sie DataSync Aufgaben im Voraus ausführen und dabei den Großteil Ihrer Daten von Ihrem Quellsystem in Ihr Zielsystem verschieben. Nachdem Sie den Datenverkehr zu Ihrem Quellsystem gestoppt haben, können Sie eine letzte Aufgabenübertragung durchführen, um alle Daten zu synchronisieren, die seit der Einstellung des Datenverkehrs neu aktualisiert wurden, und dann auf Ihr Zielsystem übertragen.

Sie können DataSync Tasks so konfigurieren, dass sie nur in bestimmten Verzeichnissen ausgeführt werden oder dass sie bestimmte Pfade ein- oder ausschließen. Dies kann nützlich sein, wenn Sie mehrere Aufgaben parallel ausführen oder wenn Sie eine Teilmenge Ihrer Daten migrieren möchten.

Sie können in Ihrem Zielsystem einen DNS-Alias erstellen, der dem DNS-Namen Ihres Quellsystems entspricht. Dadurch können Ihre Endbenutzer und Anwendungen weiterhin über den DNS-Namen Ihres Quellsystems auf Dateidaten zugreifen. Weitere Informationen zum Einrichten eines DNS-Alias finden Sie unter: [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisystem](#).

Bei dieser Art der Migration empfehlen wir Folgendes:

- Planen Sie Ihre Migration so, dass Sie keine Dateisystem-Backups, Ihr wöchentliches Wartungsfenster und Data Deduplication Jobs vermeiden. Insbesondere empfehlen wir, den Data Deduplication GarbageCollection Job zu deaktivieren, wenn er mit Ihrer geplanten Migration zusammenfällt.
- Verwenden Sie einen SSD-Speichertyp sowohl für Ihr Quell- als auch für Ihr Zielsystem. Sie können zwischen HDD- und SSD-Speichertypen wechseln, indem Sie die Daten aus dem Backup wiederherstellen. Weitere Informationen finden Sie unter: [Migration von vorhandenem Dateispeicher zu FSx for Windows File Server](#).
- Konfigurieren Sie Ihre Quell- und Zielsysteme mit ausreichender Durchsatzkapazität für die Datenmenge, die Sie übertragen müssen. Überwachen Sie bei DataSync Aufgabenprozessen

die Leistungsauslastung sowohl des Quell- als auch des Zieldateisystems. Weitere Informationen finden Sie unter: [Metriken mit Amazon überwachen CloudWatch](#).

- Richten Sie die [DataSync Überwachung](#) ein, damit Sie den Fortschritt laufender Aufgaben besser nachvollziehen können. Sie können auch DataSync Protokolle an die Amazon CloudWatch Logs-Gruppe senden, um Sie beim Debuggen Ihrer Aufgaben zu unterstützen, falls Sie auf Fehler stoßen.

## Migrieren vorhandener Dateien zu FSx for Windows File Server mit Robocopy

Amazon FSx for Windows File Server basiert auf Microsoft Windows Server und ermöglicht Ihnen die vollständige Migration Ihrer vorhandenen Datensätze in Ihre Amazon FSx-Dateisysteme. Sie können die Daten für jede Datei migrieren. Sie können auch alle relevanten Dateimetadaten migrieren, einschließlich Attribute, Zeitstempel, Zugriffskontrolllisten (ACLs), Eigentümerinformationen und Prüfungsinformationen. Mit dieser umfassenden Migrationsunterstützung ermöglicht Amazon FSx die Verlagerung Ihrer Windows-basierten Workloads und Anwendungen, die auf diesen Dateidatensätzen basieren, in die Amazon Web Services Cloud.

Verwenden Sie die folgenden Themen als Leitfaden für den Vorgang zum Kopieren vorhandener Dateidaten. Während Sie diese Kopie durchführen, behalten Sie alle Dateimetadaten aus Ihren lokalen Rechenzentren oder von Ihren selbstverwalteten Dateiservern auf Amazon EC2 bei.

### Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie Folgendes tun:

- Stellen Sie Netzwerkkonnektivität (mithilfe von AWS Direct Connect oder VPN) zwischen Ihrem lokalen Active Directory und der VPC her, auf der Sie das Amazon FSx-Dateisystem erstellen möchten.
- Erstellen Sie ein Dienstkonto in Ihrem Active Directory mit delegierten Berechtigungen, um Computer mit der Domäne zu verbinden. Weitere Informationen finden Sie unter [Delegieren von Rechten an Ihr Dienstkonto](#) im AWS Directory Service Administratorhandbuch.
- Erstellen Sie ein Amazon FSx-Dateisystem, das mit Ihrem selbstverwalteten (lokalen) Microsoft AD-Verzeichnis verknüpft ist.
- Notieren Sie sich den Speicherort (z. B. \\Source\Share) der Dateifreigabe (entweder lokal oder in AWS), die die vorhandenen Dateien enthält, die Sie an Amazon FSx übertragen möchten.

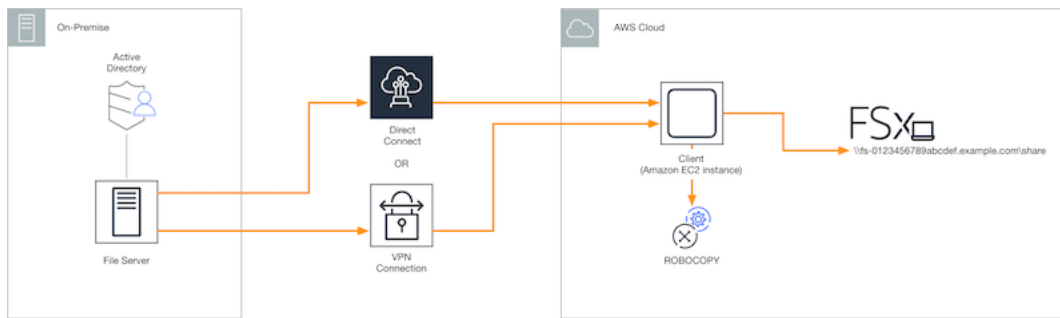
- Notieren Sie sich den Speicherort (z. B. \\Target\Share) der Dateifreigabe auf Ihrem Amazon FSx-Dateisystem, an die Sie Ihre vorhandenen Dateien übertragen möchten.

In der folgenden Tabelle sind die Barrierefreiheitsanforderungen für Quell- und Zieldateisysteme für drei Benutzerzugriffsmodelle für die Migration zusammengefasst.

| Zugriffsmodell für Migrationsbenutzer                                                 | Anforderungen an die Barrierefreiheit des Quelldateisystems                                                                  | Barrierefreiheitsanforderungen für FSx-Zieldateiserver                                                                       |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Modell für direkte Lese-/Schreibberechtigungen                                        | Der Benutzer benötigt mindestens Leseberechtigungen (NTFS-ACLs) für die zu migrierenden Dateien und Ordner.                  | Der Benutzer benötigt mindestens Schreibberechtigungen (NTFS-ACLs) für die zu migrierenden Dateien und Ordner.               |
| Berechtigungsmodell I für Backup/Restore zum Überschreiben von Zugriffsberechtigungen | Der Benutzer muss Mitglied der lokalen Active Directory-Gruppe Backup Operators sein und das Flag /b mit verwenden. RoboCopy | Der Benutzer muss Mitglied der Administratorgruppe des Amazon FSx-Dateisystems sein* und das Flag /b mit verwenden. RoboCopy |
| Domänenadministratormodell (voll) zum Außerkraftsetzen von Zugriffsberechtigungen     | Der Benutzer muss Mitglied der Domänen-Admins-Gruppe des lokalen Active Directory sein.                                      | Der Benutzer muss Mitglied der Administratorgruppe des Amazon FSx-Dateisystems sein* und das Flag /b verwenden mit RoboCopy  |

#### Note

\* Für Dateisysteme, die einem AWS Managed Microsoft AD angehören, ist die Amazon FSx-Dateisystemadministratorengruppe AWS Delegated FSx Administrators. In Ihrem selbstverwalteten Microsoft AD ist die Amazon FSx-Dateisystemadministratorengruppe Domain Admins oder die benutzerdefinierte Gruppe, die Sie bei der Erstellung Ihres Dateisystems für die Verwaltung angegeben haben.



## So migrieren Sie bestehende Dateien mit Robocopy zu Amazon FSx

Mithilfe des folgenden Verfahrens können Sie vorhandene Dateien zu Amazon FSx migrieren.

Um bestehende Dateien zu Amazon FSx zu migrieren

1. Starten Sie eine Windows Server 2016 Amazon EC2 EC2-Instance in derselben Amazon VPC wie die Ihres Amazon FSx-Dateisystems.
2. Stellen Sie eine Verbindung zu Ihrer Amazon-EC2-Instance her. Weitere Informationen finden Sie unter [Herstellen einer Verbindung mit Ihrer Windows-Instance](#) im Amazon EC2-Benutzerhandbuch für Windows-Instances.
3. Öffnen Sie die Befehlszeile und ordnen Sie die Quelldateifreigabe auf Ihrem vorhandenen Dateiserver (lokal oder lokal AWS) wie folgt einem Laufwerksbuchstaben (z. B. **Y**) zu. In diesem Rahmen geben Sie Anmeldeinformationen für ein Mitglied der Domänenadministratorgruppe Ihres lokalen Active Directory-Netzwerks ein.

```
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. Ordnen Sie die Zieldateifreigabe in Ihrem Amazon FSx-Dateisystem wie folgt einem anderen Laufwerksbuchstaben (z. B. **Z**) auf Ihrer Amazon EC2 EC2-Instance zu. Im Rahmen dessen geben Sie Anmeldeinformationen für ein Benutzerkonto an, das Mitglied der Domänenadministratorgruppe Ihres lokalen Active Directory und der Administratorgruppe Ihres Amazon FSx-Dateisystems ist. Für Dateisysteme, die mit einem AWS verwalteten Microsoft AD verbunden sind, ist diese Gruppe **AWS Delegated FSx Administrators**. In Ihrem selbstverwalteten Microsoft AD ist diese Gruppe **Domain Admins** oder die benutzerdefinierte Gruppe, die Sie bei der Erstellung Ihres Dateisystems für die Verwaltung angegeben haben.

Weitere Informationen finden Sie in der Tabelle mit den [Barrierefreiheitsanforderungen für Quell- und Zieldateisysteme](#) in der [Voraussetzungen](#).

```
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. Wählen Sie im Kontextmenü die Option Als Administrator ausführen aus. Öffnen Sie die Befehlszeile oder Windows PowerShell als Administrator und führen Sie den folgenden Robocopy-Befehl aus, um die Dateien von der Quellfreigabe auf die Zielfreigabe zu kopieren.

Der ROBOCOPY Befehl ist ein flexibles Hilfsprogramm für die Dateiübertragung mit mehreren Optionen zur Steuerung des Datenübertragungsprozesses. Aufgrund dieses ROBOCOPY Befehlsprozesses werden alle Dateien und Verzeichnisse von der Quellfreigabe auf die Amazon FSx-Zielfreigabe kopiert. Bei der Kopie werden NTFS-ACLs, Attribute, Zeitstempel, Eigentümerinformationen und Prüfungsinformationen für Dateien und Ordner beibehalten.

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

Der obige Beispielbefehl verwendet die folgenden Elemente und Optionen:

- Y — Bezieht sich auf die Quellfreigabe, die sich in der lokalen Active Directory-Gesamtstruktur mydata.com befindet.
- Z — Bezieht sich auf die Zielfreigabe \\amznfsxabcdef1.mydata.com\share auf Amazon FSx.
- /copy — Gibt die folgenden Dateieigenschaften an, die kopiert werden sollen:
  - D — Daten
  - A — Attribute
  - T — Zeitstempel
  - S — NTFS-ACLs
  - O — Informationen zum Eigentümer
  - U — Informationen zur Prüfung.
- /secfix — Behebt die Dateisicherheit für alle Dateien, auch für übersprungene.

- /e — Kopiert Unterverzeichnisse, auch leere.
- /b — Verwendet die Sicherungs- und Wiederherstellungsrechte in Windows, um Dateien zu kopieren, auch wenn deren NTFS-ACLs dem aktuellen Benutzer die Zugriffsrechte verweigern.
- /MT:8 — Gibt an, wie viele Threads für die Ausführung von Multithread-Kopien verwendet werden sollen.

#### Note

Wenn Sie große Dateien über eine langsame oder unzuverlässige Verbindung kopieren, können Sie den Neustartmodus aktivieren, indem Sie die /zb Option mit der Option anstelle der Option verwenden. `robocopy /b` Wenn im Neustartmodus die Übertragung einer großen Datei unterbrochen wird, kann ein nachfolgender Robocopy-Vorgang mitten in der Übertragung beginnen, anstatt die gesamte Datei erneut von Anfang an kopieren zu müssen. Die Aktivierung des neustartbaren Modus kann die Datenübertragungsgeschwindigkeit verringern.

## Migration von Dateifreigabekontfigurationen zu Amazon FSx

Sie können eine bestehende Dateifreigabekontfiguration mit dem folgenden Verfahren zu Amazon FSx migrieren. In diesem Verfahren ist der Quelldateiserver der Dateiserver, dessen Dateifreigabekontfiguration Sie zu Amazon FSx migrieren möchten.

#### Note

Migrieren Sie zuerst Ihre Dateien zu Amazon FSx, bevor Sie Ihre Fileshare-Konfiguration migrieren. Weitere Informationen finden Sie unter [Migration von vorhandenem Dateispeicher zu FSx for Windows File Server](#).

So migrieren Sie bestehende Dateifreigaben zu FSx for Windows File Server

1. Wählen Sie auf dem Quelldateiserver im Kontextmenü die Option Als Administrator ausführen aus. Öffnen Sie Windows PowerShell als Administrator.
2. Exportieren Sie die Dateifreigaben des Quelldateiservers in eine Datei mit dem Namen, `SmbShares.xml` indem Sie die folgenden Befehle in der ausführen PowerShell. Ersetzen Sie

F: in diesem Beispiel durch den Laufwerksbuchstaben auf Ihrem Dateiserver, von dem Sie Dateifreigaben exportieren.

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

3. Bearbeiten Sie die `SmbShares.xml` Datei und ersetzen Sie alle Verweise auf F: (Ihr Laufwerksbuchstabe) auf D:\share, da sich die Amazon FSx-Dateisysteme auf D:\share befinden
4. Importieren Sie die bestehende Dateifreigabekonfiguration in FSx for Windows File Server. Kopieren Sie auf einem Client, der Zugriff auf Ihr Amazon FSx-Zielfeldateisystem und den Quelldateiserver hat, die gespeicherte Dateifreigabekonfiguration. Importieren Sie sie dann mithilfe des folgenden Befehls in eine Variable.

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

5. Bereiten Sie das Anmeldeinformationsobjekt vor, das für die Erstellung der Dateifreigaben auf Ihrem FSx for Windows File Server Server-Dateiserver erforderlich ist, indem Sie eine der folgenden Optionen verwenden.

Verwenden Sie den folgenden Befehl, um das Anmeldeinformationsobjekt interaktiv zu generieren.

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

Verwenden Sie den folgenden Befehl, um das Anmeldeinformationsobjekt mithilfe einer AWS Secrets Manager Ressource zu generieren.

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

6. Migrieren Sie die Dateifreigabekonfiguration mithilfe des folgenden Skripts auf Ihren Amazon FSx-Dateiserver.

```
$FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",  
"ConcurrentUserLimit", "CATimeout", "FolderEnumerationMode", "CachingMode",
```



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

## Migration der DNS-Konfiguration zur Verwendung von Amazon FSx

FSx for Windows File Server bietet einen Standard-DNS-Namen (Domain Name System) für jedes Dateisystem, das Sie für den Zugriff auf die Daten in Ihrem Dateisystem verwenden können. Sie können auch mit einem beliebigen DNS-Namen Ihrer Wahl auf Ihre Dateisysteme zugreifen, indem Sie den alternativen DNS-Namen als DNS-Alias für Ihr Amazon FSx-Dateisystem konfigurieren.

Mit DNS-Aliassen können Sie weiterhin Ihre vorhandenen DNS-Namen verwenden, um auf Daten zuzugreifen, die auf Amazon FSx gespeichert sind, wenn Sie Dateisystemspeicher von lokal zu Amazon FSx migrieren. Dadurch müssen bei der Migration zu Amazon FSx keine Tools oder Anwendungen aktualisiert werden, die Ihre DNS-Namen verwenden. Sie können DNS-Aliase vorhandenen FSx for Windows File Server Server-Dateisystemen zuordnen, wenn Sie neue Dateisysteme erstellen und wenn Sie ein neues Dateisystem aus einer Sicherung erstellen. Sie können einem Dateisystem bis zu 50 DNS-Aliase gleichzeitig zuordnen. Weitere Informationen finden Sie unter [DNS-Aliase verwalten](#).

Ein DNS-Aliasname muss die folgenden Anforderungen erfüllen:

- Muss als vollqualifizierter Domänenname (FQDN) formatiert sein, z. B. `accounting.example.com`
- Kann alphanumerische Zeichen und den Bindestrich (-) enthalten.
- Am Anfang und am Ende darf kein Bindestrich stehen.
- Kann mit einem numerischen Wert beginnen.

Bei DNS-Aliasnamen speichert Amazon FSx alphabetische Zeichen als Kleinbuchstaben (a-z), unabhängig davon, wie Sie sie angeben: als Großbuchstaben, Kleinbuchstaben oder entsprechende Buchstaben in Escape-Zeichen.

Die folgenden Verfahren beschreiben, wie Sie mithilfe der Amazon FSx-Konsole, CLI und API DNS-Aliase mit Ihren vorhandenen FSx for Windows File Server-Dateisystemen verknüpfen. Weitere Informationen zur Zuordnung von DNS-Aliassen beim Erstellen neuer Dateisysteme, einschließlich neuer Dateisysteme aus einem Backup, finden Sie unter [DNS-Aliase mit Dateisystemen verknüpfen](#)

So ordnen Sie DNS-Aliase einem vorhandenen Dateisystem (Konsole) zu

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Windows-Dateisystem aus, dem Sie Ihre DNS-Aliase zuordnen möchten.
3. Wählen Sie auf der Registerkarte Netzwerk und Sicherheit die Option Für DNS-Aliase verwalten aus, um das Dialogfeld DNS-Aliase verwalten zu öffnen.

## 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)** ↻ Disassociate

< 1 > ⚙

| <input type="checkbox"/> | DNS name                                                             |  | Status      |
|--------------------------|----------------------------------------------------------------------|--|-------------|
| <input type="checkbox"/> | financials.corp.example.com <span style="font-size: 0.8em;">📄</span> |  | ✔ Available |

If you associate or disassociate DNS aliases, your file system will experience a temporary loss of availability.

Close

4. Geben Sie im Feld Neue Aliase zuordnen die DNS-Aliase ein, die Sie zuordnen möchten.
5. Wählen Sie Assoziieren, um die Aliase dem Dateisystem hinzuzufügen.

Sie können den Status der Aliase, die Sie gerade verknüpft haben, in der Liste Aktuelle Aliase überwachen. Wenn der Status Verfügbar lautet, ist der Alias dem Dateisystem zugeordnet (ein Vorgang, der bis zu 2,5 Minuten dauern kann).

So verknüpfen Sie DNS-Aliase mit einem vorhandenen Dateisystem (CLI)

- Verwenden Sie den `associate-file-system-aliases` CLI-Befehl oder die [AssociateFileSystemAliases](#) API-Operation, um DNS-Aliase einem vorhandenen Dateisystem zuzuordnen.

Die folgende CLI-Anforderung verknüpft zwei Aliase mit dem angegebenen Dateisystem.

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

Die Antwort zeigt den Status der Aliase, die Amazon FSx dem Dateisystem zuordnet.

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

Um den Status der Aliase zu überwachen, die Sie verknüpfen, verwenden Sie den `describe-file-system-aliases` CLI-Befehl ([DescribeFileSystemAliases](#) entspricht der API-Operation). Wenn `Lifecycle` ein Alias den Wert `AVAILABLE` hat, können Sie damit auf das Dateisystem zugreifen (ein Vorgang, der bis zu 2,5 Minuten dauern kann).

## Umstellung auf Amazon FSx

Um zu Ihrem Dateisystem FSx for Windows File Server zu wechseln, führen Sie die folgenden Schritte aus:

- Bereiten Sie sich auf den Cut-Over vor.
  - Trennen Sie SMB-Clients vorübergehend vom ursprünglichen Dateisystem.
  - Führen Sie eine abschließende Synchronisierung der Datei- und Dateifreigabekonfiguration durch.
- Konfigurieren Sie Service Principal Names (SPNs) für Ihr Amazon FSx-Dateisystem.

- Aktualisieren Sie DNS-CNAME-Einträge so, dass sie auf Ihr Amazon FSx-Dateisystem verweisen.

Die Verfahren zur Durchführung der einzelnen Schritte werden in den folgenden Abschnitten beschrieben.

## Themen

- [Vorbereitung der Umstellung auf Amazon FSx](#)
- [Konfigurieren Sie SPNs für die Kerberos-Authentifizierung](#)
- [Aktualisieren Sie die DNS-CNAME-Einträge für das Amazon FSx-Dateisystem](#)

## Vorbereitung der Umstellung auf Amazon FSx

Um die Umstellung auf Ihr Amazon FSx-Dateisystem vorzubereiten, müssen Sie wie folgt vorgehen:

- Trennen Sie alle Clients, die in das ursprüngliche Dateisystem schreiben.
- Führen Sie eine letzte Dateisynchronisierung mit AWS DataSync oder Robocopy durch. Weitere Informationen finden Sie unter [Migration von vorhandenem Dateispeicher zu FSx for Windows File Server](#).
- Führen Sie eine abschließende Synchronisation der Fileshare-Konfiguration durch. Weitere Informationen finden Sie unter [Migration von Dateifreigabekonfigurationen zu Amazon FSx](#).

## Konfigurieren Sie SPNs für die Kerberos-Authentifizierung

Wir empfehlen Ihnen, bei der Übertragung mit Amazon FSx die Kerberos-basierte Authentifizierung und Verschlüsselung zu verwenden. Kerberos bietet die sicherste Authentifizierung für Clients, die auf Ihr Dateisystem zugreifen. Um die Kerberos-Authentifizierung für Clients zu aktivieren, die über einen DNS-Alias auf Amazon FSx zugreifen, müssen Sie Service Principal Names (SPNs) hinzufügen, die dem DNS-Alias auf dem Active Directory-Computerobjekt Ihres Amazon FSx-Dateisystems entsprechen.

Für die Kerberos-Authentifizierung sind zwei SPNs erforderlich.

```
HOST/alias  
HOST/alias.domain
```

Wenn der Alias beispielsweise lautet `finance.domain.com`, lauten die beiden erforderlichen SPNs wie folgt.

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

Ein SPN kann jeweils nur einem einzigen Active Directory-Computerobjekt zugeordnet werden. Wenn SPNs für den DNS-Namen vorhanden sind, der für das Active Directory-Computerobjekt Ihres ursprünglichen Dateisystems konfiguriert ist, müssen Sie diese löschen, bevor Sie SPNs für Ihr Amazon FSx-Dateisystem erstellen.

Die folgenden Verfahren beschreiben, wie Sie alle vorhandenen SPNs finden, löschen und neue SPNs für das Active Directory-Computerobjekt Ihres Amazon FSx-Dateisystems erstellen.

Um das erforderliche PowerShell Active Directory-Modul zu installieren

1. Melden Sie sich bei einer Windows-Instance an, die mit dem Active Directory verbunden ist, mit dem Ihr Amazon FSx-Dateisystem verknüpft ist.
2. PowerShell Als Administrator öffnen.
3. Installieren Sie das PowerShell Active Directory-Modul mit dem folgenden Befehl.

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

So suchen und löschen Sie vorhandene DNS-Alias-SPNs auf dem Active Directory-Computerobjekt des ursprünglichen Dateisystems

1. Suchen Sie mithilfe der folgenden Befehle nach vorhandenen SPNs. `alias_fqdn` Ersetzen Sie es durch den DNS-Alias, den Sie dem Dateisystem in [Migration der DNS-Konfiguration zur Verwendung von Amazon FSx](#) zugeordnet haben.

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

2. Löschen Sie die vorhandenen HOST-SPNs, die im vorherigen Schritt zurückgegeben wurden, mithilfe des folgenden Beispielskripts.

- *alias\_fqdn* Ersetzen Sie es durch den vollständigen DNS-Alias, den Sie dem Dateisystem in [Migration der DNS-Konfiguration zur Verwendung von Amazon FSx](#) zugeordnet haben.
- *file\_system\_dns\_name* Ersetzen Sie es durch den DNS-Namen des ursprünglichen Dateisystems.

```
## 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. Wiederholen Sie diese Schritte für jeden DNS-Alias, den Sie dem Dateisystem in zugeordnet haben [Migration der DNS-Konfiguration zur Verwendung von Amazon FSx](#).

So legen Sie SPNs für das Active Directory-Computerobjekt Ihres Amazon FSx-Dateisystems fest

1. Legen Sie neue SPNs für Ihr Amazon FSx-Dateisystem fest, indem Sie die folgenden Befehle ausführen.
  - *file\_system\_dns\_name* Ersetzen Sie durch den DNS-Namen, den Amazon FSx dem Dateisystem zugewiesen hat.

Um den DNS-Namen Ihres Dateisystems auf der Amazon FSx-Konsole zu finden, wählen Sie Dateisysteme und wählen Sie Ihr Dateisystem aus. Wählen Sie auf der Seite mit den Dateisystem-Details den Bereich Netzwerk und Sicherheit. Sie können den DNS-Namen auch als Antwort auf den [DescribeFileSystems-API-Vorgang](#) abrufen.

- *alias\_fqdn* Ersetzen Sie ihn durch den vollständigen DNS-Alias, den Sie dem Dateisystem in zugeordnet haben [Migration der DNS-Konfiguration zur Verwendung von Amazon FSx](#).

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_dns_name"
$Alias = "alias_fqdn"
```

```

$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

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

```

### Note

Das Einrichten eines SPN für Ihr Amazon FSx-Dateisystem schlägt fehl, wenn ein SPN für den DNS-Alias im AD für das Computerobjekt des ursprünglichen Dateisystems vorhanden ist. Informationen zum Suchen und Löschen vorhandener SPNs finden Sie unter [So suchen und löschen Sie vorhandene DNS-Alias-SPNs auf dem Active Directory-Computerobjekt des ursprünglichen Dateisystems](#)

2. Stellen Sie mithilfe des folgenden Beispielskripts sicher, dass die neuen SPNs für den DNS-Alias konfiguriert sind. Stellen Sie sicher, dass die Antwort zwei HOST-SPNs enthält, und `HOST/alias`. `HOST/alias_fqdn`

*file\_system\_dns\_name* Ersetzen Sie durch den DNS-Namen, den Amazon FSx Ihrem Dateisystem zugewiesen hat. Um den DNS-Namen Ihres Dateisystems auf der Amazon FSx-Konsole zu finden, wählen Sie Dateisysteme, wählen Sie Ihr Dateisystem und dann auf der Seite mit den Dateisystemdetails den Bereich Netzwerk und Sicherheit.

Sie können den DNS-Namen auch in der Antwort auf den [DescribeFileSystems-API-Vorgang](#) abrufen.

```

## 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. Wiederholen Sie die vorherigen Schritte für jeden DNS-Alias, den Sie dem Dateisystem zugeordnet haben [Migration der DNS-Konfiguration zur Verwendung von Amazon FSx](#).



**Note**

Sie können die Kerberos-Authentifizierung und Verschlüsselung bei der Übertragung von Clients erzwingen, die über DNS-Aliase eine Verbindung zu Ihrem Dateisystem herstellen, indem Sie die folgenden Gruppenrichtlinienobjekte (GPOs) in Ihrem Active Directory einrichten:

- NTLM einschränken: Ausgehender NTLM-Verkehr zu Remoteservern
- NTLM einschränken: Fügen Sie Remoteserver-Ausnahmen für die NTLM-Authentifizierung hinzu

Weitere Informationen finden Sie unter [Erzwingen der Kerberos-Authentifizierung mithilfe von GPOs](#) Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliassen für den Zugriff auf Ihr Dateisystem.

## Aktualisieren Sie die DNS-CNAME-Einträge für das Amazon FSx-Dateisystem

Nachdem Sie SPNs für Ihr Dateisystem ordnungsgemäß konfiguriert haben, können Sie zu Amazon FSx wechseln, indem Sie jeden DNS-Eintrag, der in das ursprüngliche Dateisystem aufgelöst wurde, durch einen DNS-Eintrag ersetzen, der in den Standard-DNS-Namen des Amazon FSx-Dateisystems aufgelöst wird.

Um die erforderlichen Cmdlets zu installieren PowerShell

1. Melden Sie sich bei einer Windows-Instance an, die mit dem Active Directory verbunden ist, mit dem Ihr Amazon FSx-Dateisystem verknüpft ist, als Benutzer, der Mitglied einer Gruppe ist, die über DNS-Verwaltungsberechtigungen verfügt (AWS Delegated Domain Name System Administrators in AWS Managed Microsoft Active Directory und Domain Admins oder eine andere Gruppe, an die Sie DNS-Verwaltungsberechtigungen in Ihrem selbstverwalteten Active Directory delegiert haben)

Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.

2. PowerShell Als Administrator öffnen.

3. Das PowerShell DNS-Servermodul ist erforderlich, um die Anweisungen in diesem Verfahren auszuführen. Installieren Sie es mit dem folgenden Befehl.

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

Um einen vorhandenen DNS-CNAME-Eintrag zu aktualisieren

1. Das folgende Skript aktualisiert alle vorhandenen DNS-CNAME-Einträge für *alias\_fqdn* das Computerobjekt Ihres Amazon FSx-Dateisystems. Wenn keiner gefunden wird, wird ein neuer DNS-CNAME-Eintrag für den DNS-Alias erstellt *alias\_fqdn*, der in den Standard-DNS-Namen für Ihr Amazon FSx-Dateisystem aufgelöst wird.

So führen Sie das Skript aus:

- *alias\_fqdn* Ersetzen Sie ihn durch den DNS-Alias, den Sie dem Dateisystem zugeordnet haben.
- *file\_system\_dns\_name* Ersetzen Sie durch den Standard-DNS-Namen, den Amazon FSx dem Dateisystem zugewiesen hat.

```
$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. Wiederholen Sie den vorherigen Schritt für jeden DNS-Alias, den Sie dem Dateisystem in [Migration der DNS-Konfiguration zur Verwendung von Amazon FSx](#) zugeordnet haben.

# Verwenden von FSx for Windows File Server mit Microsoft SQL Server mit Microsoft SQL Server

Hochverfügbarkeit (HA) Microsoft SQL Server wird in der Regel auf mehreren Datenbankknoten in einem Windows Server Failover Cluster (WSFC) bereitgestellt, wobei jeder Knoten Zugriff auf gemeinsam genutzten Dateispeicher hat. Sie können FSx for Windows File Server als gemeinsam genutzten Speicher für Microsoft SQL Server-Bereitstellungen mit hoher Verfügbarkeit (HA) verwenden: als Speicher für aktive Datendateien und als SMB-Dateifreigabe-Zeuge.

## Note

Derzeit unterstützt Amazon FSx die Microsoft SQL Server IFI-Funktion (Instant File Initialization) nicht.

SSD-Speicher wird für SQL Server empfohlen. SSD-Speicher ist für die leistungsstärksten und latenzempfindlichsten Workloads konzipiert, einschließlich Datenbanken.

Informationen zur Verwendung von Amazon FSx zur Reduzierung der Komplexität und der Kosten für Ihre SQL Server-Hochverfügbarkeitsbereitstellungen finden Sie in den folgenden Beiträgen im AWSStorage Blog:

- [Vereinfachen Sie Ihre Microsoft SQL Server-Hochverfügbarkeitsbereitstellungen mit Amazon FSx for Windows File Server](#)
- [Optimierung der Kosten für Ihre hochverfügbaren SQL Server-Bereitstellungen auf AWS](#)
- [Vereinfachen Sie SQL Server Always-On-Bereitstellungen mit AWS Launch Wizard und Amazon FSx](#)

## Amazon FSx für aktive SQL Server-Datendateien verwenden

Microsoft SQL Server kann mit einer SMB-Dateifreigabe als Speicheroption für aktive Datendateien bereitgestellt werden. Amazon FSx ist optimiert, um gemeinsam genutzten Speicher für SQL Server-Datenbanken bereitzustellen, indem kontinuierlich verfügbare (CA) Dateifreigaben unterstützt werden. Diese Dateifreigaben sind für Anwendungen wie SQL Server konzipiert, die einen unterbrechungsfreien Zugriff auf gemeinsam genutzte Dateidaten erfordern. Sie können zwar CA-

Freigaben auf Single-AZ-Dateisystemen erstellen, es ist jedoch erforderlich, dass Sie CA-Freigaben auf Multi-AZ-Dateisystemen für alle SQL Server-Bereitstellungen verwenden, unabhängig davon, ob HA oder nicht.

## Eine kontinuierlich verfügbare Aktie erstellen

Sie können CA-Freigaben mit der Amazon FSx CLI for Remote Management auf erstellen PowerShell. Um anzugeben, dass es sich bei der Aktie um eine kontinuierlich verfügbare Aktie handelt, verwenden Sie die `New-FSxSmbShare` wobei die `-ContinuouslyAvailable` Option auf gesetzt ist `$True`. Weitere Informationen zum Erstellen einer neuen CA Share finden Sie unter [Eine kontinuierlich verfügbare \(CA-\) Freigabe wird erstellt](#).

## SMB-Timeout-Einstellungen konfigurieren

Wie unter beschrieben [Failover-Prozess für FSx for Windows File Server](#), können Failover und Failback für Multi-AZ zu I/O-Pausen führen, die normalerweise in weniger als 30 Sekunden abgeschlossen sind. Ihre SQL Server-Anwendung reagiert möglicherweise unterschiedlich empfindlich auf Timeout-Einstellungen, je nachdem, wie sie konfiguriert ist.

Sie können das Sitzungs-Timeout für die SMB-Client-Konfiguration anpassen, um sicherzustellen, dass Ihre Anwendung gegen Multi-AZ-Dateisystem-Failover resistent ist. Sie können das Verhalten Ihrer Anwendung bei Failovers testen, indem Sie die Durchsatzkapazität Ihres Dateisystems aktualisieren, wodurch ein automatischer Failover und ein Failback ausgelöst werden.

## Amazon FSx als SMB File Share Witness verwenden

Bei Windows Server-Failoverclusterbereitstellungen wird in der Regel ein SMB-Fileshare-Witness bereitgestellt, um das Quorum der Clusterressourcen aufrechtzuerhalten. Für die gemeinsame Nutzung von Zeugendateien wird nur wenig Speicherplatz für Quoruminformationen benötigt. Amazon FSx-Dateisysteme können als SMB-Fileshare-Witness für Windows Server-Failovercluster-Bereitstellungen verwendet werden.

# Verwenden von FSx for Windows File Server mit Amazon Kendra

Amazon Kendra ist ein hochgenauer und intelligenter Suchdienst. FSx for Windows File Server Server-Dateisysteme können als Datenquellen für Amazon Kendra verwendet werden, sodass Sie Informationen indizieren und intelligent nach Informationen suchen können, die in Ihrem Dateisystem gespeichert sind.

- Weitere Informationen zu Amazon Kendra finden Sie unter [Was ist Amazon Kendra](#) im Amazon Kendra Entwicklerhandbuchaus.
- Weitere Informationen zum Hinzufügen Ihres Dateisystems als Amazon Kendra-Datenquelle finden Sie unter [Erste Schritte mit einer Amazon FSx-Datenquelle \(Konsole\)](#) im Amazon Kendra Entwicklerhandbuchaus.
- Eine Übersicht über Amazon Kendra finden Sie im [Amazon Kendra-Webseite](#)aus.
- Eine Anleitung zur Suche nach Ihrem Dateisystem mit Amazon Kendra finden Sie unter [Suchen Sie sicher unstrukturierte Daten auf Windows-Dateisystemen mit dem Amazon Kendra-Konnektor für Amazon FSx for Windows File Server](#) auf der AWS Machine Learning Learning-Blogaus.

## Dateisystemleistung

Wenn Sie ein FSx für Windows File Server-Dateiserver-Dateisystem als Datenquelle hinzufügen, durchsucht Amazon Kendra die Dateien und Ordner im Dateisystem regelmäßig, um seinen Suchindex zu erstellen und beizubehalten. (Sie können die Synchronisierungsfrequenz auswählen, wenn Sie die Integration einrichten.) Diese Dateizugriffsaktivität von Amazon Kendra verbraucht Dateisystemressourcen, ähnlich wie Aktivitäten Ihrer eigenen Workloads, die auf das Dateisystem zugreifen.

Stellen Sie sicher, dass Ihr Dateisystem mit ausreichenden Ressourcen konfiguriert ist, damit Ihre Workload-Leistung nicht beeinträchtigt wird. Insbesondere wenn Sie planen, eine große Anzahl von Dateien zu indizieren, empfehlen wir die Verwendung eines Dateisystems mit SSD-Speichertyp, das einen höheren maximalen Durchsatz und IOPS-Ebenen für Anfragen bietet, die auf die Speicher-Volumes zugreifen müssen.

Weitere Informationen zum Amazon FSx-Leistungsmodell finden Sie unter [Leistung von FSx for Windows File Server](#)aus.

# Schutz Ihrer Daten durch Backups, Schattenkopien und geplante Replikation

Amazon FSx repliziert nicht nur automatisch die Daten Ihres Dateisystems, um eine hohe Haltbarkeit zu gewährleisten, sondern bietet Ihnen auch die folgenden Optionen, um die auf Ihren Dateisystemen gespeicherten Daten weiter zu schützen:

- Native Amazon FSx-Backups unterstützen Ihre Anforderungen an die Aufbewahrung von Backups und die Einhaltung von Vorschriften innerhalb von Amazon FSx.
- AWS Backup Backups Ihrer Amazon FSx-Dateisysteme sind Teil einer zentralisierten und automatisierten Backup-Lösung für alle AWS Services in der Cloud und vor Ort.
- Windows-Schattenkopien ermöglichen es Ihren Benutzern, Dateiänderungen einfach rückgängig zu machen und Dateiversionen zu vergleichen, indem Dateien auf frühere Versionen wiederhergestellt werden.
- AWS DataSync Die geplante Replikation Ihres Amazon FSx-Dateisystems auf ein zweites Dateisystem bietet Datenschutz und Wiederherstellung.

## Themen

- [Arbeiten mit Backups](#)
- [Schützen Sie Ihre Daten mit Schattenkopien](#)
- [Geplante Replikation mit AWS DataSync](#)

## Arbeiten mit Backups

Mit Amazon FSx sind Backups file-system-consistent, hoch dauerhaft und inkrementell. Jedes Backup enthält alle Informationen, die zum Erstellen eines neuen Dateisystems erforderlich sind, wodurch effektiv ein point-in-time Snapshot des Dateisystems wiederhergestellt wird. Um die Konsistenz des Dateisystems sicherzustellen, verwendet Amazon FSx den Volume Shadow Copy Service (VSS) in Microsoft Windows. Um eine hohe Haltbarkeit zu gewährleisten, speichert Amazon FSx Backups in Amazon Simple Storage Service (Amazon S3).

Amazon-FSx-Backups sind inkrementell, unabhängig davon, ob sie mit dem automatischen täglichen Backup oder der vom Benutzer initiierten Backup-Funktion generiert werden. Das bedeutet, dass nur

die Daten auf dem Dateisystem gespeichert werden, die sich nach der letzten Sicherung geändert haben. Dadurch wird der Zeitaufwand für die Erstellung des Backups minimiert und Speicherkosten eingespart, da keine Daten dupliziert werden.

Irgendwann während des Backup-Prozesses kann die Speicher-I/O kurzzeitig unterbrochen werden, in der Regel für einige Sekunden. Da der VSS-Service alle zwischengespeicherten Schreibvorgänge auf die Festplatte leeren muss, bevor die E/A-Operation fortgesetzt werden kann, kann die Dauer der Pause länger sein, wenn Ihr Workload eine große Anzahl von Schreibvorgängen pro Sekunde () aufweist `DataWriteOperations`. Bei den meisten Endbenutzern und Anwendungen tritt diese E/A-Aussetzung als kurze E/A-Aussetzung auf. Ihre Anwendungen haben je nach Konfiguration möglicherweise eine andere Empfindlichkeit gegenüber Timeout-Einstellungen.

Das Erstellen regelmäßiger Backups für Ihr Dateisystem ist eine bewährte Methode, die die Replikation ergänzt, die Amazon FSx for Windows File Server für Ihr Dateisystem durchführt. Amazon-FSx-Backups unterstützen Ihre Anforderungen an Aufbewahrung und Compliance von Backups. Das Arbeiten mit Amazon-FSx-Backups ist einfach, unabhängig davon, ob es sich um das Erstellen von Backups, das Kopieren eines Backups, das Wiederherstellen eines Dateisystems aus einem Backup oder das Löschen eines Backups handelt. Beachten Sie, dass Sie Tags für dieses spezifische Backup aktivieren und tagbasierte Fakturierungsberichte aktivieren müssen, um die Nutzung für ein einzelnes Dateisystem-Backup anzuzeigen.

## Themen

- [Arbeiten mit automatischen täglichen Backups](#)
- [Arbeiten mit vom Benutzer initiierten Backups](#)
- [Verwenden von AWS Backup mit Amazon FSx](#)
- [Kopieren eines Backups](#)
- [Wiederherstellen von Sicherungen](#)
- [Löschen eines Backups](#)
- [Größe der Backups](#)

## Arbeiten mit automatischen täglichen Backups

Standardmäßig erstellt Amazon FSx eine automatische tägliche Sicherung Ihres Dateisystems. Diese automatischen täglichen Backups erfolgen während des täglichen Backup-Fensters, das beim Erstellen des Dateisystems eingerichtet wurde. Wenn Sie Ihr tägliches Backup-Fenster wählen,

empfehlen wir Ihnen, eine bequeme Uhrzeit auszuwählen. Diese Zeit liegt idealerweise außerhalb der normalen Betriebszeiten für die Anwendungen, die das Dateisystem verwenden.

Automatische tägliche Backups werden für einen bestimmten Zeitraum aufbewahrt, der als Aufbewahrungszeitraum bezeichnet wird. Wenn Sie ein Dateisystem in der Amazon-FSx-Konsole erstellen, beträgt der standardmäßige automatische tägliche Aufbewahrungszeitraum für Backups 30 Tage. Der Standardaufbewahrungszeitraum ist in der Amazon-FSx-API und -CLI unterschiedlich. Sie können den Aufbewahrungszeitraum auf einen Wert zwischen 0 und 90 Tagen festlegen. Wenn Sie den Aufbewahrungszeitraum auf 0 (Null) Tage festlegen, werden automatische tägliche Backups deaktiviert. Automatische tägliche Backups werden gelöscht, wenn das Dateisystem gelöscht wird.

#### Note

Wenn Sie den Aufbewahrungszeitraum auf 0 Tage festlegen, wird Ihr Dateisystem nie automatisch gesichert. Wir empfehlen dringend, automatische tägliche Backups für Dateisysteme zu verwenden, denen eine beliebige kritische Funktionalität zugeordnet ist.

Sie können die AWS CLI oder eines der AWS SDKs verwenden, um das Backup-Fenster und den Aufbewahrungszeitraum für Backups für Ihre Dateisysteme zu ändern. Verwenden Sie die [UpdateFileSystem](#) -API-Operation oder den `-update-file-system` CLI-Befehl. Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 3: Aktualisieren Sie ein vorhandenes -Dateisystem](#).

## Arbeiten mit vom Benutzer initiierten Backups

Mit Amazon FSx können Sie jederzeit manuell Backups Ihrer Dateisysteme erstellen. Sie können dies über die Amazon-FSx-Konsole, die API oder die AWS Command Line Interface () tun AWS CLI. Ihre vom Benutzer initiierten Backups von Amazon-FSx-Dateisystemen laufen nie ab und sind so lange verfügbar, wie Sie sie behalten möchten. Vom Benutzer initiierte Backups werden auch nach dem Löschen des gesicherten Dateisystems aufbewahrt. Sie können vom Benutzer initiierte Backups nur mithilfe der Amazon-FSx-Konsole, API oder CLI löschen. Sie werden nie automatisch von Amazon FSx gelöscht. Weitere Informationen finden Sie unter [Löschen eines Backups](#).

Wenn eine Sicherung initiiert wird, während das Dateisystem geändert wird (z. B. während einer Aktualisierung der Durchsatzkapazität oder während der Dateisystemwartung), wird die Sicherungsanforderung in die Warteschlange gestellt und fortgesetzt, wenn die Aktivität abgeschlossen ist.



## Erstellen von vom Benutzer initiierten Backups

Das folgende Verfahren führt Sie durch die Erstellung eines vom Benutzer initiierten Backups in der Amazon-FSx-Konsole für ein vorhandenes Dateisystem.

So erstellen Sie ein vom Benutzer initiiertes Dateisystem-Backup

1. Öffnen Sie die Amazon-FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Dashboard der Konsole den Namen des Dateisystems aus, das Sie sichern möchten.
3. Wählen Sie unter Aktionen die Option Backup erstellen aus.
4. Geben Sie im sich öffnenden Dialogfeld Backup erstellen einen Namen für Ihr Backup ein. Backup-Namen dürfen maximal 256 Unicode-Zeichen enthalten, einschließlich Buchstaben, Leerzeichen, Zahlen und Sonderzeichen . + - = \_ : /
5. Wählen Sie Create backup (Backup erstellen).

Sie haben jetzt Ihr Dateisystem-Backup erstellt. Sie finden eine Tabelle all Ihrer Backups in der Amazon-FSx-Konsole, indem Sie in der linken Navigation Backups auswählen. Sie können nach dem Namen suchen, den Sie Ihrem Backup gegeben haben, und die Tabellenfilter so filtern, dass nur übereinstimmende Ergebnisse angezeigt werden.

Wenn Sie ein vom Benutzer initiiertes Backup wie in diesem Verfahren beschrieben erstellen, hat es den Typ und den CREATING Status USER\_INITIATED, bis es vollständig verfügbar ist.

## Verwenden von AWS Backup mit Amazon FSx

AWS Backup ist eine einfache und kostengünstige Möglichkeit, Ihre Daten durch Backup Ihrer Amazon-FSx-Dateisysteme zu schützen. AWS Backup ist ein einheitlicher Backup-Service, der die Erstellung vereinfachen soll. Kopieren, Wiederherstellung, und Löschen von Backups, Durch die Bereitstellung verbesserter Berichte und Prüfungen AWS Backup wird es einfacher, eine zentrale Backup-Strategie für rechtliche Vorschriften zu entwickeln. regulatorische, und Professional Compliance. macht AWS Backup auch Ihre AWS Speicher-Volumes geschützt. -Datenbanken, - und -Dateisysteme vereinfachen die Bereitstellung eines zentralen Orts, an dem Sie Folgendes tun können:

- Konfigurieren und prüfen Sie die AWS Ressourcen, die Sie sichern möchten.
- Automatisieren geplanter Sicherungen

- Festlegen von Aufbewahrungsrichtlinien
- Kopieren Sie Backups regions- AWS und AWS kontenübergreifend.
- Überwachen Sie alle letzten Sicherungs-, Kopier- und Wiederherstellungsaktivitäten.

AWS Backup verwendet die integrierte Backup-Funktionalität von Amazon FSx . Von der AWS Backup Konsole erstellte Backups haben das gleiche Maß an Dateisystemkonsistenz und -leistung und dieselben Wiederherstellungsoptionen wie Backups, die über die Amazon-FSx-Konsole erstellt wurden. Von erstellte Backups AWS Backup sind inkrementell im Vergleich zu anderen Amazon-FSx-Backups, die Sie erstellen, entweder vom Benutzer initiiert oder automatisch.

Wenn Sie verwenden, AWS Backup um diese Backups zu verwalten, erhalten Sie zusätzliche Funktionen, z. B. unbegrenzte Aufbewahrungsoptionen und die Möglichkeit, geplante Backups so oft wie jede Stunde zu erstellen. Darüber hinaus AWS Backup behält Ihre unveränderlichen Backups auch nach dem Löschen des Quelldateisystems bei. Dies schützt vor versehentlichem oder böswilligem Löschen.

Von erstellte Backups AWS Backup gelten als vom Benutzer initiierte Backups und werden auf das vom Benutzer initiierte Backup-Kontingent für Amazon FSx angerechnet. Sie können Backups von AWS Backup in der Amazon-FSx-Konsole, CLI und API anzeigen und wiederherstellen. Sie können jedoch keine Backups löschen, die von AWS Backup in der Amazon-FSx-Konsole, CLI oder API erstellt wurden. Weitere Informationen zur Verwendung von AWS Backup zum Sichern Ihrer Amazon-FSx-Dateisysteme finden Sie unter [Arbeiten mit Amazon-FSx-Dateisystemen](#) im AWS Backup - Entwicklerhandbuch.

## Kopieren eines Backups

Sie können Amazon FSx verwenden, um Backups innerhalb desselben AWS Kontos manuell in eine andere AWS Region (regionsübergreifende Kopien) oder innerhalb derselben AWS Region (regionsübergreifende Kopien) zu kopieren. Sie können regionsübergreifende Kopien nur innerhalb derselben AWS Partition erstellen. Sie können vom Benutzer initiierte Backup-Kopien mithilfe der Amazon-FSx-Konsole AWS CLI oder der API erstellen. Wenn Sie eine vom Benutzer initiierte Sicherungskopie erstellen, hat sie den Typ `USER_INITIATED`.

Sie können auch verwenden AWS Backup , um Backups über AWS Regionen und AWS Konten hinweg zu kopieren. AWS Backup ist ein vollständig verwalteter Backup-Management-Service, der eine zentrale Schnittstelle für richtlinienbasierte Backup-Pläne bietet. Mit der kontoübergreifenden Verwaltung können Sie automatisch Backup-Richtlinien verwenden, um Backup-Pläne auf die Konten in Ihrer Organisation anzuwenden.

Regionsübergreifende Backup-Kopien sind besonders nützlich für die regionsübergreifende Notfallwiederherstellung. Sie erstellen Backups und kopieren sie in eine andere AWS Region, sodass Sie im Notfall in der primären AWS Region die Verfügbarkeit in der anderen AWS Region schnell wiederherstellen können. Sie können auch Sicherungskopien verwenden, um Ihren Dateidatensatz in eine andere AWS Region oder innerhalb derselben AWS Region zu klonen. Sie erstellen Sicherungskopien innerhalb desselben AWS Kontos (regionsübergreifend oder regionsübergreifend), indem Sie die Amazon-FSx-Konsole AWS CLI oder die Amazon-FSx-API verwenden. Sie können auch verwenden, [AWS Backup](#) um Sicherungskopien durchzuführen, entweder auf Abruf oder richtlinienbasiert.

Kontoübergreifende Backup-Kopien sind nützlich, um Ihre gesetzlichen Compliance-Anforderungen zu erfüllen und Backups auf ein isoliertes Konto zu kopieren. Sie bieten auch eine zusätzliche Datenschutzebene, um versehentliches oder böswilliges Löschen von Backups, den Verlust von Anmeldeinformationen oder die Kompromittierung von AWS KMS Schlüsseln zu verhindern. Kontoübergreifende Backups unterstützen Fan-In (Kopieren von Backups aus mehreren Primärkonten in ein isoliertes Backup-Kopierkonto) und Fan-Out (Kopieren von Backups aus einem Primärkonto in mehrere isolierte Backup-Kopierkonten).

Sie können kontoübergreifende Backup-Kopien erstellen, indem Sie AWS Backup mit - AWS Organizations Unterstützung verwenden. Kontogrenzen für kontoübergreifende Kopien werden durch AWS Organizations Richtlinien definiert. Weitere Informationen zur Verwendung von AWS Backup zum Erstellen von kontoübergreifenden Backup-Kopien finden Sie unter [Erstellen von Backup-Kopien über AWS-Konten](#) hinweg im AWS Backup -Entwicklerhandbuch.

## Einschränkungen für Backup-Kopien

Die folgenden Einschränkungen gelten beim Kopieren von Backups:

- Regionsübergreifende Backup-Kopien werden nur zwischen zwei kommerziellen AWS Regionen unterstützt, zwischen den Regionen China (Peking) und China (Ningxia) sowie zwischen den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (USA-West), jedoch nicht über diese Gruppen von Regionen hinweg.
- Regionsübergreifende Backup-Kopien werden in Opt-in-Regionen nicht unterstützt.
- Sie können regionsinterne Backup-Kopien in jeder - AWS Region erstellen.
- Das Quell-Backup muss den Status haben, AVAILABLE bevor Sie es kopieren können.
- Sie können eine Quellsicherung nicht löschen, wenn sie kopiert wird. Es kann eine kurze Verzögerung zwischen dem Zeitpunkt geben, an dem das Ziel-Backup verfügbar ist, und

dem Zeitpunkt, an dem Sie das Quell-Backup löschen dürfen. Sie sollten diese Verzögerung berücksichtigen, wenn Sie erneut versuchen, eine Quellsicherung zu löschen.

- Sie können pro Konto bis zu fünf Backup-Kopieranforderungen an eine einzelne AWS Zielregion ausführen.

## Berechtigungen für regionsübergreifende Backup-Kopien

Sie verwenden eine IAM-Richtlinienanweisung, um Berechtigungen zum Ausführen eines Sicherungskopiervorgangs zu erteilen. Um mit der AWS Quellregion zu kommunizieren, um eine regionsübergreifende Sicherungskopie anzufordern, muss der Anforderer (IAM-Rolle oder IAM-Benutzer) Zugriff auf die Quellsicherung und die AWS Quellregion haben.

Sie verwenden die -Richtlinie, um Berechtigungen für die -CopyBackupAktion für den Backup-Kopiervorgang zu erteilen. Sie geben die Aktion im Action Feld der Richtlinie und den Ressourcenwert im Resource Feld der Richtlinie an, wie im folgenden Beispiel.

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

Weitere Informationen zu IAM-Richtlinien finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.

## Vollständige und inkrementelle Kopien

Wenn Sie eine Sicherung in eine andere AWS Zielregion oder ein anderes AWS Zielkonto als die Quellsicherung kopieren, ist die erste Kopie eine vollständige Sicherungskopie, auch wenn Sie denselben KMS-Schlüssel verwenden, um sowohl Quell- als auch Zielkopien der Sicherung zu verschlüsseln.

Nach der ersten Sicherungskopie sind alle nachfolgenden Sicherungskopien in dieselbe Zielregion innerhalb desselben AWS Kontos inkrementell, vorausgesetzt, Sie haben nicht alle zuvor kopierten

Sicherungen in dieser Region gelöscht und denselben AWS KMS Schlüssel verwendet. Wenn eine der Bedingungen nicht erfüllt ist, führt der Kopiervorgang zu einer vollständigen (nicht inkrementellen) Sicherungskopie.

So kopieren Sie ein Backup innerhalb desselben Kontos (regionsübergreifend oder regionsübergreifend) mithilfe der Konsole

1. Öffnen Sie die Amazon-FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Navigationsbereich Sicherungen aus.
3. Wählen Sie in der Tabelle Backups das Backup aus, das Sie kopieren möchten, und wählen Sie dann Backup kopieren aus.
4. Gehen Sie im Abschnitt Settings (Einstellungen) wie folgt vor:
  - Wählen Sie in der Liste Zielregion eine AWS Zielregion aus, in die die Sicherung kopiert werden soll. Das Ziel kann sich in einer anderen AWS Region (regionsübergreifende Kopie) oder innerhalb derselben AWS Region (regionsübergreifende Kopie) befinden.
  - (Optional) Wählen Sie Tags kopieren aus, um Tags aus der Quellsicherung in die Zielsicherung zu kopieren. Wenn Sie in Schritt 6 Tags kopieren auswählen und auch Tags hinzufügen, werden alle Tags zusammengeführt.
5. Wählen Sie für Verschlüsselung den AWS KMS Verschlüsselungsschlüssel aus, um das kopierte Backup zu verschlüsseln.
6. Geben Sie für Tags – optional einen Schlüssel und einen Wert ein, um Tags für Ihre kopierte Sicherung hinzuzufügen. Wenn Sie hier Tags hinzufügen und in Schritt 4 auch Tags kopieren ausgewählt haben, werden alle Tags zusammengeführt.
7. Klicken Sie auf Copy backup (Backup kopieren).

Ihr Backup wird innerhalb desselben AWS Kontos in die ausgewählte AWS Region kopiert.

So kopieren Sie ein Backup innerhalb desselben Kontos (regionsübergreifend oder regionsübergreifend) mithilfe der CLI

- Verwenden Sie den copy-backup CLI-Befehl oder die [CopyBackup](#) API-Operation , um ein Backup innerhalb desselben AWS Kontos zu kopieren, entweder über eine - AWS Region oder innerhalb einer - AWS Region.

Der folgende Befehl kopiert ein Backup mit der ID backup-0abc123456789cba7 aus der us-east-1 Region .

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

Die Antwort zeigt die Beschreibung der kopierten Sicherung.

Sie können Ihre Backups auf der Amazon-FSx-Konsole oder programmgesteuert mit dem `describe-backups` CLI-Befehl oder der [DescribeBackups](#) API-Operation anzeigen.

## Wiederherstellen von Sicherungen

Sie können ein verfügbares Backup verwenden, um ein neues Dateisystem zu erstellen, wodurch effektiv ein point-in-time Snapshot eines anderen Dateisystems wiederhergestellt wird. Sie können ein Backup mithilfe der Konsole AWS CLI oder eines der AWS SDKs wiederherstellen. Das Wiederherstellen eines Backups in einem neuen Dateisystem dauert genauso lange wie das Erstellen eines neuen Dateisystems. Die aus dem Backup wiederhergestellten Daten werden fazygeladen in das Dateisystem geladen. Während dieser Zeit kommt es zu einer etwas höheren Latenz.

Um sicherzustellen, dass Benutzer weiterhin auf das wiederhergestellte Dateisystem zugreifen können, stellen Sie sicher, dass die dem wiederhergestellten Dateisystem zugeordnete Active-Directory-Domain mit der des ursprünglichen Dateisystems übereinstimmt oder von der AD-Domain des ursprünglichen Dateisystems vertraut wird. Weitere Informationen zu Active Directory finden Sie unter [Arbeiten mit Microsoft Active Directory in FSx for Windows File Server](#).

Das folgende Verfahren führt Sie durch die Wiederherstellung eines Backups mithilfe der Konsole, um ein neues Dateisystem zu erstellen.

### Note

Sie können Ihr Backup nur in einem Dateisystem mit demselben Bereitstellungstyp und derselben Speicherkapazität wie das Original wiederherstellen. Sie können die Speicherkapazität Ihres wiederhergestellten Dateisystems erhöhen, sobald sie verfügbar ist. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#).

So stellen Sie ein Dateisystem aus einem Backup wieder her

1. Öffnen Sie die Amazon-FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.

2. Wählen Sie im Dashboard der Konsole in der linken Navigation die Option Backups aus.
3. Wählen Sie in der Tabelle Backups das Backup aus, das Sie wiederherstellen möchten, und wählen Sie dann Backup wiederherstellen aus.

Dadurch wird der Dateisystem-Erstellungsassistent geöffnet. Dieser Assistent ist identisch mit dem standardmäßigen Assistenten zur Erstellung des Dateisystems, mit der Ausnahme, dass Bereitstellungstyp und Speicherkapazität bereits festgelegt sind und nicht geändert werden können. Sie können jedoch die Durchsatzkapazität, die zugehörige VPC und andere Einstellungen sowie den Speichertyp ändern. Der Speichertyp ist standardmäßig auf SSD festgelegt, aber Sie können ihn unter den folgenden Bedingungen auf HDD ändern:

- Der Bereitstellungstyp des Dateisystems ist Multi-AZ oder Single-AZ 2.
  - Die Speicherkapazität beträgt mindestens 2 000 GiB.
4. Schließen Sie den Assistenten wie beim Erstellen eines neuen Dateisystems ab.
  5. Wählen Sie Review and create.
  6. Überprüfen Sie die Einstellungen, die Sie für Ihr Amazon-FSx-Dateisystem ausgewählt haben, und wählen Sie dann Dateisystem erstellen aus.

Sie haben aus einem Backup wiederhergestellt und jetzt wird ein neues Dateisystem erstellt. Wenn sich der Status in ändertAVAILABLE, können Sie das Dateisystem wie gewohnt verwenden.

## Löschen eines Backups

Das Löschen eines Backups ist eine permanente, nicht wiederherstellbare Aktion. Alle Daten in einem gelöschten Backup werden ebenfalls gelöscht. Löschen Sie ein Backup nur, wenn Sie sicher sind, dass Sie dieses Backup in Zukunft nicht mehr benötigen. Sie können keine Backups löschen AWS Backup, die von erstellt wurden, die den Typ AWS Backup haben, in der Amazon-FSx-Konsole, CLI oder API.

So löschen Sie ein Backup

1. Öffnen Sie die Amazon-FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Dashboard der Konsole in der linken Navigation die Option Backups aus.
3. Wählen Sie das Backup, das Sie löschen möchten, aus der Tabelle Backups und dann Backup löschen aus.

4. Vergewissern Sie sich im sich öffnenden Dialogfeld Backups löschen, dass die ID des Backups das Backup identifiziert, das Sie löschen möchten.
5. Vergewissern Sie sich, dass das Kontrollkästchen für das Backup aktiviert ist, das Sie löschen möchten.
6. Wählen Sie Backups löschen aus.

Ihr Backup und alle enthaltenen Daten werden jetzt dauerhaft und nicht wiederherstellbar gelöscht.

## Größe der Backups

Die Größe der Backups wird anhand des verwendeten Speichers im Dateisystem und nicht anhand der gesamten bereitgestellten Speicherkapazität bestimmt. Die Größe Ihrer Backups hängt von der genutzten Speicherkapazität sowie der Datenmenge ab, die auf Ihrem Dateisystem abwandert wird. Je nachdem, wie Ihre Daten auf die Speicher-Volumes des Dateisystems verteilt sind und wie oft sie sich ändern, kann Ihre gesamte Backup-Nutzung größer oder kleiner sein als Ihre genutzte Speicherkapazität. Wenn Sie ein Backup löschen, werden nur die für dieses Backup eindeutigen Daten entfernt. Mit Amazon FSx gelten die Speichereffizienzeinsparungen durch Deduplizierung und Komprimierung nicht nur für Ihren primären SSD/HDD-Speicher, sondern auch für Backups.

Um file-system-consistent, dauerhafte und inkrementelle Backups bereitzustellen, sichert Amazon FSx Daten auf Blockebene. Die Daten auf den Speicher-Volumes des Dateisystems können je nach Muster, in das sie geschrieben oder überschrieben wurden, in mehreren Blöcken gespeichert werden. Daher stimmt die Gesamtgröße der Backup-Nutzung möglicherweise nicht mit der genauen Größe der Dateien und Verzeichnisse im Dateisystem überein.

Ihre gesamte Backup-Nutzung und -Kosten finden Sie im AWS Billing Dashboard oder AWS Cost Management Console. Um die Größe und die Kosten einzelner Dateisystem-Backups zu berechnen, können Sie einzelne Backups markieren und tagbasierte Fakturierungsberichte aktivieren.

## Schützen Sie Ihre Daten mit Schattenkopien

Eine Microsoft Windows-Schattenkopie ist eine Momentaufnahme eines Windows-Dateisystems zu einem bestimmten Zeitpunkt. Wenn Schattenkopien aktiviert sind, können Benutzer gelöschte oder geänderte Dateien, die im Netzwerk gespeichert sind, schnell wiederherstellen und Dateiversionen vergleichen. Speicheradministratoren können mithilfe von PowerShell Windows-Befehlen auf einfache Weise planen, dass Schattenkopien regelmäßig erstellt werden.



Schattenkopien werden zusammen mit den Daten Ihres Dateisystems gespeichert und verbrauchen nur für die geänderten Teile der Dateien Speicherkapazität des Dateisystems. Alle in Ihrem Dateisystem gespeicherten Schattenkopien sind in Dateisystem-Backups enthalten.

#### Note

Schattenkopien sind auf FSx for Windows File Server standardmäßig nicht aktiviert. Um die Daten in Ihrem Dateisystem mithilfe von Schattenkopien zu schützen, müssen Sie Schattenkopien aktivieren und einen Zeitplan für Schattenkopien auf Ihrem Dateisystem einrichten. Weitere Informationen finden Sie unter [Konfiguration von Schattenkopien für die Verwendung des Standardspeichers und des Standardzeitplans](#).

#### Warning

Schattenkopien sind kein Ersatz für Backups. Wenn Sie Schattenkopien aktivieren, stellen Sie sicher, dass Sie weiterhin regelmäßige Backups durchführen.

## Themen

- [Bewährte Methoden bei der Verwendung von Schattenkopien](#)
- [Schattenkopien einrichten](#)
- [Konfiguration von Schattenkopien für die Verwendung des Standardspeichers und des Standardzeitplans](#)
- [Einzelne Dateien und Ordner wiederherstellen](#)
- [Einstellung der maximalen Speichermenge für Schattenkopien](#)
- [Ihren Schattenkopie-Speicher anzeigen](#)
- [Löschen des Schattenkopie-Speichers, des Zeitplans und aller Schattenkopien](#)
- [Einen benutzerdefinierten Zeitplan für Schattenkopien erstellen](#)
- [Ihren Schattenkopie-Zeitplan anzeigen](#)
- [Löschen eines Schattenkopie-Zeitplans](#)
- [Eine Schattenkopie erstellen](#)
- [Vorhandene Schattenkopien anzeigen](#)

- [Löschen von Schattenkopien](#)

## Bewährte Methoden bei der Verwendung von Schattenkopien

Sie können Schattenkopien für Ihr Dateisystem aktivieren, damit Endbenutzer einzelne Dateien oder Ordner aus einem früheren Snapshot im Windows-Datei-Explorer anzeigen und wiederherstellen können. Amazon FSx verwendet die Schattenkopie-Funktion, die von Microsoft Windows Server bereitgestellt wird. Verwenden Sie diese bewährten Methoden für Schattenkopien:

- Stellen Sie sicher, dass Ihr Dateisystem über ausreichende Leistungsressourcen verfügt: Microsoft Windows verwendet standardmäßig eine copy-on-write Methode, um Änderungen seit dem letzten Schattenkopiepunkt aufzuzeichnen, und diese copy-on-write Aktivität kann zu bis zu drei I/O-Vorgängen für jeden Schreibvorgang führen.
- Verwenden Sie SSD-Speicher und erhöhen Sie die Durchsatzkapazität: Da Windows für die Verwaltung von Schattenkopien ein hohes Maß an I/O-Leistung benötigt, empfehlen wir, SSD-Speicher zu verwenden und die Durchsatzkapazität auf einen Wert zu erhöhen, der dem Dreifachen der erwarteten Arbeitslast entspricht. Auf diese Weise können Sie sicherstellen, dass Ihr Dateisystem über genügend Ressourcen verfügt, um Probleme wie das ungewollte Löschen von Schattenkopien zu vermeiden.
- Behalten Sie nur die Anzahl der Schattenkopien bei, die Sie benötigen: Wenn Sie über eine große Anzahl von Schattenkopien verfügen — z. B. mehr als 64 der neuesten Schattenkopien — oder Schattenkopien, die eine große Menge an Speicherplatz (im TB-Bereich) auf einem einzigen Dateisystem belegen, können Prozesse wie Failover und Failback etwas mehr Zeit in Anspruch nehmen. Dies ist darauf zurückzuführen, dass FSx für Windows Konsistenzprüfungen auf dem Schattenkopiespeicher durchführen muss. Möglicherweise kommt es auch zu einer höheren Latenz bei I/O-Vorgängen, da FSx for Windows copy-on-write Aktivitäten ausführen und gleichzeitig die Schattenkopien beibehalten muss. Um die Verfügbarkeit und die Leistungseinbußen durch Schattenkopien zu minimieren, löschen Sie ungenutzte Schattenkopien manuell oder konfigurieren Sie Skripts so, dass alte Schattenkopien in Ihrem Dateisystem automatisch gelöscht werden.

### Note

Bei [Failover-Ereignissen](#) für Multi-AZ-Dateisysteme führt FSx for Windows eine Konsistenzprüfung durch, bei der der Schattenkopiespeicher auf Ihrem Dateisystem gescannt werden muss, bevor der neue aktive Dateiserver online geht. Die Dauer der Konsistenzprüfung hängt von der Anzahl der Schattenkopien in Ihrem Dateisystem

sowie vom belegten Speicherplatz ab. Um verzögerte Failover- und Failback-Ereignisse zu vermeiden, empfehlen wir, weniger als 64 Schattenkopien auf Ihrem Dateisystem zu verwalten und die folgenden Schritte zu befolgen, um Ihre ältesten Schattenkopien regelmäßig zu überwachen und zu löschen.

## Schattenkopien einrichten

Sie aktivieren und planen regelmäßige Schattenkopien auf Ihrem Dateisystem mithilfe von PowerShell Windows-Befehlen, die von Amazon FSx definiert wurden. Die folgenden drei Haupteinstellungen bei der Konfiguration von Schattenkopien auf Ihrem Dateisystem FSx for Windows File Server:

- Einstellung der maximalen Speichermenge, die Schattenkopien auf Ihrem Dateisystem belegen können
- (Optional) Einstellung der maximalen Anzahl von Schattenkopien, die in Ihrem Dateisystem gespeichert werden können. Der Standardwert ist 20.
- (Optional) Festlegung eines Zeitplans, der die Zeiten und Intervalle für die Erstellung von Schattenkopien definiert, z. B. täglich, wöchentlich und monatlich

Sie können zu jedem Zeitpunkt maximal 500 Schattenkopien pro Dateisystem speichern. Wir empfehlen jedoch, weniger als 64 Schattenkopien gleichzeitig zu verwalten, um Verfügbarkeit und Leistung sicherzustellen. Wenn Sie dieses Limit erreichen, ersetzt die nächste Schattenkopie, die Sie erstellen, die älteste Schattenkopie. In ähnlicher Weise werden, wenn die maximale Speichermenge für Schattenkopien erreicht ist, eine oder mehrere der ältesten Schattenkopien gelöscht, um ausreichend Speicherplatz für die nächste Schattenkopie zu schaffen.

Informationen darüber, wie Sie mithilfe der Amazon FSx-Standardinstellungen schnell regelmäßige Schattenkopien aktivieren und planen können, finden Sie unter [Konfiguration von Schattenkopien für die Verwendung des Standardspeichers und des Standardzeitplans](#).

## Überlegungen zur Zuweisung von Schattenkopie-Speicher

Eine Schattenkopie ist eine Kopie auf Blockebene von Dateiänderungen, die seit der letzten Schattenkopie vorgenommen wurden. Die gesamte Datei wird nicht kopiert, sondern nur die Änderungen. Daher beanspruchen frühere Versionen von Dateien in der Regel nicht so viel Speicherplatz wie die aktuelle Datei. Die Menge an Speicherplatz, die für Änderungen

verwendet wird, kann je nach Arbeitslast variieren. Wenn eine Datei geändert wird, hängt der von Schattenkopien verwendete Speicherplatz von Ihrer Arbeitslast ab. Wenn Sie festlegen, wie viel Speicherplatz für Schattenkopien zugewiesen werden soll, sollten Sie die Nutzungsmuster des Dateisystems Ihres Workloads berücksichtigen.

Wenn Sie Schattenkopien aktivieren, können Sie die maximale Speichermenge angeben, die Schattenkopien im Dateisystem belegen können. Das Standardlimit liegt bei 10 Prozent Ihres Dateisystems. Wir empfehlen Ihnen, das Limit zu erhöhen, wenn Ihre Benutzer häufig Dateien hinzufügen oder ändern. Wenn das Limit zu klein eingestellt wird, können die ältesten Schattenkopien häufiger gelöscht werden, als Benutzer vielleicht erwarten.

Sie können den Schattenkopie-Speicher auf unbegrenzt () `Set-FsxShadowStorage -Maxsize "UNBOUNDED"` festlegen. Eine unbegrenzte Konfiguration kann jedoch dazu führen, dass eine große Anzahl von Schattenkopien Ihren Dateisystemspeicher beansprucht. Dies kann dazu führen, dass nicht genügend Speicherkapazität für Ihre Workloads zur Verfügung steht. Wenn Sie einen unbegrenzten Speicherplatz festlegen, stellen Sie sicher, dass Sie Ihre Speicherkapazität skalieren, sobald die Grenzwerte für Schattenkopien erreicht sind. Informationen zur Konfiguration Ihres Schattenkopie-Speichers auf eine bestimmte Größe oder als unbegrenzt finden Sie unter [Einstellung der maximalen Speichermenge für Schattenkopien](#)

Nachdem Sie Schattenkopien aktiviert haben, können Sie überwachen, wie viel Speicherplatz die Schattenkopien belegen. Weitere Informationen finden Sie unter [Ihren Schattenkopie-Speicher anzeigen](#).

## Überlegungen bei der Festlegung der maximalen Anzahl von Schattenkopien

Wenn Sie Schattenkopien aktivieren, können Sie die maximale Anzahl von Schattenkopien angeben, die im Dateisystem gespeichert werden. Das Standardlimit liegt bei 20, und um die Verfügbarkeit und die Leistungsbeeinträchtigung durch Schattenkopien zu minimieren, empfiehlt Microsoft, die maximale Anzahl von Schattenkopien auf weniger als 64 zu konfigurieren. Da Windows für die Verwaltung von Schattenkopien ein hohes Maß an I/O-Leistung benötigt, empfehlen wir, SSD-Speicher zu verwenden und die Durchsatzkapazität auf einen Wert zu erhöhen, der dem Dreifachen der erwarteten Arbeitslast entspricht. Dadurch wird sichergestellt, dass Ihr Dateisystem über genügend Ressourcen verfügt, um Probleme wie das ungewollte Löschen von Schattenkopien zu vermeiden.

Sie können die maximale Anzahl von Schattenkopien auf bis zu 500 festlegen. Wenn Sie jedoch über eine große Anzahl von Schattenkopien oder Schattenkopien verfügen, die eine große

Menge an Speicherplatz (im TB-Bereich) auf einem einzigen Dateisystem belegen, können Prozesse wie Failover und Failback länger dauern als erwartet. Das liegt daran, dass Windows Konsistenzprüfungen für den Schattenkopiespeicher durchführen muss. Möglicherweise kommt es auch zu einer höheren Latenz bei I/O-Vorgängen, da Windows copy-on-write Aktivitäten ausführen und gleichzeitig die Schattenkopien beibehalten muss.

## Dateisystemempfehlungen für Schattenkopien

Im Folgenden finden Sie Dateisystemempfehlungen für die Verwendung von Schattenkopien.

- Stellen Sie sicher, dass Sie in Ihrem Dateisystem ausreichend Leistungskapazität für Ihre Workload-Anforderungen bereitstellen. Amazon FSx bietet die Shadow Copies-Funktion, wie sie von Microsoft Windows Server bereitgestellt wird. Microsoft Windows verwendet standardmäßig eine copy-on-write Methode zum Aufzeichnen der Änderungen seit dem letzten Schattenkopiepunkt, und diese copy-on-write Aktivität kann zu bis zu drei I/O-Vorgängen für jeden Schreibvorgang einer Datei führen. Wenn Windows nicht in der Lage ist, mit der eingehenden Rate an I/O-Vorgängen pro Sekunde Schritt zu halten, kann dies dazu führen, dass alle Schattenkopien gelöscht werden, da es die Schattenkopien nicht mehr verwalten kann copy-on-write. Daher ist es wichtig, dass Sie ausreichend I/O-Leistungskapazität für Ihre Workload-Anforderungen in Ihrem Dateisystem bereitstellen (sowohl die Dimension der Durchsatzkapazität, die die I/O-Leistung des Dateiservers bestimmt, als auch der Speichertyp und die Kapazität, die die Speicher-I/O-Leistung bestimmen).
- Wir empfehlen generell, Dateisysteme zu verwenden, die mit SSD-Speicher konfiguriert sind, anstatt HDD-Speicher zu verwenden, wenn Sie Schattenkopien aktivieren, da Windows eine höhere I/O-Leistung für die Verwaltung von Schattenkopien verbraucht und Festplattenspeicher eine geringere Leistungskapazität für I/O-Operationen bietet.
- Ihr Dateisystem sollte zusätzlich zu der konfigurierten maximalen Speichermenge für Schattenkopien über mindestens 320 MB freien Speicherplatz verfügen (MaxSpace). Wenn Sie beispielsweise 5 GB MaxSpace Schattenkopien zugewiesen haben, sollte Ihr Dateisystem zusätzlich zu den 5 GB immer über mindestens 320 MB freien Speicherplatz verfügenMaxSpace.

### Warning

Achten Sie bei der Konfiguration Ihres Schattenkopie-Zeitplans darauf, dass Sie bei der Migration von Daten oder bei der geplanten Ausführung von Datendeduplizierungsaufträgen keine Schattenkopien einplanen. Sie sollten Schattenkopien planen, wenn Sie davon ausgehen, dass sich Ihr Dateisystem im Leerlauf befindet. Informationen zur Konfiguration

eines benutzerdefinierten Schattenkopie-Zeitplans finden Sie unter [Einen benutzerdefinierten Zeitplan für Schattenkopien erstellen](#).

## Konfiguration von Schattenkopien für die Verwendung des Standardspeichers und des Standardzeitplans

Sie können Schattenkopien schnell auf Ihrem Dateisystem einrichten, indem Sie die standardmäßige Speichereinstellung und den Zeitplan für Schattenkopien verwenden. Mit der Standardeinstellung für Schattenkopie-Speicher belegen Schattenkopien maximal 10 Prozent der Speicherkapazität Ihres Dateisystems. Wenn Sie die Speicherkapazität Ihres Dateisystems erhöhen, wird die Größe des aktuell zugewiesenen Schattenkopie-Speichers nicht in ähnlicher Weise erhöht.

Der Standardzeitplan erstellt automatisch Schattenkopien jeden Montag, Dienstag, Mittwoch, Donnerstag und Freitag um 7:00 Uhr und 12:00 Uhr UTC.

So richten Sie die Standardspeicherebene für Schattenkopien ein

1. Stellen Sie eine Connect zu einer Windows-Recheninstanz her, die über Netzwerkkonnektivität mit Ihrem Dateisystem verfügt.
2. Melden Sie sich bei der Windows-Compute-Instanz als Mitglied der Gruppe der Dateisystemadministratoren an. In AWS Managed Microsoft AD dieser Gruppe handelt es sich um AWS Delegierte FSx-Administratoren. In Ihrem selbstverwalteten Microsoft AD ist diese Gruppe Domänen-Admins oder die benutzerdefinierte Gruppe, die Sie bei der Erstellung Ihres Dateisystems für die Verwaltung angegeben haben. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Stellen Sie mit dem folgenden Befehl die Standardmenge an Schattenspeicher ein. *FSxFileSystem-Remote-PowerShell-Endpoint* Ersetzen Sie es durch den Windows PowerShell Remote-Endpunkt des Dateisystems, das Sie verwalten möchten. Sie finden den Windows PowerShell Remote-Endpunkt in der Amazon FSx-Konsole, im Bereich Netzwerk und Sicherheit auf dem Bildschirm mit den Dateisystemdetails oder in der Antwort auf den DescribeFileSystem API-Vorgang.

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

Die Antwort sieht wie folgt aus.

```
FSx Shadow Storage Configuration

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

Um den standardmäßigen Zeitplan für Schattenkopien festzulegen

1. Stellen Sie eine Connect zu einer Windows-Recheninstanz her, die über Netzwerkkonnektivität mit Ihrem Dateisystem verfügt.
2. Melden Sie sich bei der Windows-Compute-Instanz als Mitglied der Gruppe der Dateisystemadministratoren an. In AWS Managed Microsoft AD dieser Gruppe handelt es sich um AWS Delegierte FSx-Administratoren. In Ihrem selbstverwalteten Microsoft AD ist diese Gruppe Domänen-Admins oder die benutzerdefinierte Gruppe, die Sie bei der Erstellung Ihres Dateisystems für die Verwaltung angegeben haben. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Legen Sie den standardmäßigen Zeitplan für Schattenkopien mithilfe des folgenden Befehls fest.

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

In der Antwort wird der Standardzeitplan angezeigt, der jetzt festgelegt ist.

```
FSx Shadow Copy Schedule

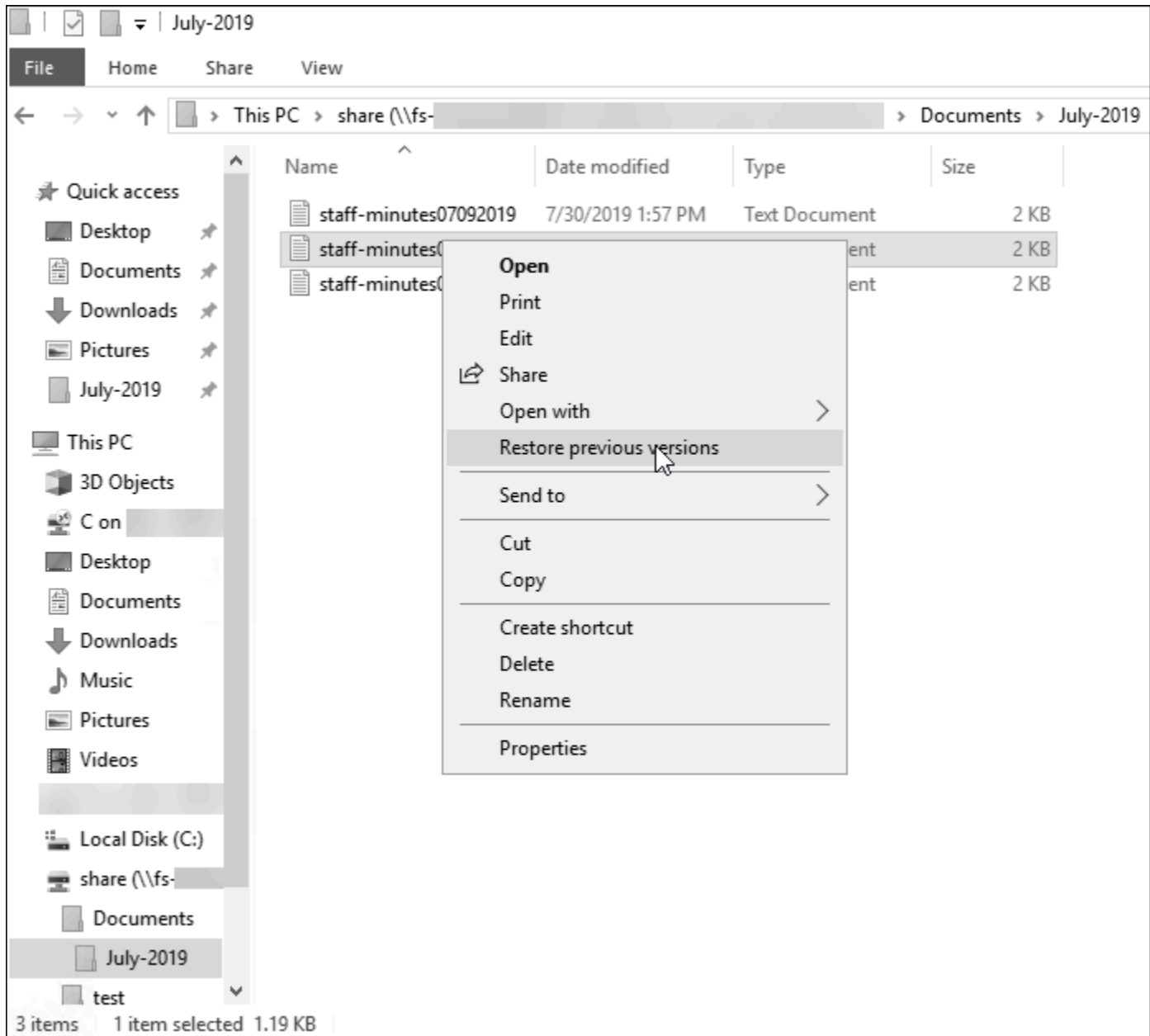
Start Time                Days of week                WeeksInterval
-----
2019-07-16T07:00:00+00:00 Monday, Tuesday, Wednesday, Thursday, Friday 1
2019-07-16T12:00:00+00:00 Monday, Tuesday, Wednesday, Thursday, Friday 1
```

Weitere Informationen zu zusätzlichen Optionen und zum Erstellen eines benutzerdefinierten Schattenkopie-Zeitplans finden Sie unter [Einen benutzerdefinierten Zeitplan für Schattenkopien erstellen](#).

## Einzelne Dateien und Ordner wiederherstellen

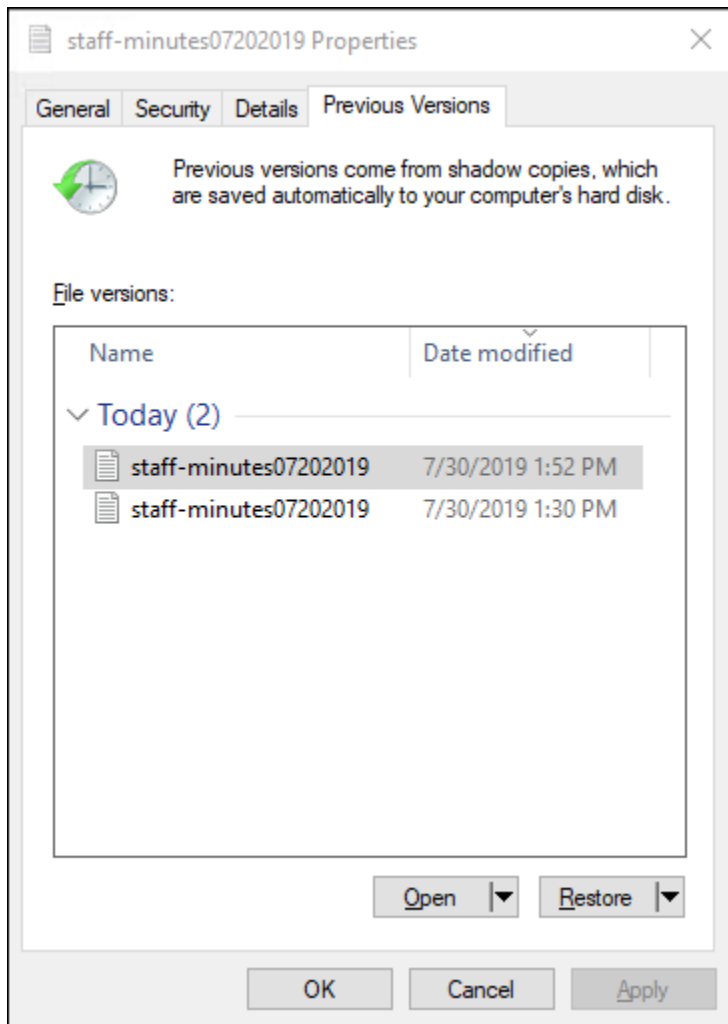
Nachdem Sie Schattenkopien auf Ihrem Amazon FSx-Dateisystem konfiguriert haben, können Ihre Benutzer schnell frühere Versionen einzelner Dateien oder Ordner wiederherstellen und gelöschte Dateien wiederherstellen.

Benutzer stellen Dateien mithilfe der vertrauten Windows-Datei-Explorer-Oberfläche auf frühere Versionen wieder her. Um eine Datei wiederherzustellen, wählen Sie die wiederherzustellende Datei aus und wählen dann im Kontextmenü (Rechtsklick) die Option Frühere Versionen wiederherstellen.





Benutzer können dann eine frühere Version aus der Liste „Frühere Versionen“ anzeigen und wiederherstellen.



## Einstellung der maximalen Speichermenge für Schattenkopien

Mit dem `Set-FsxShadowStorage` benutzerdefinierten PowerShell Befehl definieren Sie die maximale Speichermenge, die Schattenkopien in einem Dateisystem belegen können. Sie können die maximale Größe angeben, auf die Schattenkopien anwachsen können, indem Sie entweder die Parameter `-Maxsize` oder die `-Default` Parameter verwenden. Mit `Default Using` wird das Maximum auf 10% der Speicherkapazität des Dateisystems festgelegt. Sie können die `-Default` Parameter `-Maxsize` und nicht im selben Befehl angeben.

Mithilfe von `-Maxsize` können Sie den Schattenkopiespeicher wie folgt definieren:

- In Byte: `Set-FsxShadowStorage -Maxsize 2500000000`

- In Kilobyte, Megabyte, Gigabyte oder anderen Einheiten: `Set-FsxShadowStorage -Maxsize (2500MB)` `Set-FsxShadowStorage -Maxsize (2.5GB)`
- In Prozent des Gesamtspeichers: `Set-FsxShadowStorage -Maxsize "20%"`
- Als unbegrenzt: `Set-FsxShadowStorage -Maxsize "UNBOUNDED"`

Wird verwendet-Default, um den Schattenspeicher so einzustellen, dass er bis zu 10 Prozent des Dateisystems verwendet. `Set-FsxShadowStorage -Default` Weitere Informationen zur Verwendung der Standardoption finden Sie unter [Konfiguration von Schattenkopien für die Verwendung des Standardspeichers und des Standardzeitplans](#).

So legen Sie die Größe des Schattenkopiespeichers auf einem Dateisystem FSx for Windows File Server fest

1. Connect Sie als Benutzer, der Mitglied der Gruppe der Dateisystemadministratoren ist, eine Verbindung zu einer Recheninstanz her, die über Netzwerkkonnektivität mit Ihrem Dateisystem verfügt. In AWS Managed Microsoft AD dieser Gruppe handelt es sich um AWS Delegierte FSx-Administratoren. In Ihrem selbstverwalteten Microsoft AD ist diese Gruppe Domänen-Admins oder die benutzerdefinierte Gruppe, die Sie bei der Erstellung Ihres Dateisystems für die Verwaltung angegeben haben. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
2. Öffnen Sie ein PowerShell Windows-Fenster auf der Compute-Instance.
3. Verwenden Sie den folgenden Befehl, um eine PowerShell Remotesitzung auf Ihrem Amazon FSx-Dateisystem zu öffnen. `FSxFileSystem-Remote-PowerShell-Endpoint` Ersetzen Sie es durch den Windows PowerShell Remote-Endpunkt des Dateisystems, das Sie verwalten möchten. Sie finden den Windows PowerShell Remote-Endpunkt in der Amazon FSx-Konsole, im Bereich Netzwerk und Sicherheit auf dem Bildschirm mit den Dateisystemdetails oder in der Antwort auf den `DescribeFileSystem` API-Vorgang.

```
PS C:\Users\delegateadmin> enter-psession -computename FSxFileSystem-Remote-PowerShell-Endpoint -configurationname fsxremoteadmin
```

4. Stellen Sie mithilfe des folgenden Befehls sicher, dass der Schattenkopiespeicher nicht bereits im Dateisystem konfiguriert ist.

```
[fs-1234567890abcef12]: PS>Get-FsxShadowStorage  
No Fsx Shadow Storage Configured
```

5. Stellen Sie mit dieser `-Default` Option die Größe des Schattenspeichers auf 10 Prozent des Volumes und die maximale Anzahl von Schattenkopien auf 20 ein.

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace      MaxSpace MaxShadowCopyNumber
-----
                0          0 32530536858                20
```

Sie können die maximal zulässige Anzahl von Schattenkopien in Ihrem Dateisystem einschränken, indem Sie den `Set-FsxShadowStorage` Befehl mit dem `-MaxShadowCopyNumber` Parameter verwenden und einen Wert zwischen 1 und 500 angeben. Standardmäßig ist die maximale Anzahl von Schattenkopien auf 20 festgelegt, wie von Microsoft für aktive Workloads empfohlen.

## Ihren Schattenkopie-Speicher anzeigen

Mit dem `Get-FsxShadowStorage` Befehl in einer PowerShell Remotesitzung auf Ihrem Dateisystem können Sie die Menge an Speicherplatz anzeigen, die derzeit von Schattenkopien in Ihrem Dateisystem belegt wird. Anweisungen zum Starten einer PowerShell Remotesitzung auf Ihrem Dateisystem finden Sie unter [Verwenden der Amazon FSx CLI für PowerShell](#).

```
[fs-1234567890abcef12]: PS>PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

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

Die Ausgabe zeigt die Shadow-Speicherkonfiguration wie folgt:

- **AllocatedSpace**— Die Speichermenge im Dateisystem in Byte, die derzeit Schattenkopien zugewiesen ist. Anfänglich ist dieser Wert 0.
- **UsedSpace**— Die Speichermenge in Byte, die derzeit von Schattenkopien verwendet wird. Anfänglich ist dieser Wert 0.
- **MaxSpace**— Die maximale Speichermenge in Byte, auf die der Schattenspeicher anwachsen kann. Dies ist der Wert, den Sie mit dem `Set-FsxShadowStorage` Befehl für den [Schattenkopiespeicher](#) festlegen.

- **MaxShadowCopyNumber**— Die maximale Anzahl von Schattenkopien, die das Dateisystem haben kann, liegt zwischen 1 und 500.

Wenn die UsedSpace Menge die konfigurierte maximale Speichermenge für Schattenkopien erreicht (MaxSpace) oder die Anzahl der Schattenkopien die maximal konfigurierte Anzahl an Schattenkopien (MaxShadowCopyNumber) erreicht, ersetzt die nächste Schattenkopie, die Sie erstellen, die älteste Schattenkopie. Wenn Sie Ihre ältesten Schattenkopien nicht verlieren möchten, überwachen Sie Ihren Schattenkopie-Speicher, um sicherzustellen, dass Sie über ausreichend Speicherplatz für neue Schattenkopien verfügen. Wenn Sie mehr Speicherplatz benötigen, können Sie [vorhandene Schattenkopien löschen](#) oder den maximalen [Speicherplatz für Schattenkopien](#) erhöhen.

#### Note

Wenn Schattenkopien automatisch oder manuell erstellt werden, verwenden sie die Menge an Schattenkopie-Speicher, die Sie als Speicherlimit konfiguriert haben. Schattenkopien nehmen mit der Zeit an Größe zu und nutzen den in der CloudWatch FreeStorageCapacity Metrik angegebenen verfügbaren Speicherplatz bis zur konfigurierten Höchstmenge an Schattenkopie-Speicherplatz (MaxSpace).

## Löschen des Schattenkopie-Speichers, des Zeitplans und aller Schattenkopien

Sie können Ihre Schattenkopie-Konfiguration, einschließlich aller vorhandenen Schattenkopien, zusammen mit dem Schattenkopie-Zeitplan löschen. Gleichzeitig können Sie den Schattenkopie-Speicher im Dateisystem freigeben.

Geben Sie dazu den `Remove-FsxShadowStorage` Befehl in einer PowerShell Remotesitzung auf Ihrem Dateisystem ein. Anweisungen zum Starten einer PowerShell Remotesitzung auf Ihrem Dateisystem finden Sie unter [Verwenden der Amazon FSx CLI für 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.
```

## Einen benutzerdefinierten Zeitplan für Schattenkopien erstellen

Schattenkopie-Zeitpläne verwenden geplante Task-Trigger in Microsoft Windows, um anzugeben, wann Schattenkopien automatisch erstellt werden. Ein Zeitplan für Schattenkopien kann mehrere Auslöser haben, was Ihnen eine große Flexibilität bei der Planung bietet. Es kann jeweils nur ein Schattenkopie-Zeitplan existieren. Bevor Sie einen Schattenkopie-Zeitplan erstellen können, müssen Sie zunächst die Größe des [Schattenkopie-Speichers](#) festlegen.

Wenn Sie den `Set-FsxShadowCopySchedule` Befehl auf einem Dateisystem ausführen, überschreiben Sie alle vorhandenen Schattenkopie-Zeitpläne. Wenn sich Ihr Client-Computer in der UTC-Zeitzone befindet, können Sie die Zeitzone für einen Trigger auch mithilfe von Windows-Zeitzone und der `-TimeZoneId` Option angeben. Eine Liste der Windows-Zeitzone finden Sie in der Dokumentation zur [Standardzeitzone](#) von Microsoft oder führen Sie an einer Windows-Eingabeaufforderung den folgenden Befehl aus: `tzutil /?`. Weitere Informationen zu Windows-Task-Trigger finden Sie in der Dokumentation zu [Task-Trigger](#) in der Microsoft Windows Developer Center-Dokumentation.

Sie können die `-Default` Option auch verwenden, um schnell einen standardmäßigen Zeitplan für Schattenkopien einzurichten. Weitere Informationen hierzu finden Sie unter [Konfiguration von Schattenkopien für die Verwendung des Standardspeichers und des Standardzeitplans](#).

Um einen benutzerdefinierten Zeitplan für Schattenkopien zu erstellen

1. Erstellen Sie eine Reihe von Windows-Auslösern für geplante Aufgaben, um zu definieren, wann Schattenkopien im Zeitplan für Schattenkopien erstellt werden. Verwenden Sie den `new-scheduledTaskTrigger` Befehl in a PowerShell auf Ihrem lokalen Computer, um mehrere Trigger einzurichten.

Im folgenden Beispiel wird ein benutzerdefinierter Zeitplan für Schattenkopien erstellt, bei dem Schattenkopien jeden Montag bis Freitag um 6:00 Uhr und um 18:00 Uhr UTC erstellt werden. Standardmäßig werden Zeiten in UTC angegeben, es sei denn, Sie geben in den von Ihnen erstellten Windows-Auslösern für geplante Aufgaben eine Zeitzone an.

```
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. Wird verwendet `invoke-command`, um den `scriptblock` Befehl auszuführen. Dadurch wird ein Skript geschrieben, das den Schattenkopie-Zeitplan auf den `new-scheduledTaskTrigger` Wert festlegt, den Sie gerade erstellt haben. `FSxFileSystem-Remote-PowerShell-Endpoint` Ersetzen Sie es durch den Windows PowerShell Remote-Endpunkt des Dateisystems, das Sie verwalten möchten. Sie finden den Windows PowerShell Remote-Endpunkt in der Amazon FSx-Konsole, im Bereich Netzwerk und Sicherheit auf dem Bildschirm mit den Dateisystemdetails oder in der Antwort auf den `DescribeFileSystem` API-Vorgang.

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

3. Geben Sie an der `>>` Eingabeaufforderung die folgende Zeile ein, um Ihren Schattenkopie-Zeitplan mithilfe des `set-fsxshadowcopschedule` Befehls festzulegen.

```
>> set-fsxshadowcopschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2
-Confirm:$false }
```

In der Antwort wird der Schattenkopie-Zeitplan angezeigt, den Sie im Dateisystem konfiguriert haben.

```
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
```

## Ihren Schattenkopie-Zeitplan anzeigen

Geben Sie in einer PowerShell Remotesitzung in Ihrem Dateisystem den folgenden Befehl ein, um den vorhandenen Schattenkopie-Zeitplan auf Ihrem Dateisystem anzuzeigen. Anweisungen zum Starten einer PowerShell Remotesitzung auf Ihrem Dateisystem finden Sie unter [Verwenden der Amazon FSx CLI für 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
```

## Löschen eines Schattenkopie-Zeitplans

Um den vorhandenen Schattenkopie-Zeitplan auf Ihrem Dateisystem zu löschen, geben Sie in einer PowerShell Remotesitzung auf Ihrem Dateisystem den folgenden Befehl ein. Anweisungen zum Starten einer PowerShell Remotesitzung auf Ihrem Dateisystem finden Sie unter [Verwenden der Amazon FSx CLI für 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>
```

## Eine Schattenkopie erstellen

Um eine Schattenkopie manuell zu erstellen, geben Sie den folgenden Befehl in einer PowerShell Remotesitzung auf Ihrem Dateisystem ein. Anweisungen zum Starten einer PowerShell Remotesitzung auf Ihrem Dateisystem finden Sie unter [Verwenden der Amazon FSx CLI für PowerShell](#).

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy
```

```
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

## Vorhandene Schattenkopien anzeigen

Geben Sie in einer PowerShell Remotesitzung in Ihrem Dateisystem den folgenden Befehl ein, um den Satz vorhandener Schattenkopien auf Ihrem Dateisystem anzuzeigen. Anweisungen zum Starten einer PowerShell Remotesitzung auf Ihrem Dateisystem finden Sie unter [Verwenden der Amazon FSx CLI für 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 |

## Löschen von Schattenkopien

Sie können eine oder mehrere vorhandene Schattenkopien auf Ihrem Dateisystem löschen, indem Sie den `Remove-FsxShadowCopies` Befehl in einer PowerShell Remotesitzung auf Ihrem Dateisystem verwenden. Anweisungen zum Starten einer PowerShell Remotesitzung auf Ihrem Dateisystem finden Sie unter [Verwenden der Amazon FSx CLI für PowerShell](#).

Geben Sie mithilfe einer der folgenden erforderlichen Optionen an, welche Schattenkopien gelöscht werden sollen:

- `-Oldest` löscht die älteste Schattenkopie
- `-All` löscht alle vorhandenen Schattenkopien
- `-ShadowCopyId` löscht eine bestimmte Schattenkopie anhand ihrer ID.

Sie können mit dem Befehl nur eine Option verwenden. Ein Fehler tritt auf, wenn Sie nicht angeben, welche Schattenkopie gelöscht werden soll, wenn Sie mehrere Schattenkopie-IDs angeben oder wenn Sie eine ungültige Schattenkopie-ID angeben.

Um die älteste Schattenkopie auf Ihrem Dateisystem zu löschen, geben Sie in einer PowerShell Remotesitzung in Ihrem Dateisystem den folgenden Befehl ein.



```
[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
```

Um eine bestimmte Schattenkopie auf Ihrem Dateisystem zu löschen, geben Sie in einer PowerShell Remotesitzung in Ihrem Dateisystem den folgenden Befehl ein.

```
[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.
```

Um eine bestimmte Anzahl der ältesten Schattenkopien in Ihrem Dateisystem zu löschen, aktualisieren Sie Ihren `-MaxShadowCopyNumber` Parameter auf die gewünschte Anzahl von Schattenkopien, die Sie noch haben möchten. Diese Änderung wird jedoch erst wirksam, nachdem der nächste Schattenkopie-Snapshot erstellt wurde. Dann löscht das System die überschüssigen Schattenkopien automatisch. Verwenden Sie den folgenden Befehl in einer PowerShell Remotesitzung auf Ihrem Dateisystem.

```
[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                   |

## Geplante Replikation mit AWS DataSync

Sie können AWS DataSync damit die regelmäßige Replikation Ihres Dateisystems FSx for Windows File Server auf ein zweites Dateisystem planen. Diese Funktion ist sowohl für regionsinterne als auch für regionsübergreifende Bereitstellungen verfügbar. Weitere Informationen finden Sie [Migrieren vorhandener Dateien zu FSx for Windows File Server mit AWS DataSync](#) in diesem Handbuch und unter [Datenübertragung zwischen AWS Speicherdiensten](#) im AWS DataSync Benutzerhandbuch.

# Verwaltung von Dateisystemen

In diesem Kapitel wird beschrieben, wie Sie auf die Amazon FSx CLI für die Fernverwaltung zugreifen und wie Sie die verfügbaren Dateisystem-Administrationsaufgaben ausführen. PowerShell Sie können auch die systemeigene grafische Benutzeroberfläche (GUI) von Microsoft Windows verwenden, um einige Verwaltungsaufgaben auszuführen.

## Themen

- [Verwenden der Amazon FSx CLI für PowerShell](#)
- [Starten einer Amazon FSx-Remotesitzung PowerShell](#)
- [DNS-Aliase verwalten](#)
- [Verwaltung von Dateifreigaben auf FSx for Windows File Server Server-Dateisystemen](#)
- [Prüfung des Dateizugriffs](#)
- [Benutzersitzungen und geöffnete Dateien](#)
- [Datenduplizierung](#)
- [Speicherkontingente](#)
- [Verwaltung der Verschlüsselung bei der Übertragung](#)
- [Verwaltung der Speicherkonfiguration](#)
- [Verwaltung der Durchsatzkapazität](#)
- [Markieren Ihrer Amazon FSx-Ressourcen mit Tags](#)
- [Arbeiten mit Amazon FSx-Wartungsfenstern](#)
- [Bewährte Methoden für die Verwaltung von Amazon FSx-Dateisystemen](#)

## Verwenden der Amazon FSx CLI für PowerShell

Die Amazon FSx CLI for Remote Management PowerShell aktiviert die Dateisystemadministration für Benutzer in der Gruppe der Dateisystemadministratoren. Um eine PowerShell Remotesitzung auf Ihrem Dateisystem FSx for Windows File Server zu starten, müssen Sie zunächst die folgenden Voraussetzungen erfüllen:

- In der Lage sein, eine Verbindung zu einer Windows-Compute-Instanz herzustellen, die über Netzwerkkonnektivität mit Ihrem FSx for Windows File Server Server-Dateisystem verfügt.

- Seien Sie als Mitglied der Gruppe der Dateisystemadministratoren bei der Windows-Compute-Instanz angemeldet. Wenn Sie verwenden AWS Managed Microsoft AD, ist dies die Gruppe AWS Delegated FSx Administrators. Wenn Sie ein selbstverwaltetes Microsoft Active Directory verwenden, ist dies die Gruppe Domänen-Admins oder die benutzerdefinierte Gruppe, die Sie bei der Erstellung Ihres Dateisystems für die Verwaltung angegeben haben. Weitere Informationen finden Sie unter [Bewährte Methoden für selbstverwaltetes Active Directory](#).
- Die eingehenden Regeln für eingehende VPC-Sicherheitsgruppen Ihres Dateisystems lassen Datenverkehr auf Port 5985 zu.


Die Amazon FSx CLI für die Fernverwaltung PowerShell verwendet die folgenden Sicherheitsfunktionen:

- Benutzeranmeldedaten werden mithilfe der Kerberos-Authentifizierung authentifiziert.
- Die Kommunikation der Verwaltungssitzung zwischen dem verbundenen Client und dem Dateisystem wird mit Kerberos verschlüsselt.

Sie haben zwei Möglichkeiten, Remote-Management-CLI-Befehle auf Ihrem Amazon FSx-Dateisystem auszuführen:

- Sie können eine PowerShell Remote-Sitzung mit langer Laufzeit einrichten und die Befehle innerhalb der Sitzung ausführen.
- Sie können den verwenden `Invoke-Command`, um einen einzelnen Befehl oder einen einzelnen Befehlsblock auszuführen, ohne eine lang andauernde PowerShell Remotesitzung einzurichten.

Wenn Sie Variablen als Parameter festlegen und an den Fernverwaltungsbefehl übergeben möchten, müssen Sie Folgendes verwenden `Invoke-Command`.

 Note

Für Multi-AZ-Dateisysteme können Sie die Amazon FSx CLI for Remote Management nur verwenden, solange das Dateisystem seinen bevorzugten Dateiserver verwendet. Weitere Informationen finden Sie unter [Verfügbarkeit und Haltbarkeit: Single-AZ- und Multi-AZ-Dateisysteme](#).

Sie müssen den Windows Remote PowerShell Endpoint des Dateisystems verwenden, wenn Sie Remote verwenden. PowerShell Wenn Sie den verwenden AWS Management Console, finden Sie den Endpunkt auf der Registerkarte Netzwerk und Sicherheit auf der Seite mit den Dateisystemdetails. Mit dem AWS CLI `describe-file-systems` Befehl wird die `RemoteAdministrationEndpoint` Eigenschaft in der Antwort zurückgegeben. Der Endpunkt der Remoteverwaltung verwendet das Format `amznfsxctlyaa1k.ActiveDirectory-DNS-name`, zum Beispiel `amznfsxctlyaa1k.corp.example.com`.

Sie können das `Get-Command` Cmdlet verwenden, um Informationen über die in verfügbaren Cmdlets, Funktionen und Aliase abzurufen. PowerShell Weitere Informationen finden Sie in der Microsoft [Get-Command-Dokumentation](#).

Sie können Amazon FSx CLI for Remote Management CLI auch für PowerShell Befehle in Ihrem Dateisystem ausführen, indem Sie das `Invoke-Command` Cmdlet verwenden und dabei die folgende Syntax verwenden.

```
PS C:\Users\delegatedadmin> Invoke-Command -ComputerName
  amznfsxctlyaa1k.corp.example.com -ConfigurationName FSxRemoteAdmin -scriptblock { fsx-
command }
```

Anweisungen zum Starten einer langlebigen PowerShell Remotesitzung auf Ihrem Dateisystem FSx for Windows File Server finden Sie unter [Starten einer Amazon FSx-Remotesitzung PowerShell](#)

## Starten einer Amazon FSx-Remotesitzung PowerShell

Dieses Thema enthält Anweisungen zum Starten einer langlebigen PowerShell Remotesitzung auf Ihrem FSx for Windows File Server Server-Dateiserver.

So starten Sie eine PowerShell Remotesitzung auf Ihrem Dateisystem

1. Stellen Sie als Benutzer, der Mitglied der delegierten FSx-Administratorgruppe ist, die Sie bei der Erstellung des Dateisystems ausgewählt haben, eine Connect zu einer Recheninstanz her, die über Netzwerkkonnektivität mit Ihrem Dateisystem verfügt.
2. Öffnen Sie ein PowerShell Windows-Fenster auf der Recheninstanz.
3. Geben Sie in der den folgenden Befehl ein PowerShell, um eine langlebige Remotesitzung auf Ihrem Amazon FSx-Dateisystem zu öffnen. `Remote-PowerShell-Endpoint` Ersetzen Sie es durch den Windows PowerShell Remote-Endpoint des Dateisystems, das Sie verwalten möchten. Verwenden Sie `FsxRemoteAdmin` es als Namen für die Sitzungskonfiguration.

```
PS C:\Users\delegateadmin> enter-ssession -ComputerName Remote-PowerShell-Endpoint  
-ConfigurationName FsxRemoteAdmin  
[fs-0123456789abcdef0]: PS>
```

Wenn Ihre Instance nicht Teil der Amazon FSx Active Directory-Domain ist, werden Sie in einem Pop-up aufgefordert, Benutzeranmeldedaten einzugeben. Geben Sie die Anmeldeinformationen des Benutzers ein, der Mitglied der FSx-Administratorgruppe ist. Wenn Ihre Instanz mit der Domain verbunden ist, werden Sie nicht nach Anmeldeinformationen gefragt.

## DNS-Aliase verwalten

FSx for Windows File Server bietet einen Standard-DNS-Namen (Domain Name System) für jedes Dateisystem, das Sie für den Zugriff auf die Daten in Ihrem Dateisystem verwenden können. Sie können auch mit einem DNS-Alias Ihrer Wahl auf Ihre Dateisysteme zugreifen. Mit DNS-Aliassen können Sie bei der Migration von Dateisystemspeichern von lokal zu Amazon FSx vorhandene DNS-Namen weiterhin verwenden, um auf Daten zuzugreifen, die auf Amazon FSx gespeichert sind, ohne Tools oder Anwendungen aktualisieren zu müssen. Weitere Informationen finden Sie unter [Migration von vorhandenem Dateispeicher zu Amazon FSx](#).

### Note

Support für DNS-Aliase ist auf FSx for Windows File Server Server-Dateisystemen verfügbar, die am 9. November 2020 nach 12:00 Uhr ET erstellt wurden. Gehen Sie wie folgt vor, um DNS-Aliase auf einem Dateisystem zu verwenden, das vor 12:00 Uhr ET am 9. November 2020 erstellt wurde:

1. Erstellen Sie eine Sicherungskopie des vorhandenen Dateisystems. Weitere Informationen finden Sie unter [Arbeiten mit vom Benutzer initiierten Backups](#).
2. Stellen Sie das Backup in einem neuen Dateisystem wieder her. Weitere Informationen finden Sie unter [Wiederherstellen von Sicherungen](#).

Sobald das neue Dateisystem verfügbar ist, können Sie mithilfe der in diesem Abschnitt bereitgestellten Informationen mithilfe von DNS-Aliassen darauf zugreifen.

**Note**

Bei den hier aufgeführten Informationen wird davon ausgegangen, dass Sie ausschließlich in Active Directory arbeiten und keine externen DNS-Anbieter verwenden. DNS-Drittanbieter können zu unerwartetem Verhalten führen.

Amazon FSx registriert nur DNS-Einträge für ein Dateisystem, wenn die AD-Domain, mit der Sie es verbinden, Microsoft DNS als Standard-DNS verwendet. Wenn Sie DNS eines Drittanbieters verwenden, müssen Sie nach der Erstellung Ihres Dateisystems manuell DNS-Einträge für Ihre Amazon FSx-Dateisysteme einrichten. Weitere Informationen zur Auswahl der richtigen IP-Adressen für das Dateisystem finden Sie unter [Abrufen der richtigen Dateisystem-IP-Adressen zur Verwendung für DNS](#).

Sie können DNS-Aliase vorhandenen FSx for Windows File Server Server-Dateisystemen zuordnen, wenn Sie neue Dateisysteme erstellen und wenn Sie ein neues Dateisystem aus einer Sicherung erstellen. Sie können einem Dateisystem bis zu 50 DNS-Aliase gleichzeitig zuordnen.

Damit Clients über die DNS-Aliase eine Verbindung zum Dateisystem herstellen können, müssen Sie nicht nur Ihrem Dateisystem zuordnen, sondern auch folgende Schritte ausführen:

- Konfigurieren Sie Service Principal Names (SPNs) für die Kerberos-Authentifizierung und Verschlüsselung.
- Konfigurieren Sie einen DNS-CNAME-Eintrag für den DNS-Alias, der in den Standard-DNS-Namen für Ihr Amazon FSx-Dateisystem aufgelöst wird.

Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliassen für den Zugriff auf Ihr Dateisystem](#).

Ein DNS-Aliasname für Ihr Dateisystem FSx for Windows File Server muss die folgenden Anforderungen erfüllen:

- Muss als vollqualifizierter Domänenname (FQDN) formatiert sein.
- Kann alphanumerische Zeichen und Bindestriche (-) enthalten.
- Am Anfang und am Ende darf kein Bindestrich stehen.
- Kann mit einem numerischen Wert beginnen.

Bei DNS-Aliasnamen speichert Amazon FSx alphabetische Zeichen als Kleinbuchstaben (a-z), unabhängig davon, wie Sie sie angeben: als Großbuchstaben, Kleinbuchstaben oder entsprechende Buchstaben in Escape-Zeichen.

Wenn Sie versuchen, einen Alias zuzuordnen, der bereits mit dem Dateisystem verknüpft ist, hat dies keine Auswirkung. Wenn Sie versuchen, einen Alias von einem Dateisystem zu trennen, das nicht mit dem Dateisystem verknüpft ist, antwortet Amazon FSx mit einem Fehler bei der fehlerhaften Anfrage.

### Note

Wenn Amazon FSx Aliase zu einem Dateisystem hinzufügt oder entfernt, werden verbundene Clients vorübergehend getrennt und stellen automatisch wieder eine Verbindung zum Dateisystem her. Alle Dateien, die zum Zeitpunkt der Verbindungsunterbrechung von Clients geöffnet waren, die einer nicht kontinuierlich verfügbaren (nicht CA-) Freigabe zugeordnet waren, müssen vom Client erneut geöffnet werden.

## Themen

- [DNS-Aliasstatus](#)
- [Verwendung von DNS-Aliasen mit Kerberos-Authentifizierung](#)
- [DNS-Aliase für Dateisysteme und Backups anzeigen](#)
- [DNS-Aliase mit Dateisystemen verknüpfen](#)
- [Verwaltung von DNS-Aliasen auf vorhandenen Dateisystemen](#)

## DNS-Aliasstatus

DNS-Aliase können einen der folgenden Statuswerte haben:

- Verfügbar — Der DNS-Alias ist mit einem Amazon FSx-Dateisystem verknüpft.
- Erstellen — Amazon FSx erstellt den DNS-Alias und ordnet ihn dem Dateisystem zu.
- Löschen — Amazon FSx trennt den DNS-Alias vom Dateisystem und löscht ihn.
- Fehler beim Erstellen — Amazon FSx konnte den DNS-Alias nicht mit dem Dateisystem verknüpfen.
- Fehler beim Löschen — Amazon FSx konnte den DNS-Alias nicht vom Dateisystem trennen.



## Verwendung von DNS-Aliasen mit Kerberos-Authentifizierung

Wir empfehlen Ihnen, bei der Übertragung mit Amazon FSx die Kerberos-basierte Authentifizierung und Verschlüsselung zu verwenden. Kerberos bietet die sicherste Authentifizierung für Clients, die auf Ihr Dateisystem zugreifen. Um die Kerberos-Authentifizierung für Clients zu aktivieren, die über einen DNS-Alias auf Ihr Amazon FSx-Dateisystem zugreifen, müssen Sie Service Principal Names (SPNs) konfigurieren, die dem DNS-Alias auf dem Active Directory-Computerobjekt Ihres Dateisystems entsprechen.

Wenn Sie SPNs für den DNS-Alias konfiguriert haben, den Sie einem anderen Dateisystem auf einem Computerobjekt in Ihrem Active Directory zugewiesen haben, müssen Sie diese SPNs zuerst entfernen, bevor Sie SPNs zum Computerobjekt Ihres Dateisystems hinzufügen. Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisystem](#).

## DNS-Aliase für Dateisysteme und Backups anzeigen

Sie können die DNS-Aliase, die derzeit mit Dateisystemen und Backups verknüpft sind, mithilfe der Amazon FSx-Konsole, der AWS CLI und der API einsehen. Dieses Thema enthält Anweisungen zur Anzeige der DNS-Aliase für Ihre Dateisysteme und Backups.

So zeigen Sie DNS-Aliase an, die mit Dateisystemen verknüpft sind

- Verwenden der Konsole — Wählen Sie ein Dateisystem aus, um die Detailseite für Dateisysteme anzuzeigen. Wählen Sie die Registerkarte Netzwerk und Sicherheit, um die DNS-Aliase anzuzeigen.
- Verwenden der CLI oder API — Verwenden Sie den `describe-file-system-aliases` CLI-Befehl oder die [DescribeFileSystemAliases](#) API-Operation.

So zeigen Sie DNS-Aliase an, die mit Backups verknüpft sind

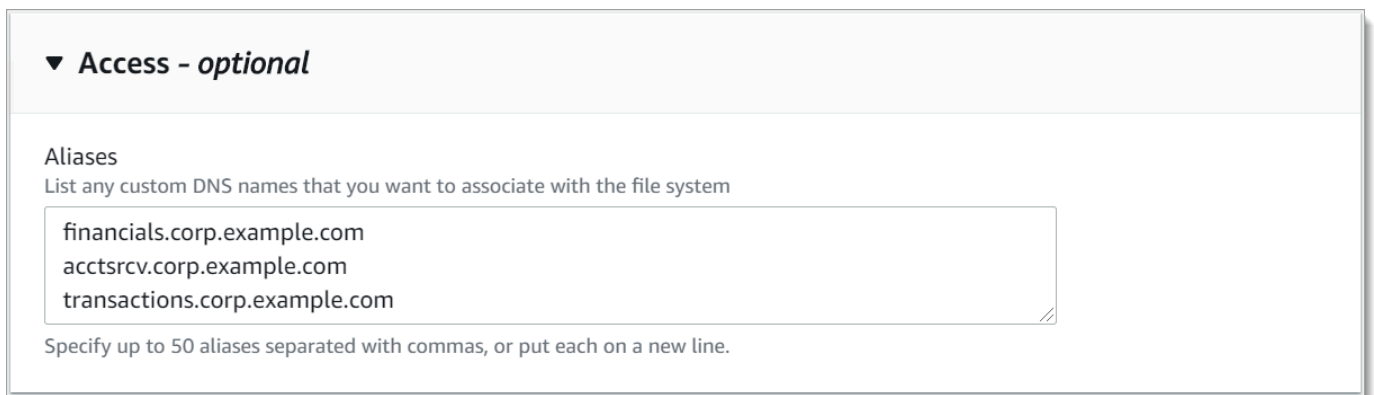
- Verwenden der Konsole — Wählen Sie im Navigationsbereich Backups und dann das Backup aus, das Sie anzeigen möchten. Sehen Sie sich im Übersichtsbereich das Feld DNS-Aliase an.
- Verwenden der CLI oder API — Verwenden Sie den `describe-backups` CLI-Befehl oder die [DescribeBackups](#) API-Operation.

## DNS-Aliase mit Dateisystemen verknüpfen

In diesem Thema wird beschrieben, wie DNS-Aliase verknüpft werden, wenn Sie ein neues FSx for Windows File Server Server-Dateisystem von Grund auf neu erstellen oder wenn Sie mithilfe der API AWS Management Console AWS CLI, und ein Dateisystem aus einer Sicherung erstellen.

So ordnen Sie DNS-Aliase zu, wenn Sie ein neues Dateisystem (Konsole) erstellen

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, das [Erstellen Sie Ihr Dateisystem](#) im Abschnitt Erste Schritte beschrieben ist.
3. Geben Sie im Abschnitt Zugriff — optional des Assistenten zum Erstellen von Dateisystemen die DNS-Aliase ein, die Sie Ihrem Dateisystem zuordnen möchten.



▼ **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. Wenn das Dateisystem verfügbar ist, können Sie mit dem DNS-Alias darauf zugreifen, indem Sie Service Principal Names (SPNs) konfigurieren und einen DNS-CNAME-Eintrag für den Alias aktualisieren oder erstellen. Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisystem](#).

So verknüpfen Sie DNS-Aliase bei der Erstellung eines neuen Amazon FSx-Dateisystems (CLI)

1. Verwenden Sie beim Erstellen eines neuen Dateisystems die [Alias-Eigenschaft](#) mit dem [CreateFileSystem](#) API-Vorgang, um DNS-Aliase mit dem neuen Dateisystem zu verknüpfen.

```
aws fsx create-file-system \  
  --file-system-type WINDOWS \  
  --storage-capacity 2000 \  
  --storage-type SSD \  
  --subnet-ids subnet-123456 \  

```

```
--windows-configuration Aliases=[financials.corp.example.com,accts-rcv.corp.example.com]
```

2. Wenn das Dateisystem verfügbar ist, können Sie mithilfe des DNS-Alias darauf zugreifen, indem Sie Service Principal Names (SPNs) konfigurieren und einen DNS-CNAME-Eintrag für den Alias aktualisieren oder erstellen. Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliassen für den Zugriff auf Ihr Dateisystem](#).

So fügen Sie DNS-Aliase bei der Wiederherstellung eines Backups hinzu oder entfernen diese (CLI)

1. Wenn Sie ein neues Dateisystem aus einer Sicherung eines vorhandenen Dateisystems erstellen, können Sie die [Aliases-Eigenschaft](#) mit der [CreateFileSystemFromBackupAPI](#)-Operation wie folgt verwenden:
  - Alle mit der Sicherung verknüpften Aliase sind standardmäßig dem neuen Dateisystem zugeordnet.
  - Um ein Dateisystem zu erstellen, ohne Aliase aus dem Backup beizubehalten, verwenden Sie die `Aliases` Eigenschaft mit einem leeren Satz.

Um zusätzliche DNS-Aliase zuzuordnen, verwenden Sie die `Aliases` Eigenschaft und geben Sie sowohl die ursprünglichen Aliase an, die mit dem Backup verknüpft sind, als auch die neuen Aliase, die Sie zuordnen möchten.

Der folgende CLI-Befehl verknüpft zwei Aliase mit dem Dateisystem, das Amazon FSx aus einer Sicherung erstellt.

```
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. Wenn das Dateisystem verfügbar ist, können Sie mit dem DNS-Alias darauf zugreifen, indem Sie Service Principal Names (SPNs) konfigurieren und einen DNS-CNAME-Eintrag für den Alias aktualisieren oder erstellen. Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliassen für den Zugriff auf Ihr Dateisystem](#).

## Verwaltung von DNS-Aliasen auf vorhandenen Dateisystemen

In diesem Thema wird beschrieben, wie Sie das AWS Management Console und verwenden AWS CLI , um Aliase in vorhandenen Dateisystemen hinzuzufügen und zu entfernen.

So verwalten Sie DNS-Aliase für Dateisysteme (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Windows-Dateisystem aus, für das Sie DNS-Aliase verwalten möchten.
3. Wählen Sie auf der Registerkarte Netzwerk und Sicherheit die Option Für DNS-Aliase verwalten aus, um das Dialogfeld DNS-Aliase verwalten anzuzeigen.

### Manage DNS aliases

Associate new DNS aliases

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

**Associate**

**Current DNS aliases (1)**

  **1**  

| <input type="checkbox"/> | DNS name                                                        | Status                                        |
|--------------------------|-----------------------------------------------------------------|-----------------------------------------------|
| <input type="checkbox"/> | financials.corp.example.com <input type="button" value="Copy"/> | <input checked="" type="checkbox"/> Available |

If you associate or disassociate DNS aliases, your file system will experience a temporary loss of availability.

**Close**

- So verknüpfen Sie DNS-Aliase — Geben Sie im Feld Neue Aliase zuordnen die DNS-Aliase ein, die Sie zuordnen möchten. Wählen Sie Associate aus.
- So trennen Sie DNS-Aliase — Wählen Sie in der Liste Aktuelle Aliase die Aliase aus, zu denen Sie die Zuordnung trennen möchten. Wählen Sie Disassociate (Zuordnung aufheben) aus.

Sie können den Status der von Ihnen verwalteten Aliase in der Liste Aktuelle Aliase überwachen. Aktualisieren Sie die Liste, um den Status zu aktualisieren. Es dauert bis zu 2,5 Minuten, bis ein Alias einem Dateisystem zugeordnet oder getrennt wird.

4. Wenn der Alias verfügbar ist, können Sie mithilfe des DNS-Alias auf Ihr Dateisystem zugreifen, indem Sie Service Principal Names (SPNs) konfigurieren und einen DNS-CNAME-Eintrag für den Alias aktualisieren oder erstellen. Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisystem](#).

So verknüpfen Sie DNS-Aliase mit vorhandenen Dateisystemen (CLI)

1. Verwenden Sie den `associate-file-system-aliases` CLI-Befehl oder die [AssociateFileSystemAliases](#) API-Operation, um DNS-Aliase einem vorhandenen Dateisystem zuzuordnen.

Die folgende CLI-Anforderung verknüpft zwei Aliase mit dem angegebenen Dateisystem.

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

Die Antwort zeigt den Status der Aliase, die Amazon FSx dem Dateisystem zuordnet.

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

```
}
```

2. Verwenden Sie den `describe-file-system-aliases` CLI-Befehl ([DescribeFileSystemAliases](#) entspricht der API-Operation), um den Status der Aliase zu überwachen, die Sie verknüpfen.
3. Wenn der den Wert `AVAILABLE Lifecycle` hat (ein Vorgang, der bis zu 2,5 Minuten dauert), können Sie mithilfe des DNS-Alias auf Ihr Dateisystem zugreifen, indem Sie Service Principal Names (SPNs) konfigurieren und einen DNS-CNAME-Eintrag für den Alias aktualisieren oder erstellen. Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisystem](#).

So trennen Sie DNS-Aliase von Dateisystemen (CLI)

- Verwenden Sie den `disassociate-file-system-aliases` CLI-Befehl oder die [DisassociateFileSystemAliases](#) API-Operation, um DNS-Aliase von einem vorhandenen Dateisystem zu trennen.

Der folgende Befehl trennt einen Alias von einem Dateisystem.

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

Die Antwort zeigt den Status der Aliase, die Amazon FSx vom Dateisystem trennt.

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

Verwenden Sie den `describe-file-system-aliases` CLI-Befehl ([DescribeFileSystemAliases](#) entspricht der API-Operation), um den Status der Aliase zu überwachen. Es dauert bis zu 2,5 Minuten, bis der Alias gelöscht ist.

# Verwaltung von Dateifreigaben auf FSx for Windows File Server Server-Dateisystemen

In diesem Thema wird beschrieben, wie Sie Dateifreigaben verwalten können, indem Sie die folgenden Aufgaben ausführen.

- Erstellen Sie eine neue Dateifreigabe
- Ändern Sie eine bestehende Dateifreigabe
- Entfernen Sie eine bestehende Dateifreigabe

Sie können die Windows-native Shared Folders-GUI und die Amazon FSx CLI für die Fernverwaltung verwenden, PowerShell um Dateifreigaben auf Ihrem FSx for Windows File Server Server-Dateisystem zu verwalten. Es kann zu Verzögerungen kommen, wenn Sie die Shared Folder-GUI (fsmgmt.msc) verwenden, wenn Sie das Kontextmenü für Shares, die sich auf einem anderen Dateisystem befinden, zum ersten Mal öffnen. Um diese Verzögerungen zu vermeiden, sollten Sie diese Option verwenden, PowerShell um Dateifreigaben zu verwalten, die sich auf mehreren Dateisystemen befinden.

Beachten Sie, dass für alle von Windows unterstützten Dateisysteme Regeln und Einschränkungen in Bezug auf die Namen von Dateien und Verzeichnissen gelten.“. Um sicherzustellen, dass Sie Ihre Daten erfolgreich erstellen und darauf zugreifen können, sollten Sie Ihre Dateien und Verzeichnisse gemäß diesen Windows-Richtlinien benennen. Weitere Informationen finden Sie unter [Namenskonventionen](#).

## Warning

Amazon FSx setzt voraus, dass der SYSTEM-Benutzer für jeden Ordner, in dem Sie eine SMB-Dateifreigabe erstellen, über NTFS-ACL-Berechtigungen mit Vollzugriff verfügt. Ändern Sie nicht die NTFS-ACL-Berechtigungen für diesen Benutzer in Ihren Ordnern, da dies dazu führen kann, dass auf Ihre Dateifreigaben nicht mehr zugegriffen werden kann.

## Verwaltung von Dateifreigaben mit der Benutzeroberfläche für gemeinsame Ordner

Um Dateifreigaben in Ihrem Amazon FSx-Dateisystem zu verwalten, können Sie die Shared Folders-GUI verwenden. Die Benutzeroberfläche für gemeinsame Ordner bietet einen zentralen Ort für die Verwaltung aller freigegebenen Ordner auf einem Windows-Server. In den folgenden Verfahren wird beschrieben, wie Sie Ihre Dateifreigaben verwalten.

So verbinden Sie gemeinsam genutzte Ordner mit Ihrem Dateisystem FSx for Windows File Server

1. Starten Sie Ihre Amazon EC2 EC2-Instanz und verbinden Sie sie mit dem Microsoft Active Directory, mit dem Ihr Amazon FSx-Dateisystem verknüpft ist. Wählen Sie dazu eines der folgenden Verfahren aus dem AWS Directory Service Administratorhandbuch aus:
  - [Schließen Sie sich nahtlos einer Windows EC2-Instanz an](#)
  - [Manuell einer Windows-Instanz beitreten](#)
2. Stellen Sie als Benutzer, der Mitglied der Gruppe der Dateisystemadministratoren ist, eine Connect zu Ihrer Instanz her. In AWS Managed Microsoft Active Directory wird diese Gruppe AWS Delegated FSx Administrators genannt. In Ihrem selbstverwalteten Microsoft Active Directory heißt diese Gruppe Domänen-Admins oder der benutzerdefinierte Name für die Administratorgruppe, den Sie bei der Erstellung angegeben haben. Weitere Informationen finden Sie unter [Connect to your Windows Instance](#) im Amazon Elastic Compute Cloud-Benutzerhandbuch für Windows-Instances.
3. Öffnen Sie das Startmenü und führen Sie fsmgmt.msc mit „Als Administrator ausführen“ aus. Dadurch wird das GUI-Tool Shared Folders geöffnet.
4. Wählen Sie unter Aktion die Option Connect zu einem anderen Computer herstellen aus.
5. Geben Sie für „Anderer Computer“ beispielsweise **amznfsxabcd0123.corp.example.com** den Namen des Domain Name System (DNS) für Ihr Amazon FSx-Dateisystem ein.

Um den DNS-Namen Ihres Dateisystems auf der Amazon FSx-Konsole zu finden, wählen Sie Dateisysteme, wählen Sie Ihr Dateisystem aus und überprüfen Sie dann den Abschnitt Netzwerk und Sicherheit auf der Seite mit den Dateisystemdetails. Sie können den DNS-Namen auch in der Antwort auf den [DescribeFileSystems-API-Vorgang](#) abrufen.

6. Wählen Sie OK aus. Ein Eintrag für Ihr Amazon FSx-Dateisystem erscheint dann in der Liste für das Tool Shared Folders.



Da Shared Folders nun mit Ihrem Amazon FSx-Dateisystem verbunden ist, können Sie die Windows-Dateifreigaben auf dem Dateisystem verwalten. Die Standardfreigabe heißt `\share`. Sie können dies mit den folgenden Aktionen tun:

- Neue Dateifreigabe erstellen — Wählen Sie im Tool Shared Folders im linken Bereich Shares aus, um die aktiven Shares für Ihr Amazon FSx-Dateisystem zu sehen. Wählen Sie Neue Freigabe und schließen Sie den Assistenten zum Erstellen eines gemeinsamen Ordners ab.

Sie müssen den lokalen Ordner erstellen, bevor Sie die neue Dateifreigabe erstellen können. Sie können das wie folgt tun:

- Verwenden des Tools für gemeinsame Ordner: Klicken Sie auf „Durchsuchen“, wenn Sie den lokalen Ordnerpfad angeben, und klicken Sie auf „Neuen Ordner erstellen“, um den lokalen Ordner zu erstellen.
- Über die Befehlszeile:

```
New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share  
  \MyNewShare
```

- Dateifreigabe ändern — Öffnen Sie im Tool „Gemeinsame Ordner“ im rechten Bereich das Kontextmenü (Rechtsklick) für die Dateifreigabe, die Sie ändern möchten, und wählen Sie „Eigenschaften“. Ändern Sie die Eigenschaften und wählen Sie OK.
- Dateifreigabe entfernen — Öffnen Sie im Tool „Gemeinsame Ordner“ im rechten Bereich das Kontextmenü (Rechtsklick) für die Dateifreigabe, die Sie entfernen möchten, und wählen Sie dann Freigabe beenden aus.

#### Note

Bei Single-AZ 2- und Multi-AZ-Dateisystemen ist das Entfernen von Dateifreigaben oder das Ändern von Dateifreigaben (einschließlich der Aktualisierung von Berechtigungen, Benutzerbeschränkungen und anderen Eigenschaften) mit dem GUI-Tool Shared Folders nur möglich, wenn Sie über den DNS-Namen des Amazon FSx-Dateisystems eine Verbindung zu `fsmgmt.msc` herstellen. Das GUI-Tool Shared Folders unterstützt diese Aktionen nicht, wenn Sie die Verbindung über die IP-Adresse oder den DNS-Aliasnamen des Dateisystems herstellen.

**Note**

Wenn Sie das GUI-Tool fsmgmt.msc Shared Folders verwenden, um auf Freigaben zuzugreifen, die sich auf mehreren FSx-Dateisystemen befinden, kann es beim ersten Öffnen des Dateifreigabe-Kontextmenüs für eine Freigabe, die sich auf einem anderen Dateisystem befindet, zu Verzögerungen kommen. Um diese Verzögerungen zu vermeiden, können Sie Dateifreigaben wie unten beschrieben verwalten. PowerShell

## Dateifreigaben verwalten mit PowerShell

Sie können Dateifreigaben mithilfe von benutzerdefinierten Fernverwaltungsbefehlen für verwalten. PowerShell Diese Befehle können Ihnen helfen, diese Aufgaben einfacher zu automatisieren:

- Migration von Fileshares auf bestehenden Dateiservern zu Amazon FSx
- Synchronisation von Dateifreigaben zwischen AWS Regionen für die Notfallwiederherstellung
- Programmatische Verwaltung von Dateifreigaben für laufende Workflows, wie z. B. die Bereitstellung von Dateifreigaben im Team

Informationen zur Verwendung der Amazon FSx CLI für die Fernverwaltung finden Sie PowerShell unter [Verwenden der Amazon FSx CLI für PowerShell](#).

In der folgenden Tabelle sind die Amazon FSx CLI Remote PowerShell Management-Befehle aufgeführt, mit denen Sie Dateifreigaben auf FSx for Windows File Server Server-Dateisystemen verwalten können.

| Befehl zur Verwaltung von Share | Beschreibung                                         |
|---------------------------------|------------------------------------------------------|
| New-FSxSmbShare                 | Erstellt eine neue Dateifreigabe.                    |
| Remove-FSxSmbShare              | Entfernt eine Dateifreigabe.                         |
| Get-FSxSmbShare                 | Ruft bestehende Dateifreigaben ab.                   |
| Set-FSxSmbShare                 | Legt Eigenschaften für eine gemeinsame Nutzung fest. |

| Befehl zur Verwaltung von Share | Beschreibung                                                                                                                               |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Get-FSxSmbShareAccess           | Ruft die Zugriffskontrollliste (ACL) einer Freigabe ab.                                                                                    |
| Grant-FSxSmbShareAccess         | Fügt der Sicherheitsbeschreibung einer Freigabe einen Eintrag zur Zugangskontrolle (Access Control Entry, ACE) für einen Treuhänder hinzu. |
| Revoke-FSxSmbShareAccess        | Entfernt alle zulässigen ACEs für einen Treuhänder aus der Sicherheitsbeschreibung einer Aktie.                                            |
| Block-FSxSmbShareAccess         | Fügt der Sicherheitsbeschreibung einer Aktie einen Deny-ACE für einen Treuhänder hinzu.                                                    |
| Unblock-FSxSmbShareAccess       | Entfernt alle Deny-ACEs für einen Treuhänder aus der Sicherheitsbeschreibung einer Aktie.                                                  |

Die Online-Hilfe für jeden Befehl enthält eine Referenz zu allen Befehlsoptionen. Um auf diese Hilfe zuzugreifen, führen Sie den Befehl `-?` beispielsweise mit einem `Get-FSxSmbShare -?`.

## Anmeldeinformationen an New-F Share SxSmb übergeben

Sie können Anmeldeinformationen an New-F übergeben, SxSmbShare sodass Sie es in einer Schleife ausführen können, um Hunderte oder Tausende von Shares zu erstellen, ohne die Anmeldeinformationen jedes Mal erneut eingeben zu müssen.

Bereiten Sie das Anmeldeinformationsobjekt vor, das für die Erstellung der Dateifreigaben auf Ihrem FSx for Windows File Server Server-Dateiserver erforderlich ist, indem Sie eine der folgenden Optionen verwenden.

- Verwenden Sie den folgenden Befehl, um das Anmeldeinformationsobjekt interaktiv zu generieren.

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

- Verwenden Sie den folgenden Befehl, um das Anmeldeinformationsobjekt mithilfe einer AWS Secrets Manager Ressource zu generieren.

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

## Eine kontinuierlich verfügbare (CA-) Freigabe wird erstellt

Sie können kontinuierlich verfügbare (CA) Shares mit der Amazon FSx CLI for Remote Management auf PowerShell erstellen. CA-Shares, die auf einem FSx for Windows File Server Multi-AZ-Dateisystem erstellt wurden, sind äußerst robust und hochverfügbar. Ein Amazon FSx Single-AZ-Dateisystem basiert auf einem einzelnen Knoten-Cluster. Aus diesem Grund sind CA-Shares, die auf einem Single-AZ-Dateisystem erstellt wurden, äußerst robust, aber nicht hochverfügbar. Verwenden Sie den `New-FSxSmbShare` Befehl, bei dem die `-ContinuouslyAvailable` Option auf gesetzt ist, `$True` um anzugeben, dass es sich bei der Freigabe um eine kontinuierlich verfügbare Freigabe handelt. Im Folgenden finden Sie einen Beispielbefehl zum Erstellen einer CA-Freigabe.

```
New-FSxSmbShare -Name "New CA Share" -Path "D:\share\new-share" -Description "CA share"
  -ContinuouslyAvailable $True
```

Sie können die `-ContinuouslyAvailable` Option für eine bestehende Dateifreigabe mit dem `Set-FSxSmbShare` Befehl ändern.

Stellen Sie fest, ob eine bestehende Dateifreigabe kontinuierlich verfügbar ist

Verwenden Sie den folgenden Befehl, um den Wert der Eigenschaft `Continuously Available` für eine bestehende Dateifreigabe anzuzeigen.

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

Wenn CA aktiviert ist, enthält die Ausgabe die folgende Zeile:

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

Wenn CA nicht aktiviert ist, enthält die Ausgabe die folgende Zeile:

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

Verwenden Sie den folgenden Befehl, um Continuously Available für eine bestehende Dateifreigabe zu aktivieren:

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

## Prüfung des Dateizugriffs

Amazon FSx for Windows File Server unterstützt die Überwachung des Endbenutzerzugriffs auf Dateien, Ordner und Dateifreigaben. Sie können sich dafür entscheiden, die Audit-Ereignisprotokolle eines Dateisystems an andere AWS Dienste zu senden, die eine Vielzahl von Funktionen bieten. Dazu gehören die Aktivierung der Abfrage, Verarbeitung, Speicherung und Archivierung von Protokollen, die Ausgabe von Benachrichtigungen und das Auslösen von Aktionen, um Ihre Sicherheits- und Compliance-Ziele weiter voranzutreiben.

Weitere Informationen zur Verwendung von Dateizugriffsprüfungen, um Einblicke in Zugriffsmuster zu erhalten und Sicherheitsbenachrichtigungen für Endbenutzeraktivitäten zu implementieren, finden Sie unter [Einblicke in Zugriffsmuster für Dateispeicher](#) und [Implementieren von Sicherheitsbenachrichtigungen für Endbenutzeraktivitäten](#).

Mit der Dateizugriffsüberwachung können Sie die Zugriffe von Endbenutzern auf einzelne Dateien, Ordner und Dateifreigaben auf der Grundlage Ihrer definierten Überwachungskontrollen aufzeichnen. Überwachungskontrollen werden auch als NTFS-Systemzugriffskontrolllisten (SACLs) bezeichnet. Wenn Sie bereits Auditkontrollen für Ihre vorhandenen Dateidaten eingerichtet haben, können Sie die Vorteile der Dateizugriffsprüfung nutzen, indem Sie ein neues Amazon FSx for Windows File Server Server-Dateisystem erstellen und Ihre Daten migrieren.

Amazon FSx unterstützt die folgenden Windows-Audit-Ereignisse für Datei-, Ordner- und Dateifreigabezugriffe:

- Für Dateizugriffe unterstützt es: Alle, Ordner durchqueren/Datei ausführen, Ordner auflisten/Daten lesen, Attribute lesen, Dateien erstellen/Daten schreiben, Ordner erstellen/Daten anhängen, Attribute schreiben, Unterordner und Dateien löschen, Löschen, Leseberechtigungen, Berechtigungen ändern und Besitz übernehmen.

- Für Dateifreigabezugriffe unterstützt es: Connect zu einer Dateifreigabe herstellen.

Bei Zugriffen auf Dateien, Ordner und Dateifreigaben unterstützt Amazon FSx die Protokollierung erfolgreicher Versuche (z. B. wenn ein Benutzer mit ausreichenden Berechtigungen erfolgreich auf eine Datei oder Dateifreigabe zugreift), fehlgeschlagener Versuche oder beides.

Sie können konfigurieren, ob Sie die Zugriffsprüfung nur für Dateien und Ordner, nur für Dateifreigaben oder beides durchführen möchten. Sie können auch konfigurieren, welche Zugriffstypen protokolliert werden sollen (nur erfolgreiche Versuche, nur fehlgeschlagene Versuche oder beides). Sie können die Dateizugriffsüberwachung auch jederzeit deaktivieren.

#### Note

Bei der Dateizugriffsüberwachung werden Endbenutzerzugriffsdaten nur ab dem Zeitpunkt aufgezeichnet, zu dem sie aktiviert sind. Das heißt, bei der Dateizugriffsüberwachung werden keine Audit-Ereignisprotokolle über die Datei-, Ordner- und Dateifreigabezugriffsaktivitäten von Endbenutzern generiert, die vor der Aktivierung der Dateizugriffsüberwachung stattgefunden haben.

Die maximale Anzahl unterstützter Zugriffsprüfungsereignisse liegt bei 5.000 Ereignissen pro Sekunde. Zugriffsprüfungsereignisse werden nicht für jeden Lese- und Schreibvorgang einer Datei generiert, sondern nur einmal pro Dateimetadaten-Vorgang generiert, z. B. wenn ein Benutzer eine Datei erstellt, öffnet oder löscht.

#### Themen

- [Überprüfen Sie die Ziele des Ereignisprotokolls](#)
- [Migrieren Sie Ihre Auditkontrollen](#)
- [Ereignisprotokolle anzeigen](#)
- [Einstellungen für die Überwachung von Dateien und Ordnern einrichten](#)
- [Verwaltung der Dateizugriffsüberwachung](#)

## Überprüfen Sie die Ziele des Ereignisprotokolls

Wenn Sie die Dateizugriffsüberwachung aktivieren, müssen Sie einen AWS Service konfigurieren, an den Amazon FSx die Audit-Ereignisprotokolle sendet. Sie können Audit-Ereignisprotokolle entweder

an einen Amazon CloudWatch Logs-Protokollstream in einer CloudWatch Logs-Protokollgruppe oder an einen Amazon Data Firehose-Lieferstream senden. Sie wählen das Ziel der Audit-Ereignisprotokolle entweder bei der Erstellung Ihres Dateisystems von Amazon FSx for Windows File Server oder jederzeit danach, indem Sie ein vorhandenes Dateisystem aktualisieren. Weitere Informationen finden Sie unter [Verwaltung der Dateizugriffsüberwachung](#).

Im Folgenden finden Sie einige Empfehlungen, die Ihnen bei der Entscheidung helfen können, welches Ziel für Audit-Ereignisprotokolle Sie wählen sollten:

- Wählen Sie CloudWatch Logs, wenn Sie Audit-Ereignisprotokolle in der CloudWatch Amazon-Konsole speichern, anzeigen und durchsuchen, mithilfe von Logs Insights Abfragen zu den CloudWatch Protokollen ausführen und CloudWatch Alarme oder Lambda-Funktionen auslösen möchten.
- Wählen Sie Firehose, wenn Sie Ereignisse kontinuierlich in den Speicher in Amazon S3, in eine Datenbank in Amazon Redshift, an Amazon OpenSearch Service oder an AWS Partnerlösungen (wie Splunk oder Datadog) zur weiteren Analyse streamen möchten.

Standardmäßig erstellt und verwendet Amazon FSx eine CloudWatch Standard-Logs-Protokollgruppe in Ihrem Konto als Ziel für Audit-Ereignisprotokolle. Wenn Sie eine benutzerdefinierte CloudWatch Protokollgruppe verwenden oder Firehose als Ziel für das Audit-Ereignisprotokoll verwenden möchten, gelten die folgenden Anforderungen für die Namen und Speicherorte des Audit-Ereignisprotokollziels:

- Der Name der CloudWatch Logs-Protokollgruppe muss mit dem `/aws/fsx/` Präfix beginnen. Wenn Sie beim Erstellen oder Aktualisieren eines Dateisystems auf der Konsole keine bestehende CloudWatch Logs-Protokollgruppe haben, kann Amazon FSx einen Standard-Log-Stream in der CloudWatch `/aws/fsx/windows` Logs-Protokollgruppe erstellen und verwenden. Wenn Sie die Standard-Protokollgruppe nicht verwenden möchten, können Sie über die Konfigurationsoberfläche eine CloudWatch Logs-Protokollgruppe erstellen, wenn Sie Ihr Dateisystem auf der Konsole erstellen oder aktualisieren.
- Der Name des Firehose-Lieferstreams muss mit dem `aws-fsx-` Präfix beginnen. Wenn Sie noch keinen Firehose-Lieferstream haben, können Sie einen erstellen, wenn Sie Ihr Dateisystem an der Konsole erstellen oder aktualisieren.
- Der Firehose-Lieferstream muss so konfiguriert sein, dass er `Direct PUT` als Quelle verwendet wird. Sie können einen vorhandenen Kinesis-Datenstream nicht als Datenquelle für Ihren Lieferstream verwenden.

- Das Ziel (entweder CloudWatch Logs-Protokollgruppe oder Firehose-Lieferstream) muss sich in derselben AWS Partition und AWS-Konto wie Ihr Amazon FSx-Dateisystem befinden. AWS-Region

Sie können das Ziel des Audit-Ereignisprotokolls jederzeit ändern (z. B. von CloudWatch Logs zu Firehose). Wenn Sie dies tun, werden neue Audit-Ereignisprotokolle nur an das neue Ziel gesendet.

## Bereitstellung des Audit-Ereignisprotokolls nach bestem Wissen

In der Regel werden die Aufzeichnungen des Audit-Ereignisprotokolls innerhalb von Minuten an das Ziel übermittelt, manchmal kann dies jedoch länger dauern. In sehr seltenen Fällen können Aufzeichnungen aus den Protokollen von Prüfungsereignissen übersehen werden. Wenn Ihr Anwendungsfall eine bestimmte Semantik erfordert (z. B. um sicherzustellen, dass keine Prüfereignisse übersehen werden), empfehlen wir Ihnen, bei der Gestaltung Ihrer Workflows verpasste Ereignisse zu berücksichtigen. Sie können nach verpassten Ereignissen suchen, indem Sie die Datei- und Ordnerstruktur in Ihrem Dateisystem scannen.

## Migrieren Sie Ihre Auditkontrollen

Wenn Sie bereits Audit Controls (SACLs) für Ihre vorhandenen Dateidaten eingerichtet haben, können Sie ein Amazon FSx-Dateisystem erstellen und Ihre Daten in Ihr neues Dateisystem migrieren. Wir empfehlen AWS DataSync die Verwendung, um Daten und die zugehörigen SACLs in Ihr Amazon FSx-Dateisystem zu übertragen. Als alternative Lösung können Sie Robocopy (Robust File Copy) verwenden. Weitere Informationen finden Sie unter [Migration von vorhandenem Dateispeicher zu Amazon FSx](#).

## Ereignisprotokolle anzeigen

Sie können die Audit-Ereignisprotokolle einsehen, nachdem Amazon FSx mit der Ausgabe begonnen hat. Wo und wie Sie die Protokolle einsehen, hängt vom Ziel des Audit-Ereignisprotokolls ab:

- Sie können die CloudWatch Protokollprotokolle anzeigen, indem Sie zur CloudWatch Konsole gehen und die Protokollgruppe und den Protokollstream auswählen, an die Ihre Audit-Ereignisprotokolle gesendet werden sollen. Weitere Informationen finden Sie unter [An CloudWatch Logs gesendete Protokolldaten anzeigen](#) im Amazon CloudWatch Logs-Benutzerhandbuch.

Sie können CloudWatch Logs Insights verwenden, um Ihre Protokolldaten interaktiv zu suchen und zu analysieren. Weitere Informationen finden Sie unter [Analysieren von Protokolldaten mit CloudWatch Logs Insights](#) im Amazon CloudWatch Logs-Benutzerhandbuch.



Sie können die Audit-Ereignisprotokolle auch nach Amazon S3 exportieren. Weitere Informationen finden Sie unter [Exportieren von Protokolldaten nach Amazon S3](#), ebenfalls im Amazon CloudWatch Logs-Benutzerhandbuch.

- Sie können die Audit-Ereignisprotokolle auf Firehose nicht anzeigen. Sie können Firehose jedoch so konfigurieren, dass die Protokolle an ein Ziel weitergeleitet werden, von dem aus Sie lesen können. Zu den Zielen gehören Amazon S3, Amazon Redshift, Amazon OpenSearch Service und Partnerlösungen wie Splunk und Datadog. Weitere Informationen finden [Sie unter Ziel auswählen](#) im Amazon Data Firehose Developer Guide.

## Ereignisfelder prüfen

Dieser Abschnitt enthält Beschreibungen der Informationen in den Protokollen von Prüfungsereignissen und Beispiele für Prüfereignisse.

Im Folgenden werden die wichtigsten Felder eines Windows-Überwachungsereignisses beschrieben.

- EventID bezieht sich auf die von Microsoft definierte Windows-Ereignisprotokoll-Event-ID. Informationen zu [Dateisystemereignissen und Dateifreigabeereignissen finden Sie in der Microsoft-Dokumentation](#).
- SubjectUserName bezieht sich auf den Benutzer, der den Zugriff durchführt.
- ObjectName bezieht sich auf die Zielfeile, den Ordner oder die Dateifreigabe, auf die zugegriffen wurde.
- ShareName ist für Ereignisse verfügbar, die für den Dateifreigabezugriff generiert werden. EventID 5140 wird beispielsweise generiert, wenn auf ein Netzwerk-Share-Objekt zugegriffen wurde.
- IpAddress bezieht sich auf den Client, der das Ereignis für Dateifreigabeereignisse ausgelöst hat.
- Schlüsselwörter, sofern verfügbar, geben an, ob der Dateizugriff erfolgreich war oder fehlgeschlagen ist. Für erfolgreiche Zugriffe ist 0x8020000000000000 der Wert. Für fehlgeschlagene Zugriffe ist der Wert 0x8010000000000000.
- TimeCreated SystemTime bezieht sich auf die Zeit, zu der das Ereignis im System generiert und im <YYYY-MM-DDThh:mm:ss.s>Z-Format angezeigt wurde.
- Computer bezieht sich auf den DNS-Namen des Dateisystems Windows Remote PowerShell Endpoint und kann zur Identifizierung des Dateisystems verwendet werden.
- AccessMask bezieht sich, sofern verfügbar, auf die Art des ausgeführten Dateizugriffs (z. B. ReadData, WriteData).

- `AccessList` bezieht sich auf den angeforderten oder gewährten Zugriff auf ein Objekt. Einzelheiten finden Sie in der Tabelle unten und in der Microsoft-Dokumentation (z. B. in [Ereignis 4556](#)).

| Art des Zugriffs                                | Zugriffsmaske | Wert   |
|-------------------------------------------------|---------------|--------|
| Daten lesen oder Verzeichnis auflisten          | 0x1           | %4416  |
| Daten schreiben oder Datei hinzufügen           | 0x2           | %4417  |
| Daten anhängen oder Unterverzeichnis hinzufügen | 0x4           | %4418  |
| Erweiterte Attribute lesen                      | 0x8           | %4419  |
| Erweiterte Attribute schreiben                  | 0x10          | %4420  |
| Ausführen/Durchqueren                           | 0x20          | %4421  |
| Kind löschen                                    | 0x40          | %4422  |
| Attribute lesen                                 | 0x80          | %%4423 |
| Schreibattribute                                | 0 x 100       | %%4424 |
| Löschen                                         | 0x10000       | %%1537 |
| ACL lesen                                       | 0x20000       | %%1538 |
| ACL schreiben                                   | 0x40000       | %%1539 |
| Besitzer schreiben                              | 0x80000       | %%1540 |
| Synchronisieren                                 | 0x100000      | %%1541 |
| Zugriffssicherheit (ACL)                        | 0x1000000     | %%1542 |

Im Folgenden finden Sie einige wichtige Ereignisse mit Beispielen. Beachten Sie, dass das XML aus Gründen der Lesbarkeit formatiert ist.

Die Ereignis-ID 4660 wird protokolliert, wenn ein Objekt gelöscht wird.

```
<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>
```

Die Ereignis-ID 4659 wird bei einer Anforderung zum Löschen einer Datei protokolliert.

```
<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>
```

Die Ereignis-ID 4663 wird protokolliert, wenn ein bestimmter Vorgang an dem Objekt ausgeführt wurde. Das folgende Beispiel zeigt das Lesen von Daten aus einer Datei, anhand derer interpretiert werden kann. 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>
```

Das folgende Beispiel zeigt das Schreiben/Anhängen von Daten aus einer Datei, anhand derer interpretiert werden kann. 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>
```

Die Ereignis-ID 4656 gibt an, dass ein bestimmter Zugriff für ein Objekt angefordert wurde. Im folgenden Beispiel wurde die Leseanforderung für ObjectName „permtest“ initiiert und war ein fehlgeschlagener Versuch, wie der Keyword-Wert von zeigt. 0x8010000000000000

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}' />
<EventID>4656</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords><TimeCreated
  SystemTime='2021-06-03T19:22:55.113783500Z' />
<EventRecordID>308919</EventRecordID><Correlation/><Execution ProcessID='4'
  ThreadID='4924' />
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0x0</Data><Data
  Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1541
  %%4416
  %%4423
```

```

</Data><Data Name='AccessReason'>%%1541: %%1805
%%4416: %%1805
%%4423: %%1811 D:(A;OICI;0x1301bf;;;AU)
</Data><Data Name='AccessMask'>0x100081</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='RestrictedSidCount'>0</Data><Data Name='ProcessId'>0x4</Data><Data
Name='ProcessName'></Data>
<Data Name='ResourceAttributes'>-</Data></EventData></Event>

```

Die Ereignis-ID 4670 wird protokolliert, wenn die Berechtigungen für ein Objekt geändert werden. Das folgende Beispiel zeigt, dass der Benutzer „admin“ die Berechtigung für „permtest“ geändert hat, um der SID ObjectName „S-1-5-21-658495921-4185342820-3824891517-1113“ Berechtigungen hinzuzufügen. Weitere Informationen zur Interpretation der Berechtigungen finden Sie in der Microsoft-Dokumentation.

```

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}' />
<EventID>4670</EventID><Version>0</Version><Level>0</Level>
<Task>13570</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='2021-06-03T19:39:47.537129500Z' /><EventRecordID>308992</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='2776' /><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0xcc8</Data>
<Data Name='OldSd'>D:PAI(A;OICI;FA;;;SY)
(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-2622)</Data>
<Data Name='NewSd'>D:PARAI(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-1113)
(A;OICI;FA;;;SY)(A;OICI;FA;;;
S-1-5-21-658495921-4185342820-3824891517-2622)</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data></EventData></Event>

```

Die Ereignis-ID 5140 wird bei jedem Zugriff auf eine Dateifreigabe protokolliert.

```

<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>

```

Die Ereignis-ID 5145 wird protokolliert, wenn der Zugriff auf Dateifreigabeebene verweigert wird. Das folgende Beispiel zeigt, dass der Zugriff auf ShareName „demoshare01“ verweigert wurde.

```

<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>
```

Wenn Sie CloudWatch Logs Insights verwenden, um Ihre Protokolldaten zu durchsuchen, können Sie Abfragen in den Ereignisfeldern ausführen, wie die folgenden Beispiele zeigen:

- So fragen Sie nach einer bestimmten Ereignis-ID ab:

```
fields @message
| filter @message like /4660/
```

- Um alle Ereignisse abzufragen, die einem bestimmten Dateinamen entsprechen:

```
fields @message
| filter @message like /event.txt/
```

Weitere Informationen zur CloudWatch Logs Insights-Abfragesprache finden Sie unter [Analysieren von Protokolldaten mit CloudWatch Logs Insights](#) im Amazon CloudWatch Logs-Benutzerhandbuch.

## Einstellungen für die Überwachung von Dateien und Ordnern einrichten

Sie müssen Überwachungskontrollen für die Dateien und Ordner einrichten, die auf Benutzerzugriffsversuche überprüft werden sollen. Überwachungskontrollen werden auch als NTFS-Systemzugriffskontrolllisten (SACLs) bezeichnet.

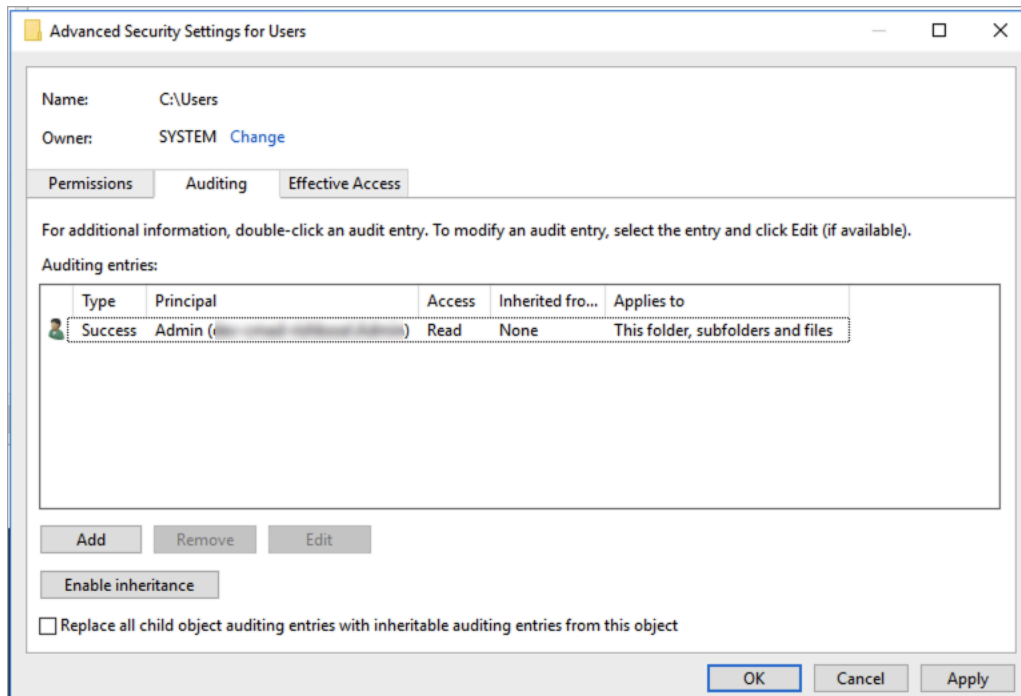
Sie konfigurieren Überwachungskontrollen mithilfe der systemeigenen GUI-Oberfläche von Windows oder programmgesteuert mithilfe von Windows-Befehlen. PowerShell Wenn die Vererbung aktiviert ist, müssen Sie die Überwachungskontrollen in der Regel nur für die Ordner der obersten Ebene einrichten, für die Sie Zugriffe protokollieren möchten.

Verwenden Sie die Windows-GUI, um den Überwachungszugriff festzulegen

Verwenden Sie den Windows-Datei-Explorer, um eine grafische Benutzeroberfläche zum Einrichten von Überwachungskontrollen für Ihre Dateien und Ordner zu verwenden. Öffnen Sie für eine bestimmte Datei oder einen Ordner den Windows-Datei-Explorer und wählen Sie die Registerkarte Eigenschaften > Sicherheit > Erweitert > Überwachung aus.

Im folgenden Beispiel für eine Überwachungssteuerung werden erfolgreiche Ereignisse für einen Ordner geprüft. Ein Eintrag im Windows-Ereignisprotokoll wird immer dann ausgegeben, wenn dieses Handle vom Admin-Benutzer erfolgreich zum Lesen geöffnet wird.





Das Feld Typ gibt an, welche Aktionen Sie überwachen möchten. Setzen Sie dieses Feld auf Erfolgreich, um erfolgreiche Versuche zu prüfen, auf Fehler bei der Prüfung fehlgeschlagener Versuche oder Alle, um sowohl erfolgreiche als auch fehlgeschlagene Versuche zu überwachen.

Weitere Informationen zu den Eingabefeldern für die Überwachung finden Sie in der Microsoft-Dokumentation unter [Anwenden einer grundlegenden Überwachungsrichtlinie auf eine Datei oder einen Ordner](#).

Verwenden von PowerShell Befehlen zum Einrichten des Überwachungszugriffs

Sie können den Microsoft Set -Ac1 Windows-Befehl verwenden, um die Auditing-SCL für jede Datei oder jeden Ordner festzulegen. Informationen zu diesem Befehl finden Sie in der Microsoft [Set-Acl-Dokumentation](#).

Im Folgenden finden Sie ein Beispiel für die Verwendung einer Reihe von PowerShell Befehlen und Variablen, um den Überwachungszugriff für erfolgreiche Versuche festzulegen. Sie können diese Beispielbefehle an die Anforderungen Ihres Dateisystems anpassen.

```
$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
```

## Verwaltung der Dateizugriffsüberwachung

Sie können die Dateizugriffsprüfung aktivieren, wenn Sie ein neues Dateisystem von Amazon FSx für Windows File Server erstellen. Die Dateizugriffsüberwachung ist standardmäßig deaktiviert, wenn Sie ein Dateisystem von der Amazon FSx-Konsole aus erstellen.

Auf vorhandenen Dateisystemen, für die die Dateizugriffsüberwachung aktiviert ist, können Sie die Einstellungen für die Dateizugriffsüberwachung ändern, einschließlich der Änderung der Zugriffsversuchstypen für Datei- und Dateifreigabezugriffe sowie des Ziels des Audit-Ereignisprotokolls. Sie können diese Aufgaben mit der Amazon FSx-Konsole oder API ausführen.

AWS CLI

### Note

Die Dateizugriffsprüfung wird nur auf Dateisystemen von Amazon FSx for Windows File Server mit einer Durchsatzkapazität von 32 MB/s oder mehr unterstützt. Sie können kein Dateisystem mit einer Durchsatzkapazität von weniger als 32 MB/s erstellen oder aktualisieren, wenn die Dateizugriffsüberwachung aktiviert ist. Sie können die Durchsatzkapazität jederzeit ändern, nachdem Sie das Dateisystem erstellt haben. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

Um die Dateizugriffsüberwachung beim Erstellen eines Dateisystems (Konsole) zu aktivieren

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, das [Erstellen Sie Ihr Dateisystem](#) im Abschnitt Erste Schritte beschrieben ist.
3. Öffnen Sie den Abschnitt Auditing — optional. Die Dateizugriffsüberwachung ist standardmäßig deaktiviert.

▼ **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. Gehen Sie wie folgt vor, um die Dateizugriffsüberwachung zu aktivieren und zu konfigurieren.
  - Wählen Sie unter Zugriff auf Dateien und Ordner protokollieren die Protokollierung erfolgreicher und/oder fehlgeschlagener Versuche aus. Die Protokollierung ist für Dateien und Ordner deaktiviert, wenn Sie keine Auswahl treffen.
  - Wählen Sie unter Zugriff auf Dateifreigaben protokollieren die Protokollierung erfolgreicher und/oder fehlgeschlagener Versuche aus. Die Protokollierung ist für Dateifreigaben deaktiviert, wenn Sie keine Auswahl treffen.
  - Wählen Sie für Wählen Sie ein Ziel für das Audit-Ereignisprotokoll die Option CloudWatch Logs oder Firehose aus. Wählen Sie dann ein vorhandenes Protokoll oder einen Zustellungsstream aus oder erstellen Sie einen neuen. Für CloudWatch Logs kann Amazon FSx einen Standard-Log-Stream in der CloudWatch /aws/fsx/windows Logs-Protokollgruppe erstellen und verwenden.

Im Folgenden finden Sie ein Beispiel für eine Konfiguration zur Dateizugriffsüberwachung, mit der erfolgreiche und fehlgeschlagene Zugriffsversuche von Endbenutzern auf Dateien, Ordner

und Dateifreigaben geprüft werden. Die Audit-Ereignisprotokolle werden an das Standardziel für die `/aws/fsx/windows` Protokollgruppe CloudWatch Logs gesendet.

**▼ 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).

**i** 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**

[Create new](#)

**Pricing**  
 Standard Amazon CloudWatch Logs pricing applies based on your usage. [Learn more](#)

5. Fahren Sie mit dem nächsten Abschnitt des Assistenten zum Erstellen von Dateisystemen fort.

Wenn das Dateisystem verfügbar ist, ist die Funktion zur Dateizugriffsüberwachung aktiviert.

So aktivieren Sie die Dateizugriffsüberwachung beim Erstellen eines Dateisystems (CLI)

1. Verwenden Sie beim Erstellen eines neuen Dateisystems die `AuditLogConfiguration` Eigenschaft zusammen mit der [CreateFileSystem](#) API-Operation, um die Dateizugriffsüberwachung für das neue Dateisystem zu aktivieren.

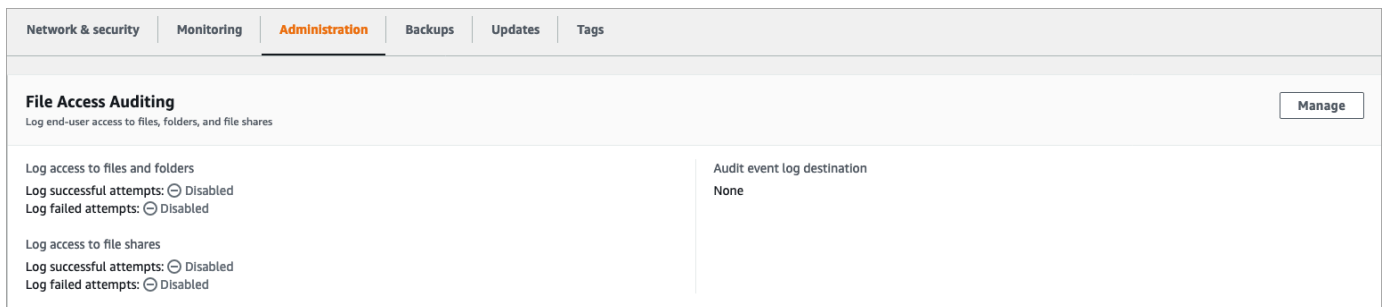
```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
  --windows-configuration
  AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
```

```
FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \  
AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-  
customer-log-group"}'
```

2. Wenn das Dateisystem verfügbar ist, ist die Funktion zur Dateizugriffsüberwachung aktiviert.

Um die Konfiguration der Dateizugriffsüberwachung zu ändern (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Windows-Dateisystem aus, für das Sie die Dateizugriffsprüfung verwalten möchten.
3. Wählen Sie die Registerkarte Administration.
4. Wählen Sie im Bereich Dateizugriffsüberwachung die Option Verwalten aus.



5. Ändern Sie im Dialogfeld „Einstellungen für die Dateizugriffsprüfung verwalten“ die gewünschten Einstellungen.

### 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

- Wählen Sie unter Zugriff auf Dateien und Ordner protokollieren die Protokollierung erfolgreicher und/oder fehlgeschlagener Versuche aus. Die Protokollierung ist für Dateien und Ordner deaktiviert, wenn Sie keine Auswahl treffen.
- Wählen Sie unter Zugriff auf Dateifreigaben protokollieren die Protokollierung erfolgreicher und/oder fehlgeschlagener Versuche aus. Die Protokollierung ist für Dateifreigaben deaktiviert, wenn Sie keine Auswahl treffen.
- Wählen Sie für Wählen Sie ein Ziel für das Audit-Ereignisprotokoll die Option CloudWatch Logs oder Firehose aus. Wählen Sie dann ein vorhandenes Protokoll oder einen Zustellungsstream aus oder erstellen Sie einen neuen.

6. Wählen Sie Speichern.

So ändern Sie die Konfiguration für die Dateizugriffsüberwachung (CLI)

- Verwenden Sie den [update-file-system](#) CLI-Befehl oder die entsprechende [UpdateFileSystem](#) API-Operation.

```
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"}'
```

## Benutzersitzungen und geöffnete Dateien

Mit dem Tool Shared Folders können Sie verbundene Benutzersitzungen überwachen und Dateien auf Ihrem Dateisystem FSx for Windows File Server öffnen. Das Tool Shared Folders bietet einen zentralen Ort, an dem Sie überwachen können, wer mit dem Dateisystem verbunden ist und welche Dateien von wem geöffnet sind. Mit diesem Tool können Sie Folgendes tun:

- Stellen Sie den Zugriff auf gesperrte Dateien wieder her.
- Trennen Sie eine Benutzersitzung, wodurch alle von diesem Benutzer geöffneten Dateien geschlossen werden.

Sie können das Windows-native GUI-Tool Shared Folders und die Amazon FSx CLI für die Fernverwaltung verwenden, um Benutzersitzungen PowerShell zu verwalten und Dateien auf Ihrem FSx for Windows File Server Server-Dateisystem zu öffnen.

## Verwenden der GUI zur Verwaltung von Benutzern und Sitzungen

Die folgenden Verfahren beschreiben, wie Sie Benutzersitzungen verwalten und Dateien auf Ihrem Amazon FSx-Dateisystem mit dem Microsoft Windows-Tool für gemeinsame Ordner öffnen können.

Um das Tool für gemeinsame Ordner zu starten

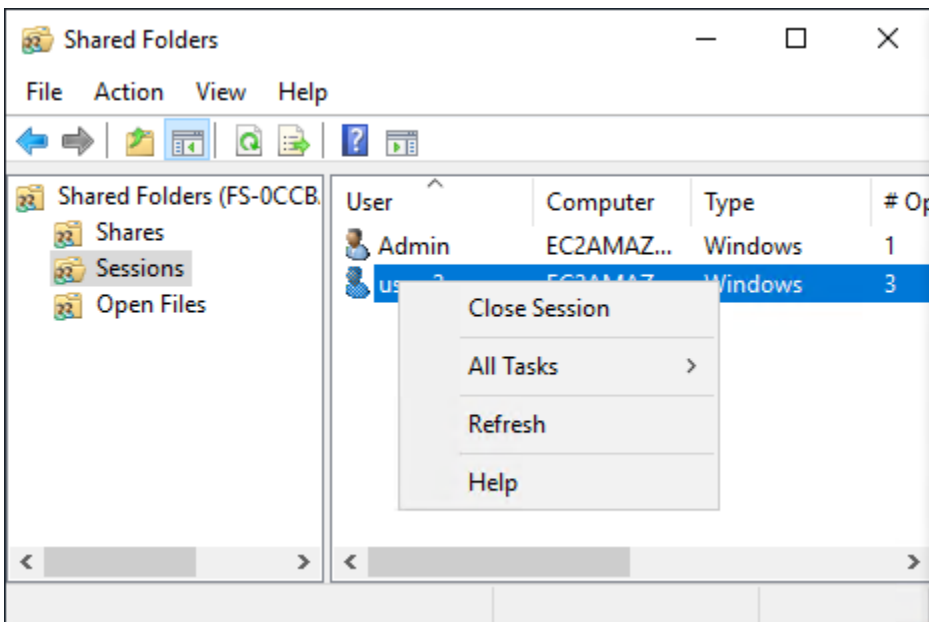
1. Starten Sie Ihre Amazon EC2 EC2-Instance und verbinden Sie sie mit dem Microsoft Active Directory, mit dem Ihr Amazon FSx-Dateisystem verknüpft ist. Wählen Sie dazu eines der folgenden Verfahren aus dem AWS Directory Service Administrationshandbuch aus:

- [Schließen Sie sich nahtlos einer Windows EC2-Instanz an](#)
  - [Manuell einer Windows-Instanz beitreten](#)
2. Stellen Sie als Benutzer, der Mitglied der Gruppe der Dateisystemadministratoren ist, eine Connect zu Ihrer Instance her. In AWS Managed Microsoft Active Directory wird diese Gruppe AWS Delegated FSx Administrators genannt. In Ihrem selbstverwalteten Microsoft Active Directory heißt diese Gruppe Domänen-Admins oder der benutzerdefinierte Name für die Administratorgruppe, den Sie bei der Erstellung angegeben haben. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
  3. Öffnen Sie das Startmenü und führen Sie `fsmgmt.msc` mit `Run As Administrator` Dadurch wird das GUI-Tool Shared Folders geöffnet.
  4. Wählen Sie unter Aktion die Option Connect zu einem anderen Computer herstellen aus.
  5. Geben Sie für „Anderer Computer“ beispielsweise `fs-012345678901234567.ad-domain.com` den DNS-Namen Ihres Amazon FSx-Dateisystems ein.
  6. Wählen Sie OK aus. Ein Eintrag für Ihr Amazon FSx-Dateisystem erscheint dann in der Liste für das Tool Shared Folders.

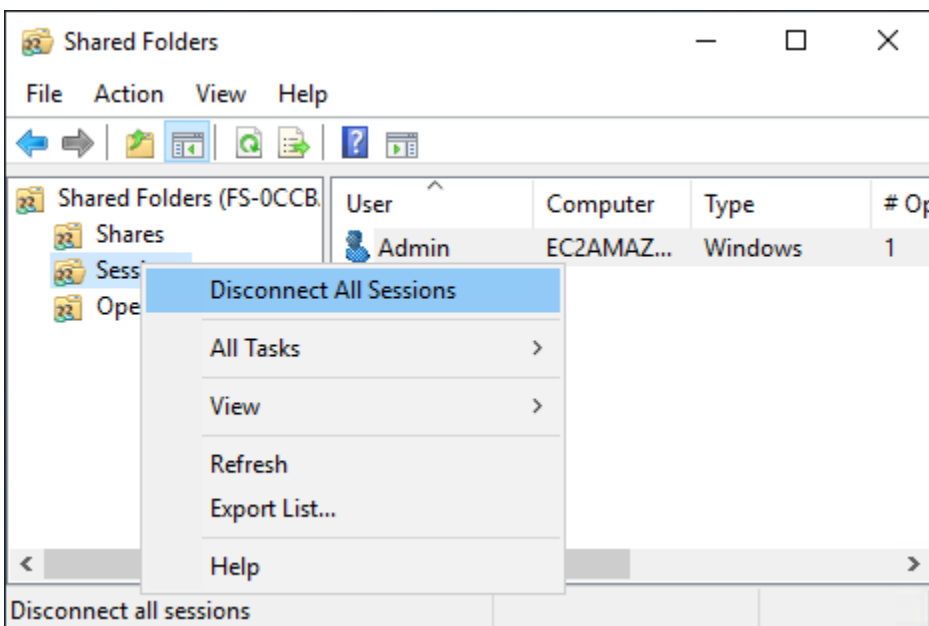
#### Um Benutzersitzungen zu verwalten (GUI)

Wählen Sie im Tool Shared Folders die Option Sessions aus, um alle Benutzersitzungen anzuzeigen, die mit Ihrem FSx for Windows File Server Server-Dateisystem verbunden sind. Wenn ein Benutzer oder eine Anwendung auf eine Dateifreigabe in Ihrem Amazon FSx-Dateisystem zugreift, zeigt Ihnen dieses Snap-In ihre Sitzung. Sie können Sitzungen trennen, indem Sie das Kontextmenü (Rechtsklick) für eine Sitzung öffnen und Sitzung schließen wählen.





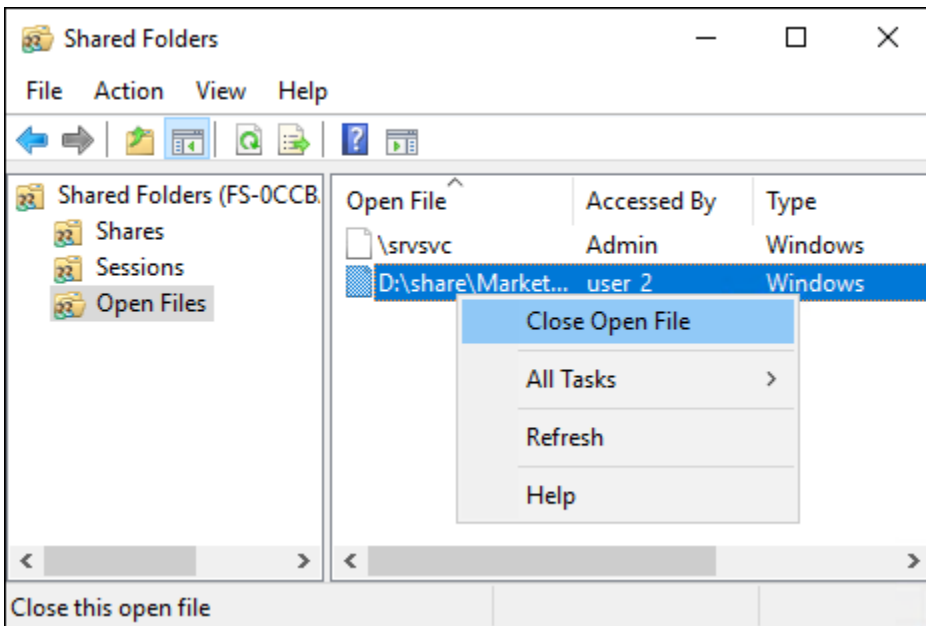
Um alle geöffneten Sitzungen zu trennen, öffnen Sie das Kontextmenü (Rechtsklick) für Sitzungen, wählen Sie Alle Sitzungen trennen und bestätigen Sie Ihre Aktion.



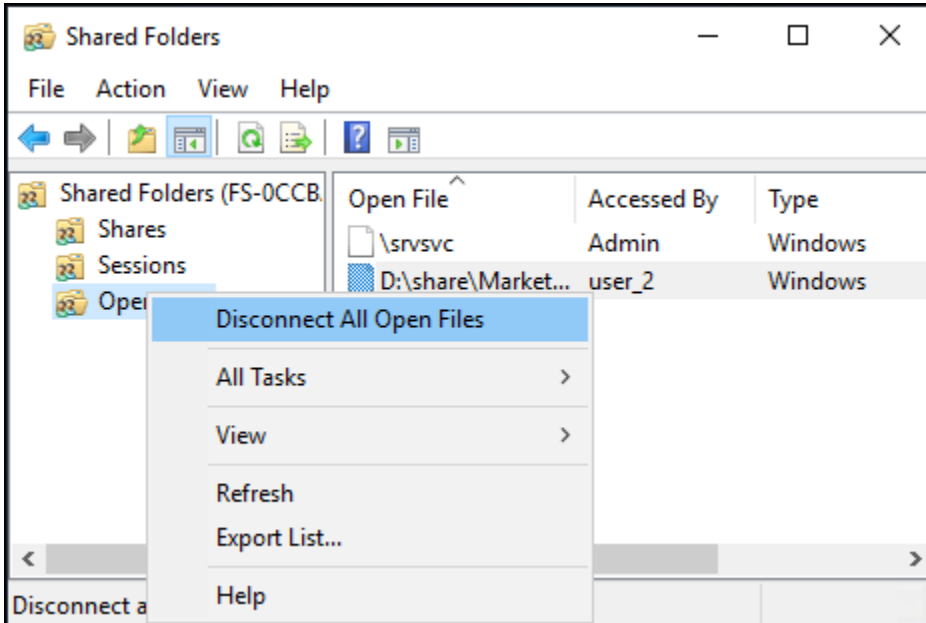
### Um geöffnete Dateien zu verwalten (GUI)

Wählen Sie im Tool „Gemeinsame Ordner“ die Option „Dateien öffnen“, um alle Dateien auf dem System anzuzeigen, die derzeit geöffnet sind. In der Ansicht wird auch angezeigt, welche Benutzer die Dateien oder Ordner geöffnet haben. Diese Informationen können hilfreich sein, um herauszufinden, warum andere Benutzer bestimmte Dateien nicht öffnen können. Sie können jede

Datei schließen, die ein Benutzer geöffnet hat, indem Sie einfach das Kontextmenü (Rechtsklick) für den Eintrag der Datei in der Liste öffnen und Datei schließen wählen.



Um die Verbindung aller geöffneten Dateien im Dateisystem zu trennen, klicken Sie im Kontextmenü (Rechtsklick) auf „Dateien öffnen“ und wählen Sie „Alle geöffneten Dateien trennen“. Bestätigen Sie Ihre Aktion.



## Wird PowerShell zur Verwaltung von Benutzersitzungen und zum Öffnen von Dateien verwendet

Sie können aktive Benutzersitzungen verwalten und Dateien auf Ihrem Dateisystem öffnen, indem Sie die Amazon FSx CLI für die Fernverwaltung verwenden. PowerShell Informationen zur Verwendung dieser CLI finden Sie unter [Verwenden der Amazon FSx CLI für PowerShell](#).

Im Folgenden finden Sie Befehle, die Sie für die Verwaltung von Benutzersitzungen und offenen Dateien verwenden können.

| Befehl               | Beschreibung                                                                                                                                               |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Get-FSxSmbSession    | Ruft Informationen über die SMB-Sitzungen (Server Message Block) ab, die derzeit zwischen dem Dateisystem und den zugehörigen Clients eingerichtet wurden. |
| Close-FSxSmbSession  | Beendet eine SMB-Sitzung.                                                                                                                                  |
| Get-FSxSmbOpenFile   | Ruft Informationen über Dateien ab, die für die mit dem Dateisystem verbundenen Clients geöffnet sind.                                                     |
| Close-FSxSmbOpenFile | Schließt eine Datei, die für einen der Clients des SMB-Servers geöffnet ist.                                                                               |

Die Online-Hilfe für jeden Befehl enthält eine Referenz zu allen Befehlsoptionen. Um auf diese Hilfe zuzugreifen, führen Sie den Befehl `-?` beispielsweise mit einem `Get-FSxSmbSession -?`.

## Datendeduplizierung

FSx unterstützt die Verwendung von Microsoft Data Deduplication zur Identifizierung und Beseitigung redundanter Daten. Große Datensätze enthalten häufig redundante Daten, was die Kosten für die Datenspeicherung erhöht. Bei Dateifreigaben von Benutzern können beispielsweise mehrere Benutzer viele Kopien oder Versionen derselben Datei speichern. Bei Shares für die Softwareentwicklung bleiben viele Binärdateien von Build zu Build unverändert.

Sie können Ihre Datenspeicherkosten senken, indem Sie die Datendeduplizierung für Ihr Dateisystem aktivieren. Durch die Datendeduplizierung werden redundante Daten reduziert oder eliminiert, indem

duplizierte Teile des Datensatzes nur einmal gespeichert werden. Die Datenkomprimierung ist standardmäßig aktiviert, wenn Sie die Datendeduplizierung verwenden. Durch die Komprimierung der Daten nach der Deduplizierung wird der Datenspeicher weiter reduziert. Die Datendeduplizierung wird als Hintergrundprozess ausgeführt, der Ihr Dateisystem kontinuierlich und automatisch scannt und optimiert und für Ihre Benutzer und verbundenen Clients transparent ist.

Die Speichereinsparungen, die Sie mit der Datendeduplizierung erzielen können, hängen von der Art Ihres Datensatzes ab, einschließlich der Menge der Duplizierung in mehreren Dateien. Bei allgemeinen Dateifreigaben liegen die Einsparungen in der Regel bei durchschnittlich 50 bis 60 Prozent. Bei Aktien liegen die Einsparungen zwischen 30 und 50 Prozent bei Benutzerdokumenten und 70 bis 80 Prozent bei Datensätzen zur Softwareentwicklung. Mit dem unten beschriebenen Befehl können Sie die potenziellen Einsparungen durch Deduplizierung messen. `Measure-FSxDedupFileMetadata`

Sie können die Datendeduplizierung auch an Ihre spezifischen Speicheranforderungen anpassen. Sie können die Deduplizierung beispielsweise so konfigurieren, dass sie nur für bestimmte Dateitypen ausgeführt wird, oder Sie können einen benutzerdefinierten Job-Zeitplan erstellen. Da Deduplizierungsaufträge Dateiserverressourcen beanspruchen können, empfehlen wir, den Status Ihrer Deduplizierungsaufträge mit dem unten beschriebenen Befehl zu überwachen. `Get-FSxDedupStatus`

Weitere Informationen zur Datendeduplizierung finden Sie in der Dokumentation Microsoft [Understanding Data Deduplication](#).

#### Note

Weitere Informationen finden Sie in unseren Best Practices für [Bewährte Methoden für die Verwendung der Datendeduplizierung](#). Falls Sie Probleme bei der erfolgreichen Ausführung von Datendeduplizierungsaufträgen haben, finden Sie weitere Informationen unter [Problembehandlung bei der Datendeduplizierung](#).

#### Warning

Es wird nicht empfohlen, bestimmte Robocopy-Befehle mit Datendeduplizierung auszuführen, da diese Befehle die Datenintegrität des Chunk Store beeinträchtigen können. Weitere Informationen finden Sie in der Dokumentation zur [Interoperabilität von Microsoft Data Deduplication](#).

## Bewährte Methoden für die Verwendung der Datendeduplizierung

Im Folgenden finden Sie einige bewährte Methoden für die Verwendung der Datendeduplizierung:

- Planen Sie Datendeduplizierungsaufträge so, dass sie ausgeführt werden, wenn Ihr Dateisystem inaktiv ist: Der Standardzeitplan beinhaltet einen wöchentlichen `GarbageCollection` Job um 2:45 Uhr UTC an Samstagen. Bei einer großen Datenflut in Ihrem Dateisystem kann die Ausführung mehrere Stunden dauern. Wenn dieser Zeitpunkt nicht ideal für Ihre Arbeitslast ist, planen Sie diesen Job so ein, dass er zu einem Zeitpunkt ausgeführt wird, zu dem Sie mit geringem Datenverkehr auf Ihrem Dateisystem rechnen.
- Richten Sie ausreichend Durchsatzkapazität ein, damit die Datendeduplizierung abgeschlossen werden kann: Höhere Durchsatzkapazitäten bieten mehr Arbeitsspeicher. Microsoft empfiehlt, für die Datendeduplizierung 1 GB Arbeitsspeicher pro 1 TB logischer Daten zur Verfügung zu haben. Verwenden Sie die [Amazon FSx-Leistungstabelle](#), um den Speicher zu ermitteln, der der Durchsatzkapazität Ihres Dateisystems zugeordnet ist, und stellen Sie sicher, dass die Speicherressourcen für die Größe Ihrer Daten ausreichend sind.
- Passen Sie die Einstellungen für die Datendeduplizierung an Ihre spezifischen Speicheranforderungen an und reduzieren Sie die Leistungsanforderungen: Sie können die Optimierung auf bestimmte Dateitypen oder Ordner beschränken oder eine Mindestdateigröße und ein Mindestalter für die Optimierung festlegen. Weitere Informationen hierzu finden Sie unter [Datendeduplizierung](#).

## Verwaltung der Datendeduplizierung

Sie können die Datendeduplizierung auf Ihrem Dateisystem mithilfe der Amazon FSx CLI für die Fernverwaltung verwalten. PowerShell Informationen zur Verwendung dieser CLI finden Sie unter [Verwenden der Amazon FSx CLI für PowerShell](#).

Im Folgenden finden Sie Befehle, die Sie für die Datendeduplizierung verwenden können.

| Befehl zur Datendeduplizierung  | Beschreibung                                                                                                                                                                      |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Enable-FSxDedup</a> | Aktiviert die Datendeduplizierung auf der Dateifreigabe. Die Datenkomprimierung nach der Deduplizierung ist standardmäßig aktiviert, wenn Sie die Datendeduplizierung aktivieren. |

| Befehl zur Datendeduplizierung       | Beschreibung                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disable-FSxDedup                     | Deaktiviert die Datendeduplizierung auf der Dateifreigabe.                                                                                                                                                                                                                                                                          |
| Get-FSxDedupConfiguration            | Ruft Informationen zur Deduplizierungskonfiguration ab, einschließlich Mindestdateigröße und Mindestalter für die Optimierung, Komprimierungseinstellungen und ausgeschlossene Dateitypen und Ordner.                                                                                                                               |
| Set-FSxDedupConfiguration            | Ändert die Konfigurationseinstellungen für die Deduplizierung, einschließlich der Mindestdateigröße und des Mindestalters für die Optimierung, der Komprimierungseinstellungen und der ausgeschlossenen Dateitypen und Ordner.                                                                                                      |
| <a href="#">Get-FSxDedupStatus</a>   | Ruft den Deduplizierungsstatus ab und enthält schreibgeschützte Eigenschaften, die die Optimierungseinsparungen und den Status der Optimierungen im Dateisystem, die Zeiten und den Abschlussstatus der letzten Jobs im Dateisystem beschreiben.                                                                                    |
| Get-FSxDedupMetadata                 | Ruft Metadaten zur Deduplizierungsoptimierung ab.                                                                                                                                                                                                                                                                                   |
| Update-FSxDedupStatus                | Berechnet aktualisierte Informationen zu Einsparungen bei der Datendeduplizierung und ruft sie ab.                                                                                                                                                                                                                                  |
| Measure-FSxDedupFileMetadata         | Misst den potenziellen Speicherplatz, den Sie in Ihrem Dateisystem zurückgewinnen können, wenn Sie eine Gruppe von Ordnern löschen, und ruft ihn ab. Dateien enthalten häufig Chunks, die von anderen Ordnern gemeinsam genutzt werden, und die Deduplizierungs-Engine berechnet, welche Chunks eindeutig sind und gelöscht würden. |
| Get-FSxDedupSchedule                 | Ruft Deduplizierungszeitpläne ab, die aktuell definiert sind.                                                                                                                                                                                                                                                                       |
| <a href="#">New-FSxDedupSchedule</a> | Erstellt einen Zeitplan für die Datendeduplizierung und passt ihn an.                                                                                                                                                                                                                                                               |

| Befehl zur Datendeduplizierung       | Beschreibung                                                                                                                   |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Set-FSxDedupSchedule</a> | Ändert die Konfigurationseinstellungen für bestehende Datendeduplizierungszeitpläne.                                           |
| Remove-FSxDedupSchedule              | Löscht einen Deduplizierungsplan.                                                                                              |
| Get-FSxDedupJob                      | Ruft Status und Informationen für alle aktuell ausgeführten oder in der Warteschlange befindlichen Deduplizierungsaufträge ab. |
| Stop-FSxDedupJob                     | Bricht einen oder mehrere angegebene Datendeduplizierungsaufträge ab.                                                          |

Die Online-Hilfe für jeden Befehl enthält eine Referenz zu allen Befehlsoptionen. Um auf diese Hilfe zuzugreifen, führen Sie den Befehl `-?` beispielsweise mit `Enable-FSxDedup -?`.

## Datendeduplizierung aktivieren

Sie aktivieren die Datendeduplizierung auf einer Amazon FSx for Windows File Server Server-Dateifreigabe mit dem `Enable-FSxDedup` folgenden Befehl.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxxxxxxx.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {Enable-FsxDedup }
```

Wenn Sie die Datendeduplizierung aktivieren, werden ein Standardzeitplan und eine Standardkonfiguration erstellt. Mit den folgenden Befehlen können Sie Zeitpläne und Konfigurationen erstellen, ändern und entfernen.

Sie können den `Disable-FSxDedup` Befehl verwenden, um die Datendeduplizierung in Ihrem Dateisystem vollständig zu deaktivieren.

## Erstellen eines Zeitplans für die Datendeduplizierung

Obwohl der Standardzeitplan in den meisten Fällen gut funktioniert, können Sie mithilfe des `New-FSxDedupSchedule` folgenden Befehls einen neuen Deduplizierungsplan erstellen. Zeitpläne für die Datendeduplizierung verwenden UTC-Zeit.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxxxxxxxxx.corp.example.com -  
ConfigurationName FSxRemoteAdmin -ScriptBlock {  
New-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Wed,Sat -  
Start 08:00 -DurationHours 7  
}
```

Dieser Befehl erstellt einen Zeitplan mit dem Namen CustomOptimization, der an den Tagen Montag, Mittwoch und Samstag ausgeführt wird und der Job jeden Tag um 8:00 Uhr (UTC) mit einer maximalen Dauer von 7 Stunden gestartet wird. Danach wird der Job beendet, falls er noch ausgeführt wird.

Beachten Sie, dass durch das Erstellen neuer, benutzerdefinierter Zeitpläne für Deduplizierungsaufträge der vorhandene Standardzeitplan nicht überschrieben oder entfernt wird. Bevor Sie einen benutzerdefinierten Deduplizierungsjob erstellen, sollten Sie den Standardjob deaktivieren, falls Sie ihn nicht benötigen.

Sie können den standardmäßigen Deduplizierungszeitplan deaktivieren, indem Sie den Set-FSxDedupSchedule folgenden Befehl verwenden.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxxxxxxxxx.corp.example.com  
-ConfigurationName FSxRemoteAdmin -ScriptBlock {Set-FSxDedupSchedule -Name  
"BackgroundOptimization" -Enabled $false}
```

Sie können einen Deduplizierungsplan mit dem Befehl entfernen. Remove-FSxDedupSchedule -Name "ScheduleName" Beachten Sie, dass der standardmäßige BackgroundOptimization Deduplizierungszeitplan nicht geändert oder entfernt werden kann und stattdessen deaktiviert werden muss.

## Ändern eines Zeitplans für die Dateneduplizierung

Sie können einen vorhandenen Deduplizierungszeitplan ändern, indem Sie den Set-FSxDedupSchedule folgenden Befehl verwenden.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxxxxxxxxx.corp.example.com -  
ConfigurationName FSxRemoteAdmin -ScriptBlock {  
Set-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days  
Mon,Tues,Wed,Sat -Start 09:00 -DurationHours 9  
}
```



Mit diesem Befehl wird der bestehende CustomOptimization Zeitplan so geändert, dass er an den Tagen Montag bis Mittwoch und Samstag ausgeführt wird und der Job jeden Tag um 9:00 Uhr (UTC) mit einer maximalen Dauer von 9 Stunden gestartet wird. Danach wird der Job beendet, falls er noch ausgeführt wird.

Verwenden Sie den Set-FSxDedupConfiguration Befehl, um die Einstellung für das Mindestdateialter vor der Optimierung zu ändern.

## Die Menge des gespeicherten Speicherplatzes anzeigen

Verwenden Sie den Get-FSxDedupStatus folgenden Befehl, um die Menge an Festplattenspeicher anzuzeigen, die Sie durch die Ausführung der Datendeduplizierung sparen.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxxxxzzzzzzz.corp.example.com -  
ConfigurationName FsxRemoteAdmin -ScriptBlock {  
Get-FSxDedupStatus } | select  
OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate
```

| OptimizedFilesCount | OptimizedFilesSize | SavedSpace        | OptimizedFilesSavingsRate |
|---------------------|--------------------|-------------------|---------------------------|
| -----<br>12587      | -----<br>31163594  | -----<br>25944826 | -----<br>83               |

### Note

Die in der Befehlsantwort für die folgenden Parameter angezeigten Werte sind nicht zuverlässig, und Sie sollten diese Werte nicht verwenden: Capacity,, FreeSpace UsedSpace UnoptimizedSize, und. SavingsRate

## Problembehandlung bei der Datendeduplizierung

Es gibt eine Reihe möglicher Ursachen für Probleme mit der Datendeduplizierung, wie im folgenden Abschnitt beschrieben.

### Themen

- [Die Datendeduplizierung funktioniert nicht](#)
- [Die Deduplizierungswerte werden unerwartet auf 0 gesetzt](#)
- [Nach dem Löschen von Dateien wird kein Speicherplatz im Dateisystem freigegeben](#)

## Die Datendeduplizierung funktioniert nicht

Führen Sie den `Get-FSxDedupStatus` Befehl gemäß den Anweisungen in unserer [Dokumentation zur Datendeduplizierung](#) aus, um den Abschlussstatus der letzten Deduplizierungsaufträge anzuzeigen. Wenn ein oder mehrere Jobs fehlschlagen, sehen Sie möglicherweise keine Erhöhung der freien Speicherkapazität in Ihrem Dateisystem.

Der häufigste Grund für Fehlschläge bei Deduplizierungsaufträgen ist unzureichender Arbeitsspeicher.

- Microsoft [empfiehlt](#), optimal 1 GB Arbeitsspeicher pro 1 TB logischer Daten (oder mindestens 300 MB + 50 MB pro 1 TB logischer Daten) zu haben. Verwenden Sie die [Amazon FSx-Leistungstabelle](#), um den Speicher zu ermitteln, der der Durchsatzkapazität Ihres Dateisystems zugeordnet ist, und stellen Sie sicher, dass die Speicherressourcen für die Größe Ihrer Daten ausreichend sind.
- Deduplizierungsaufträge sind mit der von Windows empfohlenen Standardeinstellung von 25% Speicherzuweisung konfiguriert, was bedeutet, dass für ein Dateisystem mit 32 GB Arbeitsspeicher 8 GB für die Deduplizierung verfügbar sind. Die Speicherzuweisung ist konfigurierbar (mithilfe des `Set-FSxDedupSchedule` Befehls mit Parameter `-Memory`), aber der Verbrauch von zusätzlichem Speicher kann sich auf die Leistung des Dateisystems auswirken.
- Sie können die Konfiguration von Deduplizierungsaufträgen ändern, um den Speicherbedarf weiter zu reduzieren. Sie können die Optimierung beispielsweise auf bestimmte Dateitypen oder Ordner beschränken oder eine Mindestdateigröße und ein Mindestalter für die Optimierung festlegen. Wir empfehlen außerdem, Deduplizierungsaufträge so zu konfigurieren, dass sie in Leerlaufzeiten ausgeführt werden, wenn Ihr Dateisystem nur minimal belastet wird.

Möglicherweise werden auch Fehler angezeigt, wenn für die Ausführung von Deduplizierungsaufträgen nicht genügend Zeit zur Verfügung steht. Möglicherweise müssen Sie die maximale Dauer von Aufträgen ändern, wie unter beschrieben. [Ändern eines Zeitplans für die Datendeduplizierung](#)

Wenn Deduplizierungsaufträge über einen längeren Zeitraum fehlschlagen und während dieses Zeitraums Änderungen an den Daten im Dateisystem vorgenommen wurden, benötigen nachfolgende Deduplizierungsaufträge möglicherweise mehr Ressourcen, um zum ersten Mal erfolgreich abgeschlossen zu werden.

## Die Deduplizierungswerte werden unerwartet auf 0 gesetzt

Die Werte für `SavedSpace` und `OptimizedFilesSavingsRate` sind unerwartet 0 für ein Dateisystem, für das Sie die Datendeduplizierung konfiguriert haben.

Dies kann während der Speicheroptimierung auftreten, wenn Sie die Speicherkapazität des Dateisystems erhöhen. Wenn Sie die Speicherkapazität eines Dateisystems erhöhen, storniert Amazon FSx bestehende Datendeduplizierungsaufträge während des Speicheroptimierungsprozesses, bei dem Daten von den alten Festplatten auf die neuen, größeren Festplatten migriert werden. Amazon FSx nimmt die Datendeduplizierung auf dem Dateisystem wieder auf, sobald die Speicheroptimierung abgeschlossen ist. Weitere Informationen zur Erhöhung der Speicherkapazität und zur Speicheroptimierung finden Sie unter [Verwaltung der Speicherkapazität](#)

## Nach dem Löschen von Dateien wird kein Speicherplatz im Dateisystem freigegeben

Das erwartete Verhalten der Datendeduplizierung besteht darin, dass, wenn bei den gelöschten Daten Speicherplatz gespart wurde, der Speicherplatz in Ihrem Dateisystem erst freigegeben wird, wenn der Garbage-Collection-Job ausgeführt wird.

Eine Methode, die Sie möglicherweise als hilfreich erachten, besteht darin, den Zeitplan so festzulegen, dass der Garbage-Collection-Job unmittelbar nach dem Löschen einer großen Anzahl von Dateien ausgeführt wird. Nach Abschluss der Müllabfuhr können Sie den Zeitplan für die Müllabfuhr auf die ursprünglichen Einstellungen zurücksetzen. Dadurch wird sichergestellt, dass Sie den Speicherplatz aus Ihren Löschungen sofort erkennen können.

Gehen Sie wie folgt vor, um den Garbage-Collection-Job so einzustellen, dass er in 5 Minuten ausgeführt wird.

1. Verwenden Sie den Befehl, um zu überprüfen, ob die Datendeduplizierung aktiviert ist. `Get-FSxDedupStatus` Weitere Informationen zu dem Befehl und seiner erwarteten Ausgabe finden Sie unter [Die Menge des gespeicherten Speicherplatzes anzeigen](#)
2. Gehen Sie wie folgt vor, um den Zeitplan so festzulegen, dass der Garbage-Collection-Job in 5 Minuten ausgeführt wird.

```
$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. Nachdem der Garbage-Collection-Job ausgeführt wurde und der Speicherplatz freigegeben wurde, setzen Sie den Zeitplan wieder auf die ursprünglichen Einstellungen zurück.

## Speicherkontingente

Sie können Benutzerspeicherkontingente auf Ihren Dateisystemen konfigurieren, um zu begrenzen, wie viel Datenspeicher Benutzer verbrauchen können. Nachdem Sie die Kontingente festgelegt haben, können Sie den Kontingentstatus verfolgen, um die Nutzung zu überwachen und zu sehen, wann Benutzer ihre Kontingente überschreiten.

Sie können Kontingente auch durchsetzen, indem Sie Benutzer, die ihre Kontingente erreichen, daran hindern, auf den Speicherplatz zu schreiben. Wenn Sie Kontingente erzwingen, erhält ein Benutzer, der sein Kontingent überschreitet, die Fehlermeldung „Zu wenig Speicherplatz“.

Sie können diese Schwellenwerte für die Kontingenteinstellungen festlegen:

- Warnung — Wird verwendet, um zu verfolgen, ob ein Benutzer oder eine Gruppe ihr Kontingentlimit erreicht. Dies ist nur für die Nachverfolgung relevant.
- Limit — das Speicherkontingentlimit für einen Benutzer oder eine Gruppe.

Sie können Standardkontingente konfigurieren, die für neue Benutzer gelten, die auf ein Dateisystem zugreifen, und Kontingente, die für bestimmte Benutzer oder Gruppen gelten. Sie können auch einen Bericht darüber anzeigen, wie viel Speicherplatz jeder Benutzer oder jede Gruppe verbraucht und ob sie ihre Kontingente überschreiten.

Der Speicherverbrauch auf Benutzerebene wird auf der Grundlage des Dateibesitzes verfolgt. Der Speicherverbrauch wird anhand der logischen Dateigröße berechnet, nicht anhand des tatsächlichen physischen Speicherplatzes, den Dateien belegen. Benutzerspeicherkontingente werden zu dem Zeitpunkt verfolgt, zu dem Daten in eine Datei geschrieben werden.

Um Kontingente für mehrere Benutzer zu aktualisieren, müssen Sie entweder den Aktualisierungsbefehl einmal für jeden Benutzer ausführen oder die Benutzer in einer Gruppe organisieren und das Kontingent für diese Gruppe aktualisieren.

## Verwaltung von Benutzerspeicherkontingenten

Sie können Benutzerspeicherkontingente in Ihrem Dateisystem mithilfe der Amazon FSx CLI für die Fernverwaltung verwalten. PowerShell Informationen zur Verwendung dieser CLI finden Sie unter [Verwenden der Amazon FSx CLI für PowerShell](#).

Im Folgenden finden Sie Befehle, mit denen Sie Benutzerspeicherkontingente verwalten können.

| Befehl für Benutzerspeicherkontingente | Beschreibung                                                                                                                      |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Enable-FSxUserQuotas                   | Startet die Überwachung oder Durchsetzung von Benutzerspeicherkontingenten oder beidem.                                           |
| Disable-FSxUserQuotas                  | Beendet die Nachverfolgung und Durchsetzung von Benutzerspeicherkontingenten.                                                     |
| Get-FSxUserQuotaSettings               | Ruft die aktuellen Benutzerspeicherkontingenteinstellungen für das Dateisystem ab.                                                |
| Get-FSxUserQuotaEntries                | Ruft die aktuellen Benutzerspeicherkontingenteinträge für einzelne Benutzer und Gruppen im Dateisystem ab.                        |
| Set-FSxUserQuotas                      | Legt das Benutzerspeicherkontingent für einen einzelnen Benutzer oder eine Gruppe fest. Kontingentwerte werden in Byte angegeben. |

Die Online-Hilfe für jeden Befehl enthält eine Referenz zu allen Befehlsoptionen. Um auf diese Hilfe zuzugreifen, führen Sie den Befehl `-?` beispielsweise mit `Enable-FSxUserQuotas -?`.

## Verwaltung der Verschlüsselung bei der Übertragung

Sie können eine Reihe von benutzerdefinierten PowerShell Befehlen verwenden, um die Verschlüsselung Ihrer Daten während der Übertragung zwischen Ihrem FSx for Windows File Server Server-Dateisystem und Clients zu steuern. Sie können den Dateisystemzugriff auf Clients beschränken, die SMB-Verschlüsselung unterstützen, sodass diese immer verschlüsselt data-in-transit ist. Wenn die Erzwingung für die Verschlüsselung von aktiviert ist data-in-transit, können

Benutzer, die von Clients aus auf das Dateisystem zugreifen, die die SMB 3.0-Verschlüsselung nicht unterstützen, nicht auf Dateifreigaben zugreifen, für die die Verschlüsselung aktiviert ist.

Sie können die Verschlüsselung auch auf Dateifreigabeebene statt data-in-transit auf Dateiserverebene steuern. Sie können Verschlüsselungskontrollen auf Dateifreigabeebene verwenden, um eine Mischung aus verschlüsselten und unverschlüsselten Dateifreigaben auf demselben Dateisystem einzurichten, wenn Sie für einige Dateifreigaben mit vertraulichen Daten die Verschlüsselung während der Übertragung erzwingen und allen Benutzern den Zugriff auf andere Dateifreigaben ermöglichen möchten. Die serverweite Verschlüsselung hat Vorrang vor der Verschlüsselung auf Freigabeebene. Wenn die globale Verschlüsselung aktiviert ist, können Sie die Verschlüsselung für bestimmte Shares nicht selektiv deaktivieren.

Sie können die Verschlüsselung von Benutzern während der Übertragung in Ihrem Dateisystem verwalten, indem Sie die Amazon FSx CLI für die Fernverwaltung verwenden. PowerShell Informationen zur Verwendung dieser CLI finden Sie unter [Verwenden der Amazon FSx CLI für PowerShell](#).

Im Folgenden finden Sie Befehle, mit denen Sie die Verschlüsselung von Benutzern während der Übertragung in Ihrem Dateisystem verwalten können.

| Verschlüsselung im Transit<br>Command | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Get-FSxSmbServerConfiguration         | Ruft die Server Message Block (SMB) -Serverkonfiguration ab.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Set-FSxSmbServerConfiguration         | <p>Dieser Befehl bietet zwei Optionen für die Konfiguration der Verschlüsselung bei der Übertragung:</p> <ul style="list-style-type: none"> <li>• <code>-EncryptData \$True \$False</code> — Stellen Sie diesen Parameter auf ein, <code>True</code> um die Verschlüsselung von Daten bei der Übertragung zu aktivieren. Stellen Sie diesen Parameter auf ein, <code>False</code> um die Verschlüsselung von Daten bei der Übertragung zu deaktivieren.</li> <li>• <code>-RejectUnencryptedAccess \$True \$False</code> — Legen Sie diesen Parameter auf fest <code>True</code>, um Clients, die keine Verschlüsselung unterstützen, den Zugriff auf das Dateisystem zu verbieten. Stellen Sie diesen Parameter so</li> </ul> |

| Verschlüsselung im Transit<br>Command | Beschreibung                                                                                          |
|---------------------------------------|-------------------------------------------------------------------------------------------------------|
|                                       | einFalse, dass Clients, die keine Verschlüsselung unterstützen, auf das Dateisystem zugreifen können. |

Die Online-Hilfe für jeden Befehl enthält eine Referenz zu allen Befehlsoptionen. Um auf diese Hilfe zuzugreifen, führen Sie den Befehl `-?` beispielsweise mit `awsGet-FSxSmbServerConfiguration -?`.

## Verwaltung der Speicherconfiguration

Die Speicherconfiguration Ihres Dateisystems umfasst Speicherkapazität, Speichertyp und SSD-IOPS. Sie können diese Ressourcen zusammen mit der Durchsatzkapazität konfigurieren, um während und nach der Erstellung Ihres Dateisystems das für Ihre Arbeitslast gewünschte Leistungsniveau zu erreichen. Weitere Informationen finden Sie unter den folgenden Themen.

Themen

- [Verwaltung der Speicherkapazität](#)
- [Speichertyp verwalten](#)
- [Verwalten von SSD-IOPS](#)

## Verwaltung der Speicherkapazität

Sie können die Speicherkapazität, die auf Ihrem Dateisystem FSx for Windows File Server konfiguriert ist, nach Bedarf erhöhen. Sie können dies mit der Amazon FSx-Konsole, der Amazon FSx-API oder der AWS Command Line Interface (AWS CLI) tun. Sie können nur die Speicherkapazität für ein Dateisystem erhöhen; Sie können die Speicherkapazität nicht verringern.

### Note

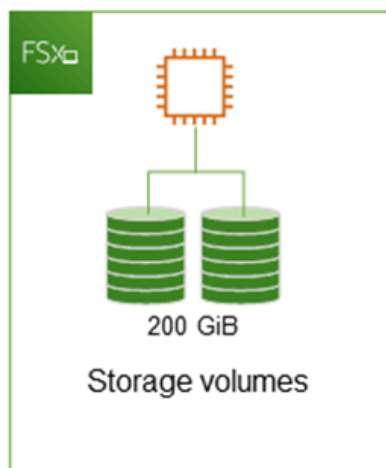
Sie können die Speicherkapazität für Dateisysteme, die vor dem 23. Juni 2019 erstellt wurden, oder für Dateisysteme, die aus einer Sicherung wiederhergestellt wurden, die zu einem Dateisystem gehört, das vor dem 23. Juni 2019 erstellt wurde, nicht erhöhen.

Wenn Sie die Speicherkapazität Ihres Amazon FSx-Dateisystems erhöhen, fügt Amazon FSx Ihrem Dateisystem im Hintergrund einen neuen, größeren Satz von Festplatten hinzu. Amazon FSx führt dann im Hintergrund einen Speicheroptimierungsprozess durch, um Daten transparent von den alten Festplatten auf die neuen Festplatten zu migrieren. Die Speicheroptimierung kann zwischen einigen Stunden und einigen Tagen dauern, mit minimalen spürbaren Auswirkungen auf die Workload-Leistung. Während dieser Optimierung ist die Backup-Auslastung vorübergehend höher, da sowohl die alten als auch die neuen Speichervolumen in den Backups auf Dateisystemebene enthalten sind. Beide Gruppen von Speichervolumen sind enthalten, um sicherzustellen, dass Amazon FSx Backups auch während der Speicherskalierung erfolgreich erstellen und wiederherstellen kann. Die Backup-Nutzung wird auf den vorherigen Basiswert zurückgesetzt, nachdem die alten Speichervolumen nicht mehr in der Backup-Historie enthalten sind. Wenn die neue Speicherkapazität verfügbar ist, wird Ihnen nur die neue Speicherkapazität in Rechnung gestellt.

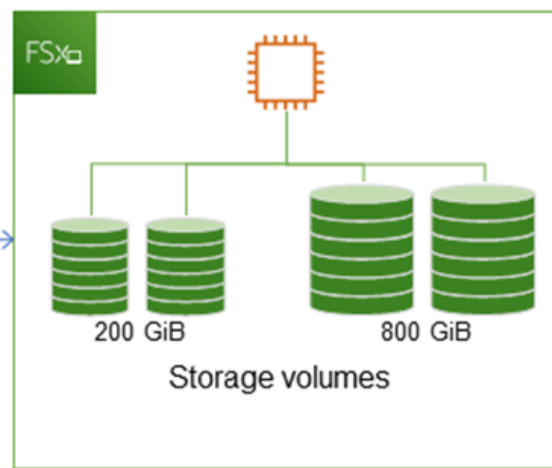
Die folgende Abbildung zeigt die vier Hauptschritte des Prozesses, den Amazon FSx bei der Erhöhung der Speicherkapazität eines Dateisystems verwendet.



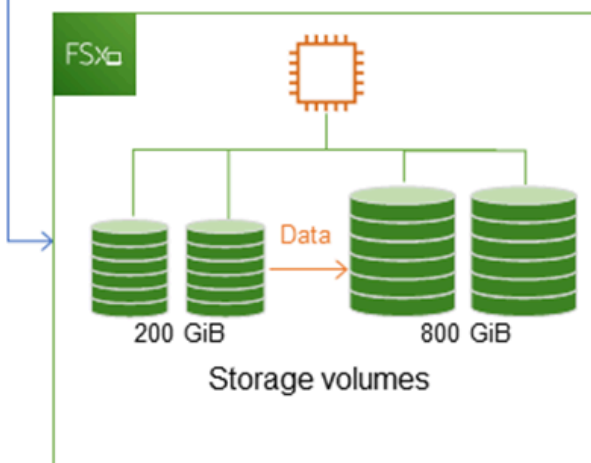
Step 1: Storage capacity increase request to 800 GiB.



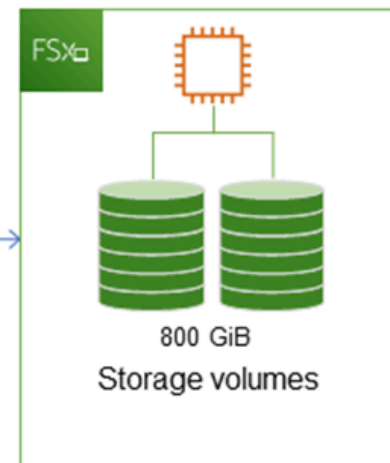
Step 2: Amazon FSx adds the new, larger disks.



Step 3: Amazon FSx migrates data to larger disks.



Step 4: Amazon FSx removes smaller disks.



Sie können den Fortschritt der Speicheroptimierung, der Erhöhung der SSD-Speicherkapazität oder der SSD-IOPS-Updates jederzeit mithilfe der Amazon FSx-Konsole, CLI oder API verfolgen. Weitere Informationen finden Sie unter [Überwachung: Die Speicherkapazität nimmt zu](#).

## Themen

- [Wichtige Punkte, die Sie bei der Erhöhung der Speicherkapazität beachten sollten](#)
- [Wann sollte die Speicherkapazität erhöht werden](#)

- [Die Speicherkapazität steigt und die Leistung des Dateisystems](#)
- [Wie kann die Speicherkapazität erhöht werden](#)
- [Überwachung: Die Speicherkapazität nimmt zu](#)
- [Dynamisches Erhöhen der Speicherkapazität eines Dateisystems FSx for Windows File Server](#)

## Wichtige Punkte, die Sie bei der Erhöhung der Speicherkapazität beachten sollten

Hier sind einige wichtige Punkte, die Sie bei der Erhöhung der Speicherkapazität berücksichtigen sollten:

- Nur erhöhen — Sie können nur die Speicherkapazität für ein Dateisystem erhöhen; Sie können die Speicherkapazität nicht verringern.
- Minimale Erhöhung — Jede Erhöhung der Speicherkapazität muss mindestens 10 Prozent der aktuellen Speicherkapazität des Dateisystems bis zum zulässigen Höchstwert von 65.536 GiB betragen.
- Minimale Durchsatzkapazität — Um die Speicherkapazität zu erhöhen, muss ein Dateisystem über eine Mindestdurchsatzkapazität von 16 MB/s verfügen. Dies liegt daran, dass der Schritt der Speicheroptimierung ein durchsatzintensiver Prozess ist.
- Zeit zwischen Erhöhungen — Sie können die Speicherkapazität in einem Dateisystem erst 6 Stunden nach der Anforderung der letzten Erhöhung weiter erhöhen oder bis der Speicheroptimierungsprozess abgeschlossen ist, je nachdem, welcher Zeitraum länger ist. Der Abschluss der Speicheroptimierung kann einige Stunden bis zu einigen Tagen dauern. Um die Zeit bis zum Abschluss der Speicheroptimierung zu minimieren, empfehlen wir, die Durchsatzkapazität Ihres Dateisystems zu erhöhen, bevor Sie die Speicherkapazität erhöhen (die Durchsatzkapazität kann nach Abschluss der Speicherskalierung wieder herunterskaliert werden) und die Speicherkapazität zu erhöhen, wenn das Dateisystem nur wenig Verkehr hat.

### Note

Bestimmte Dateisystemereignisse können Festplatten-I/O-Leistungsressourcen beanspruchen, zum Beispiel:

Die Optimierungsphase der Skalierung der Speicherkapazität kann zu einem erhöhten Festplattendurchsatz führen und möglicherweise zu Leistungswarnungen führen. Weitere Informationen finden Sie unter [Leistungswarnungen und Empfehlungen](#).

## Wann sollte die Speicherkapazität erhöht werden

Erhöhen Sie die Speicherkapazität Ihres Dateisystems, wenn die freie Speicherkapazität knapp wird. Verwenden Sie die `FreeStorageCapacity` CloudWatch Metrik, um die Menge an freiem Speicherplatz zu überwachen, der im Dateisystem verfügbar ist. Sie können einen CloudWatch Amazon-Alarm für diese Metrik erstellen und sich benachrichtigen lassen, wenn sie einen bestimmten Schwellenwert unterschreitet. Weitere Informationen finden Sie unter [Metriken mit Amazon überwachen CloudWatch](#).

Wir empfehlen, jederzeit mindestens 10% der freien Speicherkapazität in Ihrem Dateisystem beizubehalten. Die Nutzung Ihrer gesamten Speicherkapazität kann sich negativ auf Ihre Leistung auswirken und zu Dateninkonsistenzen führen.

Sie können die Speicherkapazität Ihres Dateisystems automatisch erhöhen, wenn die Menge der freien Speicherkapazität unter einen von Ihnen festgelegten Schwellenwert fällt. Verwenden Sie die AWS entwickelte benutzerdefinierte AWS CloudFormation Vorlage, um alle Komponenten bereitzustellen, die für die Implementierung der automatisierten Lösung erforderlich sind. Weitere Informationen finden Sie unter [Dynamisches Erhöhen der Speicherkapazität](#).

## Die Speicherkapazität steigt und die Leistung des Dateisystems

Bei den meisten Workloads kommt es nur zu minimalen Leistungseinbußen, während Amazon FSx den Speicheroptimierungsprozess im Hintergrund ausführt, nachdem die neue Speicherkapazität verfügbar ist. Bei schreibintensiven Anwendungen mit großen aktiven Datensätzen kann es vorübergehend zu einer Verringerung der Schreibleistung um bis zu die Hälfte kommen. In diesen Fällen können Sie zunächst die Durchsatzkapazität Ihres Dateisystems erhöhen, bevor Sie die Speicherkapazität erhöhen. Auf diese Weise können Sie weiterhin den gleichen Durchsatz bereitstellen, um den Leistungsanforderungen Ihrer Anwendung gerecht zu werden. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

## Wie kann die Speicherkapazität erhöht werden

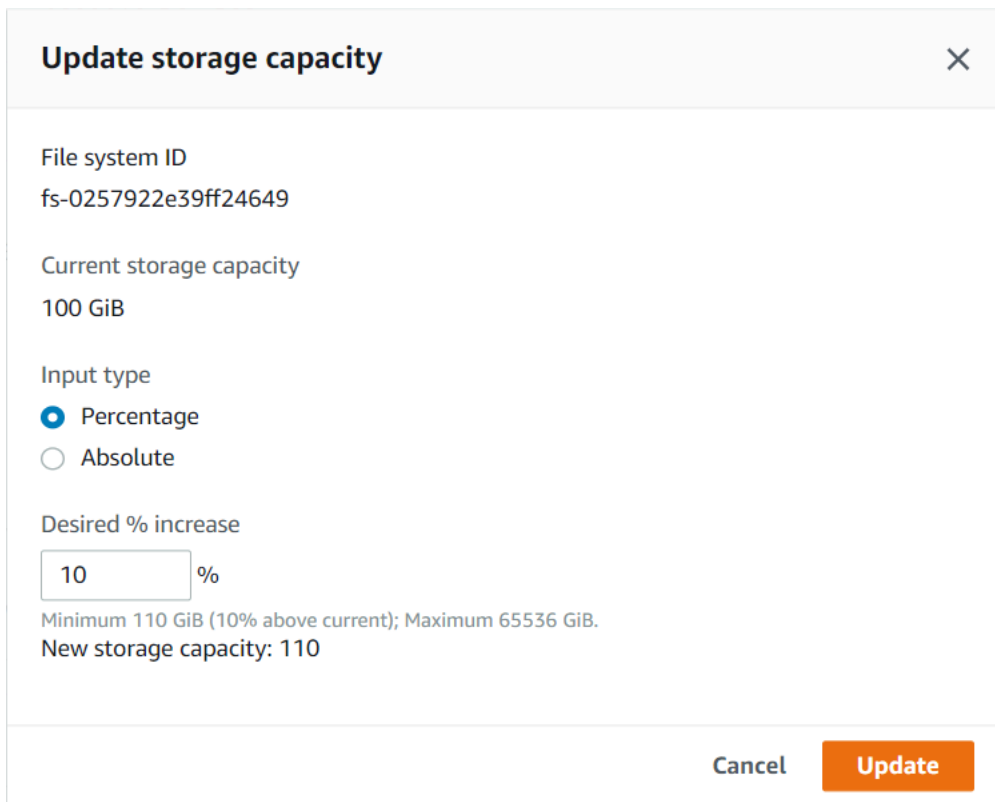
Sie können die Speicherkapazität eines Dateisystems mithilfe der Amazon FSx-Konsole AWS CLI, der oder der Amazon FSx-API erhöhen.

Um die Speicherkapazität für ein Dateisystem (Konsole) zu erhöhen

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Windows-Dateisystem aus, für das Sie die Speicherkapazität erhöhen möchten.

3. Wählen Sie unter Aktionen die Option Speicher aktualisieren aus. Oder wählen Sie im Übersichtsbereich neben der Speicherkapazität des Dateisystems die Option Aktualisieren aus.

Das Fenster „Speicherkapazität aktualisieren“ wird angezeigt.



**Update storage capacity** ✕

File system ID  
fs-0257922e39ff24649

Current storage capacity  
100 GiB

Input type  
 Percentage  
 Absolute

Desired % increase  
 %  
Minimum 110 GiB (10% above current); Maximum 65536 GiB.  
New storage capacity: 110

Cancel Update

4. Wählen Sie als Eingabetyp Prozentwert, um die neue Speicherkapazität als prozentuale Änderung gegenüber dem aktuellen Wert einzugeben, oder wählen Sie Absolut, um den neuen Wert in GiB einzugeben.
5. Geben Sie die gewünschte Speicherkapazität ein.

**Note**

Der gewünschte Kapazitätswert muss mindestens 10 Prozent über dem aktuellen Wert liegen, bis zu einem Höchstwert von 65.536 GiB.

6. Wählen Sie Update, um die Aktualisierung der Speicherkapazität zu starten.
7. Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme auf der Registerkarte Updates überwachen.

## Um die Speicherkapazität für ein Dateisystem (CLI) zu erhöhen

Verwenden Sie den AWS CLI Befehl [update-file-system](#), um die Speicherkapazität für ein Dateisystem FSx für Windows File Server zu erhöhen. Legen Sie die folgenden Parameter fest:

- `--file-system-id` auf die ID des Dateisystems, das Sie aktualisieren.
- `--storage-capacity` auf einen Wert, der mindestens 10 Prozent über dem aktuellen Wert liegt.

Sie können den Fortschritt des Updates mithilfe des AWS CLI Befehls überwachen [describe-file-systems](#). Suchen Sie `administrative-actions` in der Ausgabe nach dem.

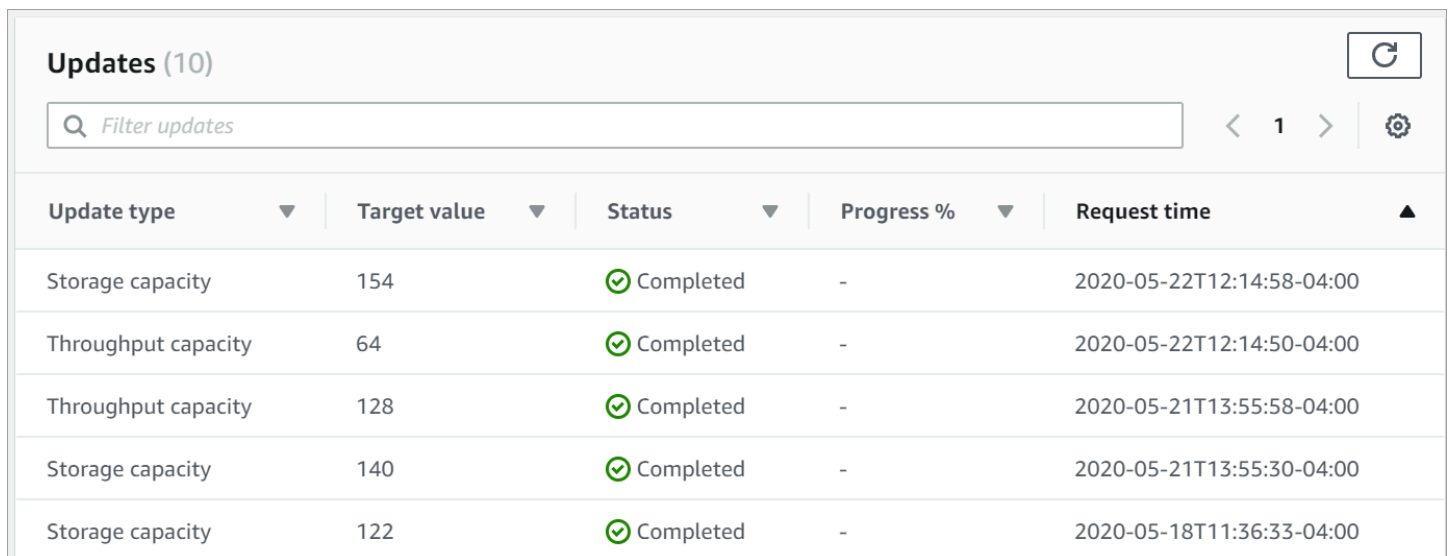
Weitere Informationen finden Sie unter [AdministrativeAction](#).

## Überwachung: Die Speicherkapazität nimmt zu

Sie können den Fortschritt einer Erhöhung der Speicherkapazität mithilfe der Amazon FSx-Konsole, der API oder der AWS CLI überwachen.

### Überwachung von Zunahmen in der Konsole

Auf der Registerkarte Updates im Fenster mit den Dateisystemdetails können Sie die 10 neuesten Updates für jeden Updatetyp einsehen.



| 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 |

Informationen zu Aktualisierungen der Speicherkapazität finden Sie in den folgenden Informationen.

### Art des Updates

Mögliche Werte sind Speicherkapazität.

## Zielwert

Der gewünschte Wert, auf den die Speicherkapazität des Dateisystems aktualisiert werden soll.

## Status

Der aktuelle Status des Updates. Für Aktualisierungen der Speicherkapazität sind die folgenden Werte möglich:

- **Ausstehend** — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.
- **In Bearbeitung** — Amazon FSx verarbeitet die Aktualisierungsanfrage.
- **Aktualisierte Optimierung** — Amazon FSx hat die Speicherkapazität des Dateisystems erhöht. Bei der Speicheroptimierung werden jetzt die Dateisystemdaten auf die neuen größeren Festplatten verschoben.
- **Abgeschlossen** — Die Erhöhung der Speicherkapazität wurde erfolgreich abgeschlossen.
- **Fehlgeschlagen** — Die Erhöhung der Speicherkapazität ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Informationen darüber zu erhalten, warum das Speicherupdate fehlgeschlagen ist.

## Fortschritt%

Zeigt den Fortschritt des Speicheroptimierungsprozesses in Prozent als abgeschlossen an.

## Uhrzeit der Anfrage

Der Zeitpunkt, zu dem Amazon FSx die Anfrage zur Aktualisierungsaktion erhalten hat.

Die Überwachung nimmt mit der AND-API AWS CLI zu

Mithilfe des [describe-file-systems](#) AWS CLIBefehls und der [DescribeFileSystems](#) API-Aktion können Sie Anfragen zur Erhöhung der Speicherkapazität des Dateisystems anzeigen und überwachen. Das `AdministrativeActions` Array listet die 10 letzten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die Speicherkapazität eines Dateisystems erhöhen, `AdministrativeActions` werden zwei generiert: eine Aktion `FILE_SYSTEM_UPDATE` und eine `STORAGE_OPTIMIZATION` Aktion.

Das folgende Beispiel zeigt einen Auszug der Antwort auf einen `describe-file-systems` CLI-Befehl. Das Dateisystem hat eine Speicherkapazität von 300 GB, und eine Verwaltungsmaßnahme zur Erhöhung der Speicherkapazität auf 1000 GB steht noch aus.

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

Amazon FSx verarbeitet die FILE\_SYSTEM\_UPDATE Aktion zuerst und fügt die neuen größeren Speicherplatten zum Dateisystem hinzu. Wenn der neue Speicher für das Dateisystem verfügbar ist, ändert sich der FILE\_SYSTEM\_UPDATE Status aufUPDATED\_OPTIMIZING. Die Speicherkapazität zeigt den neuen größeren Wert an und Amazon FSx beginnt mit der Verarbeitung der STORAGE\_OPTIMIZATION administrativen Aktion. Dies wird im folgenden Auszug aus der Antwort auf einen describe-file-systems CLI-Befehl gezeigt.

Die ProgressPercent Eigenschaft zeigt den Fortschritt des Speicheroptimierungsprozesses an. Nachdem der Speicheroptimierungsprozess erfolgreich abgeschlossen wurde, ändert sich der Status der FILE\_SYSTEM\_UPDATE Aktion inCOMPLETED, und die STORAGE\_OPTIMIZATION Aktion wird nicht mehr angezeigt.

```
{
  "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,
  }
]

```

Wenn die Erhöhung der Speicherkapazität fehlschlägt, ändert sich der Status der FILE\_SYSTEM\_UPDATE Aktion in FAILED. Die FailureDetails Eigenschaft enthält Informationen über den Fehler, wie im folgenden Beispiel dargestellt.

```

{
  "FileSystems": [
    {
      "OwnerId": "111122223333",
      .
      .
      .
      "StorageCapacity": 300,
      "AdministrativeActions": [
        {
          "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
          "FailureDetails": {
            "Message": "string"
          },
          "RequestTime": 1581694764.757,
          "Status": "FAILED",
          "TargetFileSystemValues":
            "StorageCapacity": 1000
        }
      ]
    }
  ]
}

```



```
}  
]
```

Hinweise zur Behebung fehlgeschlagener Aktionen finden Sie unter [Aktualisierungen der Speicher- oder Durchsatzkapazität schlagen fehl](#).

## Dynamisches Erhöhen der Speicherkapazität eines Dateisystems FSx for Windows File Server

Sie können die folgende Lösung verwenden, um die Speicherkapazität eines Dateisystems FSx for Windows File Server dynamisch zu erhöhen, wenn die Menge an freier Speicherkapazität unter einen von Ihnen angegebenen Schwellenwert fällt. Diese AWS CloudFormation Vorlage stellt automatisch alle Komponenten bereit, die zur Definition des Schwellenwerts für die freie Speicherkapazität, des auf diesem Schwellenwert basierenden CloudWatch Amazon-Alarms und der AWS Lambda Funktion zur Erhöhung der Speicherkapazität des Dateisystems erforderlich sind.

Die Lösung stellt automatisch alle benötigten Komponenten bereit und berücksichtigt die folgenden Parameter:

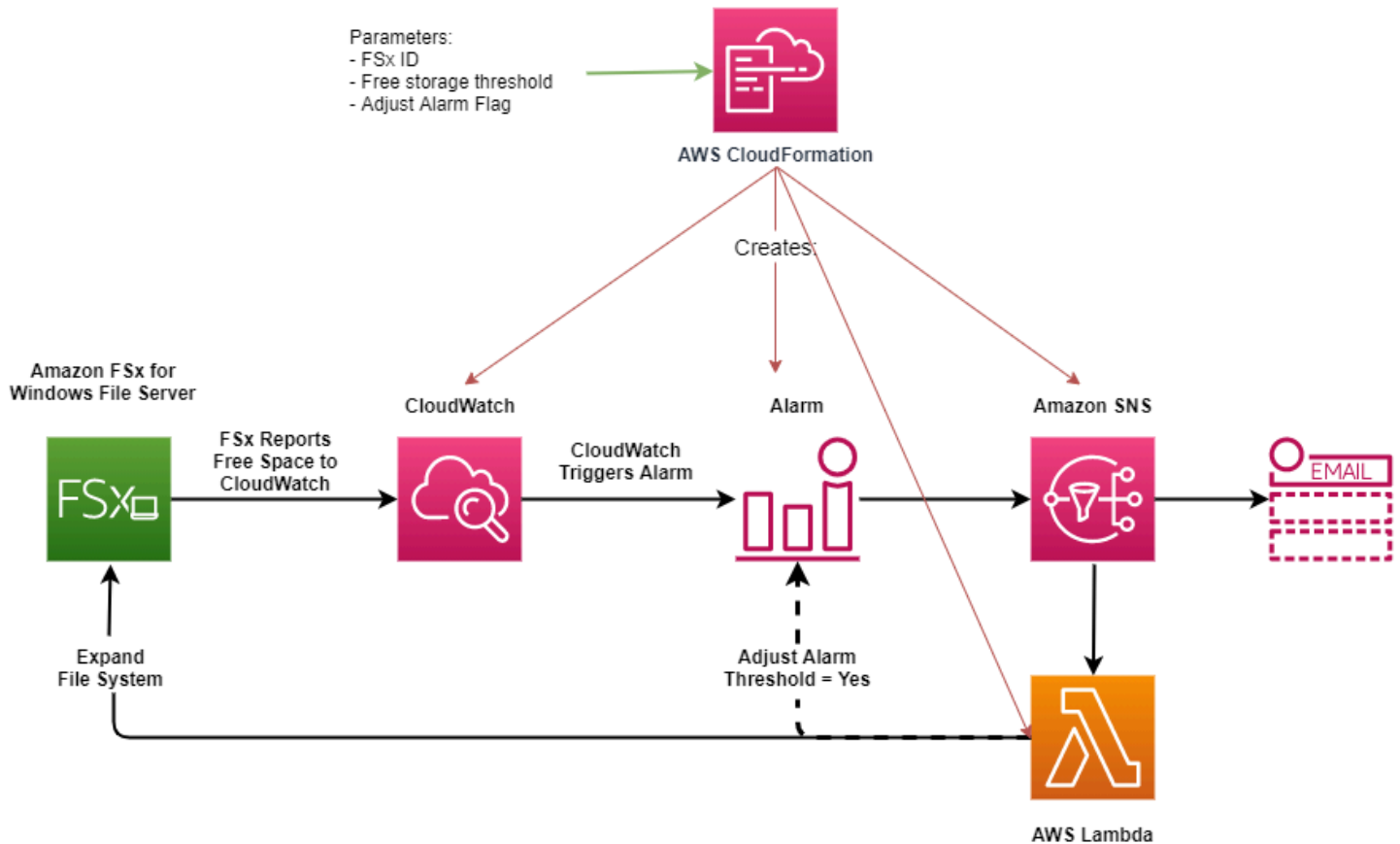
- Die Dateisystem-ID
- Der Schwellenwert für die freie Speicherkapazität (numerischer Wert)
- Maßeinheit (Prozent [Standard] oder GiB)
- Der Prozentsatz, um den die Speicherkapazität erhöht werden soll (%)
- Die E-Mail-Adresse für das SNS-Abonnement
- Passen Sie den Alarmschwellenwert an (Ja/Nein)

### Themen

- [Übersicht über die Architektur](#)
- [AWS CloudFormation-Vorlage](#)
- [Automatisierte Bereitstellung mit AWS CloudFormation](#)

### Übersicht über die Architektur

Durch die Bereitstellung dieser Lösung werden die folgenden Ressourcen in der AWS Cloud erstellt.



Die Abbildung zeigt die folgenden Schritte:

1. Die AWS CloudFormation Vorlage stellt einen CloudWatch Alarm, eine AWS Lambda Funktion, eine Amazon Simple Notification Service (Amazon SNS) -Warteschlange und alle erforderlichen Rollen AWS Identity and Access Management (IAM) bereit. Die IAM-Rolle erteilt der Lambda-Funktion die Erlaubnis, die Amazon FSx-API-Operationen aufzurufen.
2. CloudWatch löst einen Alarm aus, wenn die freie Speicherkapazität des Dateisystems den angegebenen Schwellenwert unterschreitet, und sendet eine Nachricht an die Amazon SNS SNS-Warteschlange.
3. Die Lösung löst dann die Lambda-Funktion aus, die dieses Amazon SNS SNS-Thema abonniert hat.
4. Die Lambda-Funktion berechnet die neue Dateisystemspeicherkapazität auf der Grundlage des angegebenen prozentualen Erhöhungswerts und legt die neue Dateisystemspeicherkapazität fest.
5. Die Lambda-Funktion kann optional den Schwellenwert für die freie Speicherkapazität so anpassen, dass er einem bestimmten Prozentsatz der neuen Speicherkapazität des Dateisystems entspricht.

6. Der ursprüngliche CloudWatch Alarmstatus und die Ergebnisse der Lambda-Funktionsoperationen werden an die Amazon SNS SNS-Warteschlange gesendet.

Um Benachrichtigungen über die Aktionen zu erhalten, die als Reaktion auf den CloudWatch Alarm ausgeführt werden, müssen Sie das Amazon SNS SNS-Themenabonnement bestätigen, indem Sie dem Link in der Bestätigungs-E-Mail für das Abonnement folgen.

### AWS CloudFormation-Vorlage

Diese Lösung automatisiert AWS CloudFormation die Bereitstellung der Komponenten, die zur automatischen Erhöhung der Speicherkapazität eines Dateisystems FSx for Windows File Server verwendet werden. Um diese Lösung zu verwenden, laden Sie die [IncreaseF-Vorlage SxSize](#) AWS CloudFormation herunter.

Die Vorlage verwendet die wie folgt beschriebenen Parameter. Überprüfen Sie die Vorlagenparameter und ihre Standardwerte und ändern Sie sie an die Anforderungen Ihres Dateisystems.

### FileSystemId

Kein Standardwert. Die ID des Dateisystems, für das Sie die Speicherkapazität automatisch erhöhen möchten.

### LowFreeDataStorageCapacityThreshold

Kein Standardwert. Gibt den anfänglichen Schwellenwert für freie Speicherkapazität an, bei dem ein Alarm ausgelöst und die Speicherkapazität des Dateisystems automatisch erhöht werden soll, angegeben in GiB oder als Prozentsatz (%) der aktuellen Speicherkapazität des Dateisystems. In Prozent ausgedrückt, wird die CloudFormation Vorlage entsprechend den CloudWatch Alarmeinstellungen in GiB neu berechnet.

### LowFreeDataStorageCapacityThresholdUnit

Die Standardeinstellung ist%. Gibt die Einheiten für die `anLowFreeDataStorageCapacityThreshold`, entweder in GiB oder als Prozentsatz der aktuellen Speicherkapazität.

### AlarmModificationNotification

Die Standardeinstellung ist Ja. Wenn auf Ja gesetzt `LowFreeDataStorageCapacityThreshold`, wird der Anfangswert proportional zum Wert von `PercentIncrease` für nachfolgende Alarmschwellenwerte erhöht.

Wenn beispielsweise auf 20 und auf Ja gesetzt `PercentIncrease AlarmModificationNotification` ist, wird der in GiB angegebene Schwellenwert für verfügbaren freien Speicherplatz (`LowFreeDataStorageCapacityThreshold`) bei nachfolgenden Ereignissen zur Erhöhung der Speicherkapazität um 20% erhöht.

#### EmailAddress

Kein Standardwert. Gibt die E-Mail-Adresse an, die für das SNS-Abonnement verwendet werden soll, und empfängt Warnmeldungen zu Speicherkapazitätsschwellenwerten.

#### PercentIncrease

Kein Standardwert. Gibt den Betrag an, um den die Speicherkapazität erhöht werden soll, ausgedrückt als Prozentsatz der aktuellen Speicherkapazität.

### Automatisierte Bereitstellung mit AWS CloudFormation

Mit dem folgenden Verfahren wird ein AWS CloudFormation Stack konfiguriert und bereitgestellt, um die Speicherkapazität eines Dateisystems FSx for Windows File Server automatisch zu erhöhen. Die Bereitstellung dauert etwa 5 Minuten.


#### Note

Die Implementierung dieser Lösung erfordert die Abrechnung der zugehörigen AWS Dienste. Weitere Informationen finden Sie auf den Seiten mit den Preisdetails für diese Dienste.

Bevor Sie beginnen, müssen Sie die ID des Amazon FSx-Dateisystems, das in einer Amazon Virtual Private Cloud (Amazon VPC) läuft, in Ihrem AWS Konto haben. Weitere Informationen zum Erstellen von Amazon FSx-Ressourcen finden Sie unter [Erste Schritte mit Amazon FSx for Windows File Server](#).

So starten Sie den Lösungstapel zur automatischen Erhöhung der Speicherkapazität

1. Laden Sie die [SxSizeAWS CloudFormationIncreaseF-Vorlage](#) herunter. Weitere Informationen zum Erstellen eines CloudFormation Stacks finden Sie im AWS CloudFormationBenutzerhandbuch unter [Erstellen eines Stacks auf der AWS CloudFormation Konsole](#).

 Note

Amazon FSx ist derzeit nur in bestimmten AWS Regionen verfügbar. Sie müssen diese Lösung in einer AWS Region einführen, in der Amazon FSx verfügbar ist. Weitere Informationen finden Sie unter [Amazon FSx-Endpunkte und Kontingente](#) in der Allgemeinen AWS-Referenz

2. Geben Sie unter Stackdetails an, die Werte für Ihre Lösung zur automatischen Erhöhung der Speicherkapazität ein.

## Specify stack details

**Stack name**

Stack name

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

**Alarm Notification**

LowFreeDataStorageCapacityThreshold  
Low free data storage capacity threshold (GiB or %)

LowFreeDataStorageCapacityThresholdUnit  
Specify the Storage Capacity threshold Unit (GiB or %)

EmailAddress  
The email address for alarm notification.

**Other parameters**

AlarmModificationNotification  
Would you like to adjust the percent increase for the next FSx storage increase event proportionate to the requested increase?

PercentIncrease  
Provide the percent increase for File System Storage. This value should be between 10 and 100

Cancel Previous **Next**

3. Geben Sie einen Stack-Namen ein.
4. Überprüfen Sie unter Parameter die Parameter für die Vorlage und ändern Sie sie an die Anforderungen Ihres Dateisystems. Wählen Sie anschließend Next (Weiter).
5. Geben Sie die gewünschten Optionseinstellungen für Ihre benutzerdefinierte Lösung ein, und wählen Sie dann Weiter aus.
6. Überprüfen und bestätigen Sie unter Überprüfen die Lösungseinstellungen. Sie müssen das Kontrollkästchen aktivieren, das bestätigt, dass die Vorlage IAM-Ressourcen erstellt.

## 7. Wählen Sie Create aus, um den Stack bereitzustellen.

Sie können den Status des Stacks in der AWS CloudFormation-Konsole in der Spalte Status anzeigen. In etwa 5 Minuten sollte Ihnen der Status CREATE\_COMPLETE angezeigt werden.

Der Stack wird aktualisiert

Nachdem der Stack erstellt wurde, können Sie ihn aktualisieren, indem Sie dieselbe Vorlage verwenden und neue Werte für die Parameter angeben. Weitere Informationen finden Sie unter [Stacks direkt aktualisieren](#) im AWS CloudFormationBenutzerhandbuch.

## Speichertyp verwalten

FSx for Windows File Server bietet Speichertypen wie Solid State Drive (SSD) und Magnetic Hard Disk Drive (HDD). SSD-Speicher wurde für die leistungsstärksten und latenzempfindlichsten Workloads konzipiert, darunter Datenbanken, Workloads zur Medienverarbeitung und Datenanalyseanwendungen. Festplattenspeicher sind für ein breites Spektrum an Workloads konzipiert, darunter Home-Verzeichnisse, Dateifreigaben von Benutzern und Abteilungen sowie Content-Management-Systeme.

Sie können den Speichertyp Ihres Dateisystems mithilfe der Amazon FSx-Konsole oder der Amazon FSx-API von HDD auf SSD ändern. Sie können den Speichertyp Ihres Dateisystems nicht von SSD auf HDD ändern. Denken Sie daran, dass Sie Ihre Dateisystemkonfiguration erst 6 Stunden, nachdem das letzte Update angefordert wurde, erneut aktualisieren können, oder bis der Prozess der Speicheroptimierung abgeschlossen ist — je nachdem, welcher Zeitraum länger ist. Es kann zwischen einigen Stunden und einigen Tagen dauern, bis die Speicheroptimierung abgeschlossen ist. Um diese Zeit so gering wie möglich zu halten, empfehlen wir, Ihren Speichertyp zu aktualisieren, wenn Ihr Dateisystem nur minimal ausgelastet ist.

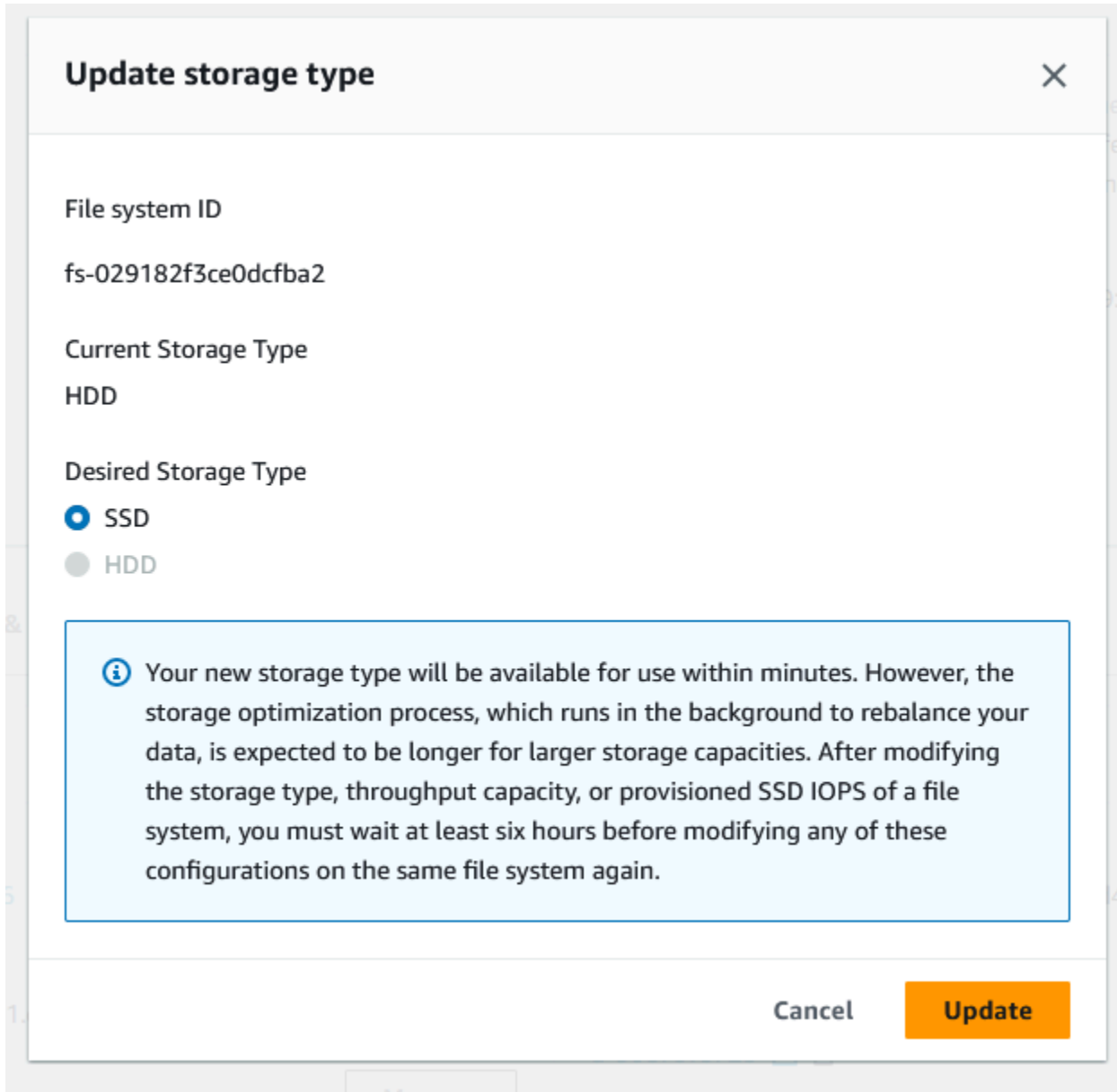
Sie können den Speichertyp Ihres Dateisystems auch von Festplatte auf SSD ändern, indem Sie ein verfügbares Backup wiederherstellen, um ein neues Dateisystem zu erstellen, und einen neuen Speichertyp auswählen. Weitere Informationen finden Sie unter [Wiederherstellen von Sicherungen](#).

## Wie aktualisiert man den Speichertyp

Sie können den Speichertyp eines Dateisystems mithilfe der Amazon FSx-Konsole, der AWS CLI, oder der Amazon FSx-API aktualisieren.

## Um den Speichertyp für ein Dateisystem (Konsole) zu aktualisieren

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Windows-Dateisystem aus, für das Sie den Speichertyp aktualisieren möchten.
3. Wählen Sie unter Aktionen die Option Speichertyp aktualisieren aus. Oder wählen Sie im Bereich „Zusammenfassung“ die Schaltfläche „Aktualisieren“ neben „Festplatte“ aus. Das Fenster Speichertyp aktualisieren wird angezeigt.



4. Wählen Sie unter Gewünschter Speichertyp die Option SSD aus. Wählen Sie Update, um das Speichertyp-Update zu starten.



- Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme auf der Registerkarte Updates überwachen.

So aktualisieren Sie den Speichertyp für ein Dateisystem (CLI)

Verwenden Sie den AWS CLI Befehl [update-file-system](#), um den Speichertyp für ein Dateisystem FSx für Windows File Server zu aktualisieren. Legen Sie die folgenden Parameter fest:

- `--file-system-id` auf die ID des Dateisystems, das Sie aktualisieren möchten.
- `--storage-type` auf SSD. Sie können nicht vom SSD-Speichertyp zum HDD-Speichertyp wechseln.

Sie können den Fortschritt des Updates mithilfe des AWS CLI Befehls überwachen [describe-file-systems](#). Suchen Sie `administrative-actions` in der Ausgabe nach dem.

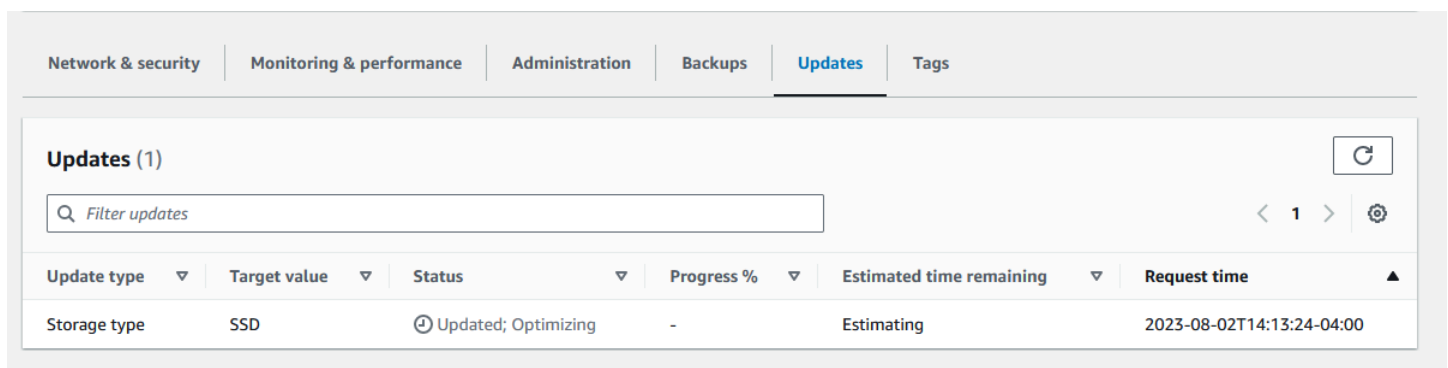
Weitere Informationen finden Sie unter [AdministrativeAction](#).

## Überwachung von Speichertyp-Updates

Sie können den Fortschritt einer Speichertyp-Aktualisierung mithilfe der Amazon FSx-Konsole, der API oder der AWS CLI überwachen.

## Überwachung von Updates in der Konsole

Auf der Registerkarte Updates im Fenster mit den Dateisystemdetails können Sie die 10 neuesten Updates für jeden Updatetyp einsehen.



| Update type  | Target value | Status              | Progress % | Estimated time remaining | Request time              |
|--------------|--------------|---------------------|------------|--------------------------|---------------------------|
| Storage type | SSD          | Updated; Optimizing | -          | Estimating               | 2023-08-02T14:13:24-04:00 |

Für Speichertyp-Updates können Sie sich die folgenden Informationen ansehen.

### Art des Updates

Möglicher Wert ist Speichertyp.

## Zielwert

SSD

## Status

Der aktuelle Status des Updates. Für Speichertyp-Updates sind die folgenden Werte möglich:

- **Ausstehend** — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.
- **In Bearbeitung** — Amazon FSx verarbeitet die Aktualisierungsanfrage.
- **Aktualisierte Optimierung** — Die SSD-Speicherleistung ist für die Schreibvorgänge Ihres Workloads verfügbar. Ihr Update wechselt in den Optimierungsstatus Aktualisiert, der in der Regel einige Stunden dauert. Während dieser Zeit weisen die Lesevorgänge Ihres Workloads ein Leistungsniveau zwischen Festplatte und SSD auf. Sobald Ihre Aktualisierungsaktion abgeschlossen ist, steht Ihre neue SSD-Leistung sowohl für Lese- als auch für Schreibvorgänge zur Verfügung.
- **Abgeschlossen** — Das Speichertyp-Update wurde erfolgreich abgeschlossen.
- **Fehlgeschlagen** — Die Aktualisierung des Speichertyps ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Details zu sehen.

## Fortschritt%

Zeigt den Fortschritt des Speicheroptimierungsprozesses in Prozent an, der abgeschlossen ist.

## Uhrzeit der Anfrage

Der Zeitpunkt, zu dem Amazon FSx die Anfrage zur Aktualisierungsaktion erhalten hat.

## Überwachung von Updates mit der AWS CLI AND-API

Mithilfe des [describe-file-systems](#) AWS CLIBefehls und der [DescribeFileSystems](#) API-Aktion können Sie Aktualisierungsanforderungen für den Dateisystem-Speichertyp anzeigen und überwachen. Das AdministrativeActions Array listet die 10 neuesten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die SSD-IOPS eines Dateisystems erhöhen, AdministrativeActions werden zwei generiert: eine FILE\_SYSTEM\_UPDATE und eine STORAGE\_TYPE\_OPTIMIZATION Aktion.

## Verwalten von SSD-IOPS

Bei SSD-Speicher-Volumes können Sie IOPS unabhängig von der Speicherkapazität auswählen und skalieren. Die maximale SSD-IOPS, die Sie bereitstellen können, hängt von der Menge der Speicherkapazität und der Durchsatzkapazität ab, die Sie für Ihr Dateisystem auswählen. Wenn Sie versuchen, Ihre SSD-IOPS über das von Ihrer Durchsatzkapazität unterstützte Limit zu erhöhen, müssen Sie möglicherweise Ihre Durchsatzkapazität erhöhen, um die angeforderte SSD-IOPS-Stufe zu unterstützen. Weitere Informationen finden Sie unter [Leistung von FSx for Windows File Server](#) und [Verwaltung der Durchsatzkapazität](#).

### Themen

- [Wichtige Punkte, die Sie bei der Aktualisierung von SSD-IOPS beachten sollten](#)
- [So aktualisieren Sie SSD-IOPS](#)
- [Überwachen von bereitgestellten SSD-IOPS-Updates](#)

### Wichtige Punkte, die Sie bei der Aktualisierung von SSD-IOPS beachten sollten

Hier sind einige wichtige Punkte, die Sie bei der Aktualisierung von SSD-IOPS berücksichtigen sollten:

- Um die Menge der bereitgestellten SSD-IOPS für Ihr Dateisystem anzugeben, müssen Sie einen von zwei IOPS-Modi auswählen:
  - Automatisch – Amazon FSx skaliert Ihre SSD-IOPS automatisch, um 3 SSD-IOPS pro GiB Speicherkapazität aufrechtzuerhalten, bis zu 400.000 SSD-IOPS pro Dateisystem.
  - Vom Benutzer bereitgestellt – Sie geben die Anzahl der SSD-IOPS im Bereich von 96 bis 400 000 an. Geben Sie eine Zahl zwischen 3 und 50 IOPS pro GiB Speicherkapazität für alle an, in AWS-Regionen denen Amazon FSx verfügbar ist, oder zwischen 3 und 500 IOPS pro GiB Speicherkapazität in USA Ost (Nord-Virginia), USA West (Oregon), USA Ost (Ohio), Europa (Irland), Asien-Pazifik (Tokio) und Asien-Pazifik (Singapur). Wenn die Menge der SSD-IOPS nicht mindestens 3 IOPS pro GiB beträgt, schlägt die Anforderung fehl. Bei höheren bereitgestellten SSD-IOPS zahlen Sie für die durchschnittlichen IOPS über 3 IOPS pro GiB pro Dateisystem.
- Aktualisierungen der Speicherkapazität – Wenn Sie Ihre Speicherkapazität erhöhen und die neue Kapazität eine höhere Menge an SSD-IOPS als die vom Benutzer bereitgestellte SSD-IOPS-Menge erfordert, wechselt Amazon FSx Ihr Dateisystem automatisch in den automatischen Modus.

- Aktualisierungen der Durchsatzkapazität – Wenn Sie Ihre Durchsatzkapazität erhöhen und die maximale von Ihrer neuen Durchsatzkapazität unterstützte SSD-IOPS höher ist als die vom Benutzer bereitgestellte SSD-IOPS-Stufe, wechselt Amazon FSx Ihr Dateisystem automatisch in den automatischen Modus.
- Zeit zwischen den Erhöhungen – Sie können keine weiteren SSD-IOPS-Erhöhungen, Erhöhungen der Durchsatzkapazität oder Speichertypaktualisierungen auf einem Dateisystem vornehmen, bis 6 Stunden nach der letzten Erhöhung angefordert wurde oder bis der Speicheroptimierungsprozess abgeschlossen ist – je nachdem, welcher Zeitraum länger ist. Die Speicheroptimierung kann einige Stunden bis zu einigen Tagen dauern. Um die Zeit bis zum Abschluss der Speicheroptimierung zu minimieren, empfehlen wir, SSD-IOPS zu skalieren, wenn nur minimaler Datenverkehr auf dem Dateisystem vorhanden ist.

#### Note

Beachten Sie, dass Durchsatzkapazitätsstufen von 4 608 MBpss und höher nur in den folgenden unterstützt werden AWS-Regionen: USA Ost (Nord-Virginia), USA West (Oregon), USA Ost (Ohio), Europa (Irland), Asien-Pazifik (Tokio) und Asien-Pazifik (Singapur).

## So aktualisieren Sie SSD-IOPS

Sie können SSD-IOPS für ein Dateisystem mithilfe der Amazon-FSx-Konsole AWS CLI, der oder der Amazon-FSx-API aktualisieren.

So aktualisieren Sie SSD-IOPS für ein Dateisystem (Konsole)

1. Öffnen Sie die Amazon-FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Windows-Dateisystem aus, für das Sie SSD-IOPS aktualisieren möchten.
3. Wählen Sie unter Aktionen die Option SSD-IOPS aktualisieren aus. Oder wählen Sie im Bereich Zusammenfassung die Schaltfläche Aktualisieren neben Bereitgestellte SSD-IOPS aus. Das Fenster IOPS-Bereitstellung aktualisieren wird geöffnet.

### Update IOPS Provisioning ✕

File system ID  
fs-0cffaa5ad762b33e6

Current file system configuration  
Storage capacity: 32 GiB  
Throughput capacity: 32 MB/s

Current Provisioned SSD IOPS  
Automatic

Desired SSD IOPS  
 Automatic (3 IOPS per GiB of SSD storage)  
 User-provisioned

User-provisioned IOPS  
  
Minimum 96 IOPS; Maximum 350,000 IOPS

**i** After modifying the storage type, throughput capacity, or provisioned SSD IOPS of a file system, you must wait at least six hours before modifying any of these configurations on the same file system again.

Cancel Update

4. Wählen Sie für Modus die Option Automatisch oder Vom Benutzer bereitgestellt aus. Wenn Sie Automatisch wählen, stellt Amazon FSx automatisch 3 SSD-IOPS pro GiB Speicherkapazität für Ihr Dateisystem bereit. Wenn Sie Vom Benutzer bereitgestellte auswählen, geben Sie eine beliebige Ganzzahl im Bereich von 96 bis 400 000 ein.
5. Wählen Sie Aktualisieren, um das bereitgestellte SSD-IOPS-Update zu initiieren.
6. Sie können den Aktualisierungsfortschritt auf der Detailseite Dateisysteme auf der Registerkarte Updates überwachen.

## So aktualisieren Sie SSD-IOPS für ein Dateisystem (CLI)

Verwenden Sie die `---windows-configuration DiskIopsConfiguration`Eigenschaft, um SSD-IOPS für ein FSx for Windows File Server-Dateisystem zu aktualisieren. Diese Eigenschaft hat zwei Parameter, `Iops` und `Mode`:

- Wenn Sie die Anzahl der SSD-IOPS angeben möchten, verwenden Sie bis `Iops=number_of_IOPS` zu maximal 400.000 in unterstützten AWS Regionen und `Mode=USER_PROVISIONED`.
- Wenn Sie möchten, dass Amazon FSx Ihre SSD-IOPS automatisch erhöht, verwenden Sie `Mode=AUTOMATIC` und nicht den `Iops` Parameter. Amazon FSx behält automatisch 3 SSD-IOPS pro GiB Speicherkapazität auf Ihrem Dateisystem bei, bis zu maximal 400.000 in unterstützten AWS Regionen.

Sie können den Fortschritt der Aktualisierung mit dem AWS CLI Befehl [überwachen](#)`describe-file-systems`. Suchen Sie `administrative-actions` in der Ausgabe nach .

Weitere Informationen finden Sie unter [AdministrativeAction](#).

## Überwachen von bereitgestellten SSD-IOPS-Updates

Sie können den Fortschritt eines bereitgestellten SSD-IOPS-Updates mithilfe der Amazon-FSx-Konsole, der API oder der `überwachenAWS CLI`.

### Überwachen von Updates in der Konsole

Auf der Registerkarte Updates im Fenster Dateisystemdetails können Sie die 10 letzten Updates für jeden Aktualisierungstyp anzeigen.

| Update type | Target value     | Status  | Progress % | Estimated time remaining | Request time              |
|-------------|------------------|---------|------------|--------------------------|---------------------------|
| IOPS Mode   | USER_PROVISIONED | Pending | -          | -                        | 2023-07-31T17:08:45-04:00 |
| SSD IOPS    | 350              | Pending | -          | -                        | 2023-07-31T17:08:45-04:00 |

Für bereitgestellte SSD-IOPS-Updates können Sie die folgenden Informationen anzeigen.

### Aktualisierungstyp

Mögliche Werte sind IOPS-Modus und SSD IOPS .

### Zielwert

Der gewünschte Wert, auf den der IOPS-Modus und die SSD-IOPS des Dateisystems aktualisiert werden sollen.

### Status

Der aktuelle Status der Aktualisierung. Für SSD-IOPS-Aktualisierungen sind die möglichen Werte wie folgt:

- Ausstehend – Amazon FSx hat die Aktualisierungsanforderung erhalten, hat aber nicht mit der Verarbeitung begonnen.
- In Bearbeitung – Amazon FSx verarbeitet die Aktualisierungsanforderung.
- Aktualisierte Optimierung – Die neue IOPS-Ebene ist für die Schreibvorgänge Ihres Workloads verfügbar. Ihr Update wechselt in den Status Aktualisierte Optimierung, der in der Regel einige Stunden dauert, während der die Lesevorgänge Ihres Workloads zwischen der vorherigen und der neuen Ebene eine IOPS-Leistung aufweisen. Nachdem Ihre Aktualisierungsaktion abgeschlossen ist, ist Ihr neuer IOPS-Wert sowohl für Lese- als auch für Schreibvorgänge verfügbar.
- Abgeschlossen – Das SSD-IOPS-Update wurde erfolgreich abgeschlossen.
- Fehlgeschlagen – Das SSD-IOPS-Update ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Details dazu anzuzeigen, warum die Speicheraktualisierung fehlgeschlagen ist.

## Fortschritt in %

Zeigt den Fortschritt des Speicheroptimierungsprozesses als abgeschlossen an.

## Anforderungszeit

Der Zeitpunkt, zu dem Amazon FSx die Aktualisierungsaktionsanforderung erhalten hat.

## Überwachen von Updates mit der AWS CLI und API

Sie können SSD-IOPS-Aktualisierungsanforderungen des Dateisystems mit dem [describe-file-systems](#) AWS CLI Befehl und der [DescribeFileSystems](#) API-Aktion anzeigen und überwachen. Das `AdministrativeActionsArray` listet die 10 letzten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die SSD-IOPS eines Dateisystems erhöhen, `AdministrativeActions` werden zwei generiert: eine - `FILE_SYSTEM_UPDATE` und eine -`IOPS_OPTIMIZATION`Aktion.

## Verwaltung der Durchsatzkapazität

Jedes Dateisystem von FSx für Windows File Server hat eine Durchsatzkapazität, die bei der Erstellung des Dateisystems konfiguriert wird. Sie können die Durchsatzkapazität Ihres Dateisystems jederzeit nach Bedarf ändern. Die Durchsatzkapazität ist ein Faktor, der die Geschwindigkeit bestimmt, mit der der Dateiserver, der das Dateisystem hostet, Dateidaten bereitstellen kann. Eine höhere Durchsatzkapazität geht auch mit höheren I/O-Vorgängen pro Sekunde (IOPS) und mehr Speicher für das Zwischenspeichern von Daten auf dem Dateiserver einher. Weitere Informationen finden Sie unter [Leistung von FSx for Windows File Server](#).

Wenn Sie die Durchsatzkapazität Ihres Dateisystems ändern, schaltet Amazon FSx den Dateiserver des Dateisystems hinter den Kulissen aus. Bei Multi-AZ-Dateisystemen führt dies zu einem automatischen Failover und einem Failback, während Amazon FSx die bevorzugten und sekundären Dateiserver ausschaltet. Bei Single-AZ-Systemen ist Ihr Dateisystem während der Skalierung der Durchsatzkapazität für einige Minuten nicht verfügbar. Die neue Menge an Durchsatzkapazität wird Ihnen in Rechnung gestellt, sobald sie Ihrem Dateisystem zur Verfügung steht.

### Note

Während eines Wartungsvorgangs am Backend können sich Systemänderungen (z. B. eine Änderung Ihrer Durchsatzkapazität) verzögern. Wartungsarbeiten können dazu führen, dass



diese Änderungen in die Warteschlange gestellt werden, bis sie als nächstes verarbeitet werden.

## Themen

- [Wann muss die Durchsatzkapazität geändert werden](#)
- [So ändern Sie die Durchsatzkapazität](#)
- [Überwachung von Änderungen der Durchsatzkapazität](#)

## Wann muss die Durchsatzkapazität geändert werden

Amazon FSx ist in Amazon integriert CloudWatch, sodass Sie die laufende Durchsatzauslastung Ihres Dateisystems überwachen können. Die Leistung (Durchsatz und IOPS), die Sie über Ihr Dateisystem erzielen können, hängt von den Eigenschaften Ihres spezifischen Workloads sowie von der Durchsatzkapazität, der Speicherkapazität und dem Speichertyp Ihres Dateisystems ab. Du kannst benutzen CloudWatch Metriken, um zu bestimmen, welche dieser Dimensionen geändert werden müssen, um die Leistung zu verbessern. Weitere Informationen finden Sie unter [Metriken mit Amazon überwachen CloudWatch](#).

Bei Multi-AZ-Dateisystemen führt die Skalierung der Durchsatzkapazität zu einem automatischen Failover und einem Failback, während Amazon FSx die bevorzugten und sekundären Dateiserver ausschaltet. Beim Austausch von Dateiservern, die während der Skalierung der Durchsatzkapazität sowie bei der Wartung des Dateisystems und bei ungeplanten Betriebsunterbrechungen erfolgen, wird der gesamte laufende Datenverkehr zum Dateisystem vom verbleibenden Dateiserver bedient. Wenn der ersetzte Dateiserver wieder online ist, führt FSx für Windows einen Resynchronisierungsjob aus, um sicherzustellen, dass die Daten wieder mit dem neu ersetzten Dateiserver synchronisiert werden.

FSx für Windows wurde entwickelt, um die Auswirkungen dieser Resynchronisierungsaktivität auf Anwendung und Benutzer zu minimieren. Der Resynchronisierungsprozess beinhaltet jedoch das Synchronisieren von Daten in großen Blöcken. Dies bedeutet, dass ein großer Datenblock eine Synchronisation erfordern kann, selbst wenn nur ein kleiner Teil aktualisiert wird. Folglich hängt das Ausmaß der Resynchronisierung nicht nur vom Ausmaß der Datenabwanderung ab, sondern auch von der Art der Datenabwanderung im Dateisystem. Wenn Ihr Workload schreib- und IOPS-lastig ist, kann der Datensynchronisierungsprozess länger dauern und zusätzliche Leistungsressourcen erfordern.

Ihr Dateisystem wird während dieser Zeit weiterhin verfügbar sein. Um die Dauer der Datensynchronisierung zu verkürzen, empfehlen wir jedoch, die Durchsatzkapazität während Leerlaufzeiten zu ändern, wenn Ihr Dateisystem nur minimal belastet wird. Wir empfehlen außerdem sicherzustellen, dass Ihr Dateisystem über eine ausreichende Durchsatzkapazität verfügt, um den Synchronisationsjob zusätzlich zu Ihrer Arbeitslast auszuführen, um die Dauer der Datensynchronisierung zu reduzieren. Schließlich empfehlen wir, die Auswirkungen von Failovers zu testen, während Ihr Dateisystem weniger ausgelastet ist.

## So ändern Sie die Durchsatzkapazität

Sie können die Durchsatzkapazität eines Dateisystems mithilfe der Amazon FSx-Konsole ändern, der AWS Command Line Interface (AWS CLI) oder die Amazon FSx-API.

So ändern Sie die Durchsatzkapazität eines Dateisystems (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme, und wählen Sie das Windows-Dateisystem aus, für das Sie die Durchsatzkapazität erhöhen möchten.
3. Für Aktionen, wählen Sie Durchsatz aktualisieren. Oder in der ZusammenfassungPanel, wählen Sie Aktualisieren neben dem Dateisystem Durchsatzkapazität.

Das Durchsatzkapazität aktualisieren Fenster erscheint.


4. Wählen Sie den neuen Wert für Durchsatzkapazität aus der Liste.

### Update throughput capacity ✕

File system ID  
fs-013771f0571a83e02


Current throughput capacity  
32 MB/s

Desired throughput capacity

Your single-AZ file system will experience a temporary loss of availability as Amazon FSx switches out the file server when you initiate a throughput capacity update action.  
[Learn more](#) 

Cancel Update

5. Wählen Sie **Aktualisieren** um die Aktualisierung der Durchsatzkapazität zu initiieren.

 **Note**

Multi-AZ-Dateisysteme führen bei Aktualisierung der Durchsatzskalierung ein Failover und ein Failback durch und sind in vollem Umfang verfügbar. Bei Single-AZ-Dateisystemen kommt es während des Updates zu einer sehr kurzen Zeit der Nichtverfügbarkeit.

6. Sie können den Aktualisierungsfortschritt auf der **Dateisysteme** Detailseite, in der **Aktualisierungen** Tab.

Sie können den Fortschritt des Updates mithilfe der Amazon FSx-Konsole überwachen, der AWS CLI und die API. Weitere Informationen finden Sie unter [Überwachung von Änderungen der Durchsatzkapazität](#).

## So ändern Sie die Durchsatzkapazität (CLI) eines Dateisystems

Um die Durchsatzkapazität eines Dateisystems zu ändern, verwenden Sie den AWS CLI-Befehl [update-file-system](#). Legen Sie die folgenden Parameter fest:

- `--file-system-id` auf die ID des Dateisystems, das Sie aktualisieren.
- `ThroughputCapacity` auf den gewünschten Wert, auf den das Dateisystem aktualisiert werden soll.

Sie können den Fortschritt des Updates mithilfe der Amazon FSx-Konsole überwachen, der AWS CLI und die API. Weitere Informationen finden Sie unter [Überwachung von Änderungen der Durchsatzkapazität](#).

## Überwachung von Änderungen der Durchsatzkapazität

Sie können den Fortschritt einer Änderung der Durchsatzkapazität mithilfe der Amazon FSx-Konsole, der API und der AWS CLI.

### Überwachung von Änderungen der Durchsatzkapazität in der Konsole

In der Aktualisierungen-Tab in der DateisystemdetailsIn diesem Fenster können Sie die 10 neuesten Aktualisierungsaktionen für jeden Aktualisierungstyp anzeigen.

| Updates (10) <span style="float: right;">↻</span>                                            |                |             |              |                           |
|----------------------------------------------------------------------------------------------|----------------|-------------|--------------|---------------------------|
| <input type="text" value="Filter updates"/> <span style="float: right;">&lt; 1 &gt; ⚙</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 |

Für Aktionen zur Aktualisierung der Durchsatzkapazität können Sie sich die folgenden Informationen ansehen.

## Typ aktualisieren

Möglicher Wert ist Durchsatzkapazität.

### Zielwert

Der gewünschte Wert, auf den die Durchsatzkapazität des Dateisystems geändert werden soll.

### Status

Der aktuelle Status des Updates. Für Aktualisierungen der Durchsatzkapazität lauten die möglichen Werte wie folgt:

- **ausstehend**— Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Verarbeitung begonnen.
- **In Bearbeitung**— Amazon FSx verarbeitet die Aktualisierungsanfrage.
- **Aktualisierte Optimierung**— Amazon FSx hat die Netzwerk-I/O-, CPU- und Speicherressourcen des Dateisystems aktualisiert. Das neue Festplatten-I/O-Leistungsniveau ist für Schreibvorgänge verfügbar. Bei Ihren Lesevorgängen wird die Festplatten-I/O-Leistung zwischen der vorherigen und der neuen Stufe gemessen, bis sich Ihr Dateisystem nicht mehr in diesem Zustand befindet.
- **Abgeschlossen**— Die Aktualisierung der Durchsatzkapazität wurde erfolgreich abgeschlossen.
- **Fehlgeschlagen**— Die Aktualisierung der Durchsatzkapazität ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um zu erfahren, warum die Durchsatzaktualisierung fehlgeschlagen ist.

### Uhrzeit anfragen

Der Zeitpunkt, zu dem Amazon FSx die Aktualisierungsanfrage erhalten hat.

## Überwachung von Änderungen mit dem AWS CLI und API

Sie können Anfragen zur Änderung der Durchsatzkapazität des Dateisystems mithilfe des [describe-file-systems](#) CLI-Befehl und der [DescribeFileSystems](#) API-Aktion.

Der `AdministrativeActions` Array listet die 10 neuesten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die Durchsatzkapazität eines Dateisystems ändern, wird `FILE_SYSTEM_UPDATE` Verwaltungsmaßnahmen werden eingeleitet.

Das folgende Beispiel zeigt den Antwortauszug von `describe-file-systems` CLI-Befehl. Das Dateisystem hat eine Durchsatzkapazität von 8 MB/s und die Zieldurchsatzkapazität von 256 MB/s.

```
.
```

```

.
.
  "ThroughputCapacity": 8,
"AdministrativeActions": [
  {
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
    "RequestTime": 1581694764.757,
    "Status": "PENDING",
    "TargetFileSystemValues": {
      "WindowsConfiguration": {
        "ThroughputCapacity": 256
      }
    }
  }
]

```

Wenn Amazon FSx die Verarbeitung der Aktion erfolgreich abgeschlossen hat, ändert sich der Status in `COMPLETED`. Die neue Durchsatzkapazität steht dann dem Dateisystem zur Verfügung und wird in `derThroughputCapacityEigentum`. Dies zeigt der folgende Antwortauszug von `describe-file-systems` CLI-Befehl.

```

.
.
.
  "ThroughputCapacity": 256,
"AdministrativeActions": [
  {
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
    "RequestTime": 1581694764.757,
    "Status": "COMPLETED",
    "TargetFileSystemValues": {
      "WindowsConfiguration": {
        "ThroughputCapacity": 256
      }
    }
  }
]

```

Schlägt die Änderung der Durchsatzkapazität fehl, ändert sich der Status in `FAILED`, und `derFailureDetails` Die Eigenschaft gibt Auskunft über den Fehler. Hinweise zur Behebung fehlgeschlagener Aktionen finden Sie unter [Aktualisierungen der Speicher- oder Durchsatzkapazität schlagen fehl](#).

# Markieren Ihrer Amazon FSx-Ressourcen mit Tags

Um Sie bei der Verwaltung Ihrer Dateisysteme und anderer Amazon FSx-Ressourcen zu unterstützen, können Sie jeder Ressource eigene Metadaten in Form von Tags zuweisen. Mit Tags (Markierungen) können Sie Ihre AWS-Ressourcen auf unterschiedliche Weise kategorisieren (z. B. nach Zweck, Eigentümer oder Umgebung). Dies ist nützlich, wenn Sie viele Ressourcen desselben Typs haben — In diesem Fall können Sie schnell bestimmte Ressourcen basierend auf den zugewiesenen Tags (Markierungen) bestimmen. In diesem Thema werden Tags (Markierungen) und deren Erstellung beschrieben.

## Themen

- [Grundlagen zu Tags \(Markierungen\)](#)
- [Markieren Ihrer -Ressourcen](#)
- [Tag \(Markierung\)-Einschränkungen](#)
- [Berechtigungen und Tag](#)

## Grundlagen zu Tags (Markierungen)

Ein Tag (Markierung) ist eine Markierung, die Sie einer AWS-Ressource zuordnen. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen.

Mit Tags (Markierungen) können Sie Ihre AWS-Ressourcen auf unterschiedliche Weise kategorisieren (z. B. nach Zweck, Eigentümer oder Umgebung). Sie können beispielsweise eine Reihe von Tags für die Amazon FSx-Dateisysteme Ihres Kontos definieren, um die Eigentümer der einzelnen Instances und die Stack-Ebene nachzuverfolgen.

Wir empfehlen die Verwendung von Tag (Markierung)-Schlüsseln, die die Anforderungen der jeweiligen Ressourcentypen erfüllen. Eine Anzahl einheitlicher Tag (Markierung)-Schlüssel vereinfacht das Verwalten der Ressourcen. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags (Markierungen) filtern und danach suchen. Weitere Informationen zum Implementieren einer effektiven Ressourcen-Markierungs-Strategie finden Sie im AWS-Whitepaper [Bewährte Methoden zur Markierung](#).

Tags haben für Amazon FSx keine semantische Bedeutung und werden ausschließlich als Zeichenfolgen interpretiert. Außerdem werden Tags (Markierungen) nicht automatisch Ihren

Ressourcen zugewiesen. Sie können Tag (Markierung)-Schlüssel und -Werte bearbeiten und Tags (Markierungen) jederzeit von einer Ressource entfernen. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht Null festlegen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben. Wenn Sie eine Ressource löschen, werden alle Tags (Markierungen) der Ressource ebenfalls gelöscht.

Wenn Sie die Amazon FSx-API verwenden, können Sie die AWS CLI oder eine AWS SDK verwenden. `TagResource` API-Aktion zum Anwenden von Tags auf bestehende Ressourcen. Zudem können Sie mit einigen Aktionen zur Ressourcenerstellung Tags beim Erstellen einer Ressource angeben. Wenn Tags (Markierungen) nicht während der Ressourcenerstellung angewendet werden können, wird die Ressourcenerstellung rückgängig gemacht. Auf diese Weise werden Ressourcen entweder mit Tags (Markierungen) oder überhaupt nicht erstellt und keine Ressourcen verbleiben ohne Tags (Markierungen). Indem Sie Ressourcen zum Erstellungszeitpunkt markieren, müssen Sie anschließend keine benutzerdefinierten Skripts ausführen. Weitere Informationen darüber, wie Sie Benutzern ermöglichen, Ressourcen bei der Erstellung zu markieren, finden Sie unter [Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung](#).

## Markieren Ihrer -Ressourcen

Sie können Amazon FSx-Ressourcen markieren, die in Ihrem Konto bestehen. Wenn Sie die Amazon FSx-Konsole verwenden, können Sie Tags auf Ressourcen anwenden, indem Sie die Registerkarte Tags auf dem entsprechenden Ressourcenbildschirm verwenden. Wenn Sie Ressourcen erstellen, können Sie den Namensschlüssel mit einem Wert anwenden, und Sie können Tags Ihrer Wahl anwenden, wenn Sie ein neues Dateisystem erstellen. Die Konsole kann Ressourcen nach dem Name -Tag organisieren, aber dieses Tag hat keine semantische Bedeutung für den Amazon FSx-Dienst.

Sie können Tag-basierte Berechtigungen auf Ressourcenebene in Ihren IAM-Richtlinien auf die Amazon FSx API-Aktionen anwenden, die das Tagging bei der Erstellung unterstützen, um eine granulare Kontrolle über die Benutzer und Gruppen zu implementieren, die Ressourcen bei der Erstellung mit Tags versehen können. Ihre Ressourcen sind ab Erstellung ordnungsgemäß geschützt. Tags (Markierungen) werden direkt auf Ihre Ressourcen angewendet. Daher treten alle Tag (Markierung)-basierten Berechtigungen auf Ressourcenebene, die die Verwendung von Ressourcen steuern, direkt in Kraft. Ihre Ressourcen können nachverfolgt und genauer erfasst werden. Sie können das Markieren neuer Ressourcen gewährleisten und steuern, welche Tag (Markierung)-Schlüssel und Werte für Ihre Ressourcen festgelegt sind.



Sie können ebenfalls Berechtigungen auf Ressourcenebene auf die `TagResource` und `UntagResource` Amazon FSx API-Aktionen in Ihren IAM-Richtlinien zur Kontrolle, welche Tag-Schlüssel und -Werte für Ihre bestehenden Ressourcen festgelegt sind.

Weitere Informationen zum Markieren von Ressourcen für die Fakturierung finden Sie unter [Verwendung von Tags \(Markierungen\) zur Kostenzuordnung](#) im Benutzerhandbuch für AWS Billing.

## Tag (Markierung)-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags (Markierungen) pro Ressource: 50
- Jeder Tag (Markierung) muss für jede Ressource eindeutig sein. Jeder Tag (Markierung) kann nur einen Wert haben.
- Maximale Schlüssellänge: 128 Unicode-Zeichen in UTF-8
- Maximale Wertlänge: 256 Unicode-Zeichen in UTF-8
- Die zulässigen Zeichen für Amazon FSx-Tags sind: Buchstaben, Zahlen und Leerzeichen, die in UTF-8 darstellbar sind, und die folgenden Zeichen: `+ - = . _ / @`.
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Das Präfix `aws :` ist zur Verwendung in AWS reserviert. Wenn der Tag (Markierung) über einen Tag (Markierung)-Schlüssel mit diesem Präfix verfügt, können Sie den Schlüssel oder Wert des Tags (Markierung) nicht bearbeiten oder löschen. Tags (Markierungen) mit dem Präfix `aws :` werden nicht als Ihre Tags (Markierungen) pro Ressourcenlimit angerechnet.

Sie können Ressourcen nicht allein auf Grundlage ihrer Tags löschen. Sie müssen den Ressourcenbezeichner angeben. Sie können beispielsweise ein Dateisystem löschen, das mit einem Tag-Schlüssel mit dem Namen versehen ist `DeleteMe` verwenden, müssen Sie verwenden `DeleteFileSystem` Aktion mit dem Dateisystem-Ressourcenbezeichner wie `fs-1234567890abcdef0`.

Wenn Sie öffentliche oder gemeinsam genutzte Ressourcen markieren, sind die von Ihnen zugewiesenen Tags nur für Ihre AWS-Konto; kein anderes AWS-Konto wird Zugriff auf diese Tags haben. Für die Tag-basierte Zugriffskontrolle auf freigegebene Ressourcen können jeweils AWS-Konto Sie müssen einen eigenen Satz von Tags (Markierungen) zuweisen, um den Zugriff auf die Ressource zu kontrollieren.

## Berechtigungen und Tag

Weitere Informationen über die erforderlichen Berechtigungen zum Tagging von Amazon FSx-Ressourcen bei der Erstellung finden Sie unter [Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung](#) aus. Weitere Informationen zur Verwendung von Tags zum Einschränken des Zugriffs auf Amazon FSx-Ressourcen in den IAM-Richtlinien finden Sie unter [Verwenden von Tags zur Steuerung des Zugriffs auf Ihre Amazon-FSx-Ressourcen](#) aus.

## Arbeiten mit Amazon FSx-Wartungsfenstern

Amazon FSx für Windows File Server führt routinemäßiges Software-Patching für die Microsoft Windows Server-Software durch, die es verwaltet. Über das Wartungsfenster können Sie den Wochentag und die Uhrzeit steuern, an denen Software-Patches durchgeführt werden. Sie wählen das Wartungsfenster bei der Erstellung des Dateisystems. Wenn Sie keine Zeitpräferenz haben, wird ein Standardfenster von 30 Minuten zugewiesen.

Mit FSx für Windows File Server können Sie Ihr Wartungsfenster an Ihre Arbeitslast und Ihre betrieblichen Anforderungen anpassen. Sie können Ihr Wartungsfenster beliebig oft verschieben, sofern mindestens einmal alle 14 Tage ein Wartungsfenster geplant ist. Wenn ein Patch veröffentlicht wird und Sie innerhalb von 14 Tagen kein Wartungsfenster geplant haben, fährt FSx für Windows File Server mit der Wartung des Dateisystems fort, um dessen Sicherheit und Zuverlässigkeit zu gewährleisten.

Während des Patches müssen Sie damit rechnen, dass Ihre Single-AZ-Dateisysteme nicht verfügbar sind, in der Regel für weniger als 20 Minuten. Ihre Multi-AZ-Dateisysteme bleiben verfügbar und führen automatisch ein Failover und ein Failback zwischen dem bevorzugten Dateiserver und dem Standby-Dateiserver durch. Weitere Informationen finden Sie unter [Failover-Prozess für FSx for Windows File Server](#). Da das Patchen für Multi-AZ-Dateisysteme Failover und Failback beinhaltet, muss der gesamte Datenverkehr zum Dateisystem während dieser Zeit zwischen dem bevorzugten Dateiserver und dem Standby-Dateiserver synchronisiert werden. Um die Patchzeit zu verkürzen, empfehlen wir, Ihr Wartungsfenster während Leerlaufzeiten zu planen, in denen Ihr Dateisystem nur minimal belastet wird.

### Note

Um die Datenintegrität während der Wartungsaktivitäten zu gewährleisten, schließt Amazon FSx für Windows File Server alle ausstehenden Schreibvorgänge auf den zugrunde

liegenden Speichervolumen ab, auf denen Ihr Dateisystem gehostet wird, bevor die Wartung beginnt.

Sie können die Amazon FSx Management Console verwenden, AWS CLI, AWSAPI oder eine der AWS SDKs, um das Wartungsfenster für Ihre Dateisysteme zu ändern.

Um das wöchentliche Wartungsfenster zu ändern (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie ein Dateisystem in der linken Navigationsspalte.
3. Wählen Sie das Dateisystem aus, für das Sie das wöchentliche Wartungsfenster ändern möchten. Die Seite mit den Dateisystemdetails wird angezeigt.
4. Wählen Sie Verwaltung, um die Dateisystemverwaltung anzuzeigen.
5. Wählen Sie Aktualisieren, um die anzuzeigenen Wartungsfenster ändern Fenster.
6. Geben Sie den neuen Tag und die neue Uhrzeit ein, an dem das wöchentliche Wartungsfenster beginnen soll.
7. Wählen Sie Save (Speichern), um Ihre Änderungen zu speichern. Die neue Startzeit der Wartung wird in der Administrationseinstellungen Panel.

Um das wöchentliche Wartungsfenster zu ändern, verwenden Sie den [update-file-system](#) CLI-Befehl, siehe [Exemplarische Vorgehensweise 3: Aktualisieren Sie ein vorhandenes -Dateisystem](#).

## Bewährte Methoden für die Verwaltung von Amazon FSx-Dateisystemen

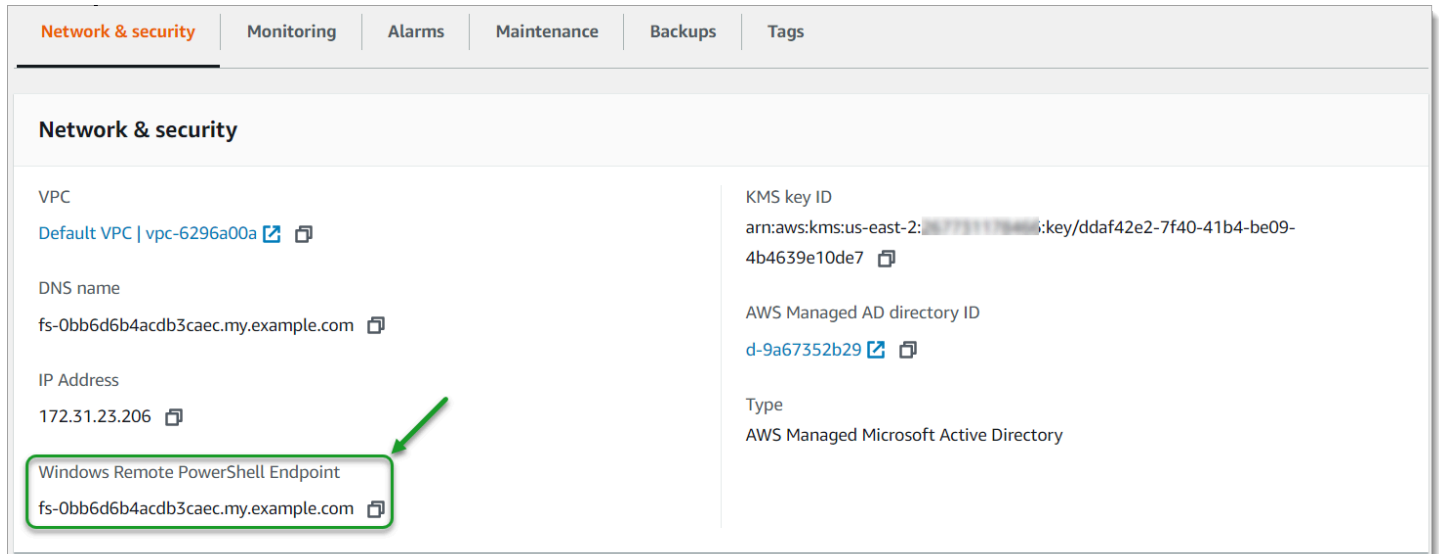
Amazon FSx bietet mehrere Funktionen, die Sie bei der Implementierung von Best Practices für die Verwaltung Ihrer Dateisysteme unterstützen können, darunter:

- Optimierung des Speicherverbrauchs
- ermöglicht Endbenutzern die Wiederherstellung von Dateien und Ordnern auf frühere Versionen
- Durchsetzung der Verschlüsselung für alle verbundenen Clients

Verwenden Sie die folgende Amazon FSx CLI for Remote Management on PowerShell Commands, um diese Best Practices schnell auf Ihren Dateisystemen zu implementieren.

Um diese Befehle ausführen zu können, müssen Sie den Windows Remote PowerShell Endpoint für Ihr Dateisystem kennen. Gehen Sie folgendermaßen vor, um diesen Endpunkt zu finden:

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie Ihr Dateisystem. Suchen Sie auf der Registerkarte Netzwerk und Sicherheit den Windows Remote PowerShell Endpoint, wie im Folgenden dargestellt.



Weitere Informationen finden Sie unter [Verwaltung von Dateisystemen](#) und [Verwenden der Amazon FSx CLI für PowerShell](#).

## Themen

- [Einmalige administrative Einrichtungsaufgaben](#)
- [Laufende Verwaltungsaufgaben zur Überwachung Ihres Dateisystems](#)

## Einmalige administrative Einrichtungsaufgaben

Im Folgenden finden Sie Aufgaben, die Sie schnell einmal für Ihr Dateisystem einrichten können.

### Verwaltung des Speicherverbrauchs

Verwenden Sie die folgenden Befehle, um den Speicherverbrauch Ihres Dateisystems zu verwalten.

- Führen Sie den folgenden Befehl aus, um die Datenduplizierung mit dem Standardzeitplan zu aktivieren.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock { Enable-FsxDedup }
```

Verwenden Sie optional den folgenden Befehl, um die Datendeduplizierung für Ihre Dateien unmittelbar nach der Erstellung einer Datei zum Laufen zu bringen, ohne dass ein Mindestalter für die Datei erforderlich ist.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock { Set-FsxDedupConfiguration -MinimumFileAgeDays 0 }
```

Weitere Informationen finden Sie unter [Datendeduplizierung](#).

- Verwenden Sie den folgenden Befehl, um Benutzerspeicherkontingente im Modus „Nachverfolgen“ zu aktivieren. Dieser Modus dient nur zu Berichtszwecken und nicht zur Durchsetzung.

```
$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 }
```

Weitere Informationen finden Sie unter [Speicherkontingente](#).

## Aktivieren von Schattenkopien, damit Endbenutzer Dateien und Ordner auf frühere Versionen wiederherstellen können

Aktivieren Sie Schattenkopien mit dem Standardzeitplan (werktags 7 Uhr und 12 Uhr) wie folgt.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock { Set-FsxShadowStorage -Default }
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock { Set-FsxShadowCopySchedule -Default -Confirm:$False }
```

Weitere Informationen finden Sie unter [Konfiguration von Schattenkopien für die Verwendung des Standardspeichers und des Standardzeitplans](#).

## Verschlüsselung bei der Übertragung erzwingen

Der folgende Befehl erzwingt die Verschlüsselung für Clients, die eine Verbindung zu Ihrem Dateisystem herstellen.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName FSxRemoteAdmin -ScriptBlock { Set-FsxSmbServerConfiguration -EncryptData $True -RejectUnencryptedAccess $True -Confirm:$False }
```

Sie können alle geöffneten Sitzungen schließen und Clients, die derzeit verbunden sind, erzwingen, sich mithilfe von Verschlüsselung erneut zu verbinden.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName FSxRemoteAdmin -ScriptBlock { Close-FsxSmbSession -Confirm:$False }
```

Weitere Informationen finden Sie unter [Verwaltung der Verschlüsselung bei der Übertragung](#) und [Benutzersitzungen und geöffnete Dateien](#).

## Laufende Verwaltungsaufgaben zur Überwachung Ihres Dateisystems

Die folgenden laufenden Aufgaben helfen Ihnen bei der Überwachung der Festplattennutzung, der Benutzerkontingente und der geöffneten Dateien in Ihrem Dateisystem.

### Überwachen des Deduplizierungsstatus

Überwachen Sie den Deduplizierungsstatus, einschließlich der in Ihrem Dateisystem erzielten Sparrate, wie folgt.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName FSxRemoteAdmin -ScriptBlock { Get-FSxDedupStatus } | select OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate
```

### Überwachung des Speicherverbrauchs auf Benutzerebene

Rufen Sie einen Bericht über die aktuellen Speicherkontingenteinträge der Benutzer ab, einschließlich des Speicherverbrauchs und der Frage, ob sie das Limit und den Warnschwellenwert überschreiten.

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

## Geöffnete Dateien überwachen und schließen

Verwalten Sie offene Dateien, indem Sie nach geöffneten Dateien suchen und diese schließen. Verwenden Sie den folgenden Befehl, um nach geöffneten Dateien zu suchen.

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

Verwenden Sie den folgenden Befehl, um geöffnete Dateien zu schließen.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock { Close-FSxSmbOpenFile -Confirm:$false}
```

# Gruppierung mehrerer Dateisysteme mit DFS-Namespaces

Amazon FSx for Windows File Server unterstützt die Verwendung der Distributed File System (DFS) -Namespaces von Microsoft. Sie können DFS-Namespaces verwenden, um Dateifreigaben auf mehreren Dateisystemen in einer gemeinsamen Ordnerstruktur (einem Namespace) zu gruppieren, die Sie für den Zugriff auf den gesamten Dateidatensatz verwenden. Mit DFS-Namespaces können Sie den Zugriff auf Ihre Dateifreigaben in mehreren Dateisystemen organisieren und vereinheitlichen. DFS-Namespaces können auch dazu beitragen, den Dateidatenspeicher für große Dateidatensätze über das hinaus zu skalieren, was jedes Dateisystem unterstützt (64 TB) — bis zu Hunderten von Petabyte.

## Einrichtung von DFS-Namespaces für die Gruppierung mehrerer Dateisysteme

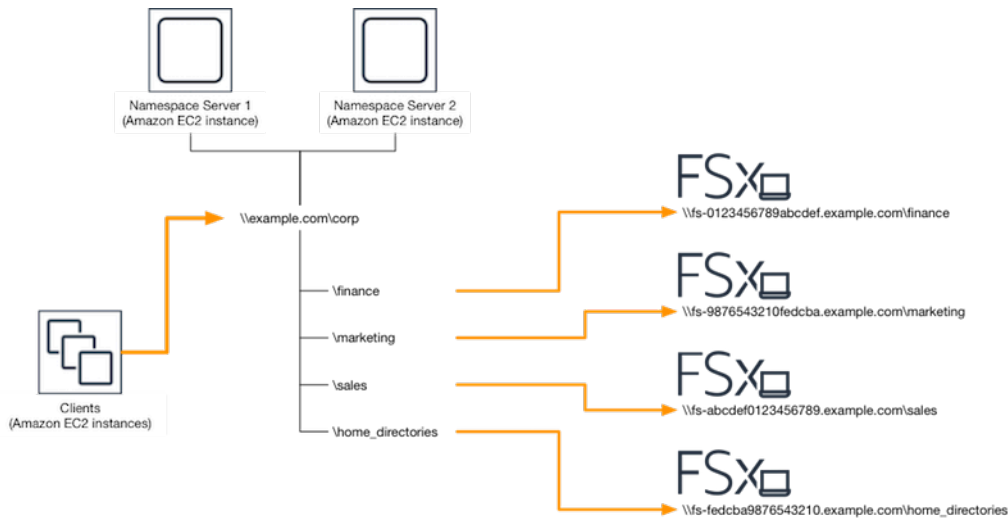
Sie können DFS-Namespaces verwenden, um mehrere Dateisysteme unter einem einzigen Namespace zu gruppieren. Im folgenden Beispiel wird der domänenbasierte Namespace (`example.com\ corp`) auf zwei Namespace-Servern erstellt, wodurch Dateifreigaben konsolidiert werden, die auf mehreren Amazon FSx-Dateisystemen (Finanzen, Marketing, Vertrieb, `home_directories`) gespeichert sind. Auf diese Weise können Ihre Benutzer über einen gemeinsamen Namespace auf Dateifreigaben zugreifen. Aus diesem Grund müssen sie nicht für jedes Dateisystem, das die Dateifreigaben hostet, DNS-Namen für das Dateisystem angeben.

### Note

Amazon FSx kann nicht zum Stammverzeichnis des DFS-Freigabepfads hinzugefügt werden.

Diese Schritte führen Sie durch die Erstellung eines einzelnen Namespaces (`example.com\ corp`) auf zwei Namespace-Servern. Sie richten außerdem vier Dateifreigaben unter dem Namespace ein, von denen jede Benutzer transparent auf Shares umleitet, die auf separaten Amazon FSx-Dateisystemen gehostet werden.





Um mehrere Dateisysteme in einem gemeinsamen DFS-Namespaceserver zu gruppieren

1. [Wenn Sie noch keine DFS-Namespaceserver ausführen, können Sie mithilfe der Vorlage Setup-DFSN-Servers.Template ein Paar hochverfügbarer DFS-Namespaceserver starten.](#) AWS CloudFormation [Weitere Informationen zum Erstellen eines Stacks finden Sie im Benutzerhandbuch unter Erstellen eines AWS CloudFormation Stacks auf der Konsole.](#) [AWS CloudFormation](#) [AWS CloudFormation](#)
2. Stellen Sie als Benutzer in der Gruppe AWS Delegierte Administratoren eine Connect zu einem der DFS-Namespaceserver her, die im vorherigen Schritt gestartet wurden. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Öffnen Sie die DFS Management Console, indem Sie sie öffnen. Öffnen Sie das Startmenü und führen Sie dfsmgmt.msc aus. Dadurch wird das DFS Management GUI-Tool geöffnet.
4. Wählen Sie Aktion und dann Neuer Namespace, geben Sie den Computernamen des ersten DFS-Namespaceservers ein, den Sie für Server gestartet haben, und wählen Sie Weiter.
5. Geben Sie unter Name den Namespace ein, den Sie erstellen (z. B. corp).
6. Wählen Sie „Einstellungen bearbeiten“ und legen Sie die entsprechenden Berechtigungen entsprechend Ihren Anforderungen fest. Wählen Sie Weiter aus.
7. Lassen Sie die Standardoption Domänenbasierter Namespace aktiviert, lassen Sie die Option Windows Server 2008-Modus aktivieren aktiviert und klicken Sie auf Weiter.

 Note

Der Windows Server 2008-Modus ist die neueste verfügbare Option für Namespaces.

8. Überprüfen Sie die Namespace-Einstellungen und wählen Sie Create aus.
9. Wählen Sie in der Navigationsleiste unter Namespaces den neu erstellten Namespace aus, wählen Sie Aktion und dann Namespace-Server hinzufügen aus.
10. Geben Sie den Computernamen des zweiten DFS-Namespace-Servers ein, den Sie für den Namespace-Server gestartet haben.
11. Wählen Sie „Einstellungen bearbeiten“, legen Sie die entsprechenden Berechtigungen entsprechend Ihren Anforderungen fest und wählen Sie „OK“.
12. Öffnen Sie das Kontextmenü (Rechtsklick) für den Namespace, den Sie gerade erstellt haben, wählen Sie Neuer Ordner, geben Sie den Namen des Ordners ein (z. B. `finance` für Name) und wählen Sie OK.
13. Geben Sie den DNS-Namen der Dateifreigabe, auf die der DFS-Namespace-Ordner verweisen soll, im UNC-Format (z. B. `\\fs-0123456789abcdef0.example.com\finance`) für Pfad zum Ordnerziel ein und wählen Sie OK aus.
14. Wenn die Freigabe nicht existiert:
  - a. Wählen Sie Ja, um es zu erstellen.
  - b. Wählen Sie im Dialogfeld „Teilen erstellen“ die Option „Durchsuchen“.
  - c. Wählen Sie einen vorhandenen Ordner aus, oder erstellen Sie einen neuen Ordner unter D\$ und klicken Sie auf OK.
  - d. Legen Sie die entsprechenden Freigabeberechtigungen fest und wählen Sie OK.
15. Wählen Sie im Dialogfeld „Neuer Ordner“ die Option „OK“. Der neue Ordner wird unter dem Namespace erstellt.
16. Wiederholen Sie die letzten vier Schritte für andere Ordner, die Sie unter demselben Namespace teilen möchten.

# Überwachung von FSx for Windows File Server

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon FSx und Ihren AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. Bevor Sie jedoch mit der Überwachung von Amazon FSx beginnen, sollten Sie einen Überwachungsplan erstellen, der Antworten auf die folgenden Fragen enthält:

- Was sind Ihre Ziele bei der Überwachung?
- Welche Ressourcen werden überwacht?
- Wie oft werden diese Ressourcen überwacht?
- Welche Überwachungstools werden verwendet?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

Weitere Informationen zur Protokollierung und Überwachung in FSx for Windows File Server finden Sie in den folgenden Themen.

## Themen

- [Überwachungstools](#)
- [Metriken mit Amazon überwachen CloudWatch](#)
- [Protokollen von Amazon FSx for Windows File Server API-Aufrufen mit AWS CloudTrail](#)

## Überwachungstools

AWS bietet verschiedene Tools, mit denen Sie Amazon FSx überwachen können. Sie können einige dieser Tools so konfigurieren, dass sie die Überwachung für Sie übernehmen, wohingegen bei einigen Tools ein manuelles Eingreifen erforderlich ist. Wir empfehlen, dass Sie die Überwachungsaufgaben möglichst automatisieren.

## Automatisierte Überwachungstools

Sie können die folgenden automatisierten Überwachungstools verwenden, um Amazon FSx zu beobachten und zu melden, wenn etwas nicht stimmt:

- Amazon CloudWatch Alarms — Überwachen Sie eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum und führen Sie eine oder mehrere Aktionen aus, die auf dem Wert der Metrik im Verhältnis zu einem bestimmten Schwellenwert über mehrere Zeiträume basieren. Die Aktion ist eine Benachrichtigung, die an ein Amazon Simple Notification Service (Amazon SNS) -Thema oder eine Amazon EC2 Auto Scaling Scaling-Richtlinie gesendet wird. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Status befinden. Der Status muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Weitere Informationen finden Sie unter [Metriken mit Amazon überwachen CloudWatch](#).
- Amazon CloudWatch Logs — Überwachen, speichern und greifen Sie auf Ihre Protokolldateien aus AWS CloudTrail oder anderen Quellen zu. Weitere Informationen finden Sie unter [Was ist Amazon CloudWatch Logs?](#) im Amazon CloudWatch Logs-Benutzerhandbuch.
- AWS CloudTrail Protokollüberwachung — Teilen Sie Protokolldateien zwischen Konten, überwachen CloudTrail Sie Protokolldateien in Echtzeit, indem Sie sie an CloudWatch Logs senden, schreiben Sie Protokollverarbeitungsanwendungen in Java und stellen Sie sicher, dass sich Ihre Protokolldateien nach der Lieferung von nicht geändert haben CloudTrail. Weitere Informationen finden Sie unter [Arbeiten mit CloudTrail Protokolldateien](#) im AWS CloudTrail Benutzerhandbuch.

## Manuelle Überwachungstools

Ein weiterer wichtiger Teil der Überwachung von Amazon FSx ist die manuelle Überwachung der Artikel, die von den CloudWatch Amazon-Alarmen nicht abgedeckt werden. Die Dashboards von Amazon FSx und anderen AWS Konsolen bieten einen at-a-glance Überblick über den Zustand Ihrer AWS Umgebung. CloudWatch

Die Überwachungs- und Leistungs-Dashboards der Amazon FSx-Konsole zeigen:

- Aktuelle Warnungen und Alarme für FSx for Windows File Server CloudWatch
- Grafiken, die eine Zusammenfassung der Dateisystemaktivitäten zeigen
- Diagramme zur Speicherkapazität und Auslastung des Dateisystems
- Diagramme zur Leistung von Dateiservern und Speichervolumen
- CloudWatch Alarme

Die CloudWatch Startseite zeigt:

- Aktuelle Alarme und Status

- Diagramme mit Alarmen und Ressourcen
- Servicestatus

Darüber hinaus können CloudWatch Sie Folgendes verwenden:

- Erstellen Sie [benutzerdefinierte Dashboards](#), um die von Ihnen verwendeten Dienste zu überwachen.
- Aufzeichnen von Metrikdaten, um Probleme zu beheben und Trends zu erkennen.
- Suchen und durchsuchen Sie alle Ihre AWS Ressourcenmetriken.
- Erstellen und Bearbeiten von Alarmen, um über Probleme benachrichtigt zu werden.

Weitere Informationen zum Amazon FSx Monitoring & Performance Dashboard finden Sie unter [So verwenden Sie FSx for Windows File Server Server-Metriken](#).

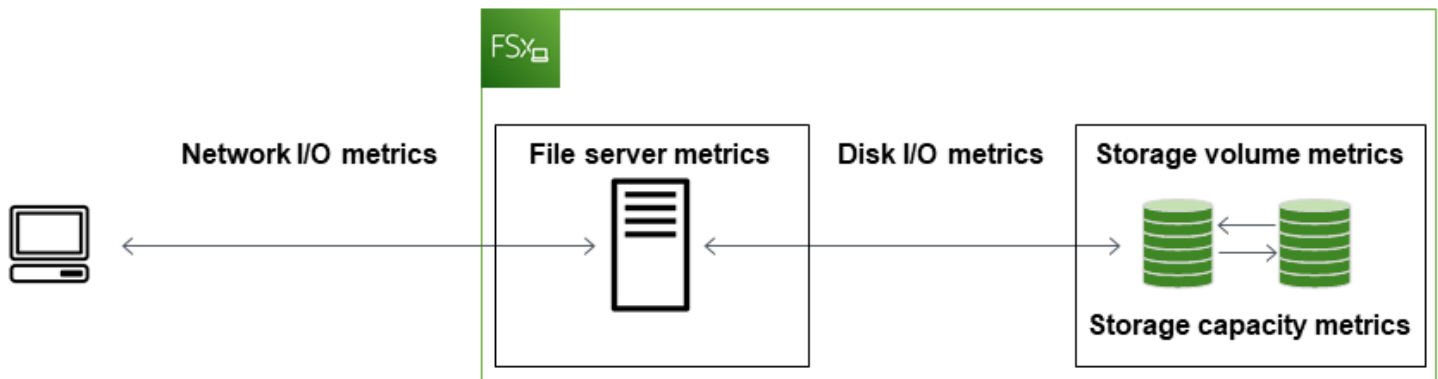
## Metriken mit Amazon überwachen CloudWatch

Sie können die Dateisysteme von FSx for Windows File Server mithilfe von Amazon überwachen. Amazon CloudWatch sammelt Rohdaten von FSx for Windows File Server und verarbeitet sie zu lesbaren, nahezu in Echtzeit verfügbaren Metriken. Diese Statistiken werden für einen Zeitraum von 15 Monaten aufbewahrt, sodass Sie auf historische Informationen zugreifen und sich einen Überblick über die Leistung Ihrer Webanwendung oder Ihres Dateisystems verschaffen können.

FSx for Windows File Server veröffentlicht CloudWatch Metriken in den folgenden Domänen:

- Netzwerk-I/O-Metriken messen die Aktivität zwischen Clients, die auf das Dateisystem zugreifen, und dem Dateiserver.
- Dateiserver-Metriken messen die Netzwerkdurchsatzauslastung, die CPU und den Arbeitsspeicher des Dateiservers sowie den Festplattendurchsatz und die IOPS-Auslastung des Dateiservers.
- Festplatten-I/O-Metriken messen die Aktivität zwischen dem Dateiserver und den Speichervolumen.
- Messwerte für das Speichervolumen messen die Festplattendurchsatzauslastung für HDD-Speichervolumen und die IOPS-Auslastung für SSD-Speichervolumen.
- Kennzahlen zur Speicherkapazität messen die Speichernutzung, einschließlich der Speichereinsparungen aufgrund der Datenduplizierung.

Das folgende Diagramm zeigt ein Dateisystem FSx for Windows File Server, seine Komponenten und die metrischen Domänen.



Standardmäßig sendet Amazon FSx for Windows File Server Metrikdaten in Abständen von 1 Minute CloudWatch an, mit den folgenden Ausnahmen, die in 5-Minuten-Intervallen ausgegeben werden:

- FileServerDiskThroughputBalance
- FileServerDiskIopsBalance

Weitere Informationen zu CloudWatch finden Sie unter [Was ist Amazon CloudWatch?](#) im CloudWatch Amazon-Benutzerhandbuch.

Metriken für Single-AZ-Dateisysteme während der Wartung des Dateisystems oder des Austauschs von Infrastrukturkomponenten und für Multi-AZ-Dateisysteme während des Failovers und Failbacks zwischen dem primären und dem sekundären Dateiserver werden möglicherweise nicht veröffentlicht.

Einige Amazon CloudWatch FSx-Metriken werden als Roh-Bytes gemeldet. Bytes werden nicht auf eine Dezimalzahl oder ein binäres Vielfaches der Einheit gerundet.

## Themen

- [Metriken und Dimensionen](#)
- [So verwenden Sie FSx for Windows File Server Server-Metriken](#)
- [Leistungswarnungen und Empfehlungen](#)
- [Zugreifen auf FSx for Windows File Server-Metriken](#)
- [CloudWatch Alarme zur Überwachung von Amazon FSx erstellen](#)

## Metriken und Dimensionen

FSx for Windows File Server veröffentlicht die folgenden Metriken im AWS/FSx Namespace in Amazon CloudWatch für alle Dateisysteme:

- DataReadBytes
- DataWriteBytes
- DataReadOperations
- DataWriteOperations
- MetadataOperations
- FreeStorageCapacity

FSx for Windows File Server veröffentlicht die im Folgenden beschriebenen Metriken im AWS/FSx Namespace in Amazon CloudWatch für Dateisysteme, die mit einer Durchsatzkapazität von mindestens 32 MBps konfiguriert sind.

### Themen

- [Netzwerk-I/O-Metriken für FSx für Windows](#)
- [Metriken für FSx für Windows-Dateiserver](#)
- [Festplatten-I/O-Metriken für FSx für Windows](#)
- [Messwerte zum Speichervolumen von FSx für Windows](#)
- [Kennzahlen zur Speicherkapazität von FSx für Windows](#)
- [Abmessungen von FSx für Windows](#)

## Netzwerk-I/O-Metriken für FSx für Windows

Der AWS/FSx Namespace umfasst die folgenden Netzwerk-I/O-Metriken.

| Metrik        | Beschreibung                                                                                                |
|---------------|-------------------------------------------------------------------------------------------------------------|
| DataReadBytes | Die Anzahl der Byte für Lesevorgänge für Clients, die auf das Dateisystem zugreifen.<br><br>Einheiten: Byte |

| Metrik              | Beschreibung                                                                                                                                   |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | Gültige Statistiken: Sum                                                                                                                       |
| DataWriteBytes      | Die Anzahl der Byte für Schreibvorgänge für Clients, die auf das Dateisystem zugreifen.<br><br>Einheiten: Byte<br><br>Gültige Statistiken: Sum |
| DataReadOperations  | Die Anzahl der Lesevorgänge für Clients, die auf das Dateisystem zugreifen.<br><br>Einheiten: Anzahl<br><br>Gültige Statistiken: Sum           |
| DataWriteOperations | Die Anzahl der Schreibvorgänge für Clients, die auf das Dateisystem zugreifen.<br><br>Einheiten: Anzahl<br><br>Gültige Statistiken: Sum        |
| MetadataOperations  | Die Anzahl der Metadatenoperationen für Clients, die auf das Dateisystem zugreifen.<br><br>Einheiten: Anzahl<br><br>Gültige Statistiken: Sum   |
| ClientConnections   | Die Anzahl der aktiven Verbindungen zwischen Clients und dem Dateiserver.<br><br>Einheiten: Anzahl                                             |

## Metriken für FSx für Windows-Dateiserver

Der AWS/FSx Namespace umfasst die folgenden Dateiserver-Metriken.



| Metrik                              | Beschreibung                                                                                                                                                                                                                                                           |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NetworkThroughputUtilization        | Der Netzwerkdurchsatz für Clients, die auf das Dateisystem zugreifen, als Prozentsatz des bereitgestellten Limits.<br><br>Einheiten: Prozent                                                                                                                           |
| CPUUtilization                      | Die prozentuale Auslastung der CPU-Ressourcen Ihres Dateiservers.<br><br>Einheiten: Prozent                                                                                                                                                                            |
| MemoryUtilization                   | Die prozentuale Auslastung der Speicherressourcen Ihres Dateiservers.<br><br>Einheiten: Prozent                                                                                                                                                                        |
| FileServerDiskThroughputUtilization | Der Festplattendurchsatz zwischen Ihrem Dateiserver und seinen Speichervolumen als Prozentsatz des bereitgestellten Limits, der durch die Durchsatzkapazität bestimmt wird.<br><br>Einheiten: Prozent                                                                  |
| FileServerDiskThroughputBalance     | Der Prozentsatz der verfügbaren Burst-Credits für den Festplattendurchsatz zwischen Ihrem Dateiserver und seinen Speichervolumen. Gültig für Dateisysteme, die mit einer Durchsatzkapazität von 256 MBps oder weniger bereitgestellt wurden.<br><br>Einheiten: Prozent |
| FileServerDiskIopsUtilization       | Die Festplatten-IOPS zwischen Ihrem Dateiserver und den Speichervolumen als Prozentsatz des bereitgestellten Limits, bestimmt durch die Durchsatzkapazität.<br><br>Einheiten: Prozent                                                                                  |
| FileServerDiskIopsBalance           | Der Prozentsatz der verfügbaren Burst-Credits für Festplatten-IOPS zwischen Ihrem Dateiserver und                                                                                                                                                                      |

| Metrik | Beschreibung                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <p>seinen Speichervolumen. Gültig für Dateisysteme, die mit einer Durchsatzkapazität von 256 MBps oder weniger bereitgestellt wurden.</p> <p>Einheiten: Prozent</p> |

## Festplatten-I/O-Metriken für FSx für Windows

Der AWS/FSx Namespace umfasst die folgenden Festplatten-I/O-Metriken.

| Metrik              | Beschreibung                                                                                                                                       |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskReadBytes       | <p>Die Anzahl der Byte für Lesevorgänge, die auf Speichervolumen zugreifen.</p> <p>Einheiten: Byte</p> <p>Gültige Statistiken: Summe</p>           |
| DiskWriteBytes      | <p>Die Anzahl der Byte für Schreibvorgänge, die auf Speichervolumen zugreifen.</p> <p>Einheiten: Byte</p> <p>Gültige Statistiken: Summe</p>        |
| DiskReadOperations  | <p>Die Anzahl der Lesevorgänge für den Dateiserver, der auf Speichervolumen zugreift.</p> <p>Einheiten: Anzahl</p> <p>Gültige Statistiken: Sum</p> |
| DiskWriteOperations | <p>Die Anzahl der Schreibvorgänge für den Dateiserver, der auf Speichervolumen zugreift.</p> <p>Einheiten: Anzahl</p>                              |

| Metrik | Beschreibung             |
|--------|--------------------------|
|        | Gültige Statistiken: Sum |

## Messwerte zum Speichervolumen von FSx für Windows

Der AWS/FSx Namespace umfasst die folgenden Messwerte für das Speichervolumen.

| Metrik                    | Beschreibung                                                                                                                                                                                                        |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DiskThroughputUtilization | (Nur Festplatte) Der Festplattendurchsatz zwischen Ihrem Dateiserver und seinen Speichervolumen als Prozentsatz des bereitgestellten Limits, der durch die Speichervolumen bestimmt wird.<br><br>Einheiten: Prozent |
| DiskThroughputBalance     | (Nur HDD) Der Prozentsatz der verfügbaren Burst-Credits für den Festplattendurchsatz für die Speichervolumen.<br><br>Einheiten: Prozent                                                                             |
| DiskIopsUtilization       | (Nur SSD) Die Festplatten-IOPS zwischen Ihrem Dateiserver und den Speichervolumen als Prozentsatz des bereitgestellten IOPS-Grenzwerts, der durch die Speichervolumen bestimmt wird.<br><br>Einheiten: Prozent      |

## Kennzahlen zur Speicherkapazität von FSx für Windows

Der AWS/FSx Namespace umfasst die folgenden Speicherkapazitätsmetriken.

| Metrik              | Beschreibung                                 |
|---------------------|----------------------------------------------|
| FreeStorageCapacity | Die Menge der verfügbaren Speicherkapazität. |

| Metrik                     | Beschreibung                                                                                                                    |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|                            | Einheiten: Byte<br><br>Gültige Statistiken: Average, Minimum                                                                    |
| StorageCapacityUtilization | Verwendete physische Speicherkapazität als Prozentsatz der gesamten Speicherkapazität.<br><br>Einheiten: Prozent                |
| DeduplicationSavedStorage  | Die Menge an Speicherplatz, die durch die Datendeduplizierung eingespart wird, sofern sie aktiviert ist.<br><br>Einheiten: Byte |

## Abmessungen von FSx für Windows

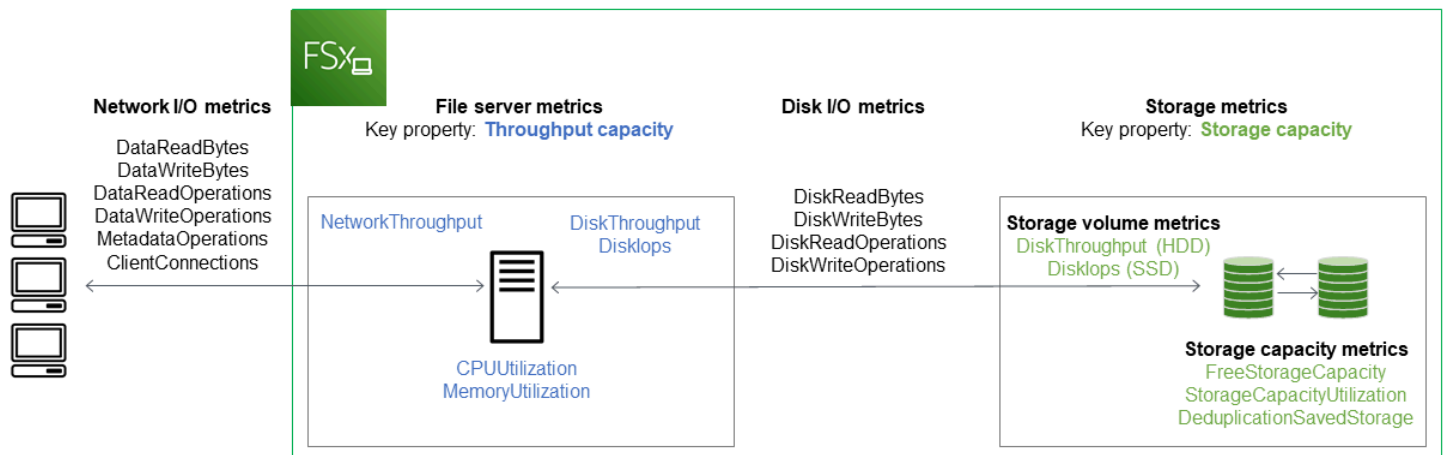
FSx for Windows File Server-Metriken verwenden den FSx Namespace und stellen Metriken für eine einzelne Dimension bereit, `FileSystemId`. Sie können die ID eines Dateisystems mithilfe des [describe-file-systems](#) AWS CLI Befehls oder des [DescribeFileSystems](#) API-Befehls ermitteln. Eine Dateisystem-ID hat die Form `fs-0123456789abcdef0`.

## So verwenden Sie FSx for Windows File Server Server-Metriken

Es gibt zwei Hauptarchitekturkomponenten jedes Amazon FSx-Dateisystems:

- Der Dateiserver, der Daten für Clients bereitstellt, die auf das Dateisystem zugreifen.
- Die Speichervolumes, die die Daten in Ihrem Dateisystem hosten.

FSx for Windows File Server meldet Metriken CloudWatch, die die Leistung und Ressourcennutzung für den Dateiserver und die Speichervolumes Ihres Dateisystems verfolgen. Das folgende Diagramm zeigt ein Amazon FSx-Dateisystem mit seinen Architekturkomponenten und den zur Überwachung verfügbaren Leistungs- und CloudWatch Ressourcenmetriken. Die wichtigste Eigenschaft, die für eine Reihe von Metriken angezeigt wird, ist die Dateisystemeigenschaft, die die Kapazität für diese Metriken bestimmt. Durch die Anpassung dieser Eigenschaft wird die Leistung des Dateisystems für diesen Satz von Metriken geändert.



Verwenden Sie den Bereich Überwachung und Leistung in der Amazon FSx-Konsole, um die in der folgenden Tabelle beschriebenen FSx for Windows File CloudWatch Server-Metriken anzuzeigen.

| Bedienfeld                 | Wie kann ich...                                                                   | Tabelle                      | Relevante Metriken                                                                             |
|----------------------------|-----------------------------------------------------------------------------------|------------------------------|------------------------------------------------------------------------------------------------|
| „Überwachung und Leistung“ | ... die Gesamt-IOPS meines Dateisystems ermitteln?                                | Gesamtzahl der IOPS          | SUMME (DataReadOperations + DataWriteOperations + MetadataOperations) / Zeitraum (in Sekunden) |
| Übersicht                  | ... den Gesamtdurchsatz meines Dateisystems ermitteln?                            | Gesamtdurchsatz              | SUMME (DataReadBytes + DataWriteBytes) / Zeitraum (in Sekunden)                                |
|                            | ... die Menge der verfügbaren Speicherkapazität auf meinem Dateisystem ermitteln? | Verfügbare Speicherkapazität | FreeStorageCapacity                                                                            |

| Bedienung<br>d<br>„Überwachung<br>und<br>Leistung | Wie kann ich...                                                                                                                                                                         | Tabelle                                                 | Relevante Metriken                  |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|-------------------------------------|
|                                                   | ... die Anzahl der Verbindungen ermitteln, die zwischen Clients und dem Dateiserver hergestellt wurden?                                                                                 | Client-Verbindungen                                     | ClientConnections                   |
|                                                   | ... die Menge des belegten physischen Festplattenspeichers als Prozentsatz der gesamten Speicherkapazität des Dateisystems ermitteln?                                                   | Auslastung der Speicherkapazität                        | StorageCapacityUtilization          |
| Speicher                                          | ... die Menge an physischem Festplattenspeicher ermitteln, die durch Datenduplizierung eingespart wird?                                                                                 | Durch die Datenduplizierung gespeicherter Speicherplatz | DeduplicationSavedStorage           |
| Leistung                                          | ... den Netzwerkdurchsatz für Clients, die auf das Dateisystem zugreifen, als Prozentsatz des bereitgestellten Durchsatzes des Dateisystems ermitteln?                                  | Nutzung des Netzwerkdurchsatzes                         | NetworkThroughputUtilization        |
| Dateiserver                                       | ... den Festplattendurchsatz zwischen dem Dateiserver und seinen Speichervolumen als Prozentsatz des bereitgestellten Limits ermitteln, der durch die Durchsatzkapazität bestimmt wird? | Auslastung des Festplattendurchsatzes                   | FileServerDiskThroughputUtilization |

| Bedienung<br>„Überwachung<br>und<br>Leistung | Wie kann ich...                                                                                                                                                                             | Tabelle                                  | Relevante Metriken              |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|---------------------------------|
|                                              | ... den Prozentsatz der verfügbaren Burst-Credits für den Festplattendurchsatz zwischen dem Dateiserver und seinen Speichervolumen ermitteln?                                               | Burst-Balance des Festplattendurchsatzes | FileServerDiskThroughputBalance |
|                                              | ... die Anzahl der Festplatten-IOPS zwischen dem Dateiserver und den Speichervolumen als Prozentsatz des bereitgestellten Limits ermitteln, der durch die Durchsatzkapazität bestimmt wird? | Festplatten-IOPS-Auslastung              | FileServerDiskIopsUtilization   |
|                                              | ... den Prozentsatz der verfügbaren Burst-Credits für Festplatten-IOPS zwischen dem Dateiserver und den Speichervolumen ermitteln?                                                          | Burst-Balance zwischen Festplatten-IOPS  | FileServerDiskIopsBalance       |
|                                              | ... den Prozentsatz der CPU-Auslastung des Dateiservers ermitteln?                                                                                                                          | CPU-Auslastung                           | CPUUtilization                  |
|                                              | ... die prozentuale Speicherauslastung des Dateiservers ermitteln?                                                                                                                          | Speicherauslastung                       | MemoryUtilization               |
| Leistung<br>—<br>Speichervolumen             | ... den Durchsatz für Operationen, die auf Speichervolumen zugreifen, als Prozentsatz des bereitgestellten Limits ermitteln, der durch die Festplattenspeicherkapazität bestimmt wird?      | Nutzung des Festplattendurchsatzes (HDD) | DiskThroughputUtilization       |

| Bedienung<br>„Überwachung<br>und<br>Leistung | Wie kann ich...                                                                                                                                                            | Tabelle                                          | Relevante Metriken    |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|-----------------------|
|                                              | ... den Prozentsatz der verfügbaren Burst-Credits für den Durchsatz von Vorgängen ermitteln, die auf HDD-Speichervolumen zugreifen?                                        | Burst-Balance (HDD) für den Festplattendurchsatz | DiskThroughputBalance |
|                                              | ... die IOPS für Operationen, die auf Speichervolumen zugreifen, als Prozentsatz des bereitgestellten Limits ermitteln, der durch die SSD-Speicherkapazität bestimmt wird? | Festplatten-IOPS-Auslastung (SSD)                | DiskIopsUtilization   |

### Note

Wir empfehlen, eine durchschnittliche Durchsatzkapazitätsauslastung von unter 50% beizubehalten, um sicherzustellen, dass genügend freie Durchsatzkapazität für unerwartete Workloadspitzen sowie für alle Windows-Speichervorgänge im Hintergrund (wie Speichersynchronisierung, Deduplizierung oder Schattenkopien) zur Verfügung steht.

## Leistungswarnungen und Empfehlungen

FSx for Windows bietet Ihnen Leistungswarnungen für Dateisysteme, die mit einer Durchsatzkapazität von mindestens 32 MBps konfiguriert sind. Amazon FSx zeigt eine Warnung für eine Reihe von CloudWatch Metriken an, wenn eine dieser Metriken für mehrere aufeinanderfolgende Datenpunkte einen vordefinierten Schwellenwert erreicht oder überschritten hat. Diese Warnungen



bieten Ihnen umsetzbare Empfehlungen, mit denen Sie die Leistung Ihres Dateisystems optimieren können.

Auf Warnungen kann in verschiedenen Bereichen des Überwachungs- und Leistungs-Dashboards zugegriffen werden. Alle aktiven oder aktuellen Amazon FSx-Leistungswarnungen und alle für das Dateisystem konfigurierten CloudWatch Alarme, die sich im ALARM-Status befinden, werden im Bereich Überwachung und Leistung im Abschnitt Zusammenfassung angezeigt. Die Warnung wird auch in dem Bereich des Dashboards angezeigt, in dem das Metrikdiagramm angezeigt wird.

Sie können CloudWatch Alarme für alle Amazon FSx-Metriken erstellen. Weitere Informationen finden Sie unter [CloudWatch Alarme zur Überwachung von Amazon FSx erstellen](#).

Verwenden Sie Leistungswarnungen, um die Leistung des Dateisystems zu verbessern

Amazon FSx bietet umsetzbare Empfehlungen, mit denen Sie die Leistung Ihres Dateisystems optimieren können. Diese Empfehlungen beschreiben, wie Sie einem potenziellen Leistungsengpass begegnen können. Sie können die empfohlene Maßnahme ergreifen, wenn Sie davon ausgehen, dass die Aktivität fortgesetzt wird oder wenn sie die Leistung Ihres Dateisystems beeinträchtigt. Je nachdem, welche Metrik eine Warnung ausgelöst hat, können Sie diese beheben, indem Sie entweder die Durchsatzkapazität oder die Speicherkapazität des Dateisystems erhöhen, wie in der folgenden Tabelle beschrieben.

| Wenn für diese Metrik eine Warnung vorliegt               | Vorgehensweise                                                                                          |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Netzwerkdurchsatz — Auslastung                            |                                                                                                         |
| Dateiserver > Festplatten-IOPS — Auslastung               |                                                                                                         |
| Dateiserver > Festplattendurchsatz — Auslastung           | <a href="#">Erhöhen Sie die Durchsatzkapazität</a>                                                      |
| Dateiserver > Festplatten-IOPS — Burst-Balance            |                                                                                                         |
| Dateiserver > Festplattendurchsatz — Burst-Balance        |                                                                                                         |
| Nutzung der Speicherkapazität                             | <a href="#">Erhöhen Sie die Speicherkapazität</a>                                                       |
| Speichervolumen > Festplattendurchsatz — Auslastung (HDD) | <a href="#">Erhöhen Sie die Speicherkapazität</a> oder <a href="#">wechseln Sie zum SDD-Speichertyp</a> |

| Wenn für diese Metrik eine Warnung vorliegt                  | Vorgehensweise                   |
|--------------------------------------------------------------|----------------------------------|
| Speichervolumen > Festplattendurchsatz — Burst-Balance (HDD) |                                  |
| Speichervolumen > Festplatten-IOPS — Auslastung (SSD)        | <a href="#">SSD-IOPS erhöhen</a> |

### Note

Bestimmte Dateisystemereignisse können Festplatten-I/O-Leistungsressourcen verbrauchen und möglicherweise Leistungswarnungen auslösen. Beispielsweise:

- Die Optimierungsphase der Skalierung der Speicherkapazität kann zu einem erhöhten Festplattendurchsatz führen, wie unter beschrieben [Die Speicherkapazität steigt und die Leistung des Dateisystems](#)
- Bei Multi-AZ-Dateisystemen führen Ereignisse wie die Skalierung der Durchsatzkapazität, der Austausch von Hardware oder die Unterbrechung der Availability Zone zu automatischen Failover- und Failback-Ereignissen. Alle Datenänderungen, die während dieser Zeit auftreten, müssen zwischen dem primären und dem sekundären Dateiserver synchronisiert werden, und Windows Server führt einen Datensynchronisierungsauftrag aus, der Festplatten-I/O-Ressourcen verbrauchen kann. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

Weitere Informationen zur Leistung des Dateisystems finden Sie unter [Leistung von FSx for Windows File Server](#).

## Zugreifen auf FSx for Windows File Server-Metriken

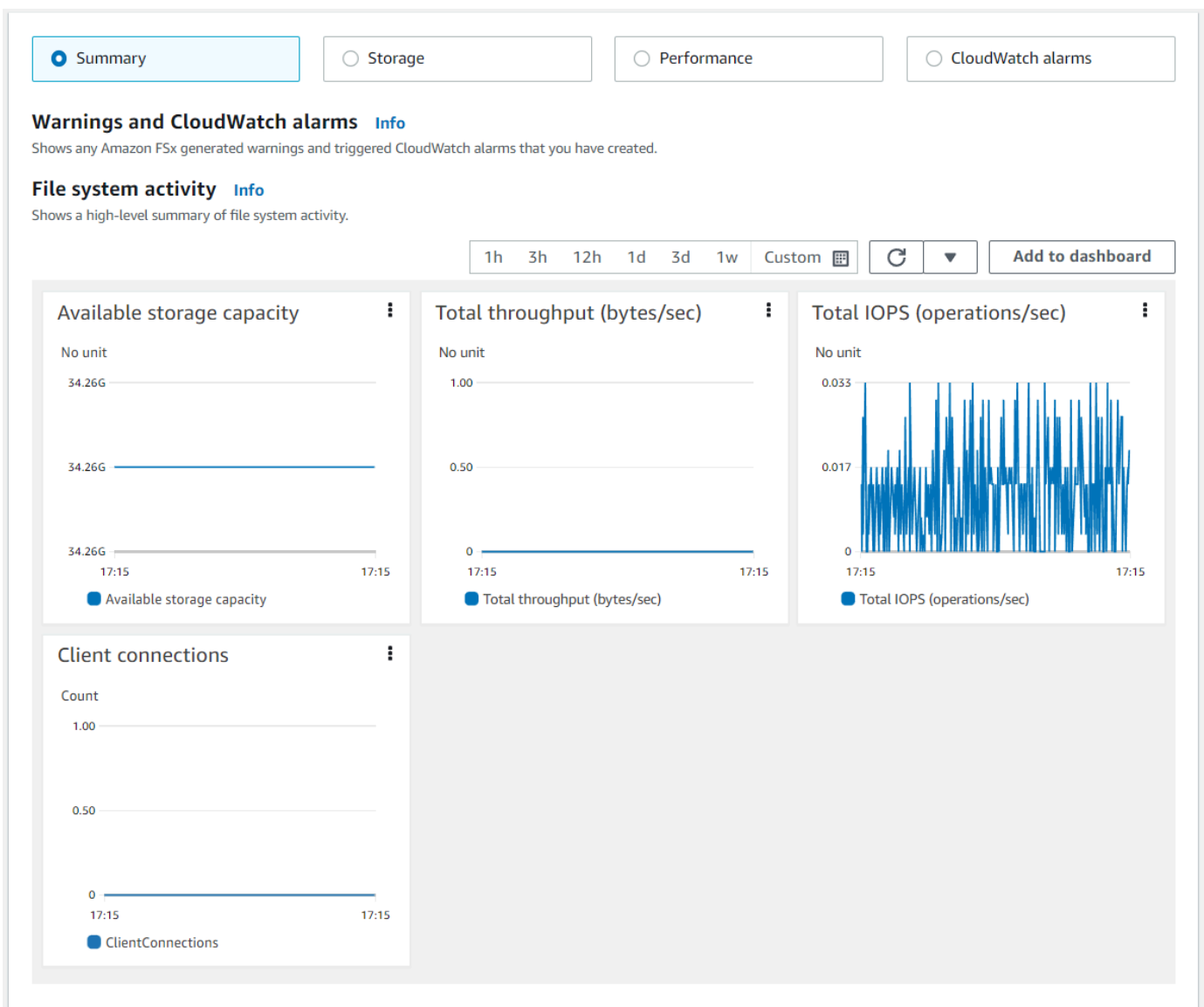
Sie können Amazon FSx-Metriken für CloudWatch auf folgende Weise einsehen.

- Die Amazon FSx-Konsole.
- Die CloudWatch Konsole.
- Die CloudWatch CLI (Befehlszeilenschnittstelle).
- Die CloudWatch API.

In den folgenden Verfahren wird beschrieben, wie Sie mit diesen verschiedenen Tools auf die Metriken Ihres Dateisystems zugreifen können.

So zeigen Sie Dateisystem-Metriken mit der Amazon FSx-Konsole an

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Um die Seite mit den Dateisystemdetails anzuzeigen, wählen Sie im Navigationsbereich Dateisysteme aus.
3. Wählen Sie das Dateisystem aus, dessen Metriken Sie anzeigen möchten.
4. Um Diagramme der Dateisystem-Metriken anzuzeigen, wählen Sie im zweiten Bereich Überwachung und Leistung aus.

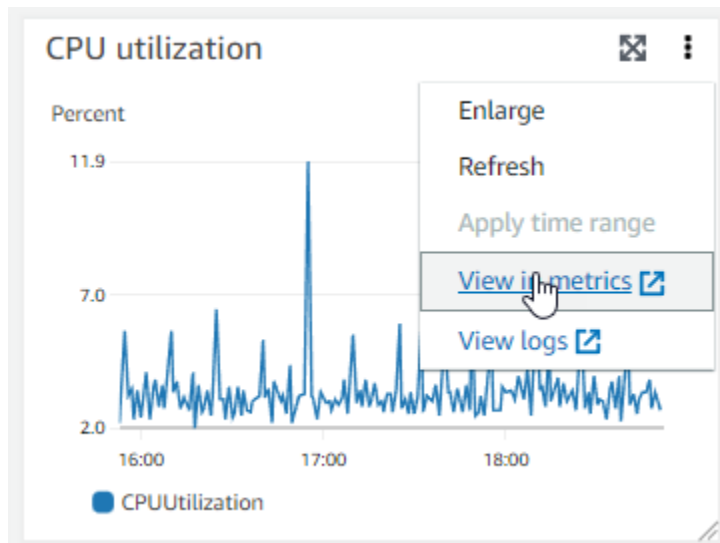


- Die Übersichtsmetriken werden standardmäßig angezeigt und enthalten alle aktiven Warnungen und CloudWatch Alarme zusammen mit den Messdaten zur Dateisystemaktivität.
- Wählen Sie Speicher, um Kennzahlen zur Speicherkapazität und Auslastung anzuzeigen.
- Wählen Sie Leistung, um Leistungskennzahlen für Dateiserver und Speicher anzuzeigen
- Wählen Sie CloudWatch Alarme, um Diagramme aller für das Dateisystem konfigurierten Alarme anzuzeigen.

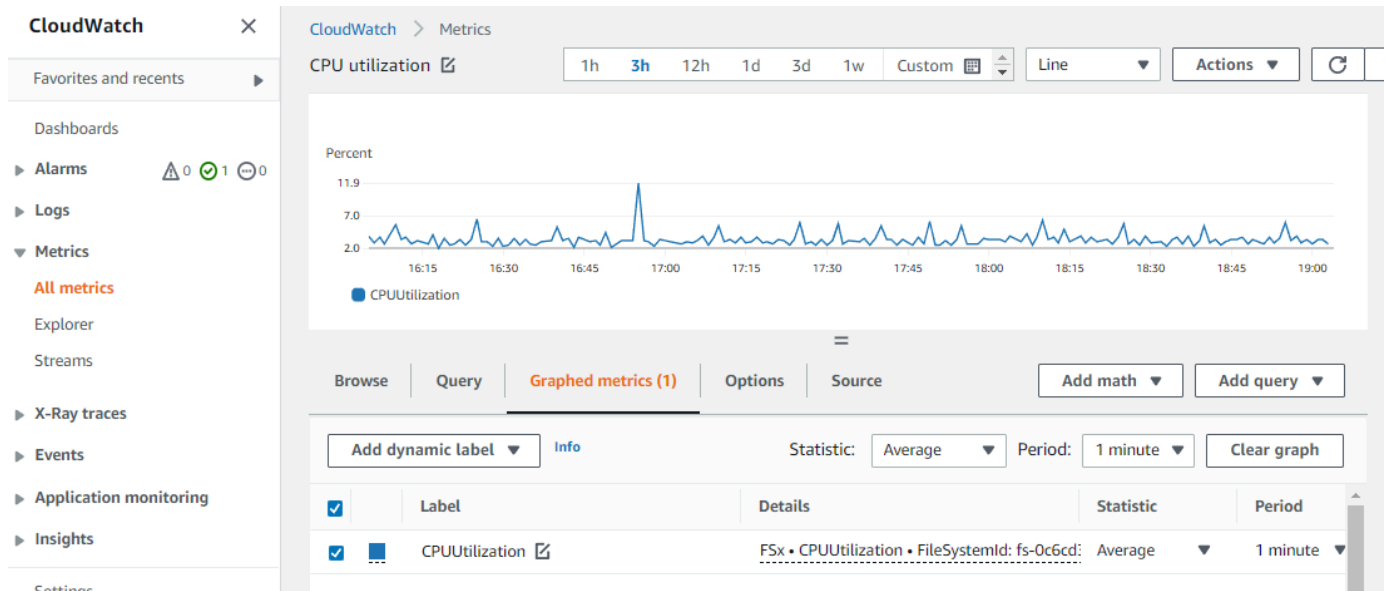
Weitere Informationen finden Sie unter [So verwenden Sie FSx for Windows File Server Server-Metriken](#).

Um Metriken in der CloudWatch Konsole anzuzeigen

1. Um eine Dateisystem-Metrik auf der Metrik-Seite der CloudWatch Amazon-Konsole anzuzeigen, navigieren Sie zu der Metrik im Bereich Monitoring & Performance der Amazon FSx-Konsole.
2. Wählen Sie im Aktionsmenü oben rechts im Metrikdiagramm die Option In Metriken anzeigen aus, wie in der folgenden Abbildung dargestellt.



Dadurch wird die Seite „Metriken“ in der CloudWatch Konsole geöffnet, auf der das Metrikdiagramm angezeigt wird, wie in der folgenden Abbildung dargestellt.



Um Metriken zu einem CloudWatch Dashboard hinzuzufügen

1. Um einen Satz von FSx for Windows-Dateisystem-Metriken zu einem Dashboard in der CloudWatch Konsole hinzuzufügen, wählen Sie den Satz von Metriken (Zusammenfassung, Speicher oder Leistung) im Bereich Überwachung und Leistung der Amazon FSx-Konsole aus.
2. Wählen Sie oben rechts im Bereich die Option Zum Dashboard hinzufügen. Dadurch wird die CloudWatch Konsole geöffnet.
3. Wählen Sie ein vorhandenes CloudWatch Dashboard aus der Liste aus oder erstellen Sie ein neues Dashboard. Weitere Informationen finden Sie unter [Verwenden von CloudWatch Amazon-Dashboards](#) im CloudWatch Amazon-Benutzerhandbuch.

Um auf Metriken zuzugreifen, klicken Sie auf AWS CLI

- Verwenden Sie den Befehl [list-metrics](#) mit dem `--namespace "AWS/FSx"`-Namespace. Weitere Informationen finden Sie in der [AWS CLI -Befehlsreferenz](#).

Mithilfe der CloudWatch API

Um über die CloudWatch API auf Metriken zuzugreifen

- Rufen Sie die folgende Seite auf [GetMetricStatistics](#). Weitere Informationen finden Sie unter [Amazon CloudWatch API-Referenz](#).

## CloudWatch Alarme zur Überwachung von Amazon FSx erstellen

Sie können einen CloudWatch Alarm erstellen, der eine Amazon SNS SNS-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum und führt eine oder mehrere Aktionen durch, die vom Wert der Metrik im Vergleich zu einem festgelegten Schwellenwert in einer Reihe von Zeiträumen abhängt. Die Aktion ist eine Benachrichtigung, die an ein Amazon SNS-Thema oder eine Auto Scaling-Richtlinie gesendet wird.

Bei Alarmen werden nur Aktionen für anhaltende Statusänderungen ausgelöst. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Zustand befinden. Der Status muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Sie können einen Alarm von der Amazon FSx-Konsole oder der CloudWatch Konsole aus erstellen.

Die folgenden Verfahren beschreiben, wie Alarme für Amazon FSx mithilfe der Konsole AWS CLI, und der API erstellt werden.

So richten Sie Alarme mit der Amazon FSx-Konsole ein

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Navigationsbereich Dateisysteme und dann das Dateisystem aus, für das Sie den Alarm erstellen möchten.
3. Wählen Sie das Menü Aktionen und dann Details anzeigen aus.
4. Wählen Sie auf der Übersichtsseite die Option Überwachung und Leistung aus.
5. Wählen Sie CloudWatch Alarme aus.
6. Wählen Sie CloudWatch Alarm erstellen. Sie werden zur CloudWatch-Konsole umgeleitet.
7. Wählen Sie Metriken auswählen und dann Weiter aus.
8. Wählen Sie im Abschnitt Metriken die Option FSX aus.
9. Wählen Sie Dateisystem-Metriken, wählen Sie die Metrik aus, für die Sie den Alarm einstellen möchten, und wählen Sie dann Metrik auswählen.
10. Wählen Sie im Abschnitt Bedingungen die Bedingungen aus, die Sie für den Alarm verwenden möchten, und klicken Sie auf Weiter.


### Note

Metriken dürfen nicht während der Dateisystemwartung für Single-AZ-Dateisysteme oder während eines Failovers und Failbacks zu oder von den primären oder sekundären

Servern für Multi-AZ-Dateisysteme veröffentlicht werden. Um unnötige und irreführende Änderungen der Alarmbedingungen zu verhindern und Ihre Alarmer so zu konfigurieren, dass sie gegen fehlende Datenpunkte resistent sind, finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Konfiguration der Behandlung fehlender Daten durch CloudWatch Alarmer](#).

11. Wenn Sie Ihnen eine E-Mail oder eine SNS-Benachrichtigung senden CloudWatch möchten, wenn der Alarmstatus die Aktion auslöst, wählen Sie einen Alarmstatus für Wann immer dieser Alarmstatus ist.

Wählen Sie ein vorhandenes SNS-Thema aus, um ein vorhandenes SNS-Thema auszuwählen. Wenn Sie Create topic auswählen, können Sie den Namen und die E-Mail Adressen für eine neue E-Mail-Abonnementliste einrichten. Diese Liste wird gespeichert und erscheint für künftige Alarmer in der Liste. Wählen Sie Weiter aus.

 Note

Wenn Sie Create topic (Thema erstellen) verwenden, um ein neues Amazon-SNS-Thema einzurichten, müssen die E-Mail Adressen überprüft werden, bevor die Empfänger Benachrichtigungen erhalten. E-Mail Nachrichten werden nur gesendet, wenn der Alarm in einen Alarmzustand wechselt. Wenn es zu dieser Änderung des Alarmzustands kommt, bevor die E-Mail Adressen überprüft wurden, erhalten die Empfänger keine Benachrichtigung.


12. Geben Sie die Werte Name, Beschreibung und Whenever für die Metrik ein und klicken Sie auf Weiter.
13. Überprüfen Sie auf der Seite Vorschau und Erstellung den Alarm, den Sie gerade erstellen möchten, und wählen Sie dann Alarm erstellen aus.

So richten Sie Alarmer mithilfe der CloudWatch Konsole ein

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie „Alarm erstellen“, um den Assistenten zum Erstellen von Alarmen zu starten.
3. Wählen Sie FSx Metrics und blättern Sie durch die Amazon FSx-Metriken, um die Metrik zu finden, für die Sie einen Alarm auslösen möchten. Um nur die Amazon FSx-Metriken in diesem

Dialogfeld anzuzeigen, suchen Sie nach der Dateisystem-ID Ihres Dateisystems. Wählen Sie die Metrik aus, um einen Alarm zu erstellen, und klicken Sie dann auf Weiter.

4. Geben Sie unter Name, Description und Whenever die Werte für die Metrik ein.
5. Wenn Sie Ihnen eine E-Mail senden CloudWatch möchten, wenn der Alarmstatus erreicht ist, wählen Sie für Wann immer dieser Alarm die Option Status ist ALARM. Wählen Sie unter Benachrichtigung senden an: ein vorhandenes SNS-Thema aus. Wenn Sie Create topic auswählen, können Sie den Namen und die E-Mail Adressen für eine neue E-Mail-Abonnementliste einrichten. Diese Liste wird gespeichert und erscheint für künftige Alarme in der Liste.

 Note

Wenn Sie Create topic (Thema erstellen) verwenden, um ein neues Amazon-SNS-Thema einzurichten, müssen die E-Mail Adressen überprüft werden, bevor die Empfänger Benachrichtigungen erhalten. E-Mail Nachrichten werden nur gesendet, wenn der Alarm in einen Alarmzustand wechselt. Wenn es zu dieser Änderung des Alarmzustands kommt, bevor die E-Mail Adressen überprüft wurden, erhalten die Empfänger keine Benachrichtigung.

6. An dieser Stelle haben Sie im Bereich Alarmvorschau die Möglichkeit, eine Vorschau des Alarms anzuzeigen, den Sie gerade erstellen möchten. Wählen Sie Alarm erstellen aus.

Um einen Alarm einzustellen, verwenden Sie AWS CLI

- Rufen Sie die folgende Seite auf [put-metric-alarm](#). Weitere Informationen finden Sie in der [AWS CLI -Befehlsreferenz](#).

Um einen Alarm mithilfe der CloudWatch API einzustellen

- Rufen Sie die folgende Seite auf [PutMetricAlarm](#). Weitere Informationen finden Sie unter [Amazon CloudWatch API-Referenz](#).



## Protokolle von Amazon FSx for Windows File Server API-Aufrufen mit AWS CloudTrail

Amazon FSx for Windows File Server ist integriert mit AWS CloudTrail, ein Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Service in Amazon FSx. CloudTrail erfasst alle API-Aufrufe für Amazon FSx als Ereignisse. Die erfassten Aufrufe umfassen Aufrufe von der Amazon-FSx-Konsole und Codeaufrufe an die Amazon-FSx-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignisse in einem Amazon S3 S3-Bucket, einschließlich Ereignisse für Amazon FSx. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole in Ereignisverlauf. Verwendung der gesammelten Informationen von CloudTrail können Sie die an Amazon FSx an Amazon FSx und weitere Details bestimmen.

Für weitere Informationen über CloudTrail, finden Sie unter [AWS CloudTrail Benutzerhandbuch](#).

### Amazon FSx Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto wenn Sie das -Konto erstellen. Erfolgreiche Aktivitäten in Amazon FSx, werden diese als CloudTrail Veranstaltung zusammen mit anderen AWS-Service-Ereignisse in Ereignisverlauf. Sie können die neuesten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter [Anzeigen von Ereignissen mit CloudTrail Ereignisverlauf](#).

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignisse für Amazon FSx, erstellen Sie einen Trail. Ein weiterer Weg aktiviert CloudTrail um Protokolldateien an einen Amazon-S3-Bucket zu übermitteln. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere konfigurieren AWS-Services zur weiteren Analyse und zur weiteren Umsetzung der in gesammelten Ereignisdaten CloudTrail protokolliert. Weitere Informationen finden Sie unter:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail In unterstützte Services und Integrationen](#)
- [Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen CloudTrail Protokolldateien von mehreren Konten](#)

Alle Amazon FSx -Aktionen werden protokolliert CloudTrail und sind dokumentiert in der [Amazon FSx API-Referenz](#). Aufrufe von `CreateFileSystem`, `CreateBackup` und `TagResource` Aktionen generieren Einträge im CloudTrail -Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

## Erläuterungen der Amazon FSx Einträge

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail -Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail Logeintrag, der das demonstriert `TagResource` Vorgang, wenn ein Tag für ein Dateisystem von der Konsole aus erstellt wird.

```
{
  "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"
}

```

Das folgende Beispiel zeigt einen CloudTrail Logeintrag, der das demonstriert `UntagResource` Aktion, wenn ein Tag für ein Dateisystem aus der Konsole gelöscht wird.

```

{
  "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"
}
```

# Leistung von FSx for Windows File Server

FSx for Windows File Server bietet Dateisystemkonfigurationsoptionen, um eine Vielzahl von Leistungsanforderungen zu erfüllen. Im Folgenden finden Sie einen Überblick über die Leistung des Amazon FSx-Dateisystems mit einer Erläuterung der verfügbaren Leistungskonfigurationsoptionen und nützlichen Tipps zur Leistung.

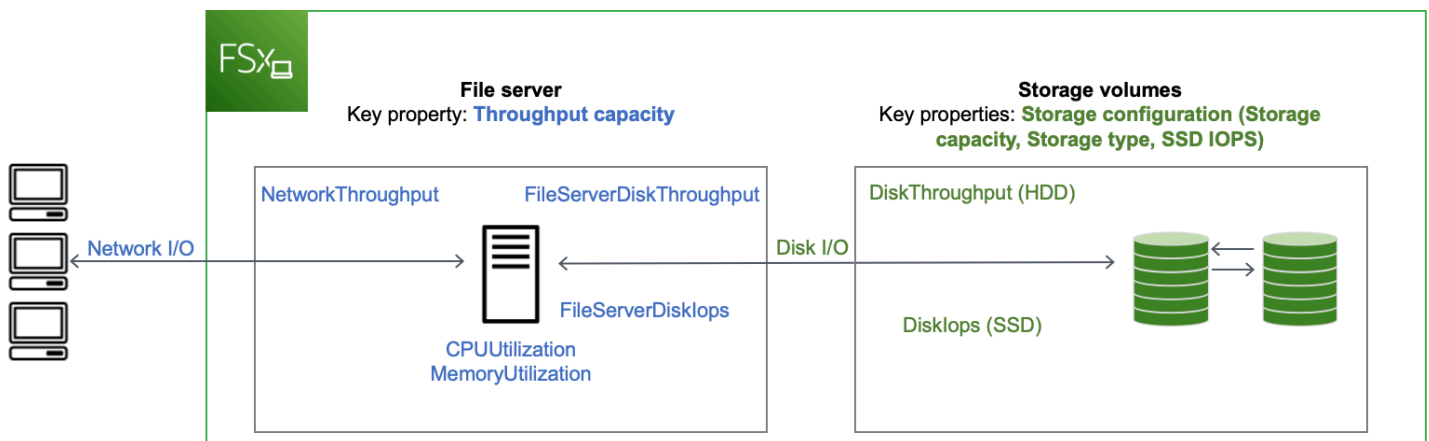
## Themen

- [Leistung des Dateisystems](#)
- [Zusätzliche Überlegungen zur Leistung](#)
- [Auswirkung der Durchsatzkapazität auf die Leistung](#)
- [Auswahl der richtigen Durchsatzkapazität](#)
- [Auswirkung der Speicherkonfiguration auf die Leistung](#)
- [Beispiel: Speicherkapazität und Durchsatzkapazität](#)
- [Messung der Leistung anhand von Metriken CloudWatch](#)
- [Behebung von Leistungsproblemen](#)

## Leistung des Dateisystems

Jedes Dateisystem FSx for Windows File Server besteht aus einem Windows-Dateiserver, mit dem Clients kommunizieren, und einer Reihe von Speichervolumen oder Festplatten, die an den Dateiserver angeschlossen sind. Jeder Dateiserver verwendet einen schnellen In-Memory-Cache, um die Leistung der Daten, auf die am häufigsten zugegriffen wird, zu verbessern.

Das folgende Diagramm zeigt, wie auf Daten von einem Dateisystem FSx for Windows File Server zugegriffen wird.



Wenn ein Client auf Daten zugreift, die im In-Memory-Cache gespeichert sind, werden die Daten als Netzwerk-I/O direkt an den anfragenden Client gesendet. Der Dateiserver muss sie nicht von der Festplatte lesen oder auf die Festplatte schreiben. Die Leistung dieses Datenzugriffs wird durch die Netzwerk-E/A-Grenzwerte und die Größe des In-Memory-Caches bestimmt.

Wenn ein Client auf Daten zugreift, die sich nicht im Cache befinden, liest der Dateiserver sie als Festplatten-I/O von der Festplatte oder schreibt sie auf die Festplatte. Die Daten werden dann vom Dateiserver an den Client als Netzwerk-I/O weitergeleitet. Die Leistung dieses Datenzugriffs wird durch die Netzwerk-I/O-Grenzwerte sowie die Festplatten-I/O-Grenzwerte bestimmt.

Die Netzwerk-I/O-Leistung und der In-Memory-Cache des Dateiservers werden durch die Durchsatzkapazität eines Dateisystems bestimmt. Die Festplatten-I/O-Leistung wird durch eine Kombination aus Durchsatzkapazität und Speicherkonfiguration bestimmt. Die maximale Festplatten-I/O-Leistung, die sich aus Festplattendurchsatz und Festplatten-IOPS-Werten zusammensetzt, die Ihr Dateisystem erreichen kann, ist der niedrigere der folgenden Werte:

- Das von Ihrem Dateiserver bereitgestellte Festplatten-I/O-Leistungsniveau, basierend auf der Durchsatzkapazität, die Sie für Ihr Dateisystem auswählen.
- Das von Ihrer Speicherkonfiguration bereitgestellte Festplatten-I/O-Leistungsniveau (die Speicherkapazität, der Speichertyp und die SSD-IOPS-Stufe, die Sie für Ihr Dateisystem auswählen).

## Zusätzliche Überlegungen zur Leistung

Die Leistung eines Dateisystems wird in der Regel anhand der Latenz, des Durchsatzes und der I/O-Operationen pro Sekunde (IOPS) gemessen.

## Latency

FSx for Windows File Server Server-Dateiserver verwenden einen schnellen In-Memory-Cache, um konsistente Latenzen von unter einer Millisekunde für aktiv abgerufene Daten zu erreichen. Für Daten, die sich nicht im In-Memory-Cache befinden, d. h. für Dateioperationen, die durch I/O auf den zugrunde liegenden Speichervolumen bedient werden müssen, bietet Amazon FSx Dateivorgangslatenzen im Submillisekundenbereich mit Solid-State-Drive-Speicher (SSD) und Latenzen im einstelligen Millisekundenbereich mit Festplattenspeicher (HDD).

## Durchsatz und IOPS

Amazon FSx-Dateisysteme bieten bis zu 2 GB/s und 80.000 IOPS in allen Ländern, in AWS-Regionen denen Amazon FSx verfügbar ist, und 12 GB/s Durchsatz und 400.000 IOPS in den USA Ost (Nord-Virginia), USA West (Oregon), USA Ost (Ohio), Europa (Irland), Asien-Pazifik (Tokio) und Asien-Pazifik (Singapur). Die spezifische Menge an Durchsatz und IOPS, die Ihr Workload in Ihrem Dateisystem erzeugen kann, hängt von der Durchsatzkapazität, der Speicherkapazität und dem Speichertyp Ihres Dateisystems sowie von der Art Ihrer Arbeitslast ab, einschließlich der Größe des aktiven Arbeitssatzes.

## Leistung eines einzelnen Clients

Mit Amazon FSx können Sie den vollen Durchsatz und die IOPS-Werte für Ihr Dateisystem von einem einzigen Client aus erreichen, der darauf zugreift. Amazon FSx unterstützt SMB Multichannel. Diese Funktion ermöglicht es, einen Durchsatz von bis zu mehreren GB/s und Hunderttausende von IOPS für einen einzelnen Client bereitzustellen, der auf Ihr Dateisystem zugreift. SMB Multichannel verwendet mehrere Netzwerkverbindungen zwischen dem Client und dem Server gleichzeitig, um die Netzwerkbandbreite für eine maximale Auslastung zu aggregieren. Zwar gibt es eine theoretische Grenze für die Anzahl der von Windows unterstützten SMB-Verbindungen, aber diese Grenze geht in die Millionen, sodass Sie praktisch eine unbegrenzte Anzahl von SMB-Verbindungen haben können.

## Leistungssteigerung

Dateibasierte Workloads sind in der Regel stark angespannt und zeichnen sich durch kurze, intensive Perioden mit hohem I/O-Aufwand und vielen Leerlaufzeiten zwischen den einzelnen Bursts aus. Um hohe Workloads zu unterstützen, bietet Amazon FSx zusätzlich zu den Basisgeschwindigkeiten, die ein Dateisystem rund um die Uhr aufrechterhalten kann, die Möglichkeit, sowohl bei Netzwerk-I/O- als auch bei Festplatten-I/O-Vorgängen für bestimmte Zeiträume höhere Geschwindigkeiten zu erreichen. Amazon FSx verwendet einen I/O-Guthabenmechanismus, um Durchsatz und IOPS auf

der Grundlage der durchschnittlichen Auslastung zuzuweisen. Dateisysteme sammeln Credits, wenn ihr Durchsatz und ihre IOPS-Nutzung unter ihren Basisgrenzwerten liegen, und können diese Credits verwenden, wenn sie I/O-Operationen ausführen.

## Auswirkung der Durchsatzkapazität auf die Leistung

Die Durchsatzkapazität bestimmt die Leistung des Dateisystems in den folgenden Kategorien:

- **Netzwerk-I/O** — Die Geschwindigkeit, mit der der Dateiserver Dateidaten an Clients weiterleiten kann, die darauf zugreifen.
- **CPU und Arbeitsspeicher des Dateiservers** — Ressourcen, die für die Bereitstellung von Dateidaten und für Hintergrundaktivitäten wie Datendeduplizierung und Schattenkopien zur Verfügung stehen.
- **Festplatten-I/O** — Die Geschwindigkeit, mit der der Dateiserver I/O zwischen dem Dateiserver und den Speichervolumen unterstützen kann.

Die folgenden Tabellen enthalten Informationen zu den maximalen Netzwerk-I/O-Werten (Durchsatz und IOPS) und Festplatten-I/O (Durchsatz und IOPS), die Sie mit jeder bereitgestellten Durchsatzkapazitätskonfiguration erreichen können, sowie zu der Menge an Arbeitsspeicher, die für das Zwischenspeichern und die Unterstützung von Hintergrundaktivitäten wie Datendeduplizierung und Schattenkopien zur Verfügung steht. Sie können zwar Durchsatzkapazitäten unter 32 Megabyte pro Sekunde (MBps) wählen, wenn Sie die Amazon FSx-API oder CLI verwenden. Beachten Sie jedoch, dass diese Stufen für Test- und Entwicklungsworkloads und nicht für Produktionsworkloads vorgesehen sind.

### Note

Beachten Sie, dass Durchsatzkapazitäten von 4.608 MBps und höher nur in den folgenden Regionen unterstützt werden: USA Ost (Nord-Virginia), USA West (Oregon), USA Ost (Ohio), Europa (Irland), Asien-Pazifik (Tokio) und Asien-Pazifik (Singapur).



## Netzwerk-I/O und Speicher

| FSx-Durchsatzkapazität (Megabyte pro Sekunde) | Netzwerkdurchsatz (Megabyte pro Sekunde) |                                     | Netzwerk-IOPS   | Speicher (GB) |
|-----------------------------------------------|------------------------------------------|-------------------------------------|-----------------|---------------|
|                                               | Basislinie                               | Burst (für ein paar Minuten am Tag) |                 |               |
| 32                                            | 32                                       | 600                                 | Tausende        | 4             |
| 64                                            | 64                                       | 600                                 | Zehntausende    | 8             |
| 128                                           | 150                                      | 1 250                               |                 | 8             |
| 256                                           | 300                                      | 1 250                               | Hunderttausende | 16            |
| 512                                           | 600                                      | 1 250                               |                 | 32            |
| 1,024                                         | 1.500                                    | –                                   |                 | 72            |
| 2 048                                         | 3.125                                    | –                                   |                 | 144           |
| 4.608                                         | 9.375                                    | –                                   | Millionen       | 192           |
| 6 144                                         | 12.500                                   | –                                   |                 | 256           |
| 9 216                                         | 18 750                                   | –                                   |                 | 384           |
| 12 288                                        | 21.250                                   | –                                   |                 | 512           |

## Festplatten-I/O

| FSx-Durchsatzkapazität (Megabyte pro Sekunde) | Festplattendurchsatz (Megabyte pro Sekunde) |                               | Festplatten-IOPS   |                               |
|-----------------------------------------------|---------------------------------------------|-------------------------------|--------------------|-------------------------------|
|                                               | Basislinie                                  | Burst (für 30 Minuten am Tag) | Ausgangswert       | Burst (für 30 Minuten am Tag) |
| 32                                            | 32                                          | 260                           | 2K                 | 12 K                          |
| 64                                            | 64                                          | 350                           | 4K                 | 16 K                          |
| 128                                           | 128                                         | 600                           | 6 K                | 20 K                          |
| 256                                           | 256                                         | 600                           | 10 K               | 20 K                          |
| 512                                           | 512                                         | –                             | 20 K               | –                             |
| 1,024                                         | 1,024                                       | –                             | 40 000             | –                             |
| 2 048                                         | 2 048                                       | –                             | 80 K               | –                             |
| 4.608                                         | 4.608                                       | –                             | 150 K              | –                             |
| 6 144                                         | 6 144                                       | –                             | 200 K              | –                             |
| 9 216                                         | 9.216 <sup>1</sup>                          | –                             | 300 K <sup>1</sup> | –                             |
| 12 288                                        | 12.288 <sup>1</sup>                         | –                             | 400 K <sup>1</sup> | –                             |

### Note

<sup>1</sup> Wenn Sie ein Multi-AZ-Dateisystem mit einer Durchsatzkapazität von 9.216 oder 12.288 MBps haben, ist die Leistung nur für Schreibverkehr auf 9.000 MBps und 262.500 IOPS begrenzt. Andernfalls unterstützt Ihr Dateisystem für den Leseverkehr auf allen Multi-AZ-Dateisystemen, den Lese- und Schreibverkehr auf allen Single-AZ-Dateisystemen und alle anderen Durchsatzkapazitätsstufen die in der Tabelle angegebenen Leistungsgrenzen.

## Auswahl der richtigen Durchsatzkapazität

Wenn Sie mit der Amazon Web Services Management Console ein Dateisystem erstellen, wählt Amazon FSx automatisch die empfohlene Durchsatzkapazität für Ihr Dateisystem auf der Grundlage der von Ihnen konfigurierten Speicherkapazität aus. Obwohl die empfohlene Durchsatzkapazität für die meisten Workloads ausreichend sein sollte, haben Sie die Möglichkeit, die Empfehlung zu überschreiben und eine bestimmte Menge an Durchsatzkapazität auszuwählen, die den Anforderungen Ihrer Anwendung entspricht. Wenn Ihre Arbeitslast beispielsweise die Übertragung von 1 Gbit/s an Datenverkehr in Ihr Dateisystem erfordert, sollten Sie eine Durchsatzkapazität von mindestens 1.024 Mbit/s wählen.

Bei der Festlegung des zu konfigurierenden Durchsatzniveaus sollten Sie auch die Funktionen berücksichtigen, die Sie in Ihrem Dateisystem aktivieren möchten. Wenn Sie beispielsweise [Schattenkopien](#) aktivieren, müssen Sie möglicherweise Ihre Durchsatzkapazität auf das Dreifache Ihrer erwarteten Arbeitslast erhöhen, um sicherzustellen, dass der Dateiserver die Schattenkopien mit der verfügbaren I/O-Leistungskapazität verwalten kann. Wenn Sie die [Datenduplizierung](#) aktivieren, sollten Sie die Speichermenge ermitteln, die der Durchsatzkapazität Ihres Dateisystems entspricht, und sicherstellen, dass diese Speichermenge für die Größe Ihrer Daten ausreichend ist.

Sie können die Größe der Durchsatzkapazität jederzeit nach der Erstellung erhöhen oder verringern. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

Sie können die Auslastung der Leistungsressourcen von Dateiservern durch Ihren Workload überwachen und Empfehlungen zur Auswahl der Durchsatzkapazität erhalten, indem Sie die Registerkarte Überwachung und Leistung > Leistung Ihrer Amazon FSx-Konsole aufrufen. Wir empfehlen, in einer Vorproduktionsumgebung zu testen, um sicherzustellen, dass die von Ihnen gewählte Konfiguration den Leistungsanforderungen Ihres Workloads entspricht. Bei Multi-AZ-Dateisystemen empfehlen wir außerdem, die Auswirkungen des Failover-Prozesses zu testen, der bei der Wartung des Dateisystems, bei Änderungen der Durchsatzkapazität und ungeplanten Betriebsunterbrechungen auf Ihre Arbeitslast stattfindet. Außerdem sollten Sie sicherstellen, dass Sie ausreichend Durchsatzkapazität bereitgestellt haben, um Leistungseinbußen bei diesen Ereignissen zu vermeiden. Weitere Informationen finden Sie unter [Zugreifen auf FSx for Windows File Server-Metriken](#).

## Auswirkung der Speicherkonfiguration auf die Leistung

Die Speicherkapazität, der Speichertyp und die SSD-IOPS-Stufe Ihres Dateisystems wirken sich alle auf die Festplatten-I/O-Leistung Ihres Dateisystems aus. Sie können diese Ressourcen so konfigurieren, dass sie die gewünschte Leistung für Ihre Arbeitslast bereitstellen.

Sie können die Speicherkapazität jederzeit erhöhen und SSD-IOPS skalieren. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#) und [Verwalten von SSD-IOPS](#). Sie können Ihr Dateisystem auch vom HDD-Speichertyp auf den SSD-Speichertyp aktualisieren. Weitere Informationen finden Sie unter [Speichertyp verwalten](#).

Ihr Dateisystem bietet die folgenden Standardstufen für Festplattendurchsatz und IOPS:

| Speichertyp | Festplattendurchsatz (MBps pro TiB Speicher)                            | Festplatten-IOPS (IOPS pro TiB Speicher) |
|-------------|-------------------------------------------------------------------------|------------------------------------------|
| SSD         | 750                                                                     | 3.000*                                   |
| HDD         | 12 Baseline; 80 Burst (bis zu einem Maximum von 1 GB/s pro Dateisystem) | 12 Basiswerte; 80 Burst                  |

### Note

\*Für Dateisysteme mit SSD-Speichertyp können Sie zusätzliche IOPS bis zu einem maximalen Verhältnis von 500 IOPS pro GiB Speicher und 400.000 IOPS pro Dateisystem bereitstellen.

## Burst-Leistung von Festplatten

Für HDD-Speichervolumen verwendet Amazon FSx aus Leistungsgründen ein Burst-Bucket-Modell. Die Volumegröße bestimmt den Basisdurchsatz Ihres Volumes; dabei handelt es sich um die Rate, mit der das Volume Durchsatzguthaben sammelt. Die Volumegröße bestimmt auch den Spitzendurchsatz Ihres Volumes; dabei handelt es sich um die Rate, mit der Sie verfügbares Guthaben verbrauchen können. Größere Volumes haben einen höheren Basis- und

Spitzendurchsatz. Je mehr Guthaben Ihr Volume aufweist, desto länger kann es einen I/O-Durchsatz mit der Spitzenrate generieren.

Der verfügbare Durchsatz eines HDD-Speichervolumens wird durch die folgende Formel ausgedrückt:

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

Bei einem 1-TiB-HDD-Volume ist der Burst-Durchsatz auf 80 MiB/s begrenzt, der Bucket füllt sich mit Credits bei 12 MiB/s und er kann Credits im Wert von bis zu 1 TiB aufnehmen.

## Beispiel: Speicherkapazität und Durchsatzkapazität

Das folgende Beispiel zeigt, wie sich Speicherkapazität und Durchsatzkapazität auf die Leistung des Dateisystems auswirken.

Ein Dateisystem, das mit 2 TiB Festplattenspeicherkapazität und 32 MBps Durchsatzkapazität konfiguriert ist, hat die folgenden Durchsatzstufen:

- Netzwerkdurchsatz — 32 MBps Baseline und 600 MBps Burst (siehe Tabelle mit der Durchsatzkapazität)
- Festplattendurchsatz — 24 MBps Baseline und 160 MBps Burst, was der niedrigere Wert ist von:
  - der vom Dateiserver unterstützte Festplattendurchsatz von 32 MB/s im Basiswert und 260 MB/s im Burst-Modus, basierend auf der Durchsatzkapazität des Dateisystems
  - die von den Speichervolumen unterstützten Festplattendurchsatzwerte von 24 MBps Baseline (12 MBps pro TB \* 2 TiB) und 160 MBps Burst (80 MBps pro TiB \* 2 TiB), je nach Speichertyp und Kapazität

Ihr Workload, der auf das Dateisystem zugreift, kann daher bis zu 32 MB/s Baseline- und 600 MB/s Burst-Durchsatz für Dateioperationen mit aktiv abgerufenen Daten, die im In-Memory-Cache des Dateiservers zwischengespeichert sind, und bis zu 24 MB/s Baseline- und 160 MBit/s Burst-Durchsatz für Dateioperationen, die beispielsweise aufgrund von Cache-Fehlern bis zur Festplatte übertragen werden müssen, steigern.

## Messung der Leistung anhand von Metriken CloudWatch

Sie können Amazon verwenden CloudWatch , um den Durchsatz und die IOPS Ihres Dateisystems zu messen und zu überwachen. Weitere Informationen finden Sie unter [Metriken mit Amazon überwachen CloudWatch](#).

## Behebung von Leistungsproblemen

Hilfe zur Behebung häufiger Leistungsprobleme finden Sie unter [Behebung von Leistungsproblemen mit dem Dateisystem](#).

# Amazon FSx Exemplarische Vorgehensweisen

Im Folgenden finden Sie eine Reihe von aufgabenorientierten Vorgehensweisen, die Sie durch verschiedene Prozesse führen.

## Themen

- [Exemplarische Vorgehensweise 1: Voraussetzungen für die ersten Schritte](#)
- [Exemplarische Vorgehensweise 2: Erstellen eines Dateisystems aus einer Sicherung](#)
- [Exemplarische Vorgehensweise 3: Aktualisieren Sie ein vorhandenes -Dateisystem](#)
- [Komplettlösung 4: Verwenden von Amazon FSx mit Amazon AppStream 2.0](#)
- [Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisystem](#)
- [Exemplarische Vorgehensweise 6: Skalierung der Leistung mit Shards](#)
- [Exemplarische Vorgehensweise 7: Kopieren einer Sicherung in ein anderes AWS-Region](#)

## Exemplarische Vorgehensweise 1: Voraussetzungen für die ersten Schritte

Bevor Sie die Übung „Erste Schritte“ abschließen können, müssen Sie bereits eine auf Microsoft Windows basierende Amazon EC2 EC2-Instanz mit Ihrer AWS Directory Service-Verzeichnis. Sie müssen auch über das Windows Remotedesktopprotokoll als Admin-Benutzer für Ihr Verzeichnis bei der Instanz angemeldet sein. Die folgende Anleitung zeigt Ihnen, wie Sie diese erforderlichen Voraussetzungen ausführen.

## Themen


- [Schritt 1: Einrichten von Active Directory](#)
- [Schritt 2: Starten Sie eine Windows-Instance in der Amazon EC2 EC2-Konsole](#)
- [Schritt 3: Herstellen einer Verbindung zu Ihrer Instance](#)
- [Schritt 4: Treten Sie Ihrer Instanz zu Ihrem AWS Directory Service Verzeichnis](#)

## Schritt 1: Einrichten von Active Directory

Mit Amazon FSx können Sie vollständig verwalteten Dateispeicher für Windows-basierte Workloads betreiben. Ebenso AWS Directory Service stellt vollständig verwaltete Verzeichnisse zur Verfügung,

die Sie in Ihrer Workload-Bereitstellung verwenden können. Wenn Sie eine vorhandene AD-Domäne für Unternehmen haben, können Sie die benutzerbasierte Authentifizierung und Zugriffskontrolle aktivieren. Sie tun dies, indem Sie eine Vertrauensstellung zwischen Ihrer Unternehmensdomäne und der AWS Managed Microsoft AD-Domäne aufbauen. Für die Windows-Authentifizierung in Amazon FSx benötigen Sie nur eine Einweg-Directional Forest Trust, bei der die AWS Managed Forest vertraut der Gesamtstruktur der Unternehmensdomäne.

Ihre Unternehmensdomäne übernimmt die Rolle der vertrauenswürdigen Domain, und die AWS Directory Service Managed Domain übernimmt die Rolle der vertrauensvollen Domäne. Validierte Authentifizierungsanfragen werden nur in einer Richtung zwischen den Domänen verlaufen, sodass sich Konten in Ihrer Unternehmensdomäne mit Ressourcen authentifizieren können, die in der verwalteten Domäne freigegeben werden. In diesem Fall interagiert Amazon FSx nur mit der verwalteten Domäne. Die verwaltete Domäne leitet dann die Authentifizierungsanfragen an Ihre Unternehmensdomäne weiter.


 Note

Sie können auch einen externen Vertrauenseinstellungstyp mit Amazon FSx für vertrauenswürdige Domains verwenden.

Ihre Active Directory-Sicherheitsgruppe muss den eingehenden Zugriff von der Sicherheitsgruppe des Amazon FSx-Dateisystems aus aktivieren.

So erstellen Sie einen AWS Verzeichnisdienst für Microsoft AD

- Wenn Sie noch kein AWS-Konto haben, verwenden Sie die AWS Directory Service, um eine verwaltete Microsoft AD-Domäne zu erstellen. Weitere Informationen finden Sie unter [Erstellen Sie Ihre AWS verwaltete Microsoft AD-Domäne](#) im AWS Directory Service Administratorhandbuch.

 Important

Denken Sie an das Passwort, das Sie Ihrem Admin-Benutzer zuweisen; Sie benötigen es später in dieser Übung mit den ersten Schritten. Wenn Sie das Passwort vergessen haben, müssen Sie die Schritte in dieser Übung mit dem neuen AWS Directory Service Verzeichnis und Admin-Benutzer.



- Wenn Sie ein vorhandenes AD haben, erstellen Sie eine Vertrauensstellung zwischen IhrenAWSManaged Microsoft AD und Ihr vorhandenes AD. Weitere Informationen finden Sie unter [Zeitpunkt zum Erstellen einer Vertrauensstellung](#) im AWS Directory Service-Administrationshandbuch.

## Schritt 2: Starten Sie eine Windows-Instance in der Amazon EC2 EC2-Konsole


Sie können eine Windows-Instance mit derAWS Management Consolewie im folgenden Verfahren beschrieben. Dies soll Ihnen helfen, Ihre erste Instance schnell zu starten, sodass nicht alle möglichen Optionen abgedeckt werden. Weitere Informationen zu den erweiterten Optionen erhalten Sie unter [Starten einer Instance](#).

So starten Sie eine Instance

1. Öffnen Sie die Amazon EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im Konsolen-Dashboard die Option Launch Instance.
3. Auf der Seite Choose an Amazon Machine Image (AMI) (Amazon Machine Image (AMI) wählen) wird eine Liste mit Basiskonfigurationen angezeigt, die als Amazon Machine Images (AMIs) bezeichnet werden und als Vorlagen für Ihre Instance dienen. Wählen Sie das AMI für Windows Server 2016 Base oder Windows Server 2012 R2 Base aus. (Diese AMIs sind als „Zur kostenlosen Nutzung berechtigt“ gekennzeichnet.)
4. Auf der Seite Choose an Instance Type können Sie die Hardware-Konfiguration Ihrer Instance auswählen. Wählen Sie den Typ `t2.micro` aus (Standardeinstellung). Beachten Sie, dass dieser Instance-Typ über die Berechtigung für das kostenlose Kontingent verfügt.
5. Wählen Sie Review and Launch, damit der Assistent die anderen Konfigurationseinstellungen für Sie vornehmen kann.
6. Auf derÜberprüfen des Instance-Startsseite, unterSicherheitsgruppenerscheint eine Sicherheitsgruppe, die der Assistent für Sie erstellt und ausgewählt hat. Sie können diese Sicherheitsgruppe verwenden oder die Sicherheitsgruppe auswählen, die Sie während der Einrichtung erstellt haben. Führen Sie hierzu die folgenden Schritte aus:
  - a. Wählen Sie Edit security groups.
  - b. Stellen Sie auf der Seite Configure Security Group (Sicherheitsgruppe konfigurieren) sicher, dass Select an existing security group aktiviert ist.

- c. Wählen Sie Ihre Sicherheitsgruppe in der Liste mit den vorhandenen Sicherheitsgruppen aus und wählen Sie anschließend Review and Launch.
7. Klicken Sie auf der Seite Review Instance Launch auf Launch.
8. Gehen Sie wie folgt vor, wenn Sie zum Eingeben eines Schlüsselpaars aufgefordert werden: Wählen Sie die Option Choose an existing key pair und dann das Schlüsselpaar aus, das Sie während der Einrichtung erstellt haben.

Alternativ hierzu können Sie auch ein neues Schlüsselpaar erstellen. Wählen Sie Create a new key pair. Geben Sie einen Namen für das Schlüsselpaar ein und klicken Sie dann auf Download Key Pair. Dies ist die einzige Möglichkeit, die Datei mit dem privaten Schlüssel zu speichern. Achten Sie also darauf, diese Datei herunterzuladen. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort. Sie müssen den Namen für Ihr Schlüsselpaar beim Starten einer Instance angeben. Der entsprechende private Schlüssel muss jedes Mal angegeben werden, wenn Sie eine Verbindung mit der Instance herstellen.

 Warning

Wählen Sie nicht die Option Proceed without a key pair aus. Wenn Sie Ihre Instance ohne Schlüsselpaar starten, können Sie keine Verbindung zu ihr herstellen.

Wenn Sie bereit sind, aktivieren Sie das Bestätigungs-Kontrollkästchen und klicken Sie dann auf Launch Instances.

9. Auf einer Bestätigungsseite wird Ihnen mitgeteilt, dass die Instance gestartet wird. Wählen Sie View Instances aus, um die Bestätigungsseite zu schließen und zur Konsole zurückzukehren.
10. Auf dem Bildschirm Instances können Sie den Status des Starts anzeigen. Es dauert einige Zeit, bis die Instance startet. Wenn Sie eine Instance starten, lautet ihr anfänglicher Status `pending`. Nachdem die Instance gestartet wurde, ändert sich der Status in `running`. Sie erhält dann einen öffentlichen DNS-Namen. (Wenn die Spalte Public DNS (IPv4) ausgeblendet ist, können Sie oben rechts auf der Seite Show/Hide Columns (das Zahnradchensymbol) und dann die Option Public DNS (IPv4) wählen.)
11. Es kann einige Minuten dauern, bis die Instance für die Verbindungsherstellung bereit ist. Prüfen Sie, ob die Instance die Statusprüfungen bestanden hat. Sie finden diese Information in der Spalte Status Checks.

**⚠ Important**

Notieren Sie sich die ID der Sicherheitsgruppe, die beim Start dieser Instance erstellt wurde. Sie benötigen es, wenn Sie Ihr Amazon FSx-Dateisystem erstellen.

Nachdem Ihre Instance gestartet wurde, können Sie eine Verbindung zu Ihrer Instance herstellen.

## Schritt 3: Herstellen einer Verbindung zu Ihrer Instance

Zur Verbindung mit einer Windows-Instance müssen Sie das anfängliche Administratorpasswort abrufen und es angeben, wenn Sie per Remote Desktop eine Verbindung mit Ihrer Instance herstellen.

Der Name des Administratorkontos hängt von der Sprache des Betriebssystems ab. Für Englisch lautet es „Administrator“, für Französisch „Administrateur“ und für Portugiesisch „Administrador“. Weitere Informationen finden Sie unter [Localized Names for Administrator Account in Windows](#) (Lokalisierte Namen für Administratorkonto in Windows) im Microsoft TechNet Wiki.


Wenn Sie Ihre Instance einer Domäne zugewiesen haben, können Sie eine Verbindung mit Ihrer Instance mithilfe von Domänen-Anmeldeinformationen herstellen, die Sie unter definiert habenAWS Directory Serviceaus. Verwenden Sie auf dem Anmeldebildschirm des Remotedesktops nicht den Namen des lokalen Computers und das generierte Kennwort. Verwenden Sie stattdessen den vollqualifizierten Benutzernamen für den Administrator und das Passwort für dieses Konto. Ein Beispiel ist **corp.example.com\Admin**.

Die Lizenz für das Windows Server-Betriebssystem (OS) ermöglicht zwei gleichzeitige Remote-Verbindungen für administrative Zwecke. Die Lizenzkosten für Windows Server sind in den Kosten für Ihre Windows-Instance enthalten. Falls Sie mehr als zwei gleichzeitige Remote-Verbindungen benötigen, ist der Erwerb einer Remote Desktop Services-Lizenz (RDS) erforderlich. Wenn Sie versuchen, eine dritte Verbindung aufzubauen, erhalten Sie eine Fehlermeldung. Weitere Informationen finden Sie unter [Konfigurieren Sie die Anzahl der gleichzeitigen Remoteverbindungen, die für eine Verbindung zulässig sind](#)aus.

Verwenden Sie einen RDP Client, um sich mit Ihrer Windows-Instance zu verbinden.

1. Wählen Sie in der Amazon EC2-Konsole die Instance und anschließend Connect (Verbinden) aus.

2. In der Herstellen einer Verbindung mit Ihrer Instance wählen Sie im Dialogfeld Passwort erhalten (Nach dem Start der Instance dauert es einige Minuten, bis das Passwort verfügbar ist).
3. Klicken Sie auf Browse (Durchsuchen) und navigieren Sie zu der privaten Schlüsseldatei, die Sie beim Starten der Instance erstellt haben. Wählen Sie die Datei aus und klicken Sie auf Open, um den gesamten Inhalt der Datei in das Inhaltsfeld zu kopieren.
4. Klicken Sie auf Decrypt Password. Die Konsole zeigt das Standard-Administrator-Passwort für die Instance im Herstellen einer Verbindung mit Ihrer Instance, ersetzen Sie den Link zu Passwort erhalten zuvor mit dem eigentlichen Passwort angezeigt.
5. Notieren Sie sich das Standard-Administratorpasswort oder kopieren Sie es in die Zwischenablage. Sie benötigen dieses Passwort, um eine Verbindung mit der Instance herzustellen.
6. Klicken Sie auf Download Remote Desktop File. Sie werden vom Browser aufgefordert, die RDP-Datei zu öffnen oder zu speichern. Sie können eine der beiden Optionen auswählen. Wenn Sie fertig sind, können Sie wählen Schließen um den Herstellen einer Verbindung mit Ihrer Instance-Dialogfeld.
  - Wenn Sie die RDP-Datei geöffnet haben, wird das Dialogfeld Remotedesktopverbindung angezeigt.
  - Wenn Sie die RDP-Datei gespeichert haben, navigieren Sie zum Download-Verzeichnis und klicken Sie auf die RDP-Datei, um das Dialogfeld zu öffnen.
7. Möglicherweise wird eine Warnmeldung angezeigt, dass der Herausgeber der Remoteverbindung unbekannt ist. Als Nächstes können Sie eine Verbindung mit Ihrer Instance herstellen.
8. Melden Sie sich bei Aufforderung mit dem Administratorkonto für das Betriebssystem und dem zuvor gespeicherten oder kopierten Passwort bei der Instance an. Wenn Ihre Remotedesktop-Verbindung bereits ein Administratorkonto eingerichtet hat, müssen Sie möglicherweise die Option Use another account (Ein anderes Konto verwenden) wählen und den Benutzernamen und das Passwort manuell eingeben.

 Note

In manchen Fällen können Inhalte durch Kopieren und Einfügen fehlerhaft werden. Sollten Sie beim Anmelden die Fehlermeldung „Password Failed“ (Passwort fehlerhaft) erhalten, versuchen Sie, das Passwort manuell einzugeben.

9. Aufgrund der Art selbst signierter Zertifikate erhalten Sie möglicherweise eine Warnmeldung, dass das Sicherheitszertifikat nicht authentifiziert werden konnte. Verifizieren Sie die Identität des Remote-Computers mithilfe der folgenden Schritte. Falls Sie dem Zertifikat vertrauen, können Sie auch direkt auf Yes oder Continue klicken.
  - a. Wenn Sie die Remote-Desktop-Verbindung von einem Windows-Computer gestartet haben, klicken Sie auf View certificate. Wenn Sie Microsoft Remote Desktop auf einem Mac verwenden, klicken Sie auf Show Certificate.
  - b. Öffnen Sie den Tab Details und scrollen Sie nach unten bis zu Thumbprint bei Windows-Computern oder bis zu SHA1 Fingerprints bei Mac. Dies ist die eindeutige Kennung für das Sicherheitszertifikat des Remote-Computers.
  - c. Wählen Sie in der Amazon EC2-Konsole die Instance, dann Actions (Aktionen) und anschließend Get System Log (Systemprotokoll abrufen).
  - d. Suchen Sie im Systemprotokoll nach einem Eintrag mit der Bezeichnung RDPCERTIFICATE-THUMBPRINT. Wenn der Wert dem Thumbprint oder Fingerprint des Sicherheitszertifikats entspricht, haben Sie die Identität des Remote-Computers erfolgreich verifiziert.
  - e. Wenn Sie die Remote-Desktop-Verbindung von einem Windows-Computer gestartet haben, kehren Sie zurück zum Dialogfeld Certificate und klicken Sie auf OK. Wenn Sie Microsoft Remote Desktop auf einem Mac verwenden, navigieren Sie zurück zum Dialogfeld Verify Certificate und klicken Sie auf Continue.
  - f. [Windows] Wählen Sie Yes im Fenster Remote Desktop Connection, um sich mit Ihrer Instance zu verbinden.

Nachdem Sie jetzt mit Ihrer Instance verbunden sind, können Sie die Instance IhrerAWS Directory Service-Verzeichnis.

## Schritt 4: Treten Sie Ihrer Instanz zu IhremAWS Directory ServiceVerzeichnis

Im Folgenden erfahren Sie, wie Sie eine vorhandene Amazon EC2 Windows-Instance manuell mit IhrerAWS Directory Service-Verzeichnis.

So schließen Sie eine Windows-Instance mit IhrerAWS Directory ServiceVerzeichnis

1. Verbinden Sie die Instance mithilfe eines beliebigen Remote Desktop Protocol-Clients.


2. Öffnen Sie in der Instance das Dialogfeld mit den Eigenschaften für TCP/IPv4.
  - a. Öffnen Sie Network Connections.

 Tip

Öffnen Sie Network Connections direkt, indem Sie folgenden Befehl über die Befehlszeile der Instance ausführen.

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

- b. Öffnen Sie für eine beliebige aktivierte Netzwerkverbindung per Rechtsklick das Kontextmenü und klicken Sie dann aufEigenschaftenaus.
  - c. Öffnen Sie im Dialogfeld für die Verbindungseigenschaften (per Doppelklick) Internet Protocol Version 4.
3. (Optional) Wählen Sie ausVerwenden Sie die folgenden DNS-Serveradressenändern Sie dieBevorzugter DNS-ServerundAlternativer DNS-Serveradressen an die IP-Adressen desAWS Directory Service—bereitgestellte DNS-Server, und wählen SieOKAYaus.
4. Öffnen SieSystemeigenschaftenWählen Sie für die Instance die OptionName des ComputersTab, und wählen SieÄnderungaus.

 Tip

Öffnen Sie das Dialogfeld System Properties direkt, indem Sie folgenden Befehl über die Befehlszeile der Instance ausführen.

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

5. In derMitglied derWählen Sie danach aus-Domäne, geben Sie den vollständig qualifizierten Namen IhrerAWS Directory Service-Verzeichnis und wählen Sie danach ausOKAYaus.
6. Wenn Sie zur Eingabe des Namens und des Passworts für den Domänenadministrator aufgefordert werden, geben Sie den Benutzernamen und das Passwort des Admin-Kontos ein.

**Note**

Sie können entweder den vollqualifizierten Namen Ihrer Domain oder NetBios Name gefolgt von einem umgekehrten Schrägstrich (\) und dann dem Benutzernamen, in diesem Fall Admin aus. Beispielsweise corp.example.com\Admin oder corp\Admin.

7. Nachdem Sie in der Domäne willkommen geheißen wurden, starten Sie die Instance neu, damit die Änderungen übernommen werden.
8. Verbinden Sie sich über RDP erneut mit Ihrer Instance und melden Sie sich mithilfe des Benutzernamens und des Passworts für Ihre Instance an AWS Directory Service Admin-Benutzer des Verzeichnisses

Nachdem Ihre Instance der Domäne zugeordnet wurde, können Sie Ihr Amazon FSx-Dateisystem erstellen. Sie können dann die anderen Aufgaben in der Übung „Erste Schritte“ abschließen. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon FSx for Windows File Server](#).

## Exemplarische Vorgehensweise 2: Erstellen eines Dateisystems aus einer Sicherung


Mit Amazon FSx können Sie ein Dateisystem aus einer Sicherung erstellen. Wenn Sie dies tun, können Sie eines der folgenden Elemente so ändern, dass es besser zu dem Anwendungsfall passt, den Sie für Ihr neu erstelltes Dateisystem haben:

- Speichertyp
- Durchsatzkapazität
- VPC
- Availability Zone
- Subnetz
- VPC-Sicherheitsgruppen
- Active Directory-Konfiguration
- AWS KMS-Verschlüsselungsschlüssel
- Tägliche Startzeit der automatischen Sicherung
- Wöchentliches Wartungsfenster

Das folgende Verfahren führt Sie durch das Erstellen eines neuen Dateisystems aus einer Sicherung. Bevor Sie dieses Dateisystem erstellen können, müssen Sie über eine vorhandene Sicherung verfügen. Weitere Informationen finden Sie unter [Arbeiten mit Backups](#)

So erstellen Sie ein Dateisystem aus einer vorhandenen Sicherung

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/> aus.
2. Wählen Sie aus der Navigationsliste rechts-Sicherungen aus.
3. Wählen Sie aus der Tabelle im Dashboard die Sicherung aus, die Sie zum Erstellen eines neuen Dateisystems verwenden möchten.

 Note

Sie können Ihre Sicherung nur in einem Dateisystem mit der gleichen Speicherkapazität wie das Original wiederherstellen. Sie können die Speicherkapazität Ihres wiederhergestellten Dateisystems erhöhen, nachdem es verfügbar ist. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#).

4. Wählen Sie Restore backup aus. Dies beginnt mit dem Assistenten zum Erstellen von Dateisystemen.
5. Wählen Sie die Einstellungen aus, die Sie für dieses neue Dateisystem ändern möchten. Der Speichertyp ist auf SSD Standardmäßig, aber Sie können es ändern zu HDD unter den folgenden Bedingungen:
  - Der Bereitstellungstyp des Dateisystems lautet Multi-AZ oder Single-AZ 2 aus.
  - Die Speicherkapazität beträgt mindestens 2.000 GiB.
6. Klicken Sie auf Review-Übersicht um Ihre Einstellungen vor dem Erstellen des Dateisystems zu überprüfen.
7. Wählen Sie Create file system (Dateisystem erstellen) aus.

Sie haben Ihr neues Dateisystem nun erfolgreich aus einer vorhandenen Sicherung erstellt.



## Exemplarische Vorgehensweise 3: Aktualisieren Sie ein vorhandenes -Dateisystem

Es gibt drei Elemente, die Sie mit den Prozeduren in dieser exemplarischen Vorgehensweise aktualisieren können. Alle anderen Elemente Ihres -Dateisystems, die Sie aktualisieren können, können Sie dies von der Konsole aus tun. Diese Verfahren gehen davon aus, dass Sie die AWS CLI auf Ihrem lokalen Computer installiert und konfiguriert. Weitere Informationen finden Sie unter [Install](#) und [Konfiguration](#) im AWS Command Line Interface-Benutzerhandbuch.

- `AutomaticBackupRetentionDays`— Die Anzahl der Tage, für die automatische Sicherungen für Ihr -Dateisystem aufbewahrt werden sollen.
- `DailyAutomaticBackupStartTime`— Die Tageszeit in koordinierter Weltzeit (UTC), zu der das tägliche automatische Sicherungsfenster gestartet werden soll. Das Fenster ist 30 Minuten ab dieser angegebenen Zeit. Dieses Fenster kann sich nicht mit dem wöchentlichen Wartungs-Backup-Fenster überschneiden.
- `WeeklyMaintenanceStartTime`— die Uhrzeit der Woche, in der das Wartungsfenster beginnen soll. Tag 1 ist Montag, 2 ist Dienstag und so weiter. Das Fenster ist 30 Minuten ab dieser angegebenen Zeit. Dieses Fenster kann sich nicht mit dem täglichen automatischen Backup-Fenster überschneiden.

Im folgenden Verfahren wird beschrieben, wie Sie Ihr -Dateisystem mit dem AWS CLI aus.

So aktualisieren Sie, wie lange automatische Backups für Ihr Dateisystem beibehalten werden

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal auf Ihrem Computer.
2. Führen Sie den folgenden Befehl aus und ersetzen Sie die Dateisystem-ID durch die ID für Ihr Dateisystem und die Anzahl der Tage, für die Sie Ihre automatischen Backups beibehalten möchten.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-configuration AutomaticBackupRetentionDays=30
```

So aktualisieren Sie das tägliche Backup-Fenster Ihres Dateisystems

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal auf Ihrem Computer.

2. Führen Sie den folgenden Befehl aus und ersetzen Sie die Dateisystem-ID durch die ID für Ihr Dateisystem und die Uhrzeit, mit der Sie das Fenster beginnen möchten.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-configuration DailyAutomaticBackupStartTime=01:00
```

So aktualisieren Sie das wöchentliche Wartungsfenster Ihres Dateisystems

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal auf Ihrem Computer.
2. Führen Sie den folgenden Befehl aus und ersetzen Sie die Dateisystem-ID durch die ID für Ihr Dateisystem sowie Datum und Uhrzeit mit dem Zeitpunkt, an dem Sie das Fenster beginnen möchten.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-configuration WeeklyMaintenanceStartTime=1:01:30
```

## Komplettlösung 4: Verwenden von Amazon FSx mit Amazon AppStream 2.0

Durch die Unterstützung des Server Message Block (SMB) -Protokolls unterstützt Amazon FSx for Windows File Server den Zugriff auf Ihr Dateisystem von Amazon EC2-, VMware Cloud on-AWS WorkSpaces, Amazon- und Amazon AppStream 2.0-Instances aus. AppStream 2.0 ist ein vollständig verwalteter Anwendungsstreaming-Dienst. Sie verwalten Ihre Desktop-Anwendungen auf AppStream 2.0 zentral und stellen sie sicher an einen Browser auf einem beliebigen Computer bereit. Weitere Informationen zu AppStream 2.0 finden Sie im [Amazon AppStream 2.0-Administrationshandbuch](#). Eine Anleitung, wie Sie die Verwaltung Ihrer Amazon AppStream 2.0-Images und -Flotten optimieren können, finden Sie im AWS Blogbeitrag [Automatisches Erstellen benutzerdefinierter AppStream 2.0-Windows-Images](#).

Verwenden Sie diese Komplettlösung als Anleitung zur Verwendung von Amazon FSx mit AppStream 2.0 für zwei Anwendungsfälle: Bereitstellung von persönlichem persistentem Speicher für jeden Benutzer und Bereitstellung eines gemeinsam genutzten Ordners für den Zugriff auf gemeinsame Dateien.

## Bereitstellung von persönlichem persistentem Speicher für jeden Benutzer

Sie können Amazon FSx verwenden, um jedem Benutzer in Ihrer Organisation innerhalb von AppStream 2.0-Streaming-Sitzungen ein eigenes Speicherlaufwerk zur Verfügung zu stellen. Ein Benutzer hat nur die Berechtigung, auf seinen Ordner zuzugreifen. Das Laufwerk wird zu Beginn einer Streaming-Sitzung automatisch gemountet, und Dateien, die dem Laufwerk hinzugefügt oder aktualisiert wurden, werden zwischen den Streaming-Sitzungen automatisch gespeichert.

Es gibt drei Verfahren, die Sie ausführen müssen, um diese Aufgabe abzuschließen.

So erstellen Sie Basisordner für Domain-Benutzer mit Amazon FSx

1. Erstellen eines Amazon-FSx-Dateisystems. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon FSx for Windows File Server](#).
2. Nachdem das Dateisystem verfügbar ist, erstellen Sie einen Ordner für jeden Domain AppStream 2.0-Benutzer in Ihrem Amazon FSx-Dateisystem. Im folgenden Beispiel wird der Domänenbenutzername des Benutzers als Name des entsprechenden Ordners verwendet. Auf diese Weise können Sie den UNC-Namen der Dateifreigabe mithilfe der Windows-Umgebungsvariablen einfach zur Zuordnung erstellen `%username%`.
3. Geben Sie jeden dieser Ordner als geteilten Ordner frei. Weitere Informationen finden Sie unter [Verwaltung von Dateifreigaben auf FSx for Windows File Server Server-Dateisystemen](#).

Um einen mit einer Domain verknüpften AppStream 2.0-Image-Builder zu starten

1. Melden Sie sich bei der AppStream 2.0-Konsole an: <https://console.aws.amazon.com/appstream2>
2. Wählen Sie Directory Configs aus dem Navigationsmenü und erstellen Sie ein Directory-Config-Objekt. Weitere Informationen finden Sie unter [Verwenden von Active Directory mit AppStream 2.0](#) im Amazon AppStream 2.0-Administratorhandbuch.
3. Wählen Sie Images, Image Builder und starten Sie einen neuen Image Builder.
4. Wählen Sie das Verzeichniskonfigurationsobjekt aus, das zuvor im Image Builder mit Ihrer Active Directory-Domäne verbunden wird.
5. Starten Sie ein Image Builder in derselben VPC Ihres Amazon-FSx-Dateisystems. Stellen Sie sicher, dass Sie den Image Builder demselben AWS Managed Microsoft AD Verzeichnis zuordnen, mit dem Ihr Amazon FSx-Dateisystem verknüpft ist. Die VPC-Sicherheitsgruppen, die Sie dem Image Builder zuordnen, müssen den Zugriff auf Ihr Amazon FSx-Dateisystem ermöglichen.

6. Sobald der Image Builder verfügbar ist, stellen Sie eine Verbindung zum Image Builder her und melden Sie sich mit Ihrem Domain-Administratorkonto an.
7. Installieren Sie Ihre Anwendungen.

So verknüpfen Sie Amazon FSx-Dateifreigaben mit AppStream 2.0

1. Erstellen Sie im Image Builder ein Batch-Skript mit dem folgenden Befehl und speichern Sie es an einem bekannten Speicherort (z. B.: C:\Scripts\map -fs.bat). Im folgenden Beispiel wird S: als Laufwerksbuchstabe verwendet, um den geteilten Ordner in Ihrem Amazon FSx-Dateisystem zuzuordnen. In diesem Skript verwenden Sie den DNS-Namen Ihres Amazon FSx-Dateisystems oder einen mit dem Dateisystem verknüpften DNS-Alias, den Sie in der Ansicht mit den Dateisystemdetails in der Amazon FSx-Konsole abrufen können.

Wenn Sie den DNS-Namen des Dateisystems verwenden:

```
@echo off
net use S: /delete
net use S: \\file-system-DNS-name\users\%username%
```

Wenn Sie einen DNS-Alias verwenden, der dem Dateisystem zugeordnet ist:

```
@echo off
net use S: /delete
net use S: \\fqdn-DNS-alias\users\%username%
```

2. Öffnen Sie eine PowerShell Eingabeaufforderung und starten Sie `Siegpedit.msc`.
3. Wählen Sie unter Benutzerkonfiguration die Option Windows-Einstellungen und dann Anmelden aus.
4. Navigieren Sie zu dem Batch-Skript, das Sie im ersten Schritt dieses Verfahrens erstellt haben, und wählen Sie es aus.
5. Wählen Sie unter Computerkonfiguration die Option Administrative Windows-Vorlagen, System und dann Gruppenrichtlinie aus.
6. Wählen Sie die Richtlinie Configure Logon Script delay. Aktivieren Sie die Richtlinie und reduzieren Sie die Zeitverzögerung auf 0. Mit dieser Einstellung wird sichergestellt, dass das Benutzeranmeldeskript sofort ausgeführt wird, wenn der Benutzer eine Streaming-Sitzung startet.

7. Erstellen Sie Ihr Image und weisen Sie es einer AppStream 2.0-Flotte zu. Stellen Sie sicher, dass Sie die AppStream 2.0-Flotte auch derselben Active Directory-Domäne hinzufügen, die Sie für Image Builder verwendet haben. Starten Sie die Flotte in derselben VPC, die von Amazon FSx-Dateisystems verwendet. Die VPC-Sicherheitsgruppen, die Sie der Flotte zuordnen, müssen Zugriff auf Ihr Amazon FSx-Dateisystem gewähren.
8. Starten Sie eine Streaming-Sitzung mit SAML SSO. Um eine Verbindung zu einer Flotte herzustellen, die mit Active Directory verbunden ist, konfigurieren Sie den Single Sign-On-Verbund mithilfe eines SAML-Anbieters. Weitere Informationen finden Sie unter [Single Sign-On Access to AppStream 2.0 Using SAML 2.0](#) im Amazon AppStream 2.0-Administratorhandbuch.
9. Ihre Amazon FSx-Dateifreigabe ist innerhalb der Streaming-Sitzung dem Laufwerksbuchstaben S: zugeordnet.

## Bereitstellung eines gemeinsam genutzten Ordners für alle Benutzer

Sie können Amazon FSx verwenden, um Benutzern in Ihrer Organisation einen gemeinsamen Ordner bereitzustellen. Ein geteilter Ordner kann verwendet werden, um gemeinsame Dateien (z. B. Demodateien, Codebeispiele, Anleitungen usw.) zu verwalten, die von allen Benutzern benötigt werden.

Es gibt drei Verfahren, die Sie ausführen müssen, um diese Aufgabe abzuschließen.

So erstellen Sie einen geteilten Ordner mit Amazon FSx

1. Erstellen eines Amazon-FSx-Dateisystems. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon FSx for Windows File Server](#).
2. Jedes Amazon FSx-Dateisystem enthält standardmäßig einen gemeinsamen Ordner, auf den Sie über die Adresse `\\ File-system-DNS-Name \ share` oder `\\ FQDN-DNS-Alias \ share` zugreifen können, wenn Sie DNS-Aliase verwenden. Sie können die Standardfreigabe verwenden oder einen anderen geteilten Ordner erstellen. Weitere Informationen finden Sie unter [Verwaltung von Dateifreigaben auf FSx for Windows File Server Server-Dateisystemen](#).

Um einen AppStream 2.0-Image-Builder zu starten

1. Starten Sie von der AppStream 2.0-Konsole aus einen neuen Image Builder oder stellen Sie eine Verbindung zu einem vorhandenen Image Builder her. Starten Sie den Image Builder in derselben VPC, die von Ihrem Amazon FSx-Dateisystem verwendet wird. Die VPC-

Sicherheitsgruppen, die Sie dem Image Builder zuordnen, müssen den Zugriff auf Ihr Amazon FSx-Dateisystem ermöglichen.

2. Sobald der Image Builder verfügbar ist, stellen Sie als Administratorbenutzer eine Verbindung zum Image Builder her.
3. Installieren oder aktualisieren Sie Ihre Anwendungen als Administrator.

Um den geteilten Ordner mit AppStream 2.0 zu verknüpfen

1. Erstellen Sie ein Batch-Skript, wie im vorherigen Verfahren beschrieben, um den geteilten Ordner automatisch zu mounten, wenn ein Benutzer eine Streaming-Sitzung startet. Um das Skript abzuschließen, benötigen Sie den DNS-Namen des Dateisystems oder einen DNS-Alias, der mit dem Dateisystem verknüpft ist (den Sie in der Ansicht mit den Dateisystemdetails in der Amazon FSx Console abrufen können), sowie Anmeldeinformationen für den Zugriff auf den geteilten Ordner.

Wenn Sie den DNS-Namen des Dateisystems verwenden:

```
@echo off
net use S: /delete
net use S: \\file-system-DNS-name\share /user:username password
```

Wenn Sie einen DNS-Alias verwenden, der dem Dateisystem zugeordnet ist:

```
@echo off
net use S: /delete
net use S: \\fqdn-DNS-alias\share /user:username password
```

2. Erstellen Sie eine Gruppenrichtlinie, um dieses Batchskript bei jeder Benutzeranmeldung auszuführen. Sie können den gleichen Anweisungen folgen, wie im vorherigen Abschnitt beschrieben.
3. Erstellen Sie Ihr Image und weisen Sie es Ihrer Flotte zu.
4. Starten Sie eine Streaming-Sitzung. Sie sollten nun sehen, dass der geteilte Ordner automatisch dem Laufwerksbuchstaben zugeordnet wird.

# Exemplarische Vorgehensweise 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisystem

FSx for Windows File Server bietet einen Standard-DNS-Namen (Domain Name System) für jedes Dateisystem, das Sie für den Zugriff auf die Daten in Ihrem Dateisystem verwenden können. Sie können auch mit einem DNS-Alias Ihrer Wahl auf Ihre Dateisysteme zugreifen. Mit DNS-Aliasen können Sie bei der Migration von Dateisystemspeichern von lokal zu Amazon FSx vorhandene DNS-Namen weiterhin verwenden, um auf Daten zuzugreifen, die auf Amazon FSx gespeichert sind, ohne Tools oder Anwendungen aktualisieren zu müssen. Sie können einem Dateisystem bis zu 50 DNS-Aliase gleichzeitig zuordnen.

Um über DNS-Aliase auf Ihre Amazon FSx-Dateisysteme zuzugreifen, müssen Sie die folgenden drei Schritte ausführen:

1. Verknüpfen Sie DNS-Aliase mit Ihrem Amazon FSx-Dateisystem.
2. Konfigurieren Sie Service Principal Names (SPNs) für das Computerobjekt Ihres Dateisystems. (Dies ist erforderlich, um die Kerberos-Authentifizierung zu erhalten, wenn Sie über DNS-Aliase auf Ihr Dateisystem zugreifen.)
3. Aktualisieren oder erstellen Sie einen DNS-CNAME-Eintrag für das Dateisystem und den DNS-Alias.

## Themen

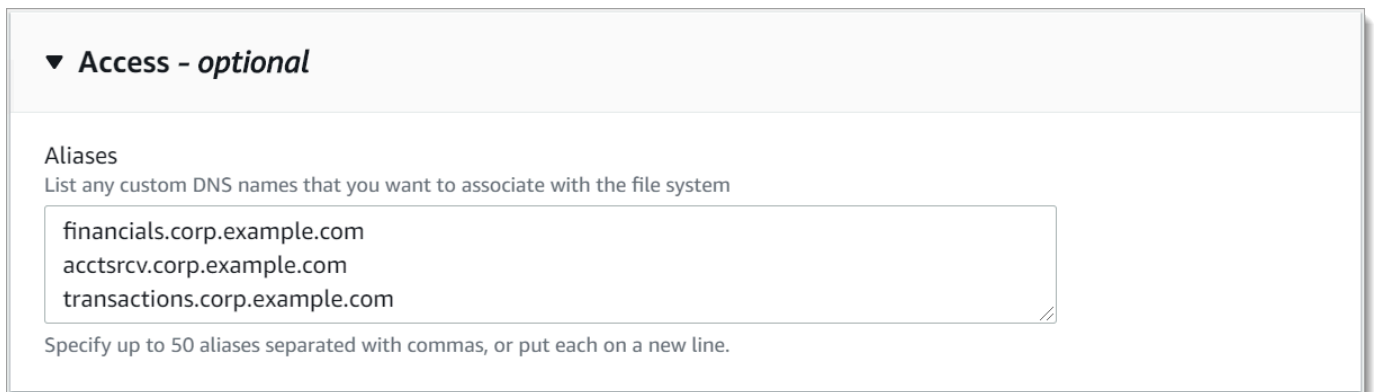
- [Schritt 1: Verknüpfen Sie DNS-Aliase mit Ihrem Amazon FSx-Dateisystem](#)
- [Schritt 2: Konfigurieren Sie Service Principal Names \(SPNs\) für Kerberos](#)
- [Schritt 3: Aktualisieren oder erstellen Sie einen DNS-CNAME-Eintrag für das Dateisystem](#)
- [Erzwingen der Kerberos-Authentifizierung mithilfe von GPOs](#)

## Schritt 1: Verknüpfen Sie DNS-Aliase mit Ihrem Amazon FSx-Dateisystem

Sie können DNS-Aliase vorhandenen FSx for Windows File Server Server-Dateisystemen zuordnen, wenn Sie neue Dateisysteme erstellen und wenn Sie mithilfe der Amazon FSx-Konsole, CLI und API ein neues Dateisystem aus einem Backup erstellen. Wenn Sie einen Alias mit einem anderen Domainnamen erstellen, geben Sie den vollständigen Namen einschließlich der übergeordneten Domain ein, um einen Alias zuzuordnen.

Dieses Verfahren beschreibt, wie DNS-Aliase beim Erstellen eines neuen Dateisystems mit der Amazon FSx-Konsole verknüpft werden. Informationen zum Zuordnen von DNS-Aliasen zu vorhandenen Dateisystemen und Einzelheiten zur Verwendung von CLI und API finden Sie unter [DNS-Aliase verwalten](#)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, wie im [Erstellen Sie Ihr Dateisystem](#) Abschnitt Erste Schritte beschrieben.
3. Geben Sie im Abschnitt Zugriff — optional des Assistenten zum Erstellen von Dateisystemen die DNS-Aliase ein, die Sie Ihrem Dateisystem zuordnen möchten.



▼ **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.

Beachten Sie bei der Angabe von DNS-Aliasen die folgenden Richtlinien:

- Muss als vollqualifizierter Domänenname (FQDN) formatiert sein *hostname.domain*, z. B. `accounting.example.com`
- Kann alphanumerische Zeichen und Bindestriche (-) enthalten.
- Am Anfang und am Ende darf kein Bindestrich stehen.
- Kann mit einem numerischen Wert beginnen.

Bei DNS-Aliasnamen speichert Amazon FSx alphabetische Zeichen als Kleinbuchstaben (a-z), unabhängig davon, wie Sie sie angeben: als Großbuchstaben, Kleinbuchstaben oder entsprechende Buchstaben in Escape-Zeichen.

4. Nehmen Sie an den Wartungseinstellungen die gewünschten Änderungen vor.
5. Fügen Sie im Abschnitt Tags — optional alle benötigten Tags hinzu und wählen Sie dann Weiter.
6. Prüfen Sie die Dateisystemkonfiguration, die auf der Seite Create File System (Dateisystem erstellen) angezeigt wird. Wählen Sie Dateisystem erstellen, um das Dateisystem zu erstellen.



Wenn Ihr neues Dateisystem verfügbar ist, fahren Sie mit Schritt 2 fort.

## Schritt 2: Konfigurieren Sie Service Principal Names (SPNs) für Kerberos

Wir empfehlen Ihnen, bei der Übertragung mit Amazon FSx die Kerberos-basierte Authentifizierung und Verschlüsselung zu verwenden. Kerberos bietet die sicherste Authentifizierung für Clients, die auf Ihr Dateisystem zugreifen.

Um die Kerberos-Authentifizierung für Clients zu aktivieren, die über einen DNS-Alias auf Amazon FSx zugreifen, müssen Sie Service Principal Names (SPNs) hinzufügen, die dem DNS-Alias auf dem Active Directory-Computerobjekt Ihres Amazon FSx-Dateisystems entsprechen. Ein SPN kann jeweils nur einem einzigen Active Directory-Computerobjekt zugeordnet werden. Wenn Sie bereits SPNs für den DNS-Namen haben, der für das Active Directory-Computerobjekt Ihres ursprünglichen Dateisystems konfiguriert ist, müssen Sie diese zuerst löschen.

Für die Kerberos-Authentifizierung sind zwei SPNs erforderlich:

```
HOST/alias  
HOST/alias.domain
```

Wenn der Alias lautet `finance.domain.com`, sind die folgenden beiden SPNs erforderlich:

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

### Note

Sie müssen alle vorhandenen HOST-SPNs löschen, die dem DNS-Alias auf dem Active Directory-Computerobjekt entsprechen, bevor Sie neue HOST-SPNs für das Active Directory (AD) -Computerobjekt Ihres Amazon FSx-Dateisystems erstellen. Versuche, SPNs für Ihr Amazon FSx-Dateisystem festzulegen, schlagen fehl, wenn ein SPN für den DNS-Alias im AD vorhanden ist.

In den folgenden Verfahren wird beschrieben, wie Sie Folgendes tun können:

- Suchen Sie nach allen vorhandenen DNS-Alias-SPNs auf dem Active Directory-Computerobjekt des ursprünglichen Dateisystems.

- Löschen Sie die vorhandenen SPNs, falls vorhanden.
- Erstellen Sie neue DNS-Alias-SPNs für das Active Directory-Computerobjekt Ihres Amazon FSx-Dateisystems.

Um das erforderliche PowerShell Active Directory-Modul zu installieren

1. Melden Sie sich bei einer Windows-Instance an, die mit dem Active Directory verbunden ist, mit dem Ihr Amazon FSx-Dateisystem verknüpft ist.
2. PowerShell Als Administrator öffnen.
3. Installieren Sie das PowerShell Active Directory-Modul mit dem folgenden Befehl.

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

So suchen und löschen Sie vorhandene DNS-Alias-SPNs auf dem Active Directory-Computerobjekt des ursprünglichen Dateisystems

1. Suchen Sie mithilfe der folgenden Befehle nach vorhandenen SPNs. *alias\_fqdn* Ersetzen Sie es durch den DNS-Alias, den Sie dem Dateisystem in [Schritt 1](#) zugeordnet haben.

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

2. Löschen Sie die vorhandenen HOST-SPNs, die im vorherigen Schritt zurückgegeben wurden, mithilfe des folgenden Beispielskripts.
  - *alias\_fqdn* Ersetzen Sie sie durch den vollständigen DNS-Alias, den Sie dem Dateisystem in [Schritt 1](#) zugeordnet haben.
  - *file\_system\_dns\_name* Ersetzen Sie es durch den DNS-Namen des ursprünglichen Dateisystems.

```
## 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. Wiederholen Sie die vorherigen Schritte für jeden DNS-Alias, den Sie dem Dateisystem in [Schritt 1](#) zugeordnet haben.

So legen Sie SPNs für das Active Directory-Computerobjekt Ihres Amazon FSx-Dateisystems fest

1. Legen Sie neue SPNs für Ihr Amazon FSx-Dateisystem fest, indem Sie die folgenden Befehle ausführen.

- *file\_system\_dns\_name* Ersetzen Sie durch den DNS-Namen, den Amazon FSx dem Dateisystem zugewiesen hat.

Um den DNS-Namen Ihres Dateisystems auf der Amazon FSx-Konsole zu finden, wählen Sie Dateisysteme, wählen Sie Ihr Dateisystem und dann auf der Seite mit den Dateisystemdetails den Bereich Netzwerk und Sicherheit.

Sie können den DNS-Namen auch in der Antwort auf den [DescribeFileSystems-API-Vorgang](#) abrufen.

- *alias\_fqdn* Ersetzen Sie ihn durch den vollständigen DNS-Alias, den Sie dem Dateisystem in [Schritt 1](#) zugeordnet haben.

```

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

##Use one of the following commands, not both:
Set-AdComputer -Identity $FSxAdComputer -Add @"msDS-
AdditionalDnsHostname"="$Alias"}
##Or
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name

```

**Note**

Das Einrichten eines SPN für Ihr Amazon FSx-Dateisystem schlägt fehl, wenn ein SPN für den DNS-Alias im AD für das Computerobjekt des ursprünglichen Dateisystems vorhanden ist. Informationen zum Suchen und Löschen vorhandener SPNs finden Sie unter. [So suchen und löschen Sie vorhandene DNS-Alias-SPNs auf dem Active Directory-Computerobjekt des ursprünglichen Dateisystems](#)

2. Stellen Sie mithilfe des folgenden Beispielskripts sicher, dass die neuen SPNs für den DNS-Alias konfiguriert sind. Stellen Sie sicher, dass die Antwort zwei HOST-SPNs HOST/*alias* und enthält HOST/*alias\_fqdn*, wie zuvor in diesem Verfahren beschrieben.

*file\_system\_dns\_name* Ersetzen Sie durch den DNS-Namen, den Amazon FSx Ihrem Dateisystem zugewiesen hat. Um den DNS-Namen Ihres Dateisystems auf der Amazon FSx-Konsole zu finden, wählen Sie Dateisysteme, wählen Sie Ihr Dateisystem und dann auf der Seite mit den Dateisystemdetails den Bereich Netzwerk und Sicherheit.

Sie können den DNS-Namen auch in der Antwort auf den [DescribeFileSystems-API-Vorgang](#) abrufen.

```
## 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. Wiederholen Sie die vorherigen Schritte für jeden DNS-Alias, den Sie dem Dateisystem in [Schritt 1](#) zugeordnet haben.

Informationen darüber, wie Sie Clients dazu zwingen können, Kerberos-Authentifizierung und Verschlüsselung zu verwenden, wenn sie sich mit Ihrem Amazon FSx-Dateisystem verbinden, finden Sie unter. [Erzwingen der Kerberos-Authentifizierung mithilfe von GPOs](#)

## Schritt 3: Aktualisieren oder erstellen Sie einen DNS-CNAME-Eintrag für das Dateisystem

Nachdem Sie SPNs für Ihr Dateisystem ordnungsgemäß konfiguriert haben, können Sie zu Amazon FSx wechseln, indem Sie jeden DNS-Eintrag, der in das ursprüngliche Dateisystem aufgelöst wurde, durch einen DNS-Eintrag ersetzen, der in den Standard-DNS-Namen des Amazon FSx-Dateisystems aufgelöst wird.

Die Module `dnsserver` und `activedirectory` Windows sind erforderlich, um die in diesem Abschnitt aufgeführten Befehle auszuführen.

Um die erforderlichen PowerShell Cmdlets zu installieren

1. Melden Sie sich bei einer Windows-Instance an, die mit dem Active Directory verbunden ist, mit dem Ihr Amazon FSx-Dateisystem verknüpft ist, als Benutzer, der Mitglied einer Gruppe ist, die über DNS-Verwaltungsberechtigungen verfügt (AWSAWS Delegated Domain Name System Administrators in AWS Managed Active Directory und Domain Admins oder eine andere Gruppe, an die Sie DNS-Verwaltungsberechtigungen in Ihrem selbstverwalteten Active Directory delegiert haben).

Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.

2. PowerShell Als Administrator öffnen.
3. Das PowerShell DNS-Servermodul ist erforderlich, um die Anweisungen in diesem Verfahren auszuführen. Installieren Sie es mit dem folgenden Befehl.

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

Um einen benutzerdefinierten DNS-Namen für Ihr Amazon FSx-Dateisystem zu aktualisieren oder zu erstellen

1. Stellen Sie eine Connect zu Ihrer Amazon EC2 EC2-Instance als Benutzer her, der Mitglied einer Gruppe mit DNS-Administrationsberechtigungen ist (AWS Delegierte Domainnamen-Systemadministratoren in AWS Managed Active Directory und Domain-Admins oder eine andere Gruppe, an die Sie DNS-Verwaltungsberechtigungen in Ihrem selbstverwalteten Active Directory delegiert haben).

Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.

2. Führen Sie an der Befehlszeile das folgende Skript aus. Dieses Skript migriert alle vorhandenen DNS-CNAME-Einträge in Ihr Amazon FSx-Dateisystem. Wenn keine gefunden werden, wird ein neuer DNS-CNAME-Eintrag für den DNS-Alias erstellt *alias\_fqdn*, der in den Standard-DNS-Namen für Ihr Amazon FSx-Dateisystem aufgelöst wird.

So führen Sie das Skript aus:

- *alias\_fqdn* Ersetzen Sie ihn durch den DNS-Alias, den Sie dem Dateisystem zugeordnet haben.
- *file\_system\_dns\_name* Ersetzen Sie durch den DNS-Namen, den Amazon FSx dem Dateisystem zugewiesen hat.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
  Select -ExpandProperty Name) | Select -First 1
foreach ($computer in $DnsServerComputerName)
{
  Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName $computer -
  HostNameAlias $FSxDnsName -ZoneName $ZoneName
}
```

3. Wiederholen Sie den vorherigen Schritt für jeden DNS-Alias, den Sie dem Dateisystem in [Schritt 1](#) zugeordnet haben.

Sie haben jetzt einen DNS-CNAME-Wert für Ihr Amazon FSx-Dateisystem mit dem DNS-Alias hinzugefügt. Sie können jetzt den DNS-Alias verwenden, um auf Ihre Daten zuzugreifen.

#### Note

Wenn ein DNS-CNAME-Eintrag aktualisiert wird, sodass er auf ein Amazon FSx-Dateisystem verweist, das zuvor auf ein anderes Dateisystem verwiesen hat, können Clients möglicherweise für einen kurzen Zeitraum keine Verbindung mit dem Dateisystem herstellen. Wenn der DNS-Cache des Clients aktualisiert wird, sollten sie in der Lage sein, mithilfe des

DNS-Alias eine Verbindung herzustellen. Weitere Informationen finden Sie unter [Mit einem DNS-Alias kann nicht auf das Dateisystem zugegriffen werden](#).

## Erzwingen der Kerberos-Authentifizierung mithilfe von GPOs

Sie können die Kerberos-Authentifizierung beim Zugriff auf das Dateisystem erzwingen, indem Sie die folgenden Gruppenrichtlinienobjekte (GPOs) in Ihrem Active Directory einrichten:

- **NTLM einschränken: Ausgehender NTLM-Verkehr auf Remoteserver** — Verwenden Sie diese Richtlinieneinstellung, um ausgehenden NTLM-Verkehr von einem Computer zu einem beliebigen Remoteserver, auf dem das Windows-Betriebssystem ausgeführt wird, zu verweigern oder zu überwachen.
  - **NTLM einschränken: Remoteserver-Ausnahmen für die NTLM-Authentifizierung hinzufügen** — Verwenden Sie diese Richtlinieneinstellung, um eine Ausnahmeliste von Remoteservern zu erstellen, auf denen Client-Geräte NTLM-Authentifizierung verwenden dürfen, wenn die Richtlinieneinstellung Netzwerksicherheit: NTLM einschränken: Ausgehender NTLM-Verkehr zu Remoteservern konfiguriert ist.
1. Melden Sie sich als Administrator bei einer Windows-Instance an, die mit dem Active Directory verbunden ist, mit dem Ihr Amazon FSx-Dateisystem verbunden ist. Wenn Sie ein selbstverwaltetes Active Directory konfigurieren, wenden Sie diese Schritte direkt auf Ihr Active Directory an.
  2. Wählen Sie Start, dann Verwaltungstools und anschließend Gruppenrichtlinienverwaltung aus.
  3. Wählen Sie Gruppenrichtlinienobjekte aus.
  4. Wenn Ihr Gruppenrichtlinienobjekt noch nicht existiert, erstellen Sie es.
  5. Suchen Sie nach der vorhandenen Richtlinie Netzwerksicherheit: NTLM einschränken: Ausgehenden NTLM-Verkehr auf Remoteserver beschränken. (Wenn es keine bestehende Richtlinie gibt, erstellen Sie eine neue Richtlinie.) Öffnen Sie auf der Registerkarte Lokale Sicherheitseinstellungen das Kontextmenü (Rechtsklick) und wählen Sie Eigenschaften aus.
  6. Wählen Sie „Alle ablehnen“.
  7. Wählen Sie Anwenden, um die Sicherheitseinstellung zu speichern.
  8. Um Ausnahmen für NTLM-Verbindungen zu bestimmten Remoteservern für den Client festzulegen, suchen Sie unter Netzwerksicherheit: NTLM einschränken: Remoteserverausnahmen hinzufügen.

Öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie auf der Registerkarte Lokale Sicherheitseinstellungen die Option Eigenschaften aus.

9. Geben Sie die Namen aller Server ein, die der Ausnahmeliste hinzugefügt werden sollen.
10. Wählen Sie Anwenden, um die Sicherheitseinstellung zu speichern.

## Exemplarische Vorgehensweise 6: Skalierung der Leistung mit Shards

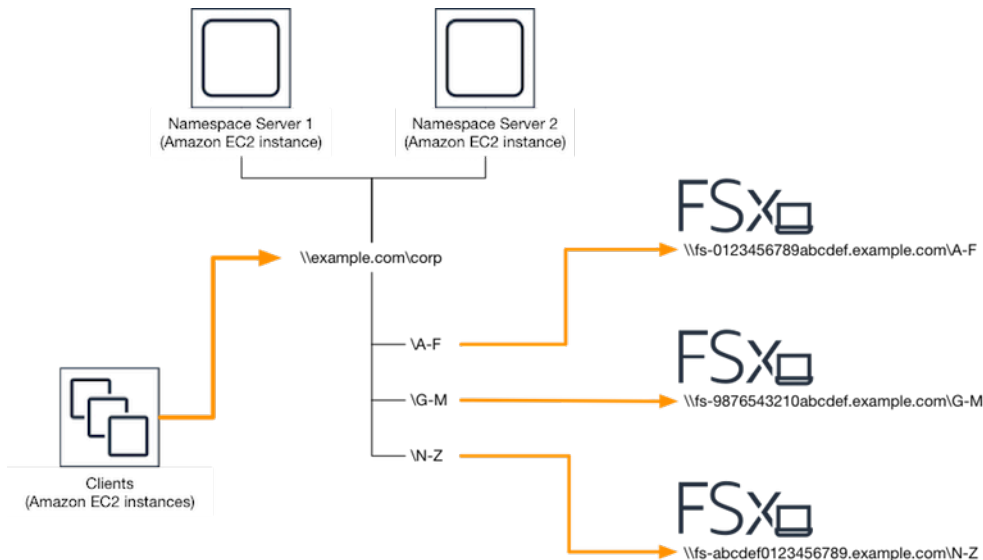
Amazon FSx for Windows File Server unterstützt die Verwendung des Microsoft Distributed File System (DFS). Mithilfe von DFS-Namespaces können Sie die Leistung (sowohl beim Lesen als auch beim Schreiben) skalieren, um I/O-intensive Workloads zu bewältigen, indem Sie Ihre Dateidaten auf mehrere Amazon FSx-Dateisysteme verteilen. Gleichzeitig können Sie Ihren Anwendungen weiterhin eine einheitliche Ansicht unter einem gemeinsamen Namespace bieten. Bei dieser Lösung werden Ihre Dateidaten in kleinere Datensätze oder Shards aufgeteilt und in verschiedenen Dateisystemen gespeichert. Anwendungen, die von mehreren Instanzen aus auf Ihre Daten zugreifen, können eine hohe Leistung erzielen, indem sie parallel auf diese Shards lesen und schreiben.

Sie können diese Lösung verwenden, wenn Ihre Arbeitslast einen gleichmäßig verteilten Lese-/Schreibzugriff auf Ihre Dateidaten erfordert (z. B. wenn jede Teilmenge der Recheninstanzen auf einen anderen Teil Ihrer Dateidaten zugreift).

### Einrichtung von DFS-Namespaces für Scale-Out-Leistung

Das folgende Verfahren führt Sie durch die Erstellung einer DFS-Lösung auf Amazon FSx für Scale-Out-Leistung. In diesem Beispiel werden die im *Corp-Namespace* gespeicherten Daten alphabetisch sortiert. Die Datendateien 'A-F', 'G-M' und 'N-Z' werden alle auf unterschiedlichen Dateifreigaben gespeichert. Je nach Datentyp, I/O-Größe und I/O-Zugriffsmuster sollten Sie entscheiden, wie Sie Ihre Daten am besten auf mehrere Dateifreigaben verteilen. Wählen Sie eine Sharding-Konvention, die I/O gleichmäßig auf alle Dateifreigaben verteilt, die Sie verwenden möchten. Beachten Sie, dass jeder Namespace insgesamt bis zu 50.000 Dateifreigaben und Hunderte von Petabyte an Speicherkapazität unterstützt.





So richten Sie DFS-Namespaces für Scale-Out-Leistung ein

1. [Wenn Sie noch keine DFS-Namespace-Server ausgeführt haben, können Sie mithilfe der Vorlage Setup-DFSN-Servers.Template ein Paar hochverfügbarer DFS-Namespace-Server starten.](#) AWS CloudFormation [Weitere Informationen zum Erstellen eines Stacks finden Sie im Benutzerhandbuch unter Erstellen eines AWS CloudFormation Stacks auf der Konsole.](#) [AWS CloudFormation AWS CloudFormation](#)
2. Stellen Sie als Benutzer in der Gruppe AWS Delegierte Administratoren eine Connect zu einem der DFS-Namespace-Server her, die im vorherigen Schritt gestartet wurden. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Greifen Sie auf die DFS Management Console zu. Öffnen Sie das Startmenü und führen Sie dfsmgmt.msc aus. Dadurch wird das DFS Management GUI-Tool geöffnet.
4. Wählen Sie Aktion und dann Neuer Namespace, geben Sie den Computernamen des ersten DFS-Namespace-Servers ein, den Sie für Server gestartet haben, und wählen Sie Weiter.
5. Geben Sie unter Name den Namespace ein, den Sie erstellen (z. B. corp).
6. Wählen Sie „Einstellungen bearbeiten“ und legen Sie die entsprechenden Berechtigungen entsprechend Ihren Anforderungen fest. Wählen Sie Weiter aus.
7. Lassen Sie die Standardoption Domänenbasierter Namespace aktiviert, lassen Sie die Option Windows Server 2008-Modus aktiviert und klicken Sie auf Weiter.

 Note

Der Windows Server 2008-Modus ist die neueste verfügbare Option für Namespaces.

8. Überprüfen Sie die Namespace-Einstellungen und wählen Sie Create aus.
9. Wählen Sie in der Navigationsleiste unter Namespaces den neu erstellten Namespace aus, wählen Sie Aktion und dann Namespace-Server hinzufügen aus.
10. Geben Sie den Computernamen des zweiten DFS-Namespace-Servers ein, den Sie für den Namespace-Server gestartet haben.
11. Wählen Sie „Einstellungen bearbeiten“, legen Sie die entsprechenden Berechtigungen entsprechend Ihren Anforderungen fest und wählen Sie „OK“.
12. Öffnen Sie das Kontextmenü (Rechtsklick) für den Namespace, den Sie gerade erstellt haben, wählen Sie Neuer Ordner, geben Sie den Namen des Ordners für den ersten Shard ein (z. B. **A-F** für Name) und wählen Sie Hinzufügen aus.
13. Geben Sie den DNS-Namen der Dateifreigabe, die diesen Shard hostet, im UNC-Format (z. B. `\fs-0123456789abcdef0.example.com\A-F`) für Pfad zum Ordnerziel ein und wählen Sie OK.
14. Wenn die Freigabe nicht existiert:
  - a. Wählen Sie Ja, um es zu erstellen.
  - b. Wählen Sie im Dialogfeld „Teilen erstellen“ die Option „Durchsuchen“.
  - c. Wählen Sie einen vorhandenen Ordner aus, oder erstellen Sie einen neuen Ordner unter D\$ und klicken Sie auf OK.
  - d. Legen Sie die entsprechenden Freigabeberechtigungen fest und wählen Sie OK.
15. Nachdem das Ordnerziel für den Shard nun hinzugefügt wurde, wählen Sie OK.
16. Wiederholen Sie die letzten vier Schritte für andere Shards, die Sie demselben Namespace hinzufügen möchten.

## Exemplarische Vorgehensweise 7: Kopieren einer Sicherung in ein anderesAWS-Region

Mit Amazon FSx können Sie ein vorhandenes Backup innerhalb derselben kopierenAWS-Konto zu einem anderenAWS-Region(eine regionsübergreifende Sicherungskopie) oder auf dieselbeAWS-Region(eine Sicherungskopie in der Region).

Das folgende Verfahren führt Sie durch das Erstellen einer Kopie einer Sicherung innerhalb derselbenAWS-Konto aus. Bevor Sie diese Sicherungskopie erstellen können, benötigen Sie eine vorhandene Sicherung. Weitere Informationen finden Sie unter [Arbeiten mit Backups](#).

So kopieren Sie eine vorhandene Sicherung innerhalb derselbenAWS-Konto(regionsübergreifend oder regionalübergreifend

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/> aus.
2. Wählen Sie im Navigationsbereich Backups aus.
3. In der-SicherungenWählen Sie die Sicherung aus, die Sie kopieren möchten.
4. Klicken Sie auf Copy backup (Backup kopieren). Dadurch öffnet sich dasKopieren einer Sicherungassistant.
5. In derZielregionauflisten, wählen Sie ein ZielAWS-Regionum das Backup zu kopieren. Das Ziel kann in einem anderen seinAWS-Regionoder innerhalb desselbenAWS-Regionaus.
6. (Optional) Wählen SieKopieren von Tagsum Tags aus der Quellsicherung in die Zielsicherung zu kopieren. Wenn Sie die OptionKopieren von Tagsund fügen Sie auch Tags in Schritt 8 hinzu, alle Tags werden zusammengeführt.
7. FürVerschlüsselung, wähle dasAWS KMSChiffrierschlüssel zum Verschlüsseln des kopierten Backups.
8. FürSchlagwörter - optionalein, geben Sie einen Schlüssel und einen Wert ein, um Tags für Ihre kopierte Sicherung hinzuzufügen. Wenn du hier Tags hinzufügst und auch ausgewählt hastKopieren von Tagsin Schritt 6 werden alle Tags zusammengeführt.
9. Klicken Sie auf Copy backup (Backup kopieren).

Sie haben nun erfolgreich ein Backup innerhalb derselben kopiertAWS-Konto zu einem anderenAWS-Regionoder innerhalb desselbenAWS-Regionaus.

# Sicherheit in Amazon FSx

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der Amazon Web Services Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS -Compliance-Programme](#) regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für Amazon FSx for Windows File Server gelten, finden Sie unter [AWS Services in Scope by Compliance Program](#).
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Amazon FSx for Windows File Server anwenden können. In den folgenden Themen erfahren Sie, wie Sie Amazon FSx konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Services nutzen können, die Ihnen helfen, Ihre Amazon FSx for Windows File Server Server-Ressourcen zu überwachen und zu sichern.

## Themen

- [Datenverschlüsselung in Amazon FSx](#)
- [Zugriffskontrolle auf Datei- und Ordner Ebene mithilfe von Windows-ACLs](#)
- [Dateisystem-Zugriffskontrolle mit Amazon VPC](#)
- [Identity and Access Management für Amazon FSx for Windows File Server](#)
- [Konformitätsprüfung für Amazon FSx for Windows File Server](#)
- [Amazon FSx for Windows File Server und Schnittstellen-VPC-Endpunkte](#)

# Datenverschlüsselung in Amazon FSx

Amazon FSx for Windows File Server unterstützt zwei Formen der Verschlüsselung für Dateisysteme: Verschlüsselung von Daten bei der Übertragung und Verschlüsselung im Ruhezustand. Die Verschlüsselung von Daten während der Übertragung wird auf Dateifreigaben unterstützt, die einer Recheninstanz zugeordnet sind, die das SMB-Protokoll 3.0 oder neuer unterstützt. Die Verschlüsselung von Daten im Ruhezustand wird automatisch aktiviert, wenn ein Amazon FSx-Dateisystem erstellt wird. Amazon FSx verschlüsselt Daten während der Übertragung automatisch mit SMB-Verschlüsselung, wenn Sie auf Ihr Dateisystem zugreifen, ohne dass Sie Ihre Anwendungen ändern müssen.

## Verwendung von Verschlüsselung

Wenn in Ihrem Unternehmen Unternehmens- oder Behördenrichtlinien für die Verschlüsselung von gespeicherten Daten und Metadaten gelten, sollten Sie ein verschlüsseltes Dateisystem erstellen, bei dem Daten während der Übertragung verschlüsselt werden.

Weitere Informationen zur Verschlüsselung mit Amazon FSx for Windows File Server finden Sie unter diesen verwandten Themen:

- [Erstellen Sie Ihr Amazon FSx for Windows File Server Server-Dateisystem](#)
- [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FSx](#) im IAM-Benutzerhandbuch

### Themen

- [Verschlüsselung im Ruhezustand](#)
- [Verschlüsselung während der Übertragung](#)

## Verschlüsselung im Ruhezustand

Alle Amazon FSx-Dateisysteme sind im Ruhezustand mit Schlüsseln verschlüsselt, die mit AWS Key Management Service (AWS KMS) verwaltet werden. Daten werden automatisch verschlüsselt, bevor sie in das Dateisystem geschrieben werden, und beim Lesen automatisch entschlüsselt. Diese Prozesse werden von Amazon FSx transparent abgewickelt, sodass Sie Ihre Anwendungen nicht ändern müssen.

Amazon FSx verwendet einen branchenüblichen AES-256-Verschlüsselungsalgorithmus, um Amazon FSx-Daten und -Metadaten im Ruhezustand zu verschlüsseln. Weitere Informationen finden Sie unter [Grundlagen der Kryptographie](#) im AWS Key Management Service -Entwicklerhandbuch.

#### Note

Die Infrastruktur AWS für die Schlüsselverwaltung verwendet von den Federal Information Processing Standards (FIPS) 140-2 anerkannte kryptografische Algorithmen. Die Infrastruktur entspricht den Empfehlungen der National Institute of Standards and Technology (NIST) 800-57.

## So verwendet Amazon FSx AWS KMS

Amazon FSx lässt sich in unsere AWS KMS Schlüsselverwaltung integrieren. Amazon FSx verwendet ein AWS KMS key , um Ihr Dateisystem zu verschlüsseln. Sie wählen den KMS-Schlüssel, der zum Verschlüsseln und Entschlüsseln von Dateisystemen (sowohl Daten als auch Metadaten) verwendet wird. Sie können Zuweisungen für diesen KMS-Schlüssel aktivieren, deaktivieren oder widerrufen. Bei diesem KMS-Schlüssel kann es sich um einen der beiden folgenden Typen handeln:

- Von AWS verwalteter Schlüssel— Dies ist der Standard-KMS-Schlüssel, der kostenlos verwendet werden kann.
- Kundenverwalteter Schlüssel – Dies ist der flexibelste KMS-Schlüssel, da Sie seine Schlüsselrichtlinien und Berechtigungen für mehrere Benutzer oder Dienste konfigurieren können. Weitere Informationen zum Erstellen von kundenverwalteten Schlüsseln finden Sie unter [Creating Keys](#) im AWS Key Management Service Developer Guide.

Wenn Sie einen vom Kunden verwalteten Schlüssel als KMS-Schlüssel für die Verschlüsselung und Entschlüsselung von Dateidaten verwenden, können Sie die Schlüsselrotation aktivieren. In diesem Fall rotiert AWS KMS Ihren Schlüssel einmal jährlich automatisch. Darüber hinaus können Sie mit einem vom Kunden verwalteten Schlüssel jederzeit wählen, wann Sie den Zugriff auf Ihren KMS-Schlüssel deaktivieren, erneut aktivieren, löschen oder widerrufen möchten. Weitere Informationen finden Sie unter [Rotating AWS KMS keys](#) im AWS Key Management Service Entwicklerhandbuch.

Die Verschlüsselung und Entschlüsselung des Dateisystems im Ruhezustand erfolgt transparent. Amazon FSx-spezifische AWS-Konto IDs erscheinen jedoch in Ihren AWS CloudTrail Protokollen, die sich auf AWS KMS Aktionen beziehen.

## Die wichtigsten Richtlinien von Amazon FSx für AWS KMS

Schlüsselrichtlinien sind die primäre Methode zur Zugriffssteuerung für KMS-Schlüssel. Weitere Informationen zu wichtigen Richtlinien finden Sie unter [Verwenden von Schlüsselrichtlinien AWS KMS im AWS Key Management Service](#) Entwicklerhandbuch. In der folgenden Liste werden alle zugehörigen Berechtigungen beschrieben AWS KMS, die von Amazon FSx für Dateisysteme mit Verschlüsselung im Ruhezustand unterstützt werden:

- kms:Encrypt – (Optional) Verschlüsselt Klartext in Geheimtext. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.
- kms:Decrypt – (Erforderlich) Entschlüsselt Geheimtext. Geheimtext ist Klartext, der zuvor verschlüsselt wurde. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.
- kms: ReEncrypt — (Optional) Verschlüsselt Daten auf der Serverseite mit einem neuen KMS-Schlüssel, ohne den Klartext der Daten auf der Clientseite offenzulegen. Die Daten werden zuerst entschlüsselt und dann neu verschlüsselt. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.
- kms: GenerateData KeyWithout Plaintext — (Erforderlich) Gibt einen mit einem KMS-Schlüssel verschlüsselten Datenverschlüsselungsschlüssel zurück. Diese Berechtigung ist in der Standardschlüsselrichtlinie unter kms: GenerateData Key\* enthalten.
- kms: CreateGrant — (Erforderlich) Fügt einem Schlüssel einen Grant hinzu, um anzugeben, wer den Schlüssel verwenden kann und unter welchen Bedingungen. Erteilungen sind eine alternative Berechtigungsmethode zu Schlüsselrichtlinien. Weitere Informationen zu Zuschüssen finden Sie unter [Verwendung von Zuschüssen](#) im AWS Key Management Service Entwicklerhandbuch. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.
- kms: DescribeKey — (Erforderlich) Stellt detaillierte Informationen zum angegebenen KMS-Schlüssel bereit. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.
- kms: ListAliases — (Optional) Listet alle Schlüsselalias im Konto auf. Wenn Sie die Konsole verwenden, um ein verschlüsseltes Dateisystem zu erstellen, füllt diese Berechtigung die Liste der KMS-Schlüssel auf. Wir empfehlen für eine optimale Benutzererfahrung diese Berechtigung. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.

## Verschlüsselung während der Übertragung

Die Verschlüsselung von Daten während der Übertragung wird auf Dateifreigaben unterstützt, die einer Recheninstanz zugeordnet sind, die das SMB-Protokoll 3.0 oder höher unterstützt. Dies umfasst alle Windows-Versionen ab Windows Server 2012 und Windows 8 sowie alle Linux-Clients mit

Samba-Client-Version 4.2 oder neuer. Amazon FSx for Windows File Server verschlüsselt Daten während der Übertragung automatisch mit SMB-Verschlüsselung, wenn Sie auf Ihr Dateisystem zugreifen, ohne dass Sie Ihre Anwendungen ändern müssen.

Die SMB-Verschlüsselung verwendet AES-128-GCM oder AES-128-CCM (wobei die GCM-Variante ausgewählt wird, wenn der Client SMB 3.1.1 unterstützt) als Verschlüsselungsalgorithmus und bietet außerdem Datenintegrität durch Signieren mit SMB-Kerberos-Sitzungsschlüsseln. Die Verwendung von AES-128-GCM führt zu einer besseren Leistung, beispielsweise bis zu einer zweifachen Leistungssteigerung beim Kopieren großer Dateien über verschlüsselte SMB-Verbindungen.

Um die Compliance-Anforderungen für eine durchgehende Verschlüsselung zu erfüllen data-in-transit, können Sie den Dateisystemzugriff so einschränken, dass nur Clients Zugriff haben, die SMB-Verschlüsselung unterstützen. Sie können auch die Verschlüsselung während der Übertragung pro Dateifreigabe oder für das gesamte Dateisystem aktivieren oder deaktivieren. Auf diese Weise können Sie eine Mischung aus verschlüsselten und unverschlüsselten Dateifreigaben auf demselben Dateisystem verwenden. Weitere Informationen zur Verwaltung in encryption-in-transit Ihrem Dateisystem finden Sie unter [Verwaltung der Verschlüsselung bei der Übertragung](#).

## Zugriffskontrolle auf Datei- und Orderebene mithilfe von Windows-ACLs

Amazon FSx for Windows File Server unterstützt die identitätsbasierte Authentifizierung über das Server Message Block (SMB) -Protokoll über Microsoft Active Directory. Active Directory ist der Verzeichnisdienst von Microsoft, der Informationen über Objekte im Netzwerk speichert und Administratoren und Benutzern das Auffinden und Verwenden dieser Informationen erleichtert. Zu diesen Objekten gehören in der Regel gemeinsam genutzte Ressourcen wie Dateiserver und Netzwerkbenutzer- und Computerkonten. Weitere Informationen zur Active Directory-Unterstützung in Amazon FSx finden Sie unter [Arbeiten mit Microsoft Active Directory in FSx for Windows File Server](#).

Ihre domänengebundenen Compute-Instances können mithilfe von Active Directory-Anmeldeinformationen auf Amazon FSx-Dateifreigaben zugreifen. Sie verwenden standardmäßige Windows-Zugriffskontrolllisten (ACLs) für eine differenzierte Zugriffskontrolle auf Datei- und Orderebene. Amazon FSx-Dateisysteme überprüfen automatisch die Anmeldeinformationen von Benutzern, die auf Dateisystemdaten zugreifen, um diese Windows-ACLs durchzusetzen.

Jedes Amazon FSx-Dateisystem verfügt über eine standardmäßige Windows-Dateifreigabe namens `share`. Die Windows-ACLs für diesen gemeinsamen Ordner sind so konfiguriert, dass Domänenbenutzern Lese-/Schreibzugriff gewährt wird. Sie gewähren außerdem der



Gruppe der delegierten Administratoren in Ihrem Active Directory, die mit der Ausführung von Verwaltungsaktionen auf Ihren Dateisystemen beauftragt ist, die volle Kontrolle. Wenn Sie Ihr Dateisystem in AWS Managed Microsoft AD integrieren, ist diese Gruppe AWS Delegated FSx Administrators. Wenn Sie Ihr Dateisystem in Ihr selbstverwaltetes Microsoft AD-Setup integrieren, kann es sich bei dieser Gruppe um Domain-Admins handeln. Oder es kann sich um eine benutzerdefinierte Gruppe delegierter Administratoren handeln, die Sie bei der Erstellung des Dateisystems angegeben haben. Um die ACLs zu ändern, können Sie die Freigabe einem Benutzer zuordnen, der Mitglied der Gruppe der delegierten Administratoren ist.

#### Warning

Amazon FSx setzt voraus, dass der SYSTEM-Benutzer über die NTFS-ACL-Rechte „Vollständige Kontrolle“ für alle Ordner in Ihrem Dateisystem verfügt. Ändern Sie nicht die NTFS-ACL-Berechtigungen für diesen Benutzer in Ihren Ordnern. Dadurch kann auf Ihre Dateifreigabe nicht mehr zugegriffen werden und Dateisystem-Backups können nicht verwendet werden.

## Weiterführende Links

- [Was ist ein AWS Directory Service?](#) im AWS Directory Service Administratorhandbuch.
- [Erstellen Sie Ihr AWS verwaltetes Microsoft AD-Verzeichnis](#) im AWS Directory Service Administrationshandbuch.
- [Wann sollten Sie im AWS Directory Service Administratorhandbuch eine Vertrauensbeziehung einrichten?](#)
- [Exemplarische Vorgehensweise 1: Voraussetzungen für die ersten Schritte.](#)

## Dateisystem-Zugriffskontrolle mit Amazon VPC

Sie greifen über eine elastic network interface auf Ihr Amazon FSx-Dateisystem zu. Diese Netzwerkschnittstelle befindet sich in der Virtual Private Cloud (VPC), die auf dem Amazon Virtual Private Cloud (Amazon VPC) -Service basiert, den Sie mit Ihrem Dateisystem verknüpfen. Sie stellen über seinen Domain Name Service (DNS) -Namen eine Verbindung zu Ihrem Amazon FSx-Dateisystem her. Der DNS-Name ist der privaten IP-Adresse der elastic network interface des Dateisystems in Ihrer VPC zugeordnet. Nur Ressourcen innerhalb der zugehörigen VPC,

Ressourcen, die über AWS Direct Connect oder VPN mit der zugehörigen VPC verbunden sind, oder Ressourcen innerhalb von Peer-VPCs können auf die Netzwerkschnittstelle Ihres Dateisystems zugreifen. Weitere Informationen finden Sie unter [Was ist Amazon VPC?](#) im Amazon VPC-Benutzerhandbuch.

#### Warning

Sie dürfen die elastic network interface (n), die mit Ihrem Dateisystem verknüpft sind, nicht ändern oder löschen. Das Ändern oder Löschen der Netzwerkschnittstelle kann zu einem dauerhaften Verbindungsverlust zwischen Ihrer VPC und Ihrem Dateisystem führen.

FSx for Windows File Server unterstützt VPC Sharing, wodurch Sie Ressourcen in einem gemeinsam genutzten Subnetz in einer VPC, die einem anderen Konto gehört, anzeigen, erstellen, ändern und löschen können. AWS Weitere Informationen finden Sie unter [Arbeiten mit freigegebenen VPCs](#) im Amazon VPC Benutzerhandbuch.

## Amazon VPC-Sicherheitsgruppen

Um den Netzwerkverkehr, der über die elastic network interface Netzwerkschnittstellen Ihres Dateisystems innerhalb Ihrer VPC fließt, weiter zu kontrollieren, verwenden Sie Sicherheitsgruppen, um den Zugriff auf Ihre Dateisysteme einzuschränken. Eine Sicherheitsgruppe ist eine Stateful-Firewall, die den Datenverkehr zu und von den zugehörigen Netzwerkschnittstellen steuert. In diesem Fall handelt es sich bei der zugehörigen Ressource um die Netzwerkschnittstelle (n) Ihres Dateisystems.

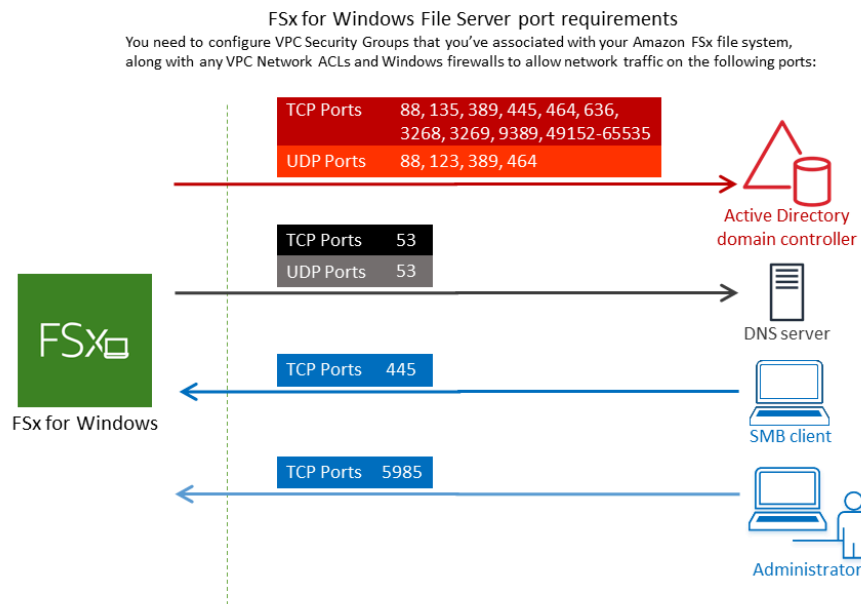
Um eine Sicherheitsgruppe zur Steuerung des Zugriffs auf Ihr Amazon FSx-Dateisystem zu verwenden, fügen Sie Regeln für eingehenden und ausgehenden Datenverkehr hinzu. Eingehende Regeln kontrollieren den eingehenden Verkehr, und ausgehende Regeln kontrollieren den ausgehenden Verkehr aus Ihrem Dateisystem. Stellen Sie sicher, dass Sie die richtigen Regeln für den Netzwerkverkehr in Ihrer Sicherheitsgruppe haben, um die Dateifreigabe Ihres Amazon FSx-Dateisystems einem Ordner auf Ihrer unterstützten Compute-Instance zuzuordnen.

Weitere Informationen zu Sicherheitsgruppenregeln finden Sie unter [Sicherheitsgruppenregeln](#) im Amazon EC2 EC2-Benutzerhandbuch.

Um eine Sicherheitsgruppe für Amazon FSx zu erstellen

1. Öffnen Sie die Amazon EC2 EC2-Konsole unter <https://console.aws.amazon.com/ec2>.


2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie Create Security Group aus.
4. Geben Sie einen Namen und eine Beschreibung für die Sicherheitsgruppe an.
5. Wählen Sie für VPC die Amazon VPC aus, die Ihrem Dateisystem zugeordnet ist, um die Sicherheitsgruppe innerhalb dieser VPC zu erstellen.
6. Fügen Sie die folgenden Regeln hinzu, um ausgehenden Netzwerkverkehr an den folgenden Ports zuzulassen:
  - a. Für VPC-Sicherheitsgruppen ist die Standardsicherheitsgruppe für Ihre standardmäßige Amazon-VPC bereits zu Ihrem Dateisystem in der Konsole hinzugefügt. Bitte stellen Sie sicher, dass die Sicherheitsgruppe und die VPC-Netzwerk-ACLs für die Subnetze, in denen Sie Ihr FSx-Dateisystem erstellen, Datenverkehr auf den Ports und in den in der folgenden Abbildung gezeigten Anweisungen zulassen.



In der folgenden Tabelle ist die Rolle der einzelnen Ports aufgeführt.

| Protokoll | Ports | Rolle                    |
|-----------|-------|--------------------------|
| TCP/UDP   | 53    | Domain Name System (DNS) |

| Protokoll | Ports       | Rolle                                                              |
|-----------|-------------|--------------------------------------------------------------------|
| TCP/UDP   | 88          | Kerberos-Authentifizierung                                         |
| TCP/UDP   | 464         | Passwort ändern/festlegen                                          |
| 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         | Directory-Services-SMB-Dateifreigabe                               |
| TCP       | 636         | Lightweight Directory Access Protocol über TLS/SSL (LDAPS)         |
| TCP       | 3268        | Globaler Microsoft-Katalog                                         |
| TCP       | 3269        | Microsoft Global Catalog über SSL                                  |
| TCP       | 5985        | WinRM 2.0 (Microsoft Windows-Fernverwaltung)                       |
| TCP       | 9389        | Microsoft AD DS-Webdienste, PowerShell                             |
| TCP       | 49152–65535 | Flüchtige Ports für RPC                                            |

 **Important**

Für Single-AZ 2- und alle Multi-AZ-Dateisystembereitstellungen ist es erforderlich, ausgehenden Verkehr auf TCP-Port 9389 zuzulassen.

- b. Stellen Sie sicher, dass diese Verkehrsregeln auch auf den Firewalls widergespiegelt werden, die für jeden der AD-Domänencontroller, DNS-Server, FSx-Clients und FSx-Administratoren gelten.

**⚠ Important**

Während Amazon VPC-Sicherheitsgruppen verlangen, dass Ports nur in der Richtung geöffnet werden, in der der Netzwerkverkehr initiiert wird, erfordern die meisten Windows-Firewalls und VPC-Netzwerk-ACLs, dass Ports in beide Richtungen geöffnet sind.

**ℹ Note**

Wenn Sie Active Directory-Standorte definiert haben, müssen Sie sicherstellen, dass die Subnetze in der VPC, die Ihrem Amazon FSx-Dateisystem zugeordnet sind, an einem Active Directory-Standort definiert sind und dass keine Konflikte zwischen den Subnetzen in Ihrer VPC und den Subnetzen an Ihren anderen Standorten bestehen. Sie können diese Einstellungen mithilfe des MMC-Snap-Ins Active Directory-Standorte und -Dienste anzeigen und ändern.

**ℹ Note**

In einigen Fällen haben Sie möglicherweise die Standardeinstellungen für die Regeln Ihrer AWS Managed Microsoft AD Sicherheitsgruppe geändert. Falls ja, stellen Sie sicher, dass diese Sicherheitsgruppe über die erforderlichen Regeln für eingehenden Datenverkehr aus Ihrem Amazon FSx-Dateisystem verfügt. Weitere Informationen zu den erforderlichen Regeln für eingehenden Datenverkehr finden Sie unter [AWS Managed Microsoft AD Voraussetzungen im AWS Directory Service Administratorhandbuch](#).

Nachdem Sie Ihre Sicherheitsgruppe erstellt haben, können Sie sie mit den elastic network interface Netzwerkschnittstellen Ihres Amazon FSx-Dateisystems verknüpfen.

So verknüpfen Sie eine Sicherheitsgruppe mit Ihrem Amazon FSx-Dateisystem

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Dashboard Ihr Dateisystem aus, um dessen Details anzuzeigen.

3. Wählen Sie die Registerkarte Netzwerk und Sicherheit und wählen Sie die Netzwerkschnittstelle (n) Ihres Dateisystems aus, z. B. ENI-01234567890123456. Bei Single-AZ-Dateisystemen sehen Sie eine einzige Netzwerkschnittstelle. Bei Multi-AZ-Dateisystemen sehen Sie eine Netzwerkschnittstelle im bevorzugten Subnetz und eine im Standby-Subnetz.
4. Wählen Sie für jede Netzwerkschnittstelle die Netzwerkschnittstelle und dann unter Aktionen die Option Sicherheitsgruppen ändern aus.
5. Wählen Sie im Dialogfeld „Sicherheitsgruppen ändern“ die zu verwendenden Sicherheitsgruppen aus und klicken Sie auf Speichern.

## Zugriff auf ein Dateisystem verbieten

Um vorübergehend allen Clients den Netzwerkzugriff auf Ihr Dateisystem zu verbieten, können Sie alle Sicherheitsgruppen entfernen, die mit den elastic network interface Netzwerkschnittstellen Ihres Dateisystems verknüpft sind, und sie durch eine Gruppe ersetzen, die keine Regeln für eingehende/ausgehende Nachrichten hat.

## Amazon VPC-Netzwerk-ACLs

Eine weitere Möglichkeit, den Zugriff auf das Dateisystem in Ihrer VPC zu sichern, besteht darin, Netzwerkzugriffskontrolllisten (Netzwerk-ACLs) einzurichten. Netzwerk-ACLs sind von Sicherheitsgruppen getrennt, verfügen jedoch über ähnliche Funktionen, um den Ressourcen in Ihrer VPC eine zusätzliche Sicherheitsebene hinzuzufügen. Weitere Informationen zu Netzwerk-ACLs finden Sie unter [Netzwerk-ACLs](#) im Amazon VPC-Benutzerhandbuch.

# Identity and Access Management für Amazon FSx for Windows File Server

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem ein Administrator den Zugriff auf - AWS Ressourcen sicher steuern kann. IAM-Administratoren steuern, wer für die Nutzung von Amazon-FSx-Ressourcen authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) werden kann. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

## Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Funktionsweise von Amazon FSx for Windows File Server mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Windows File Server](#)
- [AWS Von verwaltete Richtlinien für Amazon FSx](#)
- [Fehlerbehebung für Identität und Zugriff auf Amazon FSx for Windows File Server](#)
- [Verwenden von Tags mit Amazon FSx](#)
- [Verwenden von serviceverknüpften Rollen für Amazon FSx](#)

## Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in Amazon FSx .

**Service-Benutzer** – Wenn Sie den Amazon-FSx-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie zur Ausführung von Aufgaben weitere Amazon-FSx-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie nicht auf ein Feature in Amazon FSx zugreifen können, finden Sie weitere Informationen unter [Fehlerbehebung für Identität und Zugriff auf Amazon FSx for Windows File Server](#).

**Service-Administrator** – Wenn Sie in Ihrem Unternehmen für Amazon-FSx-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Amazon FSx . Ihre Aufgabe besteht darin, zu bestimmen, auf welche Amazon-FSx-Funktionen und -Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Amazon FSx verwenden kann, finden Sie unter [Funktionsweise von Amazon FSx for Windows File Server mit IAM](#).

**IAM-Administrator** – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Amazon FSx verfassen können. Beispiele für identitätsbasierte Amazon-FSx-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Windows File Server](#).

## Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten bei anmelden. Sie müssen als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle authentifiziert (bei angemeldet AWS) sein.

Sie können sich bei AWS als Verbundidentität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt werden. AWS IAM Identity Center (IAM Identity Center)-Benutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie AWS über einen Verbund auf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, um welchen Benutzertyp es sich handelt, können Sie sich bei der AWS Management Console oder im - AWS Zugriffsportal anmelden. Weitere Informationen zur Anmeldung bei AWS finden Sie unter [So melden Sie sich bei Ihrem an AWS-Konto](#) im AWS-Anmeldung - Benutzerhandbuch.

Wenn Sie AWS programmgesteuert auf zugreifen, AWS stellt ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (Command Line Interface, CLI) bereit, um Ihre Anforderungen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine - AWS Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenständigen Signieren von Anforderungen finden Sie unter [Signieren von AWS API-Anforderungen](#) im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. empfiehlt beispielsweise, AWS die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center - Benutzerhandbuch und [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) in AWS](#) im IAM-Benutzerhandbuch.

### AWS-Konto Root-Benutzer

Wenn Sie ein erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet und Sie melden sich mit der E-Mail-Adresse und dem Passwort an, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für



Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

## Verbundidentität

Fordern Sie als bewährte Methode menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, auf, den Verbund mit einem Identitätsanbieter zu verwenden, um AWS-Services mithilfe temporärer Anmeldeinformationen auf zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, ein Web-Identitätsanbieter, die AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit AWS-Services Anmeldeinformationen auf zugreift, die über eine Identitätsquelle bereitgestellt werden. Wenn Verbundidentitäten auf zugreifen AWS-Konten, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen oder eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie für alle Ihre AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center -Benutzerhandbuch.

## IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

## IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die [Rollen wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI - oder AWS -API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Verwenden von IAM-Rollen](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Verbundbenutzerzugriff** – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.
- **Temporäre IAM-Benutzerberechtigungen** – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- **Kontoübergreifender Zugriff** – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können AWS-Services Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.

- **Serviceübergreifender Zugriff** – Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
- **Forward Access Sessions (FAS)** – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, die Interaktionen mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- **Servicerolle**: Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.
- **Serviceverknüpfte Rolle** – Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- **Anwendungen, die auf Amazon EC2 ausgeführt werden** – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und - AWS CLI oder AWS -API-Anforderungen stellen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine - AWS Rolle zuzuweisen und sie für alle ihre Anwendungen verfügbar zu machen, erstellen Sie ein Instance-Profil, das der Instance zugeordnet ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

## Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff in , AWS indem Sie Richtlinien erstellen und sie an AWS Identitäten oder Ressourcen anfügen. Eine Richtlinie ist ein Objekt in , AWS das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus der AWS Management Console, der AWS CLI oder der AWS -API abrufen.

### Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die

Sie mehreren Benutzern, Gruppen und Rollen in Ihrem anfügen können AWS-Konto. Verwaltete Richtlinien umfassen AWS -verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

## Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen AWS-Services.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

## Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services AWS WAF, die ACLs unterstützen. Weitere Informationen zu ACLs finden Sie unter [Zugriffssteuerungsliste \(ACL\) – Übersicht](#) (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

## Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze

für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.

- **Service-Kontrollrichtlinien (SCPs)** – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in angeben AWS Organizations. AWS Organizations ist ein Service zum Gruppieren und zentralen Verwalten mehrerer AWS-Konten, die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Die SCP beschränkt Berechtigungen für Entitäten in Mitgliedskonten, einschließlich jeder Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter [Funktionsweise von SCPs](#) im AWS Organizations -Benutzerhandbuch.
- **Sitzungsrichtlinien** – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

## Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Wie AWS bestimmt, ob eine Anforderung zugelassen werden soll, wenn mehrere Richtlinientypen beteiligt sind, erfahren Sie unter [Logik zur Richtlinienbewertung](#) im IAM-Benutzerhandbuch.

## Funktionsweise von Amazon FSx for Windows File Server mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon FSx zu verwalten, erfahren Sie, welche IAM-Funktionen Sie mit Amazon FSx verwenden können.

## IAM-Funktionen, die Sie mit Amazon FSx for Windows File Server verwenden können

| IAM-Feature                                                        | FSx-Unterstützung |
|--------------------------------------------------------------------|-------------------|
| <a href="#">Identitätsbasierte Richtlinien</a>                     | Ja                |
| <a href="#">Ressourcenbasierte Richtlinien</a>                     | Nein              |
| <a href="#">Richtlinienaktionen</a>                                | Ja                |
| <a href="#">Richtlinienressourcen</a>                              | Ja                |
| <a href="#">Richtlinienbedingungsschlüssel (servicespezifisch)</a> | Ja                |
| <a href="#">ACLs</a>                                               | Nein              |
| <a href="#">ABAC (Tags in Richtlinien)</a>                         | Ja                |
| <a href="#">Temporäre Anmeldeinformationen</a>                     | Ja                |
| <a href="#">Weiterleiten von Zugriffssitzungen</a>                 | Ja                |
| <a href="#">Servicerollen</a>                                      | Nein              |
| <a href="#">Serviceverknüpfte Rollen</a>                           | Ja                |

Einen Überblick über das Zusammenwirken von FSx und anderen - AWS Services mit den meisten IAM-Funktionen finden Sie unter [-AWS Services, die mit IAM funktionieren](#) im IAM-Benutzerhandbuch.

## Identitätsbasierte Richtlinien für FSx

|                                              |    |
|----------------------------------------------|----|
| Unterstützt Richtlinien auf Identitätsbasis. | Ja |
|----------------------------------------------|----|

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen

ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für FSx

Beispiele für identitätsbasierte Amazon-FSx-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Windows File Server](#).

Ressourcenbasierte Richtlinien in FSx

|                                            |      |
|--------------------------------------------|------|
| Unterstützt ressourcenbasierte Richtlinien | Nein |
|--------------------------------------------|------|

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen AWS-Services.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen befinden AWS-Konten, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipal-Entität (Benutzer oder Rolle) die Berechtigung für den Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal



in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich.

Weitere Informationen finden Sie unter [Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden](#) im IAM-Benutzerhandbuch.

## Richtlinienaktionen für FSx

|                                 |    |
|---------------------------------|----|
| Unterstützt Richtlinienaktionen | Ja |
|---------------------------------|----|

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der FSx-Aktionen finden Sie unter [Von Amazon FSx for Windows File Server definierte Aktionen](#) in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in FSx verwenden das folgende Präfix vor der Aktion:

```
fsx
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [  
  "fsx:action1",  
  "fsx:action2"  
]
```

Beispiele für identitätsbasierte Amazon-FSx-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Windows File Server](#).

## Richtlinienressourcen für FSx

|                                   |    |
|-----------------------------------|----|
| Unterstützt Richtlinienressourcen | Ja |
|-----------------------------------|----|

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (\*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"

```

Eine Liste der FSx-Ressourcentypen und ihrer ARNs finden Sie unter [Von Amazon FSx for Windows File Server definierte Ressourcen](#) in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter [Von Amazon FSx for Windows File Server definierte Aktionen](#).

Beispiele für identitätsbasierte Amazon-FSx-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Windows File Server](#).

## Richtlinienbedingungsschlüssel für FSx

|                                                               |    |
|---------------------------------------------------------------|----|
| Unterstützt servicespezifische Richtlinienbedingungsschlüssel | Ja |
|---------------------------------------------------------------|----|

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. `ist gleich` oder `kleiner als`, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungschlüssel und servicespezifische Bedingungschlüssel. Informationen zum Anzeigen aller AWS globalen Bedingungschlüssel finden Sie unter [AWS Globale Bedingungskontextschlüssel](#) im IAM-Benutzerhandbuch.

Eine Liste der FSx-Bedingungsschlüssel finden Sie unter [Bedingungschlüssel für Amazon FSx for Windows File Server](#) in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungschlüssel verwenden können, finden Sie unter [Von Amazon FSx for Windows File Server definierte Aktionen](#).

Beispiele für identitätsbasierte Amazon-FSx-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Windows File Server](#).

## ACLs in FSx

Unterstützt ACLs

Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

## ABAC mit FSx

|                                        |    |
|----------------------------------------|----|
| Unterstützt ABAC (Tags in Richtlinien) | Ja |
|----------------------------------------|----|

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWSdiese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter [Was ist ABAC?](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

## Verwenden temporärer Anmeldeinformationen mit FSx

|                                            |    |
|--------------------------------------------|----|
| Unterstützt temporäre Anmeldeinformationen | Ja |
|--------------------------------------------|----|

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich der , die mit temporären Anmeldeinformationen AWS-Services funktionieren, finden Sie unter [AWS-Services , die mit IAM funktionieren](#) im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich AWS Management Console mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der anmelden. Wenn

Sie beispielsweise AWS über den SSO-Link (Single Sign-On) Ihres Unternehmens auf zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Sie können temporäre Anmeldeinformationen manuell mit der AWS CLI oder der AWS API erstellen. Sie können diese temporären Anmeldeinformationen dann verwenden, um auf zuzugreifen AWS. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

## Weiterleiten von Zugriffssitzungen für FSx

|                                           |    |
|-------------------------------------------|----|
| Unterstützt Forward Access Sessions (FAS) | Ja |
|-------------------------------------------|----|

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, die Interaktionen mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

## Servicerollen für FSx

|                           |      |
|---------------------------|------|
| Unterstützt Servicerollen | Nein |
|---------------------------|------|

Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.

**⚠ Warning**

Das Ändern der Berechtigungen für eine Servicerolle könnte die FSx-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn FSx dazu Anleitungen gibt.

## Serviceverknüpfte Rollen für FSx

|                                      |    |
|--------------------------------------|----|
| Unterstützt serviceverknüpfte Rollen | Ja |
|--------------------------------------|----|

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem Service verbunden ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören dem Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Weitere Informationen zum Erstellen oder Verwalten von serviceverknüpften Amazon-FSx-Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#).

## Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Windows File Server

Benutzer und Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von Amazon-FSx-Ressourcen. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von FSx definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FSx for Windows File Server](#) in der Service-Autorisierungs-Referenz.

### Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der FSx-Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)

## Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon-FSx-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu erteilen, verwenden Sie die -AWS verwalteten Richtlinien, die Berechtigungen für viele häufige Anwendungsfälle gewähren. Sie sind in Ihrem verfügbar AWS-Konto. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die für Ihre Anwendungsfälle spezifisch sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten: Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn sie über eine bestimmte verwendet werden AWS-Service, z. B. AWS CloudFormation. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON)

und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienuvalidierung zum IAM Access Analyzer](#) im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich – Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

## Verwenden der FSx-Konsole

Um auf die Amazon FSx for Windows File Server-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon-FSx-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Für Benutzer, die nur Aufrufe an die AWS CLI oder die AWS API durchführen, müssen Sie keine Mindestberechtigungen für die Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen weiterhin die FSx-Konsole verwenden können, fügen Sie den Entitäten auch die von FSx `AmazonFSxConsoleReadOnlyAccess` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter [Hinzufügen von Berechtigungen zu einem Benutzer](#) im IAM-Benutzerhandbuch.

## Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen zum Ausführen dieser Aktion auf der -Konsole oder programmgesteuert mithilfe der - AWS CLI oder AWS -API.

```
{
```



```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "ViewOwnUserInfo",
    "Effect": "Allow",
    "Action": [
      "iam:GetUserPolicy",
      "iam:ListGroupsWithUser",
      "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 Von verwaltete Richtlinien für Amazon FSx

Eine AWS von verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. Von AWS verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele häufige Anwendungsfälle bereitstellen, sodass Sie mit der Zuweisung von Berechtigungen für Benutzer, Gruppen und Rollen beginnen können.

Beachten Sie, dass von AWS verwaltete Richtlinien möglicherweise keine Berechtigungen mit den geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle - AWS

Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [kundenverwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in verwalteten AWS Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS von verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert, wirkt sich die Aktualisierung auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie angefügt ist. Aktualisiert am AWS wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer gestartet AWS-Service wird oder neue API-Operationen für vorhandene Services verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

## AmazonFSxServiceRolePolicy

Ermöglicht Amazon FSx, AWS Ressourcen in Ihrem Namen zu verwalten. Weitere Informationen hierzu finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#).

## AWS Von verwaltete Richtlinie: AmazonFSxDeleteServiceLinkedRoleAccess

Sie können `AmazonFSxDeleteServiceLinkedRoleAccess` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einem Service verknüpft und wird nur mit der serviceverknüpften Rolle für diesen Service verwendet. Sie können diese Richtlinie nicht anhängen, trennen, ändern oder löschen. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#).

Diese Richtlinie gewährt Administratorberechtigungen, die es Amazon FSx ermöglichen, seine serviceverknüpfte Rolle für den Amazon S3-Zugriff zu löschen, die nur von Amazon FSx für Lustre verwendet wird.

### Details zu Berechtigungen

Diese Richtlinie enthält Berechtigungen in `iam` damit Amazon FSx den Löschstaus für die mit dem FSx Service verknüpften Rollen für den Amazon S3-Zugriff anzeigen, löschen und anzeigen kann.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter [AmazonFSxDeleteServiceLinkedRoleAccess](#) im Referenzhandbuch zu - AWS verwalteten Richtlinien.

## AWS Von verwaltete Richtlinie: AmazonFSxFullAccess

Sie können AmazonFSxFullAccess an Ihre IAM-Entitäten anfügen. Amazon FSx fügt diese Richtlinie auch an eine Servicerolle an, die es Amazon FSx ermöglicht, Aktionen in Ihrem Namen durchzuführen.

Bietet vollständigen Zugriff auf Amazon FSx und Zugriff auf verwandte - AWS Services.

### Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx` – Ermöglicht Prinzipalen Vollzugriff auf alle Amazon-FSx-Aktionen mit Ausnahme von `BypassSnaplockEnterpriseRetention`.
- `ds` – Ermöglicht es Prinzipalen, Informationen über die AWS Directory Service Verzeichnisse anzuzeigen.
- `ec2`
  - Ermöglicht es Prinzipalen, Tags unter den angegebenen Bedingungen zu erstellen.
  - So stellen Sie eine verbesserte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereit, die mit einer VPC verwendet werden können.
- `iam` – Ermöglicht es Prinzipalen, eine serviceverknüpfte Amazon-FSx-Rolle im Namen des Benutzers zu erstellen. Dies ist erforderlich, damit Amazon FSx AWS Ressourcen im Namen des Benutzers verwalten kann.
- `logs` – Ermöglicht es Prinzipalen, Protokollgruppen zu erstellen, Streams zu protokollieren und Ereignisse in Protokollstreams zu schreiben. Dies ist erforderlich, damit Benutzer den Zugriff auf das FSx-für-Windows-File-Server-Dateisystem überwachen können, indem sie Audit-Zugriffsprotokolle an CloudWatch -Protokolle senden.
- `firehose` – Ermöglicht es Prinzipalen, Datensätze in Amazon Data Firehose zu schreiben. Dies ist erforderlich, damit Benutzer den Zugriff auf das FSx-für-Windows-File-Server-Dateisystem überwachen können, indem sie Audit-Zugriffsprotokolle an Firehose senden.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter [AmazonFSxFullAccess](#) im Referenzhandbuch zu - AWS verwalteten Richtlinien.

## AWS Von verwaltete Richtlinie: AmazonFSxConsoleFullAccess

Sie können die AmazonFSxConsoleFullAccess-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die vollen Zugriff auf Amazon FSx und Zugriff auf verwandte - AWS Services über die ermöglichen AWS Management Console.

### Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx` – Ermöglicht es Prinzipalen, alle Aktionen in der Amazon-FSx-Managementkonsole auszuführen, mit Ausnahme von `BypassSnaplockEnterpriseRetention`.
- `cloudwatch` – Ermöglicht es Prinzipalen, CloudWatch Alarme und Metriken in der Amazon-FSx-Managementkonsole anzuzeigen.
- `ds` – Ermöglicht es Prinzipalen, Informationen über ein - AWS Directory Service Verzeichnis aufzulisten.
- `ec2`
  - Ermöglicht es Prinzipalen, Tags in Routing-Tabellen zu erstellen, Netzwerkschnittstellen, Routing-Tabellen, Sicherheitsgruppen, Subnetze und die VPC aufzulisten, die einem Amazon FSx-Dateisystem zugeordnet ist.
  - So stellen Sie eine verbesserte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereit, die mit einer VPC verwendet werden können.
- `kms` – Ermöglicht es Prinzipalen, Aliase für AWS Key Management Service Schlüssel aufzulisten.
- `s3` – Ermöglicht es Prinzipalen, einige oder alle Objekte in einem Amazon S3-Bucket (bis zu 1000) aufzulisten.
- `iam` – Gewährt die Berechtigung zum Erstellen einer serviceverknüpften Rolle, die es Amazon FSx ermöglicht, Aktionen im Namen des Benutzers durchzuführen.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter [AmazonFSxConsoleFullAccess](#) im Referenzhandbuch zu - AWS verwalteten Richtlinien.

## AWS Von verwaltete Richtlinie: AmazonFSxConsoleReadOnlyAccess

Sie können die AmazonFSxConsoleReadOnlyAccess-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Amazon FSx und verwandten AWS Services Leseberechtigungen, sodass Benutzer Informationen zu diesen Services in der anzeigen können AWS Management Console.

## Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx` – Ermöglicht es Prinzipalen, Informationen über Amazon-FSx-Dateisysteme, einschließlich aller Tags, in der Amazon-FSx-Managementkonsole anzuzeigen.
- `cloudwatch` – Ermöglicht es Prinzipalen, CloudWatch Alarme und Metriken in der Amazon-FSx-Managementkonsole anzuzeigen.
- `ds` – Ermöglicht es Prinzipalen, Informationen über ein - AWS Directory Service Verzeichnis in der Amazon-FSx-Managementkonsole anzuzeigen.
- `ec2`
  - Ermöglicht es Prinzipalen, Netzwerkschnittstellen, Sicherheitsgruppen, Subnetze und die VPC anzuzeigen, die einem Amazon-FSx-Dateisystem in der Amazon-FSx-Managementkonsole zugeordnet ist.
  - So stellen Sie eine verbesserte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereit, die mit einer VPC verwendet werden können.
- `kms` – Ermöglicht es Prinzipalen, Aliase für AWS Key Management Service Schlüssel in der Amazon-FSx-Managementkonsole anzuzeigen.
- `log` – Ermöglicht es Prinzipalen, die Amazon CloudWatch -Logs-Protokollgruppen zu beschreiben, die dem Konto zugeordnet sind, das die Anforderung stellt. Dies ist erforderlich, damit Prinzipale die vorhandene Konfiguration der Dateizugriffsprüfung für ein FSx for Windows File Server-Dateisystem anzeigen können.
- `firehose` – Ermöglicht es Prinzipalen, die Amazon-Data-Firehose-Bereitstellungsdatenströme zu beschreiben, die dem Konto zugeordnet sind, das die Anforderung stellt. Dies ist erforderlich, damit Prinzipale die vorhandene Konfiguration der Dateizugriffsprüfung für ein FSx for Windows File Server-Dateisystem anzeigen können.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter [AmazonFSxConsoleReadOnlyAccess](#) im Referenzhandbuch zu - AWS verwalteten Richtlinien.

## AWS Von verwaltete Richtlinie: AmazonFSxReadOnlyAccess

Sie können die AmazonFSxReadOnlyAccess-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die schreibgeschützten Zugriff auf Amazon FSx ermöglichen.

- `fsx` – Ermöglicht es Prinzipalen, Informationen über Amazon-FSx-Dateisysteme, einschließlich aller Tags, in der Amazon-FSx-Managementkonsole anzuzeigen.
- `ec2` – Um eine verbesserte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter [AmazonFSxReadOnlyAccess](#) im Referenzhandbuch zu - AWS verwalteten Richtlinien.

### Amazon-FSx-Aktualisierungen für - AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für - AWS verwaltete Richtlinien für Amazon FSx, seit dieser Service mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Amazon-FSx-[Dokumentverlauf](#)Seite.

| Änderung                                                                                 | Beschreibung                                                                                                                                                                                                                                                      | Datum          |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">AmazonFSxServiceRolePolicy</a> – Aktualisierung einer vorhandenen Richtlinie | Amazon FSx hat eine neue Berechtigung hinzugefügt, <code>ec2:GetSecurityGroupsForVpc</code> die es Prinzipalen ermöglicht, eine verbesserte Sicherheitsgruppenvalidierung für alle Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können. | 9. Januar 2024 |
| <a href="#">AmazonFSxReadOnlyAccess</a> – Aktualisierung einer vorhandenen Richtlinie    | Amazon FSx hat eine neue Berechtigung hinzugefügt, <code>ec2:GetSecurityGro</code>                                                                                                                                                                                | 9. Januar 2024 |

| Änderung                                                                                            | Beschreibung                                                                                                                                                                                                                                                              | Datum                 |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                                                                                                     | <p>upsForVpc die es Prinzipal en ermöglicht, eine verbesserte Sicherheitsgruppenvalidierung für alle Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.</p>                                                                                   |                       |
| <p><a href="#">AmazonFSxConsoleReadOnlyAccess</a> – Aktualisierung einer vorhandenen Richtlinie</p> | <p>Amazon FSx hat eine neue Berechtigung hinzugefügt, <code>ec2:GetSecurityGroupsForVpc</code> die es Prinzipal en ermöglicht, eine verbesserte Sicherheitsgruppenvalidierung für alle Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.</p> | <p>9. Januar 2024</p> |
| <p><a href="#">AmazonFSxFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie</p>            | <p>Amazon FSx hat eine neue Berechtigung hinzugefügt, <code>ec2:GetSecurityGroupsForVpc</code> die es Prinzipal en ermöglicht, eine verbesserte Sicherheitsgruppenvalidierung für alle Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.</p> | <p>9. Januar 2024</p> |

| Änderung                                                                                 | Beschreibung                                                                                                                                                                                                                                                       | Datum             |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| <a href="#">AmazonFSxConsoleFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie | Amazon FSx hat eine neue Berechtigung hinzugefügt, <code>ec2:GetSecurityGroupsForVpc</code> die es Prinzipal en ermöglicht, eine verbesserte Sicherheitsgruppenvalidierung für alle Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können. | 9. Januar 2024    |
| <a href="#">AmazonFSxFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie        | Amazon FSx hat eine neue Berechtigung hinzugefügt, mit der Benutzer eine regions- und kontoübergreifende Datenreplikation für FSx-für-OpenZFS-Dateisysteme durchführen können.                                                                                     | 20. Dezember 2023 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie | Amazon FSx hat eine neue Berechtigung hinzugefügt, mit der Benutzer eine regions- und kontoübergreifende Datenreplikation für FSx-für-OpenZFS-Dateisysteme durchführen können.                                                                                     | 20. Dezember 2023 |
| <a href="#">AmazonFSxFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie        | Amazon FSx hat eine neue Berechtigung hinzugefügt, mit der Benutzer eine On-Demand-Replikation von Volumes für FSx-für-OpenZFS-Dateisysteme durchführen können.                                                                                                    | 26. November 2023 |



| Änderung                                                                                   | Beschreibung                                                                                                                                                                                  | Datum             |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| <a href="#">AmazonFSxConsoleFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie   | Amazon FSx hat eine neue Berechtigung hinzugefügt, mit der Benutzer eine On-Demand-Replikation von Volumes für FSx-für-OpenZFS-Dateisysteme durchführen können.                               | 26. November 2023 |
| <a href="#">AmazonFSxFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie          | Amazon FSx hat neue Berechtigungen hinzugefügt, damit Benutzer gemeinsam genutzte VPC-Unterstützung für Multi-AZ-Dateisysteme von FSx für ONTAP anzeigen, aktivieren und deaktivieren können. | 14. November 2023 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – Aktualisierung auf eine vorhandene Richtlinie | Amazon FSx hat neue Berechtigungen hinzugefügt, damit Benutzer gemeinsam genutzte VPC-Unterstützung für Multi-AZ-Dateisysteme von FSx für ONTAP anzeigen, aktivieren und deaktivieren können. | 14. November 2023 |
| <a href="#">AmazonFSxFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie          | Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Netzwerkonfigurationen für Multi-AZ-Dateisysteme von FSx für OpenZFS verwalten kann.                                         | 9. August 2023    |

| Änderung                                                                                                                  | Beschreibung                                                                                                                                                           | Datum         |
|---------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <a href="#">AWS Von verwaltete Richtlinie: AmazonFSxServiceRolePolicy</a> – Aktualisierung auf eine vorhandene Richtlinie | Amazon FSx hat die vorhandene <code>cloudwatch:PutMetricData</code> Berechtigung so geändert, dass Amazon FSx CloudWatch Metriken im AWS/FSx Namespace veröffentlicht. | 24. Juli 2023 |
| <a href="#">AmazonFSxFullAccess</a> – Aktualisierung auf eine vorhandene Richtlinie                                       | Amazon FSx hat die Richtlinie aktualisiert, um die <code>fsx:*</code> Berechtigung zu entfernen und bestimmte <code>fsx</code> Aktionen hinzuzufügen.                  | 13. Juli 2023 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – Aktualisierung auf eine vorhandene Richtlinie                                | Amazon FSx hat die Richtlinie aktualisiert, um die <code>fsx:*</code> Berechtigung zu entfernen und bestimmte <code>fsx</code> Aktionen hinzuzufügen.                  | 13. Juli 2023 |
| <a href="#">AmazonFSxFullAccess</a> – Aktualisierung auf eine vorhandene Richtlinie                                       | Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Netzwerkonfigurationen für Multi-AZ-Dateisysteme von FSx für OpenZFS verwalten kann.                  | 31. Mai 2023  |

| Änderung                                                                                     | Beschreibung                                                                                                                                                                                                    | Datum              |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">AmazonFSxConsoleReadOnlyAccess</a> – Aktualisierung einer vorhandenen Richtlinie | Amazon FSx hat neue Berechtigungen hinzugefügt, damit Benutzer erweiterte Leistungsmetriken und empfohlene Aktionen für Dateisysteme von FSx für Windows File Server in der Amazon-FSx-Konsole anzeigen können. | 21. September 2022 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie     | Amazon FSx hat neue Berechtigungen hinzugefügt, damit Benutzer erweiterte Leistungsmetriken und empfohlene Aktionen für Dateisysteme von FSx für Windows File Server in der Amazon-FSx-Konsole anzeigen können. | 21. September 2022 |
| <a href="#">AmazonFSxReadOnlyAccess</a> – Nachverfolgungsrichtlinie gestartet                | Diese Richtlinie gewährt schreibgeschützten Zugriff auf alle Amazon-FSx-Ressourcen und alle ihnen zugeordneten Tags.                                                                                            | 4. Februar 2022    |
| <a href="#">AmazonFSxDeleteServiceLinkedRoleAccess</a> – Nachverfolgungsrichtlinie gestartet | Diese Richtlinie gewährt Administratorberechtigungen, die es Amazon FSx ermöglichen, seine serviceverknüpfte Rolle für den Amazon S3-Zugriff zu löschen.                                                        | 7. Januar 2022     |

| Änderung                                                                                 | Beschreibung                                                                                                                                             | Datum             |
|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| <a href="#">AmazonFSxServiceRolePolicy</a> – Aktualisierung einer vorhandenen Richtlinie | Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Netzwerkonfigurationen für Dateisysteme von Amazon FSx für NetApp ONTAP verwalten kann. | 2. September 2021 |
| <a href="#">AmazonFSxFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie        | Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Tags in EC2-Routing-Tabellen für eingeschränkte Aufrufe erstellen kann.                 | 2. September 2021 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie | Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Multi-AZ-Dateisysteme von Amazon FSx für NetApp ONTAP erstellen kann.                   | 2. September 2021 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie | Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Tags in EC2-Routing-Tabellen für eingeschränkte Aufrufe erstellen kann.                 | 2. September 2021 |

| Änderung                                                                                 | Beschreibung                                                                                                                                                                                                                                                                                                                                        | Datum        |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <a href="#">AmazonFSxServiceRolePolicy</a> – Aktualisierung einer vorhandenen Richtlinie | <p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx CloudWatch Protokollstreams beschreiben und in sie schreiben kann.</p> <p>Dies ist erforderlich, damit Benutzer mithilfe von - CloudWatch Protokollen Dateizugriffs-Auditprotokolle für FSx-für-Windows-File-Server-Dateisysteme anzeigen können.</p>                           | 8. Juni 2021 |
| <a href="#">AmazonFSxServiceRolePolicy</a> – Aktualisierung einer vorhandenen Richtlinie | <p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Amazon-Data-Firehose-Bereitstellungsdatenströme beschreiben und darin schreiben kann.</p> <p>Dies ist erforderlich, damit Benutzer mithilfe von Amazon Data Firehose Audit-Protokolle für den Dateizugriff für ein FSx for Windows File Server-Dateisystem anzeigen können.</p> | 8. Juni 2021 |

| Änderung                                                                          | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                | Datum        |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <a href="#">AmazonFSxFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie | <p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale CloudWatch Protokollgruppen beschreiben und erstellen, Streams protokollieren und Ereignisse in Protokollstreams schreiben können.</p> <p>Dies ist erforderlich, damit Prinzipale mithilfe von - CloudWatch Protokollen Dateizugriffs-Auditprotokolle für FSx-für-Windows-File-Server-Dateisysteme anzeigen können.</p> | 8. Juni 2021 |
| <a href="#">AmazonFSxFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie | <p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale Datensätze in Amazon Data Firehose beschreiben und schreiben können.</p> <p>Dies ist erforderlich, damit Benutzer mithilfe von Amazon Data Firehose Audit-Protokolle für den Dateizugriff für ein FSx for Windows File Server-Dateisystem anzeigen können.</p>                                                          | 8. Juni 2021 |

| Änderung                                                                                 | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                      | Datum        |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <a href="#">AmazonFSxConsoleFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie | <p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale die Amazon CloudWatch -Logs-Protokollgruppen beschreiben können, die dem Konto zugeordnet sind, das die Anforderung stellt.</p> <p>Dies ist erforderlich, damit Prinzipale bei der Konfiguration der Dateizugriffsprüfung für ein FSx for Windows File Server-Dateisystem eine vorhandene CloudWatch Protokollgruppe auswählen können.</p>                    | 8. Juni 2021 |
| <a href="#">AmazonFSxConsoleFullAccess</a> – Aktualisierung einer vorhandenen Richtlinie | <p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale die Amazon-Data-Firehose-Bereitstellungsdatenströme beschreiben können, die dem Konto zugeordnet sind, das die Anforderung stellt.</p> <p>Dies ist erforderlich, damit Prinzipale einen vorhandenen Firehose-Bereitstellungsdatenstrom auswählen können, wenn sie die Dateizugriffsprüfung für ein FSx for Windows File Server-Dateisystem konfigurieren.</p> | 8. Juni 2021 |

| Änderung                                                                                            | Beschreibung                                                                                                                                                                                                                                                                                                                                                                     | Datum        |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <p><a href="#">AmazonFSxConsoleReadOnlyAccess</a> – Aktualisierung einer vorhandenen Richtlinie</p> | <p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale die Amazon CloudWatch -Logs-Protokollgruppen beschreiben können, die dem Konto zugeordnet sind, das die Anforderung stellt.</p> <p>Dies ist erforderlich, damit Prinzipale die vorhandene Konfiguration der Dateizugriffsprüfung für ein FSx for Windows File Server-Datensystem anzeigen können.</p>        | 8. Juni 2021 |
| <p><a href="#">AmazonFSxConsoleReadOnlyAccess</a> – Aktualisierung einer vorhandenen Richtlinie</p> | <p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale die Amazon-Data-Firehose-Bereitstellungsdatenströme beschreiben können, die dem Konto zugeordnet sind, das die Anforderung stellt.</p> <p>Dies ist erforderlich, damit Prinzipale die vorhandene Konfiguration der Dateizugriffsprüfung für ein FSx for Windows File Server-Datensystem anzeigen können.</p> | 8. Juni 2021 |



| Änderung                                                  | Beschreibung                                                                                         | Datum        |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------|--------------|
| Amazon FSx hat mit der Verfolgung von Änderungen begonnen | Amazon FSx hat mit der Verfolgung von Änderungen für seine von AWS verwalteten Richtlinien begonnen. | 8. Juni 2021 |

## Fehlerbehebung für Identität und Zugriff auf Amazon FSx for Windows File Server

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon FSx und IAM auftreten können.

### Themen

- [Ich bin nicht autorisiert, eine Aktion in FSx auszuführen](#)
- [Ich bin nicht autorisiert, iam durchzuführen:PassRole](#)
- [Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine FSx-Ressourcen gewähren](#)

### Ich bin nicht autorisiert, eine Aktion in FSx auszuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven `my-example-widget`-Ressource anzuzeigen, jedoch nicht über `fsx:GetWidget`-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
fsx:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `fsx:GetWidget`-Aktion auf die `my-example-widget`-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

## Ich bin nicht autorisiert, iam durchzuführen:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Amazon FSx übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine vorhandene Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder serviceverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon FSx auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

## Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine FSx-Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Amazon FSx diese Funktionen unterstützt, finden Sie unter [Funktionsweise von Amazon FSx for Windows File Server mit IAM](#).
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen in Ihrem Besitz finden AWS-Konten Sie unter [Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , das Sie besitzen](#) im IAM-Benutzerhandbuch.

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre -Ressourcen gewähren AWS-Konten, finden Sie unter [Gewähren von Zugriff auf im AWS-Konten Besitz von Dritten](#) im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.

## Verwenden von Tags mit Amazon FSx

Sie können Tags verwenden, um den Zugriff auf Amazon-FSx-Ressourcen zu steuern und eine attributbasierte Zugriffskontrolle (ABAC) zu implementieren. Benutzer benötigen die Berechtigung, während der Erstellung Tags auf Amazon-FSx-Ressourcen anzuwenden.

### Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung

Einige Aktionen zur Erstellung von Amazon FSx-APIs ermöglichen es Ihnen, beim Erstellen der Ressource Tags anzugeben. Sie können Ressourcen-Tags verwenden, um eine attributbasierte Zugriffskontrolle (ABAC) zu implementieren. Weitere Informationen finden Sie unter [Was ist ABAC für AWS](#) im IAM-Benutzerhandbuch.

Damit Benutzer diese Möglichkeit erhalten, benötigen sie die Berechtigungen zum Verwenden der Aktion, die die Ressource wie `fsx:CreateFileSystem` oder `fsx:CreateBackup` erstellt. Wenn Tags in der Aktion angegeben werden, mit der die Ressource erstellt wird, führt Amazon eine zusätzliche Autorisierung für die `fsx:TagResource`-Aktion aus, um die Berechtigungen der Benutzer zum Erstellen von Tags zu überprüfen. Daher benötigen die Benutzer außerdem die expliziten Berechtigungen zum Verwenden der `fsx:TagResource`-Aktion.

Das folgende Beispiel zeigt eine Richtlinie, die es Benutzern ermöglicht, während der Erstellung in einer bestimmten Dateisysteme zu erstellen und Tags auf Dateisysteme anzuwenden AWS-Konto.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
```

```

    "fsx:TagResource"
  ],
  "Resource": "arn:aws:fsx:region:account-id:file-system/*"
}
]
}

```

In ähnlicher Weise können Benutzer mit der folgenden Richtlinie Backups auf einem bestimmten Dateisystem erstellen und während der Erstellung des Backups alle Tags auf das Backup anwenden.

```

{
  "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/*"
    }
  ]
}

```

Die `fsx:TagResource`-Aktion wird nur ausgewertet, wenn die Tags während der Aktion zur Ressourcenerstellung angewendet werden. Folglich benötigt ein Benutzer, der über die Berechtigungen zum Erstellen einer Ressource verfügt (vorausgesetzt, es bestehen keine Markierungsbedingungen), keine Berechtigungen zur Verwendung der `fsx:TagResource`-Aktion, wenn keine Tags in der Anforderung angegeben werden. Wenn der Benutzer allerdings versucht, eine Ressource mit Tags zu erstellen, schlägt die Anforderung fehl, wenn der Benutzer nicht über die Berechtigungen für die `fsx:TagResource`-Aktion verfügt.

Weitere Informationen zum Markieren von Amazon-FSx-Ressourcen finden Sie unter [Markieren Ihrer Amazon FSx-Ressourcen mit Tags](#). Weitere Informationen zur Verwendung von Tags zum Steuern des Zugriffs auf FSx-Ressourcen finden Sie unter [Verwenden von Tags zur Steuerung des Zugriffs auf Ihre Amazon-FSx-Ressourcen](#).

## Verwenden von Tags zur Steuerung des Zugriffs auf Ihre Amazon-FSx-Ressourcen

Um den Zugriff auf Amazon-FSx-Ressourcen und -Aktionen zu steuern, können Sie AWS Identity and Access Management (IAM)-Richtlinien verwenden, die auf Tags basieren. Sie können die Steuerung auf zwei Arten bereitstellen:

1. Steuern Sie den Zugriff auf Amazon-FSx-Ressourcen basierend auf den Tags auf diesen Ressourcen.
2. Bestimmen, welche Tags in einer IAM-Anfragebedingung weitergeleitet werden können

Informationen zur Verwendung von Tags zum Steuern des Zugriffs auf - AWS Ressourcen finden Sie unter [Steuern des Zugriffs mithilfe von Tags](#) im IAM-Benutzerhandbuch. Weitere Informationen zum Markieren von Amazon-FSx-Ressourcen bei der Erstellung finden Sie unter [Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung](#). Weitere Informationen über das Markieren von -Ressourcen mit Tags finden Sie unter [Markieren Ihrer Amazon FSx-Ressourcen mit Tags](#).

### Bestimmung des Zugriffs auf Ressourcen basierend auf Tags

Um zu steuern, welche Aktionen ein Benutzer oder eine Rolle für eine Amazon-FSx-Ressource ausführen kann, können Sie Tags für die Ressource verwenden. So können Sie beispielsweise bestimmte API-Vorgänge für eine Dateisystemressource auf der Grundlage des Schlüssel-Wert-Paares des Tags der Ressource zulassen oder verbieten.

Example Richtlinie – Erstellen Sie ein Dateisystem auf , wenn Sie ein bestimmtes Tag bereitstellen

Diese Richtlinie erlaubt es dem Benutzer, ein Dateisystem nur zu erstellen, wenn er es mit einem bestimmten Tag-Schlüssel-Wert-Paar markiert, in diesem Beispiel `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 Richtlinie – Erstellen Sie Backups nur von Amazon-FSx-Dateisystemen mit einem bestimmten Tag

Diese Richtlinie ermöglicht es Benutzern, Backups nur von Dateisystemen zu erstellen, die mit dem Schlüssel-Wert-Paar gekennzeichnet sind `key=Department, value=Finance`, und das Backup wird mit dem Tag erstellt `Department=Finance`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:TagResource",
        "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Department": "Finance"
        }
      }
    }
  ]
}

```

## Example Richtlinie – Erstellen Sie ein Dateisystem mit einem bestimmten Tag aus Backups mit einem bestimmten Tag

Diese Richtlinie ermöglicht es Benutzern, Dateisysteme zu erstellen, die Department=Finance nur aus Backups mit dem Tag versehen sind Department=Finance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystemFromBackup",
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    }
  ]
}
```

## Example Richtlinie – Löschen von Dateisystemen mit bestimmten Tags

Diese Richtlinie ermöglicht es einem Benutzer, nur Dateisysteme zu löschen, die mit gekennzeichnet sind Department=Finance. Wenn sie ein endgültiges Backup erstellen, muss es mit markiert werden Department=Finance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx>DeleteFileSystem"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    }
  ]
}
```

```
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "fsx:TagResource"
  ],
  "Resource": "arn:aws:fsx:region:account-id:backup/*",
  "Condition": {
    "StringEquals": {
      "aws:RequestTag/Department": "Finance"
    }
  }
}
]
```

## Verwenden von serviceverknüpften Rollen für Amazon FSx

Amazon FSx for Windows File Server verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte Rollen](#). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Amazon FSx verknüpft ist. Serviceverknüpfte Rollen werden von Amazon FSx vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer - AWS Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Amazon FSx, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon FSx definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur Amazon FSx die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Amazon-FSx-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.



## Serviceverknüpfte Rollenberechtigungen für Amazon FSx

Amazon FSx verwendet die serviceverknüpfte Rolle namens `AWSServiceRoleForAmazonFSx` – Diese führt bestimmte Aktionen in Ihrem Konto aus, z. B. das Erstellen von Elastic Network Interfaces für Ihre Dateisysteme in Ihrer VPC.

Die Rollenberechtigungsrichtlinie erlaubt es Amazon FSx, die folgenden Aktionen für alle zutreffenden AWS Ressourcen durchzuführen:

Sie können `AmazonFSxServiceRolePolicy` nicht an Ihre IAM-Entitäten anfügen. Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es FSx ermöglicht, - AWS Ressourcen in Ihrem Namen zu verwalten. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#).

Aktualisierungen dieser Richtlinie finden Sie unter [AmazonFSxServiceRolePolicy](#)

Diese Richtlinie gewährt administrative Berechtigungen, die es FSx ermöglichen, AWS Ressourcen im Namen des Benutzers zu verwalten.

### Details zu Berechtigungen

Die `AmazonFSxServiceRolePolicy` -Rollenberechtigungen werden durch die von `AmazonFSxServiceRolePolicy` AWS verwaltete Richtlinie definiert. `AmazonFSxServiceRolePolicy` verfügt über die folgenden Berechtigungen:

#### Note

`AmazonFSxServiceRolePolicy` wird von allen Amazon-FSx-Dateisystemtypen verwendet. Einige der aufgelisteten Berechtigungen gelten möglicherweise nicht für FSx for Windows.

- `ds` – Ermöglicht FSx das Anzeigen, Autorisieren und Aufheben der Autorisierung von Anwendungen in Ihrem AWS Directory Service Verzeichnis.
- `ec2` – Ermöglicht FSx Folgendes:
  - Netzwerkschnittstellen anzeigen, erstellen und die Zuordnung aufheben, die einem Amazon FSx-Dateisystem zugeordnet sind.
  - Zeigen Sie eine oder mehrere Elastic IP-Adressen an, die einem Amazon FSx-Dateisystem zugeordnet sind.

- Zeigen Sie Amazon-VPCs, Sicherheitsgruppen und Subnetze an, die einem Amazon-FSx-Dateisystem zugeordnet sind.
- So stellen Sie eine verbesserte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereit, die mit einer VPC verwendet werden können.
- Erstellen Sie eine Berechtigung für einen von AWS autorisierten Benutzer, um bestimmte Operationen auf einer Netzwerkschnittstelle auszuführen.
- `cloudwatch` – Ermöglicht FSx das Veröffentlichen von Metrikdatenpunkten in CloudWatch unter dem AWS/FSx-Namespace.
- `route53` – Ermöglicht FSx, eine Amazon VPC einer privat gehosteten Zone zuzuordnen.
- `logs` – Ermöglicht FSx das Beschreiben und Schreiben in CloudWatch Logs-Protokollstreams. Auf diese Weise können Benutzer Dateizugriffs-Auditprotokolle für ein FSx for Windows File Server-Dateisystem an einen CloudWatch Logs-Stream senden.
- `firehose` – Ermöglicht FSx das Beschreiben und Schreiben in Amazon-Data-Firehose-Bereitstellungsdatenströme. Auf diese Weise können Benutzer die Dateizugriffs-Auditprotokolle für ein FSx for Windows File Server-Dateisystem in einem Amazon Data Firehose-Bereitstellungs-Stream veröffentlichen.

```
{
  "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-*"
}
]
```

Alle Aktualisierungen dieser Richtlinie werden unter beschrieben [Amazon-FSx-Aktualisierungen für - AWS verwaltete Richtlinien](#).

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigungen](#) im IAM-Benutzerhandbuch.

## Erstellen einer serviceverknüpften Rolle für Amazon FSx

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein Dateisystem in der AWS Management Console, der IAM-CLI oder der IAM-API erstellen, erstellt Amazon FSx die serviceverknüpfte Rolle für Sie.

### Important

Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Weitere Informationen finden Sie unter [Eine neue Rolle ist in meinem IAM-Konto erschienen](#).

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie ein Dateisystem erstellen, erstellt Amazon FSx die serviceverknüpfte Rolle erneut für Sie.

## Bearbeiten einer serviceverknüpften Rolle für Amazon FSx

Amazon FSx erlaubt es Ihnen nicht, die serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

## Löschen einer serviceverknüpften Rolle für Amazon FSx

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch alle Ihre Dateisysteme und Backups löschen, bevor Sie die serviceverknüpfte Rolle manuell löschen können.

### Note

Wenn der Amazon-FSx-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die -serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Leitfaden.

## Unterstützte Regionen für serviceverknüpfte Amazon-FSx-Rollen

Amazon FSx unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [AWS Regionen und Endpunkte](#).


## Konformitätsprüfung für Amazon FSx for Windows File Server

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt](#), finden Sie unter [Umfang nach Compliance-Programm AWS-Services unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter heruntergeladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte heruntergeladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

 Note

AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der [Referenz für HIPAA-berechtigte Services](#).

- [AWS Compliance-Ressourcen](#) — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#)— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).
- [Amazon GuardDuty](#) — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- [AWS Audit Manager](#)— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

# Amazon FSx for Windows File Server und Schnittstellen-VPC-Endpunkte

Sie können die Sicherheit Ihrer VPC verbessern, indem Sie Amazon FSx so konfigurieren, dass ein Schnittstellen-VPC-Endpunkt verwendet wird. Schnittstellen-VPC-Endpunkte werden unterstützt von [AWS PrivateLink](#), einer Technologie, die es Ihnen ermöglicht, ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung privat auf Amazon FSx-APIs zugreifen zu können. AWS Direct Connect-Verbindung. Die Instances in Ihrer VPC benötigen für die Kommunikation mit Amazon FSx-APIs keine öffentlichen IP-Adressen. Datenverkehr zwischen Ihrer VPC und Amazon FSx verlässt die AWS-Netzwerk.

Jeder Schnittstellen-VPC-Endpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt. Eine Netzwerkschnittstelle stellt eine private IP-Adresse bereit, die als Einstiegspunkt für den Datenverkehr zur Amazon FSx API dient.

## Überlegungen zu Amazon FSx Schnittstellen-VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Amazon FSx einrichten, überprüfen Sie unbedingt [Eigenschaften und Einschränkungen des Schnittstellen-VPC-Endpunkts](#) im Amazon VPC User Guide aus.

Sie können alle Amazon FSx API-Operationen von Ihrer VPC aus aufrufen. Sie können beispielsweise ein FSx for Windows File Server-Dateisystem erstellen, indem Sie die CreateFileSystem API aus Ihrer VPC heraus. Die vollständige Liste der Amazon FSx-APIs finden Sie unter [Aktionen](#) in der Amazon FSx API-Referenz.

## Überlegungen zu VPC-Peering

Sie können andere VPCs mit Schnittstellen-VPC-Endpunkten über VPC-Peering mit der VPC verbinden. VPC-Peering ist eine Netzwerkverbindung zwischen zwei VPCs. Sie können eine VPC-Peering-Verbindung zwischen Ihren eigenen beiden VPCs oder mit einer VPC in einer anderen herstellen AWS-Konto aus. Die VPCs können auch in zwei verschiedenen sein AWS-Regionen aus.

Der Datenverkehr zwischen über Peering verbundenen VPCs bleibt im AWS-Netzwerk und wird nicht über das öffentliche Internet übertragen. Sobald VPCs per Peering verbunden sind, können Ressourcen wie Amazon-Elastic-Compute-Cloud Elastic Compute Cloud (Amazon EC2) -Instances in beiden VPCs über Schnittstellen-VPC-Endpunkte, die in einem der VPCs erstellt wurden, auf die Amazon FSx API zugreifen.



## Erstellen eines Schnittstellen-VPC-Endpunkts für die Amazon FSx API

Sie können einen VPC-Endpunkt für die Amazon FSx API mithilfe der Amazon VPC-Konsole oder der AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter [Erstellen eines Schnittstellen-VPC-Endpunkts](#) im Amazon VPC User Guide aus.

Um einen Schnittstellen-VPC-Endpunkt für Amazon FSx zu erstellen, verwenden Sie einen der folgenden Optionen:

- **com.amazonaws.region.fsx**— Erstellt einen Endpunkt für Amazon FSx API-Operationen.
- **com.amazonaws.region.fsx-fips**— Erstellt einen Endpunkt für die Amazon FSx API, der den entspricht [Federal Information Processing Standard \(FIPS\) 140-2](#) aus.

Um die private DNS-Option verwenden zu können, müssen Sie die `enableDnsHostnames` und `enableDnsSupport` Attribute Ihrer VPC. Weitere Informationen finden Sie unter [Anzeigen und Aktualisieren des DNS-Supports für Ihre VPC](#) im Amazon VPC User Guide aus.

**EXCDEAWS-Regionen** Wenn Sie einen privaten DNS für den Endpunkt aktivieren, können Sie API-Anforderungen an Amazon FSx senden, indem VPC seinen standardmäßigen DNS-Namen für die AWS-Region, zum Beispiel `fsx.us-east-1.amazonaws.com` aus. Für China (Peking) und China (Ningxia) AWS-Regionen können Sie API-Anforderungen mit dem VPC-Endpunkt mittels `fsx-api.cn-north-1.amazonaws.com.cn` und `fsx-api.cn-northwest-1.amazonaws.com.cn` bzw.

Weitere Informationen finden Sie unter [Zugriff auf einen Service über einen Schnittstellen-VPC-Endpunkt](#) im Amazon VPC User Guide aus.

## Erstellen einer VPC-Endpunkt-Richtlinie für Amazon FSx

Um den Zugriff auf die Amazon FSx API weiter zu kontrollieren, können Sie optional eine AWS Identity and Access Management (IAM) -Richtlinie zu Ihrem VPC-Endpunkt. Die Richtlinie legt Folgendes fest:

- Prinzipal, der die Aktionen ausführen kann
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter [Steuerung des Zugriffs auf Services mit VPC-Endpunkten](#) im Amazon-VPC-Benutzerhandbuch.

# Kontingente

Im Folgenden erfahren Sie mehr über die Kontingente bei der Arbeit mit Amazon FSx for Windows File Server.

## Themen

- [Kontingente, die Sie erhöhen können](#)
- [Ressourcenkontingente für jedes Dateisystem](#)
- [Weitere Überlegungen](#)
- [Kontingente für Microsoft Windows](#)

## Kontingente, die Sie erhöhen können

Im Folgenden finden Sie die Kontingente für Amazon FSx for Windows File Server für jede AWS-Konto, pro AWS-Region, die Sie erhöhen können.

| Ressource                     | Standard | Beschreibung                                                                                                                           |
|-------------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------|
| Windows-Dateisysteme          | 100      | Die maximale Anzahl der Dateisysteme von Amazon FSx für Windows Server, die Sie in diesem Konto erstellen können.                      |
| Windows-Durchsatzkapazität    | 10240    | Die Gesamtmenge der Durchsatzkapazität (in Mbit/s), die für alle Dateisysteme von Amazon FSx für Windows in diesem Konto zulässig ist. |
| Windows-HDD-Speicherkapazität | 524288   | Die maximale Festplattenspeicherkapazität (in GiB), die für alle Dateisysteme von Amazon FSx für Windows                               |

| Ressource                     | Standard | Beschreibung                                                                                                                                                 |
|-------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               |          | File Server in diesem Konto zulässig ist.                                                                                                                    |
| Windows-SSD-Speicherkapazität | 524288   | Die maximal zulässige SSD-Speicherkapazität (in GiB) für alle Dateisysteme von Amazon FSx für Windows File Server in diesem Konto.                           |
| Gesamt-SSD-IOPS für Windows   | 500 000  | Die Gesamtmenge der SSD-IOPS, die für alle Dateisysteme von Amazon FSx für Windows File Server in diesem Konto zulässig ist.                                 |
| Windows-Backups               | 500      | Die maximale Anzahl der vom Benutzer initiierten Backups für alle Dateisysteme von Amazon FSx für Windows File Server, die Sie in diesem Konto haben können. |

So fordern Sie eine Kontingenterhöhung an

1. Öffnen Sie die [Service Quotas-Konsole](#).
2. Wählen Sie im Navigationsbereich AWS-Services.
3. Wählen Sie Amazon FSx .
4. Wählen Sie ein Kontingent aus.
5. Wählen Sie Kontingenterhöhung anfordern und folgen Sie den Anweisungen, um eine Kontingenterhöhung anzufordern.
6. Um den Status der Kontingentanforderung anzuzeigen, wählen Sie im Navigationsbereich der Konsole die Option Verlauf der Kontingentanforderung aus.

Weitere Informationen finden Sie unter [Beantragen einer Kontingenterhöhung](#) im Service-Quotas-Benutzerhandbuch.

## Ressourcenkontingente für jedes Dateisystem

Im Folgenden sind die Kontingente für Amazon FSx for Windows File Server-Ressourcen für jedes Dateisystem in einer aufgeführten AWS-Region.

| Ressource                                                                                                    | Limit pro Dateisystem |
|--------------------------------------------------------------------------------------------------------------|-----------------------|
| Maximale Anzahl von Tags                                                                                     | 50                    |
| Maximale Aufbewahrungsdauer für automatisierte Backups                                                       | 90 Tage               |
| Maximale Anzahl von Backup-Kopieranforderungen, die pro Konto an eine einzelne Zielregion ausgeführt werden. | 5                     |
| Minimale Speicherkapazität, SSD-Dateisysteme                                                                 | 32 GiB                |
| Minimale Speicherkapazität, HDD-Dateisysteme                                                                 | 2 000 GiB             |
| Maximale Speicherkapazität, SSD und HDD                                                                      | 64 TiB                |
| Minimale SSD-IOPS                                                                                            | 96                    |
| Maximale SSD-IOPS                                                                                            | 400 000               |
| Minimale Durchsatzkapazität                                                                                  | 8 MBps                |
| Maximale Durchsatzkapazität                                                                                  | 12 288 MBps           |
| Maximale Anzahl von Dateifreigaben                                                                           | 100 000               |

## Weitere Überlegungen

Beachten Sie außerdem Folgendes:

- Sie können jeden AWS Key Management Service (AWS KMS)-Schlüssel auf bis zu 125 Amazon-FSx-Dateisystemen verwenden.
- Eine Liste der , AWS-Regionen in denen Sie Dateisysteme erstellen können, finden Sie unter [Amazon-FSx-Endpunkte und -Kontingente](#) im Allgemeine AWS-Referenz.
- Sie ordnen Ihre Dateifreigaben von Amazon EC2-Instances in Ihrer Virtual Private Cloud (VPC) ihren DNS-Namen (Domain Name Service) zu.

## Kontingente für Microsoft Windows

Weitere Informationen finden Sie unter [NTFS](#)-Limits im Microsoft Windows Dev Center.

# Problembhebung bei Amazon FSx

Verwenden Sie die folgenden Abschnitte, um Probleme mit Amazon FSx zu beheben.

Wenn Sie bei der Nutzung von Amazon FSx auf Probleme stoßen, die im Folgenden nicht aufgeführt sind, versuchen Sie, eine Frage im [Amazon FSx-Forum](#) zu stellen.

## Themen

- [Sie können nicht auf Ihr Dateisystem zugreifen](#)
- [Das Erstellen eines neuen Amazon FSx-Dateisystems schlägt fehl](#)
- [Das Dateisystem befindet sich in einem falsch konfigurierten Zustand](#)
- [Problembehandlung mit Remote Power Shell auf FSx for Windows File Server](#)
- [Sie können DFS-R nicht auf einem Multi-AZ- oder Single-AZ 2-Dateisystem konfigurieren](#)
- [Aktualisierungen der Speicher- oder Durchsatzkapazität schlagen fehl](#)
- [Das Umschalten des Speichertyps auf Festplatte während der Wiederherstellung eines Backups schlägt fehl](#)
- [Problembehandlung bei Schattenkopien](#)
- [Behebung von Leistungsproblemen mit dem Dateisystem](#)

## Sie können nicht auf Ihr Dateisystem zugreifen

Es gibt eine Reihe möglicher Ursachen dafür, dass Sie nicht auf Ihr Dateisystem zugreifen können. Jede davon hat ihre eigene Lösung, wie folgt.

## Themen

- [Die elastic network interface des Dateisystems wurde geändert oder gelöscht](#)
- [Die Elastic IP-Adresse, die an die elastic network interface des Dateisystems angehängt ist, wurde gelöscht.](#)
- [Der Sicherheitsgruppe des Dateisystems fehlen die erforderlichen Regeln für eingehenden oder ausgehenden Datenverkehr.](#)
- [In der Sicherheitsgruppe der Compute-Instanz fehlen die erforderlichen Regeln für ausgehenden Datenverkehr](#)

- [Die Compute-Instanz ist nicht mit einem Active Directory verbunden](#)
- [Die Dateifreigabe ist nicht vorhanden](#)
- [Dem Active Directory-Benutzer fehlen die erforderlichen Berechtigungen](#)
- [Vollzugriff zulassen: NTFS-ACL-Berechtigungen wurden entfernt](#)
- [Mit einem lokalen Client kann nicht auf ein Dateisystem zugegriffen werden](#)
- [Das neue Dateisystem ist nicht im DNS registriert](#)
- [Mit einem DNS-Alias kann nicht auf das Dateisystem zugegriffen werden](#)
- [Über eine IP-Adresse kann nicht auf das Dateisystem zugegriffen werden](#)

## Die elastic network interface des Dateisystems wurde geändert oder gelöscht

Sie dürfen die elastic network interface des Dateisystems nicht ändern oder löschen. Das Ändern oder Löschen der Netzwerkschnittstelle kann zu einem dauerhaften Verbindungsverlust zwischen Ihrer VPC und Ihrem Dateisystem führen. Erstellen Sie ein neues Dateisystem und ändern oder löschen Sie die elastic network interface von Amazon FSx nicht. Weitere Informationen finden Sie unter [Dateisystem-Zugriffskontrolle mit Amazon VPC](#).

## Die Elastic IP-Adresse, die an die elastic network interface des Dateisystems angehängt ist, wurde gelöscht.

Amazon FSx unterstützt nicht den Zugriff auf Dateisysteme über das öffentliche Internet. Amazon FSx trennt automatisch jede Elastic IP-Adresse, bei der es sich um eine öffentliche IP-Adresse handelt, die über das Internet erreichbar ist und die an die elastic network interface eines Dateisystems angehängt wird. Weitere Informationen finden Sie unter [Unterstützte Clients, Zugriffsmethoden und Umgebungen für Amazon FSx for Windows File Server](#).

## Der Sicherheitsgruppe des Dateisystems fehlen die erforderlichen Regeln für eingehenden oder ausgehenden Datenverkehr.

Überprüfen Sie die unter angegebenen Regeln für eingehenden Datenverkehr und stellen Sie sicher [Amazon VPC-Sicherheitsgruppen](#), dass die Ihrem Dateisystem zugeordnete Sicherheitsgruppe über die entsprechenden Regeln für eingehenden Datenverkehr verfügt.



## In der Sicherheitsgruppe der Compute-Instanz fehlen die erforderlichen Regeln für ausgehenden Datenverkehr

Überprüfen Sie die unter angegebenen Regeln für ausgehenden Datenverkehr und stellen Sie sicher [Amazon VPC-Sicherheitsgruppen](#), dass die Ihrer Compute-Instance zugeordnete Sicherheitsgruppe über die entsprechenden Regeln für ausgehenden Datenverkehr verfügt.

## Die Compute-Instanz ist nicht mit einem Active Directory verbunden

Ihre Recheninstanzen sind möglicherweise nicht korrekt mit einem von zwei Active Directory-Typen verbunden:

- Das AWS Managed Microsoft AD Verzeichnis, mit dem Ihr Dateisystem verknüpft ist.
- Ein Microsoft Active Directory-Verzeichnis, für das eine unidirektionale Gesamtvertrauensstellung mit dem AWS Managed Microsoft AD Verzeichnis eingerichtet wurde.

Stellen Sie sicher, dass Ihre Recheninstanzen mit einem von zwei Verzeichnistypen verknüpft sind. Ein Typ ist das AWS Managed Microsoft AD Verzeichnis, mit dem Ihr Dateisystem verknüpft ist. Der andere Typ ist ein Microsoft Active Directory-Verzeichnis, für das eine unidirektionale Gesamtvertrauensstellung mit dem AWS Managed Microsoft AD Verzeichnis eingerichtet wurde. Weitere Informationen finden Sie unter [Verwenden von Amazon FSx mit AWS Directory Service for Microsoft Active Directory](#).

## Die Dateifreigabe ist nicht vorhanden

Die Microsoft Windows-Dateifreigabe, auf die Sie zugreifen möchten, ist nicht vorhanden.

Wenn Sie eine bestehende Dateifreigabe verwenden, stellen Sie sicher, dass der DNS-Name und der Freigabename des Dateisystems korrekt angegeben sind. Informationen zur Verwaltung Ihrer Dateifreigaben finden Sie unter [Verwaltung von Dateifreigaben auf FSx for Windows File Server Server-Dateisystemen](#).

## Dem Active Directory-Benutzer fehlen die erforderlichen Berechtigungen

Dem Active Directory-Benutzer, als den Sie auf die Dateifreigabe zugreifen, fehlen die erforderlichen Zugriffsberechtigungen.

Stellen Sie sicher, dass die Zugriffsberechtigungen für die Dateifreigabe und die Windows-Zugriffssteuerungslisten (ACLs) für den freigegebenen Ordner den Active Directory-Benutzern, die darauf zugreifen müssen, Zugriff gewähren.

## Vollzugriff zulassen: NTFS-ACL-Berechtigungen wurden entfernt

Wenn Sie die Option NTFS-ACL-Rechte mit Vollzugriff für den SYSTEM-Benutzer in einem von Ihnen freigegebenen Ordner deaktivieren, kann auf diese Freigabe nicht mehr zugegriffen werden, und alle Dateisystemsicherungen, die ab diesem Zeitpunkt erstellt wurden, können möglicherweise nicht mehr verwendet werden.

Sie müssen die betroffene Dateifreigabe neu erstellen. Weitere Informationen finden Sie unter [Verwaltung von Dateifreigaben auf FSx for Windows File Server Server-Dateisystemen](#). Nachdem Sie den Ordner oder die Freigabe neu erstellt haben, können Sie die Windows-Dateifreigaben Ihrer Recheninstanzen zuordnen und verwenden.

## Mit einem lokalen Client kann nicht auf ein Dateisystem zugegriffen werden

Sie verwenden Ihr Amazon FSx-Dateisystem lokal AWS Direct Connect oder über VPN und Sie verwenden einen nicht privaten IP-Adressbereich für den lokalen Client.

Amazon FSx unterstützt nur den Zugriff von lokalen Clients mit nicht privaten IP-Adressen auf Dateisystemen, die nach dem 17. Dezember 2020 erstellt wurden.

Wenn Sie auf Ihr Dateisystem FSx for Windows File Server zugreifen müssen, das vor dem 17. Dezember 2020 mit einem nicht privaten IP-Adressbereich erstellt wurde, können Sie ein neues Dateisystem erstellen, indem Sie eine Sicherungskopie des Dateisystems wiederherstellen. Weitere Informationen finden Sie unter [Arbeiten mit Backups](#).

## Das neue Dateisystem ist nicht im DNS registriert

Für Dateisysteme, die mit einem selbstverwalteten Active Directory verbunden sind, hat Amazon FSx das Dateisystem-DNS bei der Erstellung nicht registriert, da das Kundennetzwerk kein Microsoft DNS verwendet.

Amazon FSx registriert Dateisysteme nicht in DNS, wenn Ihr Netzwerk einen DNS-Service eines Drittanbieters anstelle von Microsoft DNS verwendet. Sie müssen DNS-A-Einträge für Ihre Amazon FSx-Dateisysteme manuell einrichten. Für Single-AZ 1-Dateisysteme müssen Sie einen DNS-A-Eintrag hinzufügen; für Single-AZ 2- und Multi-AZ-Dateisysteme müssen Sie zwei DNS-A-Einträge

hinzufügen. Gehen Sie wie folgt vor, um die IP-Adresse oder Adressen des Dateisystems abzurufen, die Sie beim manuellen Hinzufügen der DNS-A-Einträge verwenden möchten.

1. Wählen Sie [unter `https://console.aws.amazon.com/fsx/`](https://console.aws.amazon.com/fsx/) das Dateisystem aus, dessen IP-Adresse Sie abrufen möchten, um die Seite mit den Dateisystemdetails anzuzeigen.
2. Führen Sie auf der Registerkarte Netzwerk und Sicherheit einen der folgenden Schritte aus:
  - Für ein Single-AZ 1-Dateisystem:
    - Wählen Sie im Bereich Subnet die elastic network interface aus, die unter Netzwerkschnittstelle angezeigt wird, um die Seite Netzwerkschnittstellen in Amazon EC2 zu öffnen.
    - Die IP-Adresse für das zu verwendende Single-AZ 1-Dateisystem wird in der Spalte Primäre private IPv4-IP angezeigt.
  - Für ein Single-AZ 2- oder Multi-AZ-Dateisystem:
    - Wählen Sie im Bereich Bevorzugtes Subnetz die elastic network interface aus, die unter Netzwerkschnittstelle angezeigt wird, um die Seite Netzwerkschnittstellen in Amazon EC2 zu öffnen.
    - Die IP-Adresse für das bevorzugte zu verwendende Subnetz wird in der Spalte Sekundäre private IPv4-IP angezeigt.
    - Wählen Sie im Amazon FSx Standby-Subnetz-Panel die Elastic Network-Schnittstelle aus, die unter Netzwerkschnittstelle angezeigt wird, um die Seite Netzwerkschnittstellen in der Amazon EC2 EC2-Konsole zu öffnen.
    - Die IP-Adresse für das zu verwendende Standby-Subnetz wird in der Spalte Sekundäre private IPv4-IP angezeigt.

## Mit einem DNS-Alias kann nicht auf das Dateisystem zugegriffen werden

Wenn Sie mit einem DNS-Alias nicht auf ein Dateisystem zugreifen können, gehen Sie wie folgt vor, um das Problem zu beheben.

1. Stellen Sie sicher, dass der Alias dem Dateisystem zugeordnet ist, indem Sie einen der folgenden Schritte ausführen:
  - a. Verwenden der Amazon FSx-Konsole — Wählen Sie das Dateisystem aus, auf das Sie zugreifen möchten. Auf der Seite mit den Dateisystemdetails werden die DNS-Aliase auf der Registerkarte Netzwerk und Sicherheit angezeigt.

- b. Verwenden der CLI oder API — Verwenden Sie den [describe-file-system-aliases](#) CLI-Befehl oder die [DescribeFileSystemAliases](#) API-Operation, um die Aliase abzurufen, die derzeit mit dem Dateisystem verknüpft sind.
2. Wenn der DNS-Alias nicht aufgeführt ist, müssen Sie ihn dem Dateisystem zuordnen. Weitere Informationen finden Sie unter [Verwaltung von DNS-Aliassen auf vorhandenen Dateisystemen](#).
3. Wenn der DNS-Alias dem Dateisystem zugeordnet ist, stellen Sie sicher, dass Sie auch die folgenden erforderlichen Elemente konfiguriert haben:

- Es wurden Service Principal Names (SPNs) erstellt, die dem DNS-Alias auf dem Active Directory-Computerobjekt Ihres Amazon FSx-Dateisystems entsprechen.

Weitere Informationen finden Sie unter [Schritt 2: Konfigurieren Sie Service Principal Names \(SPNs\) für Kerberos](#).

- Es wurde ein DNS-CNAME-Eintrag für den DNS-Alias erstellt, der in den Standard-DNS-Namen des Amazon FSx-Dateisystems aufgelöst wird.

Weitere Informationen finden Sie unter [Schritt 3: Aktualisieren oder erstellen Sie einen DNS-CNAME-Eintrag für das Dateisystem](#).

4. Wenn Sie gültige SPNs und einen DNS-CNAME-Eintrag erstellt haben, stellen Sie sicher, dass das DNS des Clients über den DNS-CNAME-Eintrag verfügt, der in das richtige Dateisystem aufgelöst wird.
  - a. Führen Sie `nslookup` den Befehl aus, um zu überprüfen, ob der Eintrag vorhanden ist und ob er in den Standard-DNS-Namen des Dateisystems aufgelöst wird.
  - b. Wenn der DNS-CNAME in ein anderes Dateisystem aufgelöst wird, warten Sie, bis der DNS-Cache des Clients aktualisiert ist, und überprüfen Sie dann erneut den CNAME-Eintrag. Sie können den Vorgang beschleunigen, indem Sie den DNS-Cache des Clients mit dem folgenden Befehl leeren.

```
ipconfig /flushdns
```

5. Wenn der DNS-CNAME-Eintrag in das Standard-DNS des Amazon FSx-Dateisystems aufgelöst wird und der Client immer noch nicht auf das Dateisystem zugreifen kann, finden Sie weitere Schritte [Sie können nicht auf Ihr Dateisystem zugreifen](#) zur Fehlerbehebung unter.

## Über eine IP-Adresse kann nicht auf das Dateisystem zugegriffen werden

Wenn Sie nicht über eine IP-Adresse auf Ihr Dateisystem zugreifen können, versuchen Sie es stattdessen mit dem DNS-Namen oder dem zugehörigen DNS-Alias.

Sie finden den DNS-Namen des Dateisystems und alle zugehörigen DNS-Aliase auf der [Amazon FSx-Konsole](#), indem Sie Windows File Server, Network & Security wählen. Sie können sie auch in der Antwort auf die Operation [CreateFileSystem](#) oder die [DescribeFileSystems](#) API finden. Weitere Hinweise zur Verwendung von DNS-Aliassen finden Sie unter [DNS-Aliase verwalten](#).

- Für ein Single-AZ-Dateisystem, das mit einem AWS verwalteten Microsoft Active Directory verknüpft ist, sieht der DNS-Name wie folgt aus.

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

- Für alle Multi-AZ-Dateisysteme und Single-AZ-Dateisysteme, die zu einem selbstverwalteten Active Directory gehören, sieht der DNS-Name wie folgt aus.

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

## Das Erstellen eines neuen Amazon FSx-Dateisystems schlägt fehl

Es gibt eine Reihe möglicher Ursachen, wenn eine Anfrage zur Erstellung eines Dateisystems fehlschlägt, wie im folgenden Abschnitt beschrieben.

### Themen

- [Problembehandlung bei Dateisystemen, die mit einem AWS verwalteten Microsoft Active Directory verbunden sind](#)
- [Das Erstellen eines Dateisystems, das mit einem selbstverwalteten Active Directory verknüpft ist, schlägt fehl](#)

## Problembehandlung bei Dateisystemen, die mit einem AWS verwalteten Microsoft Active Directory verbunden sind

Verwenden Sie die folgenden Abschnitte, um Probleme beim Versuch zu beheben, ein FSx for Windows File Server Server-Dateisystem zu erstellen, das mit Ihrem selbstverwalteten Active Directory verknüpft ist.

## Falsch konfigurierte VPC-Sicherheitsgruppen und Netzwerk-ACLs

Stellen Sie sicher, dass die VPC-Sicherheitsgruppen und Netzwerk-ACLs mit der empfohlenen Sicherheitsgruppenkonfiguration konfiguriert sind. Weitere Informationen finden Sie unter [Sicherheitsgruppen erstellen](#).

## Das Erstellen eines Dateisystems, das mit einem selbstverwalteten Active Directory verknüpft ist, schlägt fehl

### Themen

- [Doppelte Gruppennamen für Dateisystemadministratoren](#)
- [DNS-Server oder Domänencontroller sind nicht erreichbar](#)
- [Ungültige Anmeldeinformationen für das Dienstkonto](#)
- [Unzureichende Dienstkontoberechtigungen](#)
- [Die Kapazität des Dienstkontos wurde überschritten](#)
- [Amazon FSx kann nicht auf die Organisationseinheit \(OU\) zugreifen](#)
- [Das Dienstkonto kann nicht auf die Administratorgruppe zugreifen](#)
- [Amazon FSx hat die Konnektivität in der Domain verloren](#)
- [Das Servicekonto hat nicht die richtigen Berechtigungen](#)
- [In Erstellungsparametern verwendete Unicode-Zeichen](#)

### Doppelte Gruppennamen für Dateisystemadministratoren

Das Erstellen eines Dateisystems, das mit Ihrem selbstverwalteten Active Directory verknüpft ist, schlägt fehl und es wird die folgende Fehlermeldung angezeigt:

```
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.
```

Amazon FSx hat das Dateisystem nicht erstellt, da es in der Domain mehrere Administratorgruppen mit demselben Namen gibt.

Wenn Sie keinen Gruppennamen angeben, versucht Amazon FSx, den Standardwert „Domain-Admins“ als Administratorgruppe zu verwenden. Die Anfrage schlägt fehl, wenn es mehr als eine Gruppe gibt, die den Standardnamen „Domain-Admins“ verwendet.

Gehen Sie wie folgt vor, um das Problem zu beheben.

1. Überprüfen Sie die [Voraussetzungen](#) für den Beitritt Ihres Dateisystems zu Ihrem selbstverwalteten Active Directory.
2. Verwenden Sie das [Amazon FSx Active Directory Validation Tool](#), um Ihre selbstverwaltete Active Directory-Konfiguration zu validieren, bevor Sie ein FSx for Windows File Server Server-Dateisystem erstellen, das mit einem selbstverwalteten Active Directory verknüpft ist.
3. Erstellen Sie ein neues Dateisystem mit dem oder der AWS Management Console oder der AWS CLI. Weitere Informationen finden Sie unter [Verbinden eines Amazon-FSx-Dateisystems mit einer selbstverwalteten Microsoft-Active-Directory-Domäne](#).
4. Geben Sie einen Namen für die Dateisystemadministratorgruppe ein, der in der Domäne Ihres selbstverwalteten Active Directory einzigartig ist.

## DNS-Server oder Domänencontroller sind nicht erreichbar


Das Erstellen eines Dateisystems, das mit Ihrem selbstverwalteten Active Directory verknüpft ist, schlägt fehl und es wird die folgende Fehlermeldung angezeigt:

```
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.
```

Gehen Sie wie folgt vor, um das Problem zu beheben.


1. Stellen Sie sicher, dass Sie die Voraussetzungen für die Einrichtung von Netzwerkkonnektivität und Routing zwischen dem Subnetz, in dem Sie ein Amazon FSx-Dateisystem erstellen, und Ihrem selbstverwalteten Active Directory erfüllt haben. Weitere Informationen finden Sie unter [Voraussetzungen für die Verwendung eines selbstverwalteten Microsoft Active Directory](#).

Verwenden Sie das [Amazon FSx Active Directory Validation Tool](#), um diese Netzwerkeinstellungen zu testen und zu verifizieren.

 Note

Wenn Sie mehrere Active Directory-Standorte definiert haben, stellen Sie sicher, dass die Subnetze in der VPC, die Ihrem Amazon FSx-Dateisystem zugeordnet sind, an einem Active Directory-Standort definiert sind und dass keine IP-Konflikte zwischen den Subnetzen in Ihrer VPC und den Subnetzen an Ihren anderen Standorten bestehen. Sie können diese Einstellungen mithilfe des MMC-Snap-Ins Active Directory-Standorte und -Dienste anzeigen und ändern.

2. Stellen Sie sicher, dass Sie die VPC-Sicherheitsgruppen, die Sie Ihrem Amazon FSx-Dateisystem zugeordnet haben, zusammen mit allen VPC-Netzwerk-ACLs so konfiguriert haben, dass ausgehender Netzwerkverkehr auf allen Ports zugelassen wird.

 Note

Wenn Sie Least-Privilegien implementieren möchten, können Sie ausgehenden Datenverkehr nur zu den spezifischen Ports zulassen, die für die Kommunikation mit den Active Directory-Domänencontrollern erforderlich sind. Weitere Informationen finden Sie in der [Microsoft Active Directory-Dokumentation](#).

3. Vergewissern Sie sich, dass die Werte für die administrativen Eigenschaften des Microsoft Windows-Dateiservers oder des Netzwerks keine anderen Zeichen als Latin-1 enthalten. Beispielsweise schlägt die Erstellung des Dateisystems fehl, wenn Sie den Namen der Domänen-Admins Gruppe der Dateisystemadministratoren verwenden.
4. Stellen Sie sicher, dass die DNS-Server und Domänencontroller Ihrer Active Directory-Domäne aktiv sind und auf Anfragen für die angegebene Domäne antworten können.
5. Stellen Sie sicher, dass die Funktionsebene Ihrer Active Directory-Domäne Windows Server 2008 R2 oder höher ist.
6. Stellen Sie sicher, dass die Firewall-Regeln auf den Domain-Controllern Ihrer Active Directory-Domäne Datenverkehr von Ihrem Amazon FSx-Dateisystem zulassen. Weitere Informationen finden Sie in der [Microsoft Active Directory-Dokumentation](#).



## Ungültige Anmeldeinformationen für das Dienstkonto

Das Erstellen eines Dateisystems, das mit einem selbstverwalteten Active Directory verknüpft ist, schlägt fehl und es wird die folgende Fehlermeldung angezeigt:

```
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.
```

Gehen Sie wie folgt vor, um das Problem zu beheben.

1. Stellen Sie sicher, dass Sie nur den Benutzernamen als Eingabe für den Benutzernamen des Dienstkontos eingeben, z. B. `ServiceAcct` in der selbstverwalteten Active Directory-Konfiguration.

### Important

Geben Sie bei der Eingabe des Benutzernamens für das Dienstkonto KEIN Domänenpräfix (`corp.com\ServiceAcctServiceAcct@corp.com`) oder Domänensuffix (`()`) an.

Verwenden Sie NICHT den definierten Namen (DN) bei der Eingabe des Benutzernamens für das Dienstkonto (`CN=ServiceAcct, OU=Example, DC=Corp, DC=com`).

2. Stellen Sie sicher, dass das von Ihnen angegebene Dienstkonto in Ihrer Active Directory-Domäne vorhanden ist.
3. Stellen Sie sicher, dass Sie die erforderlichen Berechtigungen an das von Ihnen angegebene Dienstkonto delegiert haben. Das Dienstkonto muss in der Lage sein, Computerobjekte in der Organisationseinheit in der Domäne zu erstellen und zu löschen, zu der Sie das Dateisystem hinzufügen. Das Dienstkonto muss außerdem mindestens über die folgenden Berechtigungen verfügen:
  - Zurücksetzen von Passwörtern
  - Beschränken Sie das Lesen und Schreiben von Daten durch Konten
  - Bestätigte Fähigkeit, in den DNS-Hostnamen zu schreiben
  - Überprüfte Fähigkeit zum Schreiben in den Prinzipalnamen des Service

Weitere Informationen zum Erstellen eines Dienstkontos mit den richtigen Berechtigungen finden Sie unter [Delegieren von Berechtigungen an Ihr Amazon-FSx-Servicekonto](#).

## Unzureichende Dienstkontoberechtigungen

Das Erstellen eines Dateisystems, das mit Ihrem selbstverwalteten Active Directory verknüpft ist, schlägt fehl und es wird die folgende Fehlermeldung angezeigt:

```
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.
```

Gehen Sie wie folgt vor, um das Problem zu beheben.

- Stellen Sie sicher, dass Sie die erforderlichen Berechtigungen an das von Ihnen angegebene Dienstkonto delegiert haben. Das Dienstkonto muss in der Lage sein, Computerobjekte in der Organisationseinheit in der Domäne zu erstellen und zu löschen, zu der Sie das Dateisystem hinzufügen. Das Dienstkonto muss außerdem mindestens über die folgenden Berechtigungen verfügen:
  - Zurücksetzen von Passwörtern
  - Beschränken Sie das Lesen und Schreiben von Daten durch Konten
  - Bestätigte Fähigkeit, in den DNS-Hostnamen zu schreiben
  - Überprüfte Fähigkeit zum Schreiben in den Prinzipalnamen des Service

Weitere Informationen zum Erstellen eines Dienstkontos mit den richtigen Berechtigungen finden Sie unter [Delegieren von Berechtigungen an Ihr Amazon-FSx-Servicekonto](#).

## Die Kapazität des Dienstkontos wurde überschritten

Das Erstellen eines Dateisystems, das mit Ihrem selbstverwalteten Active Directory verknüpft ist, schlägt fehl und es wird die folgende Fehlermeldung angezeigt:

```
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.
```

Um das Problem zu beheben, stellen Sie sicher, dass das von Ihnen angegebene Dienstkonto die maximale Anzahl von Computern erreicht hat, die es der Domäne hinzufügen kann. Wenn das maximale Limit erreicht wurde, erstellen Sie ein neues Dienstkonto mit den richtigen Berechtigungen. Verwenden Sie das neue Dienstkonto und erstellen Sie ein neues Dateisystem. Weitere Informationen finden Sie unter [Delegieren von Berechtigungen an Ihr Amazon-FSx-Servicekonto](#).

## Amazon FSx kann nicht auf die Organisationseinheit (OU) zugreifen

Das Erstellen eines Dateisystems, das mit Ihrem selbstverwalteten Active Directory verknüpft ist, schlägt fehl und es wird die folgende Fehlermeldung angezeigt:

```
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.
```

Gehen Sie wie folgt vor, um das Problem zu beheben.

1. Stellen Sie sicher, dass sich die von Ihnen angegebene Organisationseinheit in Ihrer Active Directory-Domäne befindet.
2. Stellen Sie sicher, dass Sie die erforderlichen Berechtigungen an das von Ihnen angegebene Dienstkonto delegiert haben. Das Dienstkonto muss in der Lage sein, Computerobjekte in der Organisationseinheit in der Domäne zu erstellen und zu löschen, zu der Sie das Dateisystem hinzufügen. Das Dienstkonto muss außerdem mindestens über die folgenden Berechtigungen verfügen:

- Zurücksetzen von Passwörtern
- Beschränken Sie das Lesen und Schreiben von Daten durch Konten
- Bestätigte Fähigkeit, in den DNS-Hostnamen zu schreiben
- Überprüfte Fähigkeit zum Schreiben in den Prinzipalnamen des Service
- Ihnen wurde die Kontrolle zum Erstellen und Löschen von Computerobjekten übertragen
- Bestätigte Fähigkeit, Kontoeinschränkungen zu lesen und zu schreiben

Weitere Informationen zum Erstellen eines Dienstkontos mit den richtigen Berechtigungen finden Sie unter [Delegieren von Berechtigungen an Ihr Amazon-FSx-Servicekonto](#).

## Das Dienstkonto kann nicht auf die Administratorgruppe zugreifen

Das Erstellen eines Dateisystems, das mit Ihrem selbstverwalteten Active Directory verknüpft ist, schlägt mit der folgenden Fehlermeldung fehl:

```
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.
```

Gehen Sie wie folgt vor, um das Problem zu beheben.

1. Stellen Sie sicher, dass Sie nur den Namen der Gruppe als Zeichenfolge für den Gruppenparameter des Administrators angeben.

### Important

Geben Sie KEIN Domänenpräfix (`corp.com\FSxAdmins`) oder Domänensuffix (`FSxAdmins@corp.com`) an, wenn Sie den Gruppennamenparameter angeben. Verwenden Sie NICHT den definierten Namen (DN) für die Gruppe. Ein Beispiel für einen eindeutigen Namen ist `CN=FSxAdmins, OU=Example, DC=Corp, DC=com`.

2. Stellen Sie sicher, dass die angegebene Administratorgruppe in derselben Active Directory-Domäne vorhanden ist wie die, zu der Sie das Dateisystem hinzufügen möchten.
3. Wenn Sie keinen Administratorgruppenparameter angegeben haben, versucht Amazon FSx, die Built-in Domain Admins Gruppe in Ihrer Active Directory-Domäne zu verwenden. Wenn der Name dieser Gruppe geändert wurde oder wenn Sie eine andere Gruppe für die Domänenverwaltung verwenden, müssen Sie diesen Namen für die Gruppe angeben.

## Amazon FSx hat die Konnektivität in der Domain verloren

Das Erstellen eines Dateisystems, das mit Ihrem selbstverwalteten Active Directory verknüpft ist, schlägt mit der folgenden Fehlermeldung fehl:

```
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.
```

Bei der Erstellung Ihres Dateisystems konnte Amazon FSx die DNS-Server und Domain-Controller Ihrer Active Directory-Domäne erreichen und das Dateisystem erfolgreich mit Ihrer Active Directory-Domäne verbinden. Beim Abschluss der Dateisystemerstellung hat Amazon FSx jedoch die Verbindung zu oder die Mitgliedschaft in Ihrer Domain verloren. Gehen Sie wie folgt vor, um das Problem zu beheben und zu lösen.

1. Stellen Sie sicher, dass die Netzwerkverbindung zwischen Ihrem Amazon FSx-Dateisystem und Ihrem Active Directory weiterhin besteht. Und stellen Sie mithilfe von Routingregeln, VPC-Sicherheitsgruppenregeln, VPC-Netzwerk-ACLs und Firewallregeln für Domänencontroller sicher, dass Netzwerkverkehr zwischen ihnen weiterhin zugelassen wird.
2. Stellen Sie sicher, dass die von Amazon FSx für Ihre Dateisysteme in Ihrer Active Directory-Domäne erstellten Computerobjekte noch aktiv sind und nicht gelöscht oder anderweitig manipuliert wurden.

## Das Servicekonto hat nicht die richtigen Berechtigungen

Das Erstellen eines Dateisystems, das mit Ihrem selbstverwalteten Active Directory verknüpft ist, schlägt fehl und es wird die folgende Fehlermeldung angezeigt:

```
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.

Stellen Sie sicher, dass Sie die erforderlichen Berechtigungen an das von Ihnen angegebene Dienstkonto delegiert haben. Gehen Sie wie folgt vor, um das Problem zu beheben.

Das Dienstkonto muss mindestens über die folgenden Berechtigungen verfügen:

- Ihnen wurde die Kontrolle zum Erstellen und Löschen von Computerobjekten in der Organisationseinheit übertragen, zu der Sie das Dateisystem hinzufügen
- Verfügen Sie in der Organisationseinheit, der Sie dem Dateisystem beitreten, über die folgenden Berechtigungen:
  - Fähigkeit, Passwörter zurückzusetzen
  - Möglichkeit, Konten am Lesen und Schreiben von Daten zu hindern
  - Bestätigte Fähigkeit, in den DNS-Hostnamen zu schreiben
  - Überprüfte Fähigkeit zum Schreiben in den Prinzipalnamen des Service
  - Fähigkeit (kann delegiert werden), Computerobjekte zu erstellen und zu löschen
  - Bestätigte Fähigkeit, Kontoeinschränkungen zu lesen und zu schreiben
  - Fähigkeit, Berechtigungen zu ändern

Weitere Informationen zum Erstellen eines Dienstkontos mit den richtigen Berechtigungen finden Sie unter [Delegieren von Berechtigungen an Ihr Amazon-FSx-Servicekonto](#).

## In Erstellungsparametern verwendete Unicode-Zeichen

Das Erstellen eines Dateisystems, das mit Ihrem selbstverwalteten Active Directory verknüpft ist, schlägt fehl und es wird die folgende Fehlermeldung angezeigt:

```
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.
```

Amazon FSx unterstützt keine Unicode-Zeichen. Stellen Sie sicher, dass keiner der Erstellungsparameter Unicode-Zeichen wie Akzentzeichen enthält. Dazu gehören auch Parameter, die leer gelassen werden können und bei denen ein Standardwert automatisch eingegeben wird. Stellen Sie sicher, dass die entsprechenden Standardwerte in Ihrem Active Directory auch keine Unicode-Zeichen enthalten.

Wenn Sie bei der Verwendung von Amazon FSx auf Probleme stoßen, die hier nicht aufgeführt sind, stellen Sie eine Frage im [Amazon FSx-Forum](#) oder wenden Sie sich an den [Amazon Web Services Services-Support](#).

## Das Dateisystem befindet sich in einem falsch konfigurierten Zustand

Ein Dateisystem von FSx for Windows File Server kann aufgrund einer Änderung in Ihrer Active Directory-Umgebung in einen falsch konfigurierten Zustand geraten. In diesem Zustand ist Ihr Dateisystem entweder derzeit nicht verfügbar oder es besteht die Gefahr, dass die Verfügbarkeit verloren geht, und Backups sind möglicherweise nicht erfolgreich.

Der Status Falsch konfiguriert enthält eine Fehlermeldung und empfohlene Korrekturmaßnahmen, auf die Sie über die Amazon FSx-Konsole, API oder zugreifen können. AWS CLI Nachdem Sie die Korrekturmaßnahme ergriffen haben, stellen Sie sicher, dass sich der Status Ihres Dateisystems irgendwann ändert. Beachten Sie, dass es mehrere Minuten dauern kann, Available bis diese Änderung abgeschlossen ist.

Ihr Dateisystem kann aus verschiedenen Gründen in den Status „Falsch konfiguriert“ geraten, z. B. aus den folgenden Gründen:

- Die IP-Adressen des DNS-Servers sind nicht mehr gültig.
- Die Anmeldeinformationen für das Dienstkonto sind nicht mehr gültig oder es fehlen die erforderlichen Berechtigungen.
- Der Active Directory-Domänencontroller ist aufgrund von Netzwerkverbindungsproblemen nicht erreichbar, z. B. aufgrund ungültiger VPC-Sicherheitsgruppen, VPC-Netzwerk-ACL- oder Routingtabellenkonfiguration oder Domänencontroller-Firewalleinstellungen.

(Die vollständige Liste der Active Directory-Anforderungen finden Sie unter [Voraussetzungen für die Verwendung eines selbstverwalteten Microsoft Active Directory](#) Sie können auch überprüfen, ob Ihre

Active Directory-Umgebung ordnungsgemäß konfiguriert ist, um diese Anforderungen zu erfüllen, indem Sie das [Amazon FSx Active Directory Validation Tool](#) verwenden.)

Um einige dieser Probleme zu lösen, müssen Sie einen oder mehrere Parameter in der [Active Directory-Konfiguration](#) Ihres Dateisystems direkt aktualisieren, z. B. die Änderung der IP-Adressen des DNS-Servers oder die Änderung des Benutzernamens oder des Kennworts des Dienstkontos. In diesen Fällen beinhaltet Ihre Korrekturmaßnahme zwangsläufig die Verwendung der Amazon FSx-Konsole, API oder AWS CLI die Aktualisierung der erforderlichen Konfigurationsparameter.

Bei anderen Problemen müssen möglicherweise keine Active Directory-Konfigurationsparameter geändert werden, z. B. das Ändern der Firewallinstellungen Ihres Domänencontrollers oder der VPC-Sicherheitsgruppen. In diesen Fällen müssen Sie jedoch weitere Maßnahmen ergreifen, bevor das Dateisystem dies tun kann. Available Nachdem Sie sichergestellt haben, dass Ihre Active Directory-Umgebung ordnungsgemäß konfiguriert ist, klicken Sie in der Amazon FSx-Konsole auf die Schaltfläche „Wiederherstellung versuchen“ neben dem Status „Fehlkonfiguriert“ oder verwenden Sie den `StartMisconfiguredStateRecovery` Befehl in der Amazon FSx-Konsole, API oder. AWS CLI

## Themen

- [Falsch konfiguriertes Dateisystem: Amazon FSx kann weder die DNS-Server noch die Domain-Controller für Ihre Domain erreichen.](#)
- [Falsch konfiguriertes Dateisystem: Die Anmeldeinformationen für das Dienstkonto sind ungültig](#)
- [Falsch konfiguriertes Dateisystem: Das angegebene Servicekonto ist nicht berechtigt, das Dateisystem mit der Domain zu verbinden](#)
- [Falsch konfiguriertes Dateisystem: Das Servicekonto kann keine weiteren Computer zur Domäne hinzufügen](#)
- [Falsch konfiguriertes Dateisystem: Das Servicekonto hat keinen Zugriff auf die Organisationseinheit](#)

## Falsch konfiguriertes Dateisystem: Amazon FSx kann weder die DNS-Server noch die Domain-Controller für Ihre Domain erreichen.

Ein Dateisystem geht in einen `Misconfigured` Zustand über, in dem Amazon FSx nicht mit Ihrem oder Ihren Microsoft Active Directory-Domänencontrollern kommunizieren kann.

Gehen Sie wie folgt vor, um dieses Problem zu lösen:



1. Stellen Sie sicher, dass Ihre Netzwerkkonfiguration den Datenverkehr vom Dateisystem zum Domänencontroller zulässt.
2. Verwenden Sie das [Amazon FSx Active Directory Validation Tool](#), um die Netzwerkeinstellungen für Ihr selbstverwaltetes Active Directory zu testen und zu verifizieren. Weitere Informationen finden Sie unter [Verwenden von Amazon FSx mit Ihrem selbstverwaltetem Microsoft Active Directory](#).
3. Überprüfen Sie die selbstverwaltete Active Directory-Konfiguration des Dateisystems in der Amazon FSx-Konsole.
4. Um die selbstverwaltete Active Directory-Konfiguration des Dateisystems zu aktualisieren, können Sie die Amazon FSx-Konsole verwenden.
  - a. Wählen Sie im Navigationsbereich Dateisysteme und dann das zu aktualisierende Dateisystem aus. Die Seite mit den Dateisystemdetails wird angezeigt.
  - b. Wählen Sie auf der Seite mit den Dateisystemdetails auf der Registerkarte Netzwerk und Sicherheit die Option Update aus.

Sie können auch den Amazon FSx `update-file-system` CLI-Befehl oder die API-Operation [UpdateFileSystem](#) verwenden.

## Falsch konfiguriertes Dateisystem: Die Anmeldeinformationen für das Dienstkonto sind ungültig

Amazon FSx kann keine Verbindung mit Ihrem oder Ihren Microsoft Active Directory-Domänencontrollern herstellen. Dies liegt daran, dass die angegebenen Anmeldeinformationen für das Dienstkonto ungültig sind. Weitere Informationen finden Sie unter [Verwenden von Amazon FSx mit Ihrem selbstverwaltetem Microsoft Active Directory](#).

Gehen Sie wie folgt vor, um die Fehlkonfiguration zu beheben:

1. Stellen Sie sicher, dass Sie das richtige Dienstkonto und die richtigen Anmeldeinformationen für dieses Konto verwenden.
2. Aktualisieren Sie dann mithilfe der Amazon FSx-Konsole die Konfiguration des Dateisystems mit dem richtigen Dienstkonto oder den richtigen Kontoanmeldeinformationen.
  - a. Wählen Sie im Navigationsbereich Dateisysteme und dann das falsch konfigurierte Dateisystem aus, das aktualisiert werden soll.

- b. Wählen Sie auf der Seite mit den Dateisystemdetails auf der Registerkarte Netzwerk und Sicherheit die Option Update aus.

Sie können auch den Amazon FSx-API-Vorgang `update-file-system` verwenden. Weitere Informationen finden Sie [UpdateFileSystem](#) in der Amazon FSx API-Referenz.

## Falsch konfiguriertes Dateisystem: Das angegebene Servicekonto ist nicht berechtigt, das Dateisystem mit der Domain zu verbinden

Amazon FSx kann keine Verbindung zu Ihren Microsoft Active Directory-Domain-Controllern herstellen. Dies liegt daran, dass das angegebene Dienstkonto nicht berechtigt ist, das Dateisystem mit der angegebenen Organisationseinheit der Domäne hinzuzufügen.

Gehen Sie wie folgt vor, um die Fehlkonfiguration zu beheben:

1. Fügen Sie dem Amazon FSx-Servicekonto die erforderlichen Berechtigungen hinzu oder erstellen Sie ein neues Dienstkonto mit den erforderlichen Berechtigungen. Weitere Informationen dazu finden Sie unter [Delegieren von Berechtigungen an Ihr Amazon-FSx-Servicekonto](#).
2. Aktualisieren Sie anschließend die selbstverwaltete Active Directory-Konfiguration des Dateisystems mit den neuen Anmeldeinformationen für das Dienstkonto. Um die Konfiguration zu aktualisieren, können Sie die Amazon FSx-Konsole verwenden.
  - a. Wählen Sie im Navigationsbereich Dateisysteme und dann das zu aktualisierende Dateisystem aus. Die Seite mit den Dateisystemdetails wird angezeigt.
  - b. Wählen Sie auf der Seite mit den Dateisystemdetails auf der Registerkarte Netzwerk und Sicherheit die Option Update aus.

Sie können auch den Amazon FSx-API-Vorgang `update-file-system` verwenden. Weitere Informationen finden Sie [UpdateFileSystem](#) in der Amazon FSx API-Referenz.

## Falsch konfiguriertes Dateisystem: Das Servicekonto kann keine weiteren Computer zur Domäne hinzufügen

Amazon FSx kann keine Verbindung zu Ihren Microsoft Active Directory-Domain-Controllern herstellen. In diesem Fall liegt dies daran, dass das angegebene Dienstkonto die maximale Anzahl von Computern erreicht hat, die es der Domäne hinzufügen kann.

Gehen Sie wie folgt vor, um die Fehlkonfiguration zu beheben:

1. Identifizieren Sie ein anderes Dienstkonto oder erstellen Sie ein neues Dienstkonto, mit dem neue Computer zur Domäne hinzugefügt werden können.
2. Aktualisieren Sie anschließend mithilfe der Amazon FSx-Konsole die selbstverwaltete Active Directory-Konfiguration des Dateisystems mit den neuen Anmeldeinformationen für das Dienstkonto.
  - a. Wählen Sie im Navigationsbereich Dateisysteme und dann das zu aktualisierende Dateisystem aus. Die Seite mit den Dateisystemdetails wird angezeigt.
  - b. Wählen Sie auf der Seite mit den Dateisystemdetails auf der Registerkarte Netzwerk und Sicherheit die Option Update aus.

Sie können auch den Amazon FSx-API-Vorgang `update-file-system` verwenden. Weitere Informationen finden Sie [UpdateFileSystem](#) in der Amazon FSx API-Referenz.

## Falsch konfiguriertes Dateisystem: Das Servicekonto hat keinen Zugriff auf die Organisationseinheit

Amazon FSx kann keine Verbindung zu Ihren Microsoft Active Directory-Domänencontrollern herstellen, da das angegebene Servicekonto keinen Zugriff auf die angegebene Organisationseinheit hat.

Gehen Sie wie folgt vor, um die Fehlkonfiguration zu beheben:

1. Identifizieren Sie ein anderes Dienstkonto, oder erstellen Sie ein neues Dienstkonto, das Zugriff auf die Organisationseinheit hat.
2. Aktualisieren Sie anschließend die selbstverwaltete Active Directory-Konfiguration des Dateisystems mit den neuen Anmeldeinformationen für das Dienstkonto.

- a. Wählen Sie im Navigationsbereich Dateisysteme und dann das zu aktualisierende Dateisystem aus. Daraufhin wird die Seite mit den Dateisystemdetails angezeigt.
- b. Wählen Sie auf der Seite mit den Dateisystemdetails auf der Registerkarte Netzwerk und Sicherheit die Option Update aus.

Sie können auch den Amazon FSx-API-Vorgang `update-file-system` verwenden. Weitere Informationen finden Sie [UpdateFileSystem](#) in der Amazon FSx API-Referenz.

## Problembehandlung mit Remote Power Shell auf FSx for Windows File Server

Sie können Ihre FSx for Windows File Server Server-Dateisysteme mit benutzerdefinierten PowerShell Fernverwaltungsbefehlen verwalten.

Themen

- [Der Befehl New-F schlägt bei unidirektionaler Vertrauensstellung fehl SxSmbShare](#)
- [Sie können mit Remote nicht auf Ihr Dateisystem zugreifen PowerShell](#)

### Der Befehl New-F schlägt bei unidirektionaler Vertrauensstellung fehl SxSmbShare

Amazon FSx unterstützt die Ausführung des `New-FSxSmbShare` PowerShell Befehls nicht in Fällen, in denen Sie eine unidirektionale Vertrauensstellung haben und die Domain, in der sich der Benutzer befindet, nicht so konfiguriert ist, dass sie der mit dem Amazon FSx-Dateisystem verknüpften Domain vertraut.

Sie können dieses Problem mit einer der folgenden Lösungen lösen:

- Der Benutzer, der den `New-FSxSmbShare` Befehl ausführt, muss sich in derselben Domäne wie das FSx-Dateisystem befinden.
- Sie können die `fsmgmt.msc`-GUI verwenden, um Freigaben in Ihrem Dateisystem zu erstellen. Weitere Informationen finden Sie unter [Verwaltung von Dateifreigaben mit der Benutzeroberfläche für gemeinsame Ordner](#).

## Sie können mit Remote nicht auf Ihr Dateisystem zugreifen PowerShell

Es gibt eine Reihe möglicher Ursachen dafür, dass Sie mit Remote PowerShell keine Verbindung zu Ihrem Dateisystem herstellen können. Jede davon hat ihre eigene Auflösung, wie folgt.

Um zunächst sicherzustellen, dass Sie erfolgreich eine Verbindung zum Windows Remote PowerShell Endpoint herstellen können, können Sie auch einen grundlegenden Konnektivitätstest durchführen. Sie können den `test-netconnection endpoint -port 5985` Befehl beispielsweise ausführen.

In der Sicherheitsgruppe des Dateisystems fehlen die erforderlichen Regeln für eingehende Nachrichten, um eine PowerShell Remoteverbindung zu ermöglichen

Die Sicherheitsgruppe des Dateisystems muss über eine Regel für eingehenden Datenverkehr verfügen, die Datenverkehr auf Port 5985 zulässt, um eine Remotesitzung einzurichten. PowerShell Weitere Informationen finden Sie unter [Amazon VPC-Sicherheitsgruppen](#).

Sie haben eine externe Vertrauensstellung zwischen dem AWS verwalteten Microsoft Active Directory und Ihrem lokalen Active Directory konfiguriert

Um Amazon FSx Remote PowerShell mit Kerberos-Authentifizierung zu verwenden, müssen Sie auf dem Client eine lokale Gruppenrichtlinie für die Gesamtsuchreihenfolge konfigurieren. Weitere Informationen finden Sie in der Microsoft-Dokumentation [Configure Kerberos Forest Search Order \(KFSO\)](#).

Beim Versuch, eine Remotesitzung zu starten, tritt ein Sprachlokalisierungsfehler auf PowerShell

Sie müssen Ihrem Befehl Folgendes `-SessionOption` hinzufügen: `-SessionOption (New-PSSessionOption -uiCulture "en-US")`

Im Folgenden finden Sie zwei Beispiele, die `-SessionOption` beim Initiieren einer PowerShell Remotesitzung auf Ihrem Dateisystem verwendet werden.

```
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")
```

## Sie können DFS-R nicht auf einem Multi-AZ- oder Single-AZ 2-Dateisystem konfigurieren

Microsoft Distributed File System Replication (DFS-R) wird auf Multi-AZ- und Single-AZ 2-Dateisystemen nicht unterstützt.

Multi-AZ-Dateisysteme sind nativ für Redundanz über mehrere Zugriffszonen hinweg konfiguriert. Verwenden Sie den Multi-AZ-Bereitstellungstyp für hohe Verfügbarkeit in mehreren Availability Zones. Weitere Informationen finden Sie unter [Verfügbarkeit und Haltbarkeit: Single-AZ- und Multi-AZ-Dateisysteme](#).

## Aktualisierungen der Speicher- oder Durchsatzkapazität schlagen fehl

Es gibt eine Reihe möglicher Ursachen dafür, dass Anfragen zur Aktualisierung der Dateisystemspeicher- und Durchsatzkapazität fehlschlagen, wobei jede davon ihre eigene Lösung hat.

### Die Erhöhung der Speicherkapazität schlägt fehl, weil Amazon FSx nicht auf den KMS-Verschlüsselungsschlüssel des Dateisystems zugreifen kann

Eine Anfrage zur Erhöhung der Speicherkapazität schlug fehl, da Amazon FSx nicht auf den Verschlüsselungsschlüssel des Dateisystems AWS Key Management Service (AWS KMS) zugreifen konnte.

Sie müssen sicherstellen, dass Amazon FSx Zugriff auf den AWS KMS Schlüssel hat, um die Verwaltungsaktion ausführen zu können. Verwenden Sie die folgenden Informationen, um das Problem mit dem Schlüsselzugriff zu lösen.

- Wenn der KMS-Schlüssel gelöscht wurde, müssen Sie mithilfe eines neuen KMS-Schlüssels aus einer Sicherung ein neues Dateisystem erstellen. Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 2: Erstellen eines Dateisystems aus einer Sicherung](#). Sie können die Anfrage erneut versuchen, nachdem das neue Dateisystem verfügbar ist.

- Wenn der KMS-Schlüssel deaktiviert ist, aktivieren Sie ihn erneut und wiederholen Sie dann die Anforderung zur Erhöhung der Speicherkapazität. Weitere Informationen finden Sie unter [Schlüssel aktivieren und deaktivieren](#) im Entwicklerhandbuch.AWS Key Management Service
- Wenn der Schlüssel aufgrund seines ausstehenden Löschvorgangs ungültig ist, müssen Sie mithilfe eines neuen KMS-Schlüssels aus einer Sicherung ein neues Dateisystem erstellen. Sie können die Anfrage erneut versuchen, nachdem das neue Dateisystem verfügbar ist. Weitere Informationen finden Sie unter [Exemplarische Vorgehensweise 2: Erstellen eines Dateisystems aus einer Sicherung](#).
- Wenn der Schlüssel aufgrund des ausstehenden Imports ungültig ist, müssen Sie warten, bis der Import abgeschlossen ist, und dann erneut versuchen, die Anforderung zur Speichererweiterung zu stellen.
- Wenn das Grant-Limit des Schlüssels überschritten wurde, müssen Sie eine Erhöhung der Anzahl der Grants für den Schlüssel beantragen. Weitere Informationen finden Sie unter [Ressourcenkontingente](#) im AWS Key Management Service Entwicklerhandbuch. Wenn die Erhöhung des Kontingents gewährt wurde, wiederholen Sie die Anfrage zur Speichererhöhung.

## Die Aktualisierung der Speicher- oder Durchsatzkapazität schlägt fehl, weil das selbstverwaltete Active Directory falsch konfiguriert ist

Die Anfrage zur Aktualisierung der Speicherkapazität oder der Durchsatzkapazität ist fehlgeschlagen, weil sich das selbstverwaltete Active Directory Ihres Dateisystems in einem falsch konfigurierten Zustand befindet.

Informationen zur Behebung eines bestimmten fehlerhaft konfigurierten Zustands finden Sie unter [Das Dateisystem befindet sich in einem falsch konfigurierten Zustand](#)

## Die Erhöhung der Speicherkapazität schlägt aufgrund unzureichender Durchsatzkapazität fehl

Die Anforderung zur Erhöhung der Speicherkapazität ist fehlgeschlagen, da die Durchsatzkapazität des Dateisystems auf 8 MB/s festgelegt ist.

Erhöhen Sie die Durchsatzkapazität des Dateisystems auf mindestens 16 MB/s und wiederholen Sie dann die Anforderung. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

## Die Aktualisierung der Durchsatzkapazität auf 8 MB/s schlägt fehl

Eine Anfrage zur Änderung der Durchsatzkapazität eines Dateisystems auf 8 MB/s ist fehlgeschlagen.

Dies kann der Fall sein, wenn eine Anfrage zur Erhöhung der Speicherkapazität aussteht oder gerade bearbeitet wird. Für die Erhöhung der Speicherkapazität ist ein Mindestdurchsatz von 16 MB/s erforderlich. Warten Sie, bis die Anfrage zur Erhöhung der Speicherkapazität abgeschlossen ist, und wiederholen Sie dann die Anfrage zur Änderung der Durchsatzkapazität.

## Das Umschalten des Speichertyps auf Festplatte während der Wiederherstellung eines Backups schlägt fehl

Das Erstellen eines Dateisystems aus einer Sicherung schlägt fehl und es wird die folgende Fehlermeldung angezeigt:

```
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.
```

Dieses Problem tritt auf, wenn Sie ein Backup wiederherstellen und Sie den Speichertyp von SSD auf HDD geändert haben. Die Wiederherstellung aus dem Backup schlägt fehl, weil das Backup, das Sie wiederherstellen, erstellt wurde, während im ursprünglichen Dateisystem noch eine Erhöhung der Speicherkapazität im Gange war. Die SSD-Speicherkapazität des Dateisystems vor der Erhöhungsanforderung betrug weniger als 2000 GiB. Dies ist die Mindestspeicherkapazität, die für die Erstellung eines HDD-Dateisystems erforderlich ist.

Gehen Sie wie folgt vor, um dieses Problem zu beheben.

1. Warten Sie, bis die Anforderung zur Erhöhung der Speicherkapazität abgeschlossen ist und das Dateisystem über mindestens 2000 GiB SSD-Speicherkapazität verfügt. Weitere Informationen finden Sie unter [Überwachung: Die Speicherkapazität nimmt zu](#).
2. Erstellen Sie eine vom Benutzer initiierte Sicherung des Dateisystems. Weitere Informationen finden Sie unter [Arbeiten mit vom Benutzer initiierten Backups](#).



3. Stellen Sie das vom Benutzer initiierte Backup mithilfe von Festplattenspeicher in einem neuen Dateisystem wieder her. Weitere Informationen finden Sie unter [Wiederherstellen von Sicherungen](#).

## Problembehandlung bei Schattenkopien

Es gibt eine Reihe möglicher Ursachen dafür, dass Schattenkopien fehlen oder nicht darauf zugegriffen werden kann, wie im folgenden Abschnitt beschrieben.

### Themen

- [Die ältesten Schattenkopien fehlen](#)
- [Alle meine Schattenkopien fehlen](#)
- [Auf einem kürzlich wiederhergestellten oder aktualisierten Dateisystem können keine Amazon FSx-Backups erstellt oder auf Schattenkopien zugegriffen werden](#)

### Die ältesten Schattenkopien fehlen

Die ältesten Schattenkopien werden in einer der folgenden Situationen gelöscht:

- Wenn Sie über 500 Schattenkopien verfügen, ersetzt die nächste Schattenkopie die älteste Schattenkopie, unabhängig vom verbleibenden zugewiesenen Speicherplatz auf dem Volume für Schattenkopien.
- Wenn die konfigurierte maximale Speichermenge für Schattenkopien erreicht ist, ersetzt die nächste Schattenkopie eine oder mehrere der ältesten Schattenkopien, auch wenn Sie über weniger als 500 Schattenkopien verfügen.

Bei beiden Ergebnissen handelt es sich um erwartetes Verhalten. Wenn Ihnen nicht genügend Speicherplatz für Schattenkopien zugewiesen ist, sollten Sie erwägen, den zugewiesenen Speicherplatz zu erhöhen.

### Alle meine Schattenkopien fehlen

Eine unzureichende I/O-Leistungskapazität in Ihrem Dateisystem (z. B. weil Sie Festplattenspeicher verwenden, weil der Festplattenspeicher keine Burst-Kapazität mehr hat oder weil die Durchsatzkapazität nicht ausreicht) kann dazu führen, dass alle Schattenkopien von Windows Server gelöscht werden, da Windows Server die Schattenkopien nicht mit der verfügbaren I/O-

Leistungskapazität verwalten kann. Beachten Sie die folgenden Empfehlungen, um dieses Problem zu vermeiden:

- Wenn Sie Festplattenspeicher verwenden, verwenden Sie die Amazon FSx-Konsole oder die Amazon FSx-API, um zur Verwendung von SSD-Speicher zu wechseln. Weitere Informationen finden Sie unter [Speichertyp verwalten](#).
- Erhöhen Sie die Durchsatzkapazität des Dateisystems auf einen Wert, der dreimal so hoch ist wie Ihre erwartete Arbeitslast.
- Stellen Sie sicher, dass Ihr Dateisystem zusätzlich zu der konfigurierten maximalen Speichermenge für Schattenkopien über mindestens 320 MB freien Speicherplatz verfügt.
- Planen Sie Schattenkopien, wenn Sie davon ausgehen, dass sich Ihr Dateisystem im Leerlauf befindet.

Weitere Informationen finden Sie unter [Dateisystemempfehlungen für Schattenkopien](#).

**Auf einem kürzlich wiederhergestellten oder aktualisierten Dateisystem können keine Amazon FSx-Backups erstellt oder auf Schattenkopien zugegriffen werden**

Dieses Verhalten wird erwartet. Amazon FSx erstellt den Schattenkopie-Status auf einem kürzlich wiederhergestellten Dateisystem neu und erlaubt während der Wiederherstellung des Schattenkopiestatus keinen Zugriff auf Schattenkopien oder Backups.

## Behebung von Leistungsproblemen mit dem Dateisystem

Die Leistung des Dateisystems hängt von mehreren Faktoren ab, darunter dem Datenverkehr, den Sie in Ihr Dateisystem leiten, wie Sie Ihr Dateisystem bereitstellen und von allen aktivierten Funktionen wie Datendeduplizierung oder Schattenkopien. Informationen zum Verständnis der Leistung Ihres Dateisystems finden Sie unter [Leistung von FSx for Windows File Server](#)

### Themen

- [Wie ermittle ich den Durchsatz und die IOPS-Grenzwerte für mein Dateisystem?](#)
- [Was ist der Unterschied zwischen Netzwerk-I/O und Festplatten-I/O? Warum unterscheidet sich meine Netzwerk-I/O von meiner Festplatten-I/O?](#)
- [Warum ist meine CPU- oder Speicherauslastung hoch, obwohl meine Netzwerk-E/A gering ist?](#)

- [Was ist Bursting? Wie viel Bursting verwendet mein Dateisystem? Was passiert, wenn das Burst-Guthaben aufgebraucht ist?](#)
- [Auf der Seite Überwachung und Leistung wird eine Warnung angezeigt. Muss ich die Konfiguration meines Dateisystems ändern?](#)
- [Meine Messwerte fehlten vorübergehend, sollte ich mir Sorgen machen?](#)

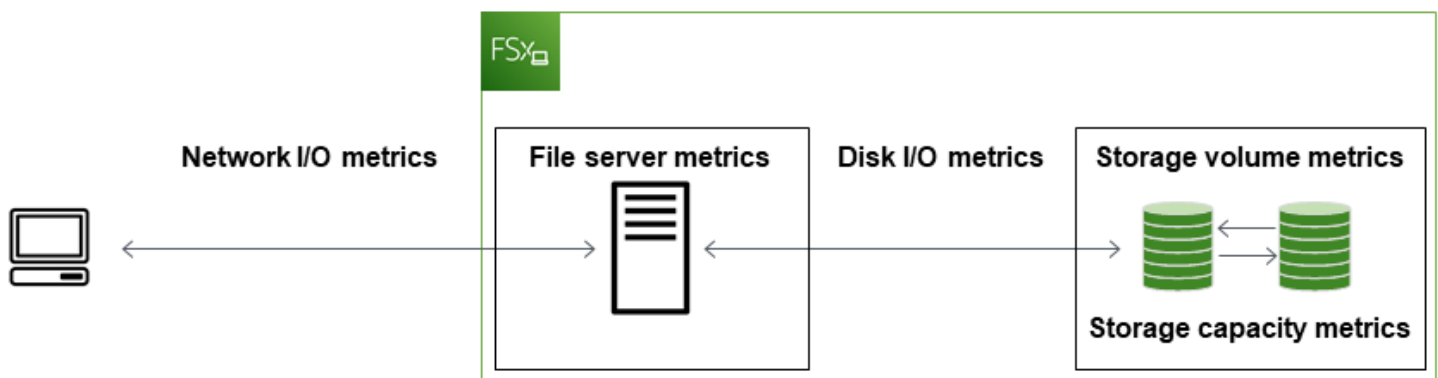
## Wie ermittle ich den Durchsatz und die IOPS-Grenzwerte für mein Dateisystem?

Den Durchsatz und die IOPS-Grenzwerte eines Dateisystems finden Sie in der [Tabelle, in der die Leistungsstufen](#) auf der Grundlage der bereitgestellten Durchsatzkapazität aufgeführt sind.

## Was ist der Unterschied zwischen Netzwerk-I/O und Festplatten-I/O?

## Warum unterscheidet sich meine Netzwerk-I/O von meiner Festplatten-I/O?

Amazon FSx-Dateisysteme umfassen einen oder mehrere Dateiserver, die den Clients, die auf das Dateisystem zugreifen, Daten über das Netzwerk bereitstellen. Dies ist die Netzwerk-I/O. Der Dateiserver verfügt über einen schnellen In-Memory-Cache, um die Leistung für die am häufigsten aufgerufenen Daten zu verbessern. Die Dateiserver leiten auch den Datenverkehr zu den Speichervolumen weiter, die Ihre Dateisystemdaten hosten. Dies ist die Festplatten-I/O. Das folgende Diagramm zeigt Netzwerk- und Festplatten-I/O für ein Amazon FSx-Dateisystem.



Weitere Informationen finden Sie unter [Metriken mit Amazon überwachen CloudWatch](#).

## Warum ist meine CPU- oder Speicherauslastung hoch, obwohl meine Netzwerk-E/A gering ist?

Die CPU- und Speicherauslastung des Dateiservers hängt nicht nur vom Netzwerkverkehr ab, den Sie steuern, sondern auch von den Funktionen, die Sie in Ihrem Dateisystem aktiviert haben. Wie Sie diese Funktionen konfigurieren und planen, kann sich auf die CPU- und Speicherauslastung auswirken.

Laufende Datendeduplizierungsaufträge können Speicherplatz beanspruchen. Sie können die Konfiguration von Deduplizierungsaufträgen ändern, um den Speicherbedarf zu reduzieren. Sie können die Optimierung beispielsweise auf bestimmte Dateitypen oder Ordner beschränken oder eine Mindestdateigröße und ein Mindestalter für die Optimierung festlegen. Wir empfehlen außerdem, Deduplizierungsaufträge so zu konfigurieren, dass sie in Leerlaufzeiten ausgeführt werden, wenn Ihr Dateisystem nur minimal belastet wird. Weitere Informationen finden Sie unter [Datendeduplizierung](#).

Wenn Sie die zugriffsbasierte Aufzählung aktiviert haben, stellen Sie möglicherweise eine hohe CPU-Auslastung fest, wenn Ihre Endbenutzer Dateifreigaben aufrufen oder auflisten, oder während der Optimierungsphase eines Speicherskalierungsauftrags. Weitere Informationen finden Sie unter [Aktivieren der zugriffsbasierten Aufzählung für einen Namespace](#) in der Microsoft Storage-Dokumentation.

## Was ist Bursting? Wie viel Bursting verwendet mein Dateisystem? Was passiert, wenn das Burst-Guthaben aufgebraucht ist?

Dateibasierte Workloads weisen in der Regel hohe Geschwindigkeiten auf. Sie zeichnen sich durch kurze, intensive Perioden mit hohem I/O-Aufwand und Leerlaufzeiten zwischen den einzelnen Bursts aus. Um diese Arten von Workloads zu unterstützen, bietet Amazon FSx zusätzlich zu den Basisgeschwindigkeiten, die ein Dateisystem aushalten kann, die Möglichkeit, sowohl für Netzwerk-I/O- als auch für Festplatten-I/O-Operationen für bestimmte Zeiträume höhere Geschwindigkeiten zu erreichen.

Amazon FSx verwendet einen I/O-Guthabenmechanismus, um Durchsatz und IOPS auf der Grundlage der durchschnittlichen Auslastung zuzuweisen. Dateisysteme sammeln Credits, wenn ihr Durchsatz und ihre IOPS-Nutzung unter ihren Basisgrenzwerten liegen, und können diese Credits verwenden, um bei Bedarf die Basisgrenzwerte (bis zu den Burst-Grenzwerten) zu überschreiten. Weitere Informationen zu den Burst-Grenzwerten und der Dauer Ihres Dateisystems finden Sie unter [Leistung von FSx for Windows File Server](#)

## Auf der Seite Überwachung und Leistung wird eine Warnung angezeigt. Muss ich die Konfiguration meines Dateisystems ändern?

Die Seite Überwachung und Leistung enthält Warnungen, die darauf hinweisen, wenn die aktuellen Workload-Anforderungen die Ressourcengrenzen, die von der Konfiguration Ihres Dateisystems abhängen, erreicht oder überschritten haben. Dies bedeutet nicht unbedingt, dass Sie Ihre Konfiguration ändern müssen, obwohl Ihr Dateisystem möglicherweise nicht ausreichend für Ihre Arbeitslast bereitgestellt ist, wenn Sie nicht die empfohlenen Maßnahmen ergreifen.

Wenn der Workload, der die Warnung ausgelöst hat, untypisch war und Sie nicht erwarten, dass er weitergeht, können Sie sicher sein, keine Maßnahmen zu ergreifen und Ihre Auslastung in Zukunft genau zu überwachen. Wenn die Arbeitslast, die die Warnung verursacht hat, jedoch typisch ist und Sie erwarten, dass sie andauert oder sogar zunimmt, empfehlen wir, die empfohlenen Maßnahmen zur Steigerung der Dateiserverleistung (durch Erhöhung der Durchsatzkapazität) oder zur Steigerung der Leistung des Speichervolumens (durch Erhöhung der Speicherkapazität oder durch den Wechsel von HDD- zu SSD-Speicher) zu befolgen.

### Note

Bestimmte Dateisystemereignisse können Festplatten-I/O-Leistungsressourcen verbrauchen und möglicherweise Leistungswarnungen auslösen. Beispielsweise:

- Die Optimierungsphase der Skalierung der Speicherkapazität kann zu einem erhöhten Festplattendurchsatz führen, wie unter beschrieben [Die Speicherkapazität steigt und die Leistung des Dateisystems](#)
- Bei Multi-AZ-Dateisystemen führen Ereignisse wie die Skalierung der Durchsatzkapazität, der Austausch von Hardware oder die Unterbrechung der Availability Zone zu automatischen Failover- und Failback-Ereignissen. Alle Datenänderungen, die während dieser Zeit auftreten, müssen zwischen dem primären und dem sekundären Dateiserver synchronisiert werden, und Windows Server führt einen Datensynchronisierungsauftrag aus, der Festplatten-I/O-Ressourcen verbrauchen kann. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

## Meine Messwerte fehlten vorübergehend, sollte ich mir Sorgen machen?

Single-AZ-Dateisysteme sind während der Wartung des Dateisystems, beim Austausch von Infrastrukturkomponenten und wenn eine Availability Zone nicht verfügbar ist, nicht verfügbar. Während dieser Zeiten sind keine Metriken verfügbar.

In einer Multi-AZ-Bereitstellung stellt Amazon FSx automatisch einen Standby-Dateiserver in einer anderen Availability Zone bereit und verwaltet ihn. Bei Wartungsarbeiten am Dateisystem oder einer ungeplanten Serviceunterbrechung schaltet Amazon FSx automatisch auf den sekundären Dateiserver um, sodass Sie ohne manuelles Eingreifen weiterhin auf Ihre Daten zugreifen können. Während des kurzen Zeitraums, in dem Ihr Dateisystem einen Failover und ein Failback durchführt, sind die Messwerte möglicherweise vorübergehend nicht verfügbar.

## Zusätzliche Informationen

Dieser Abschnitt enthält eine Referenz zu unterstützten, aber veralteten Amazon FSx-Funktionen.

Themen

- [Einen benutzerdefinierten Backup-Zeitplan einrichten](#)
- [Verwenden von Microsoft Distributed File System Replication](#)

### Einen benutzerdefinierten Backup-Zeitplan einrichten

Wir empfehlen AWS Backup die Verwendung, um einen benutzerdefinierten Backup-Zeitplan für Ihr Dateisystem einzurichten. Die hier bereitgestellten Informationen dienen zu Referenzzwecken, falls Sie Backups häufiger planen müssen, als dies bei der Verwendung möglich ist AWS Backup.

Wenn diese Option aktiviert ist, erstellt Amazon FSx for Windows File Server innerhalb eines täglichen Backup-Fensters automatisch einmal täglich eine Sicherungskopie Ihres Dateisystems. Amazon FSx erzwingt eine Aufbewahrungsfrist, die Sie für diese automatischen Backups angeben. Es unterstützt auch vom Benutzer initiierte Backups, sodass Sie jederzeit Backups erstellen können.

Im Folgenden finden Sie die Ressourcen und die Konfiguration für die Implementierung einer benutzerdefinierten Backup-Planung. Die benutzerdefinierte Sicherungsplanung führt vom Benutzer initiierte Backups auf einem Amazon FSx-Dateisystem nach einem von Ihnen definierten Zeitplan durch. Beispiele könnten einmal alle sechs Stunden, einmal pro Woche usw. sein. Dieses Skript konfiguriert auch das Löschen von Backups, die älter als der angegebene Aufbewahrungszeitraum sind.

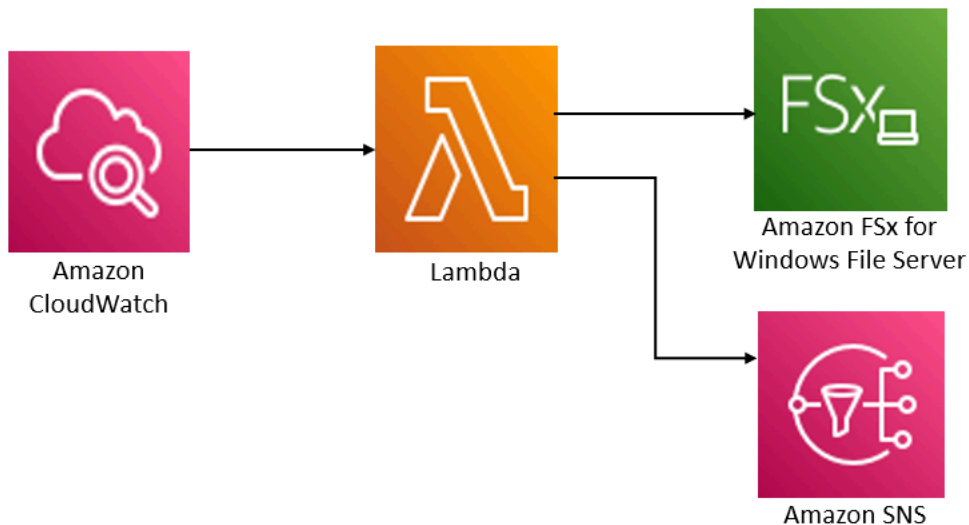
Die Lösung stellt automatisch alle benötigten Komponenten bereit und berücksichtigt die folgenden Parameter:

- Das Dateisystem
- Ein CRON-Zeitplanmuster für die Durchführung von Backups
- Die Aufbewahrungsfrist für Backups (in Tagen)
- Die Backup-Namensschilder

Weitere Informationen zu CRON-Zeitplanmustern finden Sie unter [Schedule Expressions for Rules](#) im CloudWatch Amazon-Benutzerhandbuch.

## Übersicht über die Architektur

Durch die Bereitstellung dieser Lösung werden die folgenden Ressourcen in der AWS Cloud bereitgestellt.



Diese Lösung macht Folgendes:

1. Die AWS CloudFormation Vorlage stellt ein CloudWatch Ereignis, eine Lambda-Funktion, eine Amazon SNS SNS-Warteschlange und eine IAM-Rolle bereit. Die IAM-Rolle erteilt der Lambda-Funktion die Erlaubnis, die Amazon FSx-API-Operationen aufzurufen.
2. Das CloudWatch Ereignis wird während der ersten Bereitstellung nach einem Zeitplan ausgeführt, den Sie als CRON-Muster definieren. Dieses Ereignis ruft die Lambda-Funktion des Backup-Managers der Lösung auf, die den Amazon CreateBackup FSx-API-Vorgang aufruft, um ein Backup zu initiieren.
3. Der Backup-Manager ruft mithilfe von eine Liste vorhandener benutzerinitiiert Backup für das angegebene Dateisystem ab. DescribeBackups Anschließend werden Backups gelöscht, die älter sind als der Aufbewahrungszeitraum, den Sie bei der ersten Bereitstellung angegeben haben.
4. Der Backup-Manager sendet bei einem erfolgreichen Backup eine Benachrichtigung an die Amazon SNS SNS-Warteschlange, wenn Sie die Option wählen, bei der ersten Bereitstellung benachrichtigt zu werden. Im Falle eines Fehlers wird immer eine Benachrichtigung gesendet.



## AWS CloudFormation Vorlage

Diese Lösung automatisiert AWS CloudFormation die Bereitstellung der benutzerdefinierten Backup-Planungslösung von Amazon FSx. Um diese Lösung zu verwenden, laden Sie die Vorlage [AWS CloudFormation fsx-scheduled-backup.template](#) herunter.

### Automatisierte Bereitstellung

Mit dem folgenden Verfahren wird diese benutzerdefinierte Lösung zur Planung von Backups konfiguriert und bereitgestellt. Die Bereitstellung dauert etwa fünf Minuten. Bevor Sie beginnen, müssen Sie die ID eines Amazon FSx-Dateisystems, das in einer Amazon Virtual Private Cloud (Amazon VPC) läuft, in Ihrem AWS Konto haben. Weitere Informationen zur Erstellung dieser Ressourcen finden Sie unter [Erste Schritte mit Amazon FSx for Windows File Server](#)

#### Note

Bei der Implementierung dieser Lösung müssen die zugehörigen AWS Dienste in Rechnung gestellt werden. Weitere Informationen finden Sie auf den Seiten mit den Preisdetails für diese Dienste.

Um den Stack für benutzerdefinierte Backup-Lösungen zu starten

1. Laden Sie die Vorlage [AWS CloudFormation fsx-scheduled-backup.template](#) herunter. Weitere Informationen zum Erstellen eines AWS CloudFormation Stacks finden Sie im Benutzerhandbuch unter [Erstellen eines Stacks](#) auf der Konsole. AWS CloudFormation AWS CloudFormation

#### Note

Standardmäßig wird diese Vorlage in der AWS Region USA Ost (Nord-Virginia) gestartet. Amazon FSx ist derzeit nur in bestimmten AWS-Regionen Fällen verfügbar. Sie müssen diese Lösung in einer AWS Region einführen, in der Amazon FSx verfügbar ist. Weitere Informationen finden Sie im Abschnitt Amazon FSx von [AWS-Regionen und Endpoints](#) in der Allgemeinen AWS-Referenz

2. Überprüfen Sie unter Parameter die Parameter für die Vorlage und ändern Sie sie an die Anforderungen Ihres Dateisystems. Diese Lösung verwendet die folgenden Standardwerte.

| Parameter                        | Standard                      | Beschreibung                                                                                                                                                                                  |
|----------------------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Amazon FSx-Dateisystem-ID        | Kein Standardwert             | Die Dateisystem-ID für das Dateisystem, das Sie sichern möchten.                                                                                                                              |
| CRON-Zeitplanmuster für Backups. | 0 0/4 * *? *                  | Der Zeitplan für die Ausführung des CloudWatch Ereignisses, das Auslösen eines neuen Backups und das Löschen alter Backups außerhalb des Aufbewahrungszeitraums.                              |
| Aufbewahrung von Backup (Tage)   | 30                            | Die Anzahl der Tage, für die vom Benutzer initiierte Backups aufbewahrt werden sollen. Die Lambda-Funktion löscht vom Benutzer initiierte Backups, die älter als diese Anzahl von Tagen sind. |
| Name für Backups                 | vom Benutzer geplante Backups | Der Name für diese Backups, der in der Spalte Backup-Name der Amazon FSx Management Console angezeigt wird.                                                                                   |
| Backup-Benachrichtigungen        | Ja                            | Wählen Sie aus, ob Sie benachrichtigt werden möchten, wenn Backups erfolgreich initiiert wurden. Bei einem Fehler wird immer eine Benachrichtigung gesendet.                                  |

| Parameter      | Standard          | Beschreibung                                                     |
|----------------|-------------------|------------------------------------------------------------------|
| E-Mail-Adresse | Kein Standardwert | Die E-Mail-Adresse, um die SNS-Benachrichtigungen zu abonnieren. |

3. Wählen Sie Weiter aus.
4. Wählen Sie unter Optionen die Option Weiter aus.
5. Überprüfen und bestätigen Sie die Einstellungen zur Überprüfung. Sie müssen das Kontrollkästchen aktivieren, das bestätigt, dass die Vorlage IAM-Ressourcen erstellt.
6. Wählen Sie Create aus, um den Stack bereitzustellen.

Sie können den Status des Stacks in der AWS CloudFormation Konsole in der Spalte Status einsehen. In etwa fünf Minuten sollte der Status CREATE\_COMPLETE angezeigt werden.

## Zusätzliche Optionen

Sie können die mit dieser Lösung erstellte Lambda-Funktion verwenden, um benutzerdefinierte geplante Backups von mehr als einem Amazon FSx-Dateisystem durchzuführen. Die Dateisystem-ID wird in der Eingabe-JSON für das CloudWatch Ereignis an die Amazon FSx-Funktion übergeben. Das Standard-JSON, das an die Lambda-Funktion übergeben wird, lautet wie folgt, wobei die Werte für `FileSystemId` und aus den Parametern übergeben `SuccessNotification` werden, die beim Starten des AWS CloudFormation Stacks angegeben wurden.

```
{
  "start-backup": "true",
  "purge-backups": "true",
  "filesystem-id": "${FileSystemId}",
  "notify_on_success": "${SuccessNotification}"
}
```

Um Backups für ein zusätzliches Amazon FSx-Dateisystem zu planen, erstellen Sie eine weitere CloudWatch Ereignisregel. Dazu verwenden Sie die Schedule-Ereignisquelle mit der von dieser Lösung erstellten Lambda-Funktion als Ziel. Wählen Sie unter Eingabe konfigurieren die Option Constant (JSON-Text) aus. Ersetzen Sie für die JSON-Eingabe einfach die Dateisystem-ID des zu sichernden Amazon FSx-Dateisystems anstelle von `${FileSystemId}`. Ersetzen Sie außerdem `No` im obigen JSON-Code entweder `Yes` oder anstelle von `${SuccessNotification}`.

Alle zusätzlichen CloudWatch Event-Regeln, die Sie manuell erstellen, sind nicht Teil des Amazon FSx-Lösungspakets für benutzerdefinierte geplante Backups AWS CloudFormation . Sie werden also nicht entfernt, wenn Sie den Stack löschen.

## Verwenden von Microsoft Distributed File System Replication

### Note

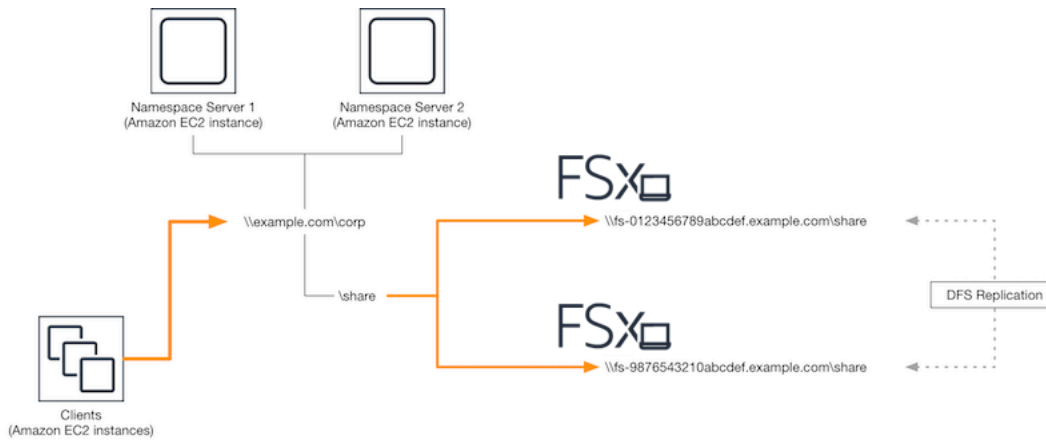
Um Hochverfügbarkeit für einen FSx for Windows File Server zu implementieren, empfehlen wir die Verwendung von Amazon FSx Multi-AZ. Weitere Informationen zu Amazon FSx Multi-AZ finden Sie unter [Verfügbarkeit und Haltbarkeit: Single-AZ- und Multi-AZ-Dateisysteme](#)

Amazon FSx unterstützt die Verwendung des Microsoft Distributed File System (DFS) für Dateisystembereitstellungen in mehreren Availability Zones (AZs), um Multi-AZ-Verfügbarkeit und Beständigkeit zu gewährleisten. Mithilfe der DFS-Replikation können Sie Daten automatisch zwischen zwei Dateisystemen replizieren. Mithilfe von DFS-Namespaces können Sie ein Dateisystem als Ihr primäres und das andere als Ihr Standby-Dateisystem konfigurieren, wobei ein automatischer Failover auf das Standby-Dateisystem erfolgt, falls das primäre Dateisystem nicht mehr reagiert.

Bevor Sie die DFS-Replikation verwenden, führen Sie die folgenden Schritte aus:

- Richten Sie Ihre Sicherheitsgruppen wie unter Erste Schritte mit Amazon FSx beschrieben ein.  
[Step 8](#)
- Erstellen Sie zwei Amazon FSx-Dateisysteme in verschiedenen AZs innerhalb einer AWS Region. Weitere Informationen zur Erstellung Ihrer Dateisysteme finden Sie unter [Schreiben Sie Daten in Ihre Dateifreigabe](#).
- Stellen Sie sicher, dass sich beide Dateisysteme in demselben befinden AWS Directory Service for Microsoft Active Directory.
- Notieren Sie sich nach der Erstellung der Dateisysteme ihre Dateisystem-IDs für später.

In den folgenden Themen finden Sie eine Beschreibung, wie Sie DFS-Replikation und DFS-Namespaces-Failover über AZs hinweg mit Amazon FSx einrichten und verwenden.



## Einrichtung der DFS-Replikation

Sie können DFS Replication verwenden, um Daten automatisch zwischen zwei Amazon FSx-Dateisystemen zu replizieren. Diese Replikation ist bidirektional, was bedeutet, dass Sie in eines der beiden Dateisysteme schreiben können und die Änderungen auf das andere repliziert werden.

### ⚠ Important

Sie können die DFS-Verwaltungsschnittstelle in den Microsoft Windows-Verwaltungstools (`dfsmanagement.msc`) nicht verwenden, um die DFS-Replikation auf Ihrem FSx for Windows File Server Server-Dateisystem zu konfigurieren.

So richten Sie die DFS-Replikation ein (skriptgesteuert)

1. Beginnen Sie mit der Verwaltung von DFS, indem Sie Ihre Instance starten und sie mit dem Microsoft Active Directory verbinden, mit dem Sie Ihre Amazon FSx-Dateisysteme verknüpft haben. Wählen Sie dazu eines der folgenden Verfahren aus dem AWS Directory Service Administratorhandbuch aus:
  - [Nahtlose Anbindung an eine Windows EC2-Instance](#)
  - [Manuelle Anbindung an eine Windows-Instance](#)
2. Stellen Sie als Active Directory-Benutzer, der Mitglied der Gruppe der Dateisystemadministratoren ist, eine Connect zu Ihrer Instanz her. In AWS Managed AD wird diese Gruppe AWS Delegated FSx Administrators genannt. In Ihrem selbstverwalteten Microsoft AD heißt diese Gruppe Domänen-Admins oder der benutzerdefinierte Name für die Administratorgruppe, den Sie bei der Erstellung angegeben haben.

Dieser Benutzer muss auch Mitglied einer Gruppe sein, an die DFS-Verwaltungsberechtigungen delegiert wurden. In AWS Managed AD wird diese Gruppe als AWS Delegated Distributed File System Administrators bezeichnet. In Ihrem selbstverwalteten AD muss dieser Benutzer Mitglied von Domain Admins oder einer anderen Gruppe sein, an die Sie DFS-Verwaltungsberechtigungen delegiert haben.

Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.

3. Laden Sie das [FSX-DFSR-Setup.ps1-Skript PowerShell](#) herunter.
4. Öffnen Sie das Startmenü und geben Sie ein. PowerShell Wählen Sie aus der Liste Windows aus PowerShell.
5. Führen Sie das PowerShell Skript mit den folgenden angegebenen Parametern aus, um die DFS-Replikation zwischen Ihren beiden Dateisystemen einzurichten:
  - Die Namen der DFS-Replikationsgruppe und des DFS-Replikationsordners
  - Der lokale Pfad zu dem Ordner, den Sie auf Ihren Dateisystemen replizieren möchten (z. B. D:\share für die Standardfreigabe, die in Ihrem Amazon FSx-Dateisystem enthalten ist)
  - Die DNS-Namen der primären und Standby-Amazon FSx-Dateisysteme, die Sie in den erforderlichen Schritten erstellt haben

### Example

```
FSx-DFSR-Setup.ps1 -group Group -folder Folder -path ContentPath -  
primary FSxFileSystem1-DNS-Name -standby FSxFileSystem2-DNS-Name
```

So richten Sie die DFS-Replikation ein (Schritt für Schritt)

1. Beginnen Sie mit der Verwaltung von DFS, indem Sie Ihre Instance starten und sie mit dem Microsoft Active Directory verbinden, mit dem Sie Ihre Amazon FSx-Dateisysteme verknüpft haben. Wählen Sie dazu eines der folgenden Verfahren aus dem AWS Directory Service Administratorhandbuch aus:
  - [Nahtlose Anbindung an eine Windows EC2-Instance](#)
  - [Manuelle Anbindung an eine Windows-Instance](#)

2. Stellen Sie als Active Directory-Benutzer, der Mitglied der Gruppe der Dateisystemadministratoren ist, eine Connect zu Ihrer Instanz her. In AWS Managed AD wird diese Gruppe AWS Delegated FSx Administrators genannt. In Ihrem selbstverwalteten Microsoft AD heißt diese Gruppe Domänen-Admins oder der benutzerdefinierte Name für die Administratorgruppe, den Sie bei der Erstellung angegeben haben.

Dieser Benutzer muss auch Mitglied einer Gruppe sein, an die DFS-Verwaltungsberechtigungen delegiert wurden. In AWS Managed AD wird diese Gruppe als AWS Delegated Distributed File System Administrators bezeichnet. In Ihrem selbstverwalteten AD muss dieser Benutzer Mitglied von Domain Admins oder einer anderen Gruppe sein, an die Sie DFS-Verwaltungsberechtigungen delegiert haben.

Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.

3. Öffnen Sie das Startmenü und geben Sie ein PowerShell. Wählen Sie aus der Liste Windows aus PowerShell.
4. Wenn Sie die DFS Management Tools noch nicht installiert haben, installieren Sie sie mit dem folgenden Befehl auf Ihrer Instanz.

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

5. Erstellen Sie von der PowerShell Eingabeaufforderung aus eine DFS-Replikationsgruppe und einen Ordner mit den folgenden Befehlen.

```
$Group = "Name of the DFS Replication group"  
$Folder = "Name of the DFS Replication folder"  
  
New-DfsReplicationGroup -GroupName $Group  
New-DfsReplicatedFolder -GroupName $Group -FolderName $Folder
```

6. Ermitteln Sie mit den folgenden Befehlen den Active Directory-Computernamen, der jedem Dateisystem zugeordnet ist.

```
$Primary = "DNS name of the primary FSx file system"  
$Standby = "DNS name of the standby FSx file system"  
  
$C1 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -eq 'HOST/$Primary']").Name
```

```
$C2 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -eq 'HOST/$Standby').Name
```

7. Fügen Sie Ihre Dateisysteme als Mitglieder der DFS-Replikationsgruppe hinzu, die Sie mit den folgenden Befehlen erstellt haben.

```
Add-DfsrMember -GroupName $Group -ComputerName $C1  
Add-DfsrMember -GroupName $Group -ComputerName $C2
```

8. Verwenden Sie die folgenden Befehle, um der DFS-Replikationsgruppe den lokalen Pfad (z. B. D:\share) für jedes Dateisystem hinzuzufügen. *file system 1* dient in diesem Verfahren als primäres Mitglied, was bedeutet, dass sein Inhalt zunächst mit dem anderen Dateisystem synchronisiert wird.

```
$ContentPath1 = "Local path to the folder you want to replicate on file system 1"  
$ContentPath2 = "Local path to the folder you want to replicate on file system 2"  
  
Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath1  
-ComputerName $C1 -PrimaryMember $True  
Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath2  
-ComputerName $C2 -PrimaryMember $False
```

9. Fügen Sie mit dem folgenden Befehl eine Verbindung zwischen den Dateisystemen hinzu.

```
Add-DfsrConnection -GroupName $Group -SourceComputerName $C1 -  
DestinationComputerName $C2
```

Innerhalb weniger Minuten sollten beide Dateisysteme damit beginnen, den Inhalt der zuvor ContentPath angegebenen Datei zu synchronisieren.

## DFS-Namespaces für Failover einrichten


Sie können DFS-Namespaces verwenden, um ein Dateisystem als Ihr primäres und das andere als Ihr Standby-Dateisystem zu behandeln. Auf diese Weise können Sie einen automatischen Failover auf den Standby-Modus konfigurieren, falls der primäre Server nicht mehr reagiert. Mit DFS-Namespaces können Sie gemeinsam genutzte Ordner auf verschiedenen Servern in einem einzigen Namespace gruppieren, wobei ein einziger Ordnerpfad zu Dateien führen kann, die auf mehreren Servern gespeichert sind. DFS-Namespaces werden von DFS-Namespace-Servern verwaltet, die



Recheninstanzen, die einen DFS-Namespaces-Ordner zuordnen, den entsprechenden Dateiservern zuordnen.

So richten Sie DFS-Namespaces für Failover (UI) ein

1. [Wenn Sie noch keine DFS-Namespaces-Server ausführen, starten Sie ein Paar hochverfügbarer DFS-Namespaces-Server mithilfe der Vorlage Setup-DFS-Server.Template.](#) AWS CloudFormation [Weitere Informationen zum Erstellen eines Stacks finden Sie im Benutzerhandbuch unter Erstellen eines AWS CloudFormation Stacks auf der Konsole.](#) [AWS CloudFormation AWS CloudFormation](#)
2. Stellen Sie als Benutzer in der Gruppe AWS Delegierte Administratoren eine Connect zu einem der DFS-Namespaces-Server her, die im vorherigen Schritt gestartet wurden. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Öffnen Sie die DFS-Managementkonsole. Öffnen Sie das Startmenü und starten Sie `dfsmanagement.msc`. Dadurch wird das DFS Management GUI-Tool geöffnet.
4. Wählen Sie unter Aktion die Option Neuer Namespace aus, geben Sie den Computernamen des ersten DFS-Namespaces-Servers ein, den Sie für Server gestartet haben, und wählen Sie Weiter.
5. Geben Sie unter Name den Namespace ein, den Sie erstellen (z. B.). **corp**
6. Wählen Sie „Einstellungen bearbeiten“ und legen Sie die entsprechenden Berechtigungen entsprechend Ihren Anforderungen fest. Wählen Sie Weiter aus.
7. Lassen Sie die Standardoption Domänenbasierter Namespace aktiviert, lassen Sie die Option Windows Server 2008-Modus aktivieren aktiviert und klicken Sie auf Weiter.

 Note

Der Windows Server 2008-Modus ist die neueste verfügbare Option für Namespaces.

8. Überprüfen Sie die Namespace-Einstellungen und wählen Sie Create aus.
9. Wählen Sie in der Navigationsleiste unter Namespaces den neu erstellten Namespace aus, wählen Sie Aktion und dann Namespace-Server hinzufügen aus.
10. Geben Sie für Namespace-Server den Computernamen des zweiten DFS-Namespaces-Servers ein, den Sie gestartet haben.
11. Wählen Sie „Einstellungen bearbeiten“, legen Sie die entsprechenden Berechtigungen entsprechend Ihren Anforderungen fest und wählen Sie „OK“.

12. **Wählen Sie Hinzufügen, geben Sie den UNC-Namen der Dateifreigabe auf dem primären Amazon FSx-Dateisystem (z. B. \\ fs-0123456789abcdef0 .example.com\ share) als Pfad zum Ordnerziel ein und wählen Sie OK.**
13. **Wählen Sie Hinzufügen, geben Sie den UNC-Namen der Dateifreigabe auf dem Amazon FSx-Standby-Dateisystem (z. B. \\ fs-fedbca9876543210f .example.com\ share) als Pfad zum Ordnerziel ein, und wählen Sie OK.**
14. Wählen Sie im Fenster „Neuer Ordner“ die Option OK. Der neue Ordner wird mit den beiden Ordnerzielen unter Ihrem Namespace erstellt.
15. Wiederholen Sie die letzten drei Schritte für jede Dateifreigabe, die Sie Ihrem Namespace hinzufügen möchten.

So richten Sie DFS-Namespace für Failover ein () PowerShell

1. [Wenn Sie noch keine DFS-Namespace-Server ausführen, starten Sie ein Paar hochverfügbarer DFS-Namespace-Server mithilfe der Vorlage Setup-DFSN-Servers.Template.](#) AWS CloudFormation [Weitere Informationen zum Erstellen eines Stacks finden Sie im Benutzerhandbuch unter Erstellen eines AWS CloudFormation Stacks auf der Konsole.](#) [AWS CloudFormation AWS CloudFormation](#)
2. Stellen Sie als Benutzer in der Gruppe AWS Delegierte Administratoren eine Connect zu einem der DFS-Namespace-Server her, die im vorherigen Schritt gestartet wurden. Weitere Informationen finden Sie unter [Connecting to Your Windows Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Öffnen Sie das Startmenü und geben Sie ein PowerShell. Windows PowerShell erscheint in der Liste der Treffer.
4. Öffnen Sie das Kontextmenü (Rechtsklick) für Windows PowerShell und wählen Sie Als Administrator ausführen.
5. Wenn Sie die DFS Management Tools noch nicht installiert haben, installieren Sie sie mit dem folgenden Befehl auf Ihrer Instanz.

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

6. Wenn Sie noch keinen vorhandenen DFS-Namespace haben, können Sie einen mit den folgenden Befehlen erstellen. PowerShell

```
$NSS1 = computer name of the 1st DFS Namespace server  
$NSS2 = computer name of the 2nd DFS Namespace server
```

```

$DNSRoot = fully qualified Active Directory domain name (e.g. mydomain.com)
$Namespace = Namespace name you want to use
$Folder = Folder path you want to use within the Namespace
$FS1FolderTarget = Share path to Folder Target on File System 1
$FS2FolderTarget = Share path to Folder Target on File System 2

```

```

$NSS1,$NSS2 | ForEach-Object { Invoke-Command -ComputerName $_ -ScriptBlock { mkdir
  "C:\DFS\${using:Namespace}";
  New-SmbShare -Name ${using:Namespace} -Path "C:\DFS\${using:Namespace}" } }

```

```

New-DfsnRoot -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS1}.${DNSRoot}\
${Namespace}" -Type DomainV2
New-DfsnRootTarget -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS2}.
${DNSRoot}\${Namespace}"

```

- Um einen Ordner in Ihrem DFS-Namespace zu erstellen, können Sie den folgenden Befehl verwenden. PowerShell Dadurch wird ein Ordner erstellt, der Compute-Instances, die auf den Ordner zugreifen, standardmäßig an Ihr primäres Amazon FSx-Dateisystem weiterleitet.

```

$FS1 = DNS name of primary FSx file system
New-DfsnFolder -Path "\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath "\\${FS1}\
${FS1FolderTarget}" -EnableTargetFailback $True -ReferralPriorityClass GlobalHigh

```

- Fügen Sie Ihr Amazon FSx-Standby-Dateisystem demselben DFS-Namespace-Ordner hinzu. Compute-Instances, die auf den Ordner zugreifen, greifen auf dieses Dateisystem zurück, wenn sie keine Verbindung zum primären Amazon FSx-Dateisystem herstellen können.

```

$FS2 = DNS name of secondary FSx file system
New-DfsnFolderTarget -Path "\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath "\\
${FS2}\${FS2FolderTarget}"

```

Sie können jetzt von Compute-Instances aus auf Ihre Daten zugreifen, indem Sie den zuvor angegebenen Remote-Pfad des DFS-Namespace-Ordners verwenden. Dadurch werden die Compute-Instances an das primäre Amazon FSx-Dateisystem weitergeleitet (und an das Standby-Dateisystem, falls das primäre Dateisystem nicht reagiert).

Öffnen Sie beispielsweise das Startmenü und geben Sie ein. PowerShell Wählen Sie aus der Liste den folgenden Befehl aus `Windows PowerShell` und führen Sie ihn aus.

```
net use Z: \\${DNSRoot}\${Namespace}\${Folder} /persistent:yes
```

## Arbeiten mit Maintenance Windows und FSx Multi-AZ

Um die hohe Verfügbarkeit Ihrer Multi-AZ-Dateisystembereitstellung sicherzustellen, empfehlen wir Ihnen, für die beiden Amazon FSx-Dateisysteme in Ihrer Multi-AZ-Bereitstellung Wartungsfenster zu wählen, die sich nicht überschneiden. Auf diese Weise können Sie sicherstellen, dass Ihre Dateidaten während der Systemwartungsfenster weiterhin für Ihre Anwendungen und Benutzer verfügbar sind.

### Note

Um DFS-Replikationsverkehr zu und von den Dateisystemen zuzulassen, stellen Sie sicher, dass Sie Regeln für eingehende und ausgehende VPC-Sicherheitsgruppen hinzufügen, wie unter beschrieben. [Amazon VPC-Sicherheitsgruppen](#)

# Dokumentverlauf

- API-Version: 2018-03-01
- Letzte Aktualisierung der Dokumentation: 17. Januar 2024

In der folgenden Tabelle werden wichtige Änderungen am Amazon-FSx-Windows-Benutzerhandbuch beschrieben. Um Benachrichtigungen über Dokumentationsaktualisierungen zu erhalten, können Sie den RSS-Feed abonnieren.

| Änderung                                                                                                                                                                    | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                          | Datum           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">Unterstützung für höhere IOPS-Werte auf Dateisystemen mit Durchsatzkapazitäten von 4 GB/s und höher hinzugefügt</a>                                             | FSx for Windows File Server erhöht die maximalen IOPS von 130K000 auf 150K000 für Dateisysteme mit 4 GB/s Durchsatzkapazität oder höher, von 175K auf 200K Dateisysteme mit 6 GB/s Durchsatzkapazität oder höher, von 260K000 auf 300K.000.00350K0 für Dateisysteme 400K mit 12 GB/s Durchsatzkapazität oder höher. Weitere Informationen finden Sie unter <a href="#">Leistung von FSx für Windows File Server</a> . | 17. Januar 2024 |
| <a href="#">Amazon FSx hat die von verwalteten Richtlinien AmazonFSxFullAccess, AmazonFSxConsoleFullAccess, AmazonFSxReadOnlyAccess, AmazonFSxConsoleReadOnlyAccess und</a> | Amazon FSx hat die Richtlinien AmazonFSxFullAccess, AmazonFSxConsoleFullAccess, AmazonFSxReadOnlyAccess, AmazonFSxConsoleReadOnlyAccess und AmazonFSxServiceRolePolicy aktualisiert, um die                                                                                                                                                                                                                           | 9. Januar 2024  |

[AmazonFSxServiceRolePolicy](#)  
[AWS aktualisiert](#)

ec2:GetSecurityGroupsForVpc Berechtigung hinzuzufügen. Weitere Informationen finden Sie unter [Amazon-FSx-Updates für - AWS verwaltete Richtlinien](#).

[Amazon FSx hat die von AmazonFSxFullAccess und den von AmazonFSxConsoleFullAccess AWS verwalteten Richtlinien aktualisiert](#)

Amazon FSx hat die AmazonFSxFullAccess - und AmazonFSxConsoleFullAccess -Richtlinien aktualisiert, um die ManageCrossAccountDataReplication Aktion hinzuzufügen. Weitere Informationen finden Sie unter [Amazon-FSx-Updates für - AWS verwaltete Richtlinien](#).

20. Dezember 2023

[Amazon FSx hat die von AmazonFSxFullAccess und den von AmazonFSxConsoleFullAccess AWS verwalteten Richtlinien aktualisiert](#)

Amazon FSx hat die AmazonFSxFullAccess - und AmazonFSxConsoleFullAccess -Richtlinien aktualisiert, um die fsx:CopySnapshotAndUpdateVolume Berechtigung hinzuzufügen. Weitere Informationen finden Sie unter [Amazon-FSx-Updates für - AWS verwaltete Richtlinien](#).

26. November 2023

[Amazon FSx hat die von AmazonFSxFullAccess und die von AmazonFSxConsoleFullAccess AWS verwalteten Richtlinien aktualisiert](#)

Amazon FSx hat die AmazonFSxFullAccess - und AmazonFSxConsoleFullAccess -Richtlinien aktualisiert, um die fsx:UpdateSharedVPCConfiguration Berechtigungen fsx:DescribeSharedVPCConfiguration und hinzuzufügen. Weitere Informationen finden Sie unter [Amazon-FSx-Updates für - AWS verwaltete Richtlinien](#).

14. November 2023

[Unterstützung für die Aktualisierung des Dateisystemspeichertyps hinzugefügt](#)

Dateisysteme von FSx für Windows File Server unterstützen jetzt die Aktualisierung vom HDD-Speichertyp zum SSD-Speichertyp. Weitere Informationen finden Sie unter [Verwalten des Speichertyps](#).

9. August 2023

[Unterstützung für höhere maximale Durchsatzkapazität hinzugefügt](#)

Dateisysteme von FSx für Windows File Server unterstützen jetzt eine Durchsatzkapazität von bis zu 12 GBps. Weitere Informationen finden Sie unter [Leistung von FSx für Windows File Server](#).

9. August 2023

[Unterstützung für die SSD-IOPS-Bereitstellung hinzugefügt](#)

Dateisysteme von FSx für Windows File Server unterstützen jetzt die Bereitstellung von SSD-IOPS unabhängig von der Speicherkapazität bis zu einem Maximum von 350.000 IOPS. Weitere Informationen finden Sie unter [Verwalten von SSD-IOPS](#).

9. August 2023

[Amazon FSx hat die von AmazonFSxServiceRolePolicy AWS verwaltete Richtlinie aktualisiert](#)

Amazon FSx hat die `cloudwatch:PutMetricData` Berechtigung in der `AmazonFSxServiceRolePolicy` aktualisiert. Weitere Informationen finden Sie unter [AmazonFSxServiceRolePolicy](#).

24. Juli 2023

[Amazon FSx hat die von AmazonFSxFullAccess AWS verwaltete Richtlinie aktualisiert](#)

Amazon FSx hat die `AmazonFSxFullAccess` - Richtlinie aktualisiert, um die `fsx:*` Berechtigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen. Weitere Informationen finden Sie unter [AmazonFSxFullAccess](#)-Richtlinie.

13. Juli 2023



[Amazon FSx hat die von AmazonFSxConsoleFullAccess AWS verwaltete Richtlinie aktualisiert](#)

Amazon FSx hat die AmazonFSxConsoleFullAccess -Richtlinie aktualisiert, um die fsx : \* Berechtigung zu entfernen und bestimmte fsx Aktionen hinzuzufügen. Weitere Informationen finden Sie unter [AmazonFSx ConsoleFullAccess](#)-Richtlinie.

13. Juli 2023

[Unterstützung für neue CloudWatch Metriken für Amazon FSx for Windows File Server hinzugefügt](#)

FSx for Windows File Server bietet jetzt zusätzliche CloudWatch Metriken, die die Leistung und Kapazität des Dateiservers und des Speicher-Volumes überwachen. Weitere Informationen finden Sie unter [Metriken und Dimensionen](#).

22. September 2022

[Unterstützung für Leistungswarnungen des Dateisystems hinzugefügt](#)

Amazon FSx stellt jetzt Warnungen im Fenster Leistung und Überwachung bereit, wenn sich eine Reihe von CloudWatch Metriken oder überverdefinierte Schwellenwerte für diese Metriken nähert. Jede Warnung enthält auch eine umsetzbare Empfehlung zur Verbesserung der Leistung des Dateisystems. Weitere Informationen finden Sie unter [Leistungswarnungen und Empfehlungen](#).

22. September 2022

[Unterstützung für verbesserte Überwachung der Dateisystemleistung hinzugefügt](#)

Das Dashboard zur Überwachung des Amazon-FSx-Konsolendateisystems für FSx-für-Windows-File-Server-Dateisysteme enthält neue Abschnitte Summary, Storage und Performance. In diesen Abschnitten werden Diagramme mit neuen CloudWatch Metriken angezeigt, die Ihnen eine verbesserte Leistungsüberwachung bieten. Weitere Informationen finden Sie unter [Überwachen von Metriken mit CloudWatch](#).

22. September 2022

[Unterstützung für AWS PrivateLink Schnittstellen-VPC-Endpunkte hinzugefügt](#)

Sie können jetzt Schnittstellen-VPC-Endpunkte verwenden, um von Ihrer VPC aus auf die Amazon-FSx-API zuzugreifen, ohne Datenverkehr über das Internet zu senden. Weitere Informationen finden Sie unter [Amazon FSx und Schnittstellen-VPC-Endpunkte](#).

5. April 2022

### [Unterstützung für Amazon Kendra hinzugefügt](#)

Sie können jetzt Ihr FSx for Windows File Server-Dateisystem als Datenquelle für Amazon Kendra verwenden, sodass Sie Informationen in Dokumenten in Ihrem Dateisystem indizieren und suchen können. Weitere Informationen finden Sie unter [Verwenden von FSx für Windows File Server mit Amazon Kendra](#).

26. März 2022

### [Unterstützung für die Prüfung des Dateizugriffs hinzugefügt](#)

Sie können jetzt die Prüfung von Endbenutzerzugriffen auf Dateien, Ordner und Dateifreigaben aktivieren. Sie können Audit-Ereignisprotokolle an die Services von Amazon CloudWatch Logs oder Amazon Data Firehose senden. Weitere Informationen finden Sie unter [Dateizugriffsprüfung](#).

8. Juni 2021

### [Unterstützung für das Kopieren von Backups hinzugefügt](#)

Sie können jetzt Amazon FSx verwenden, um Backups innerhalb desselben AWS Kontos in ein anderes AWS-Region (regionsübergreifende Kopien) oder innerhalb desselben AWS-Region (regionsübergreifende Kopien) zu kopieren. Weitere Informationen finden Sie unter [Kopieren von Sicherungen](#).

12. April 2021

### [Automatisches Erhöhen der Speicherkapazität eines Dateisystems](#)

Verwenden Sie eine AWS von entwickelte anpassbare AWS CloudFormation Vorlage, um die Speicherkapazität Ihres Dateisystems automatisch zu erhöhen, wenn seine Kapazität einen von Ihnen angegebenen Schwellenwert erreicht. Weitere Informationen finden Sie unter [Dynamisches Erhöhen der Speicherkapazität](#).

17. Februar 2021

### [Unterstützung für den Clientzugriff mit nicht privaten IP-Adressen hinzugefügt](#)

Sie können auf FSx für Windows File Server-Datensysteme mit On-Premises-Clients unter Verwendung nicht privater IP-Adressen zugreifen. Weitere Informationen finden Sie unter [Unterstützte Umgebungen](#). Sie können das Dateisystem von FSx für Windows File Server mit einem selbstverwalteten Microsoft Active Directory mit DNS-Servern und AD-Domain-Controllern verbinden, die nicht private IP-Adressen verwenden. Weitere Informationen finden Sie unter [Verwenden von Amazon FSx mit Ihrem selbstverwalteten Microsoft Active Directory](#).

17. Dezember 2020

[Unterstützung für die Verwendung von DNS-Aliasen hinzugefügt](#)

Sie können jetzt DNS-Alias e mit Ihren FSx for Windows File Server-Dateisystemen verknüpfen, mit denen Sie auf die Daten in Ihrem Dateisyst em zugreifen können. Weitere Informationen finden Sie unter [Verwalten von DNS-Aliasen](#) und [Walkthrough 5: Verwenden von DNS-Aliasen für den Zugriff auf Ihr Dateisyst em](#).

9. November 2020

[Unterstützung für Amazon Elastic Container Service hinzugefügt](#)

Sie können jetzt FSx for Windows File Server mit Amazon ECS verwenden. Weitere Informationen finden Sie unter [Unterstützte Clients](#).

9. November 2020

[Amazon FSx ist jetzt in integriert AWS Backup](#)

Sie können jetzt verwenden AWS Backup , um Ihre FSx-Dateisysteme zusätzlich zur Verwendung nativer Amazon-FSx-Backups zu sichern und wiederherzustellen. Weitere Informationen finden Sie unter [Verwenden von AWS Backup mit Amazon FSx](#).

9. November 2020

[Unterstützung für die Skalierung der Durchsatzkapazität hinzugefügt](#)

Sie können jetzt die Durchsatzkapazität für vorhandene FSx for Windows File Server-Datensysteme ändern, wenn sich Ihre Durchsatzanforderungen weiterentwickeln. Weitere Informationen finden Sie unter [Verwalten der Durchsatzkapazität](#).

1. Juni 2020

[Unterstützung für die Skalierung der Speicherkapazität hinzugefügt](#)

Sie können jetzt die Speicherkapazität für bestehende FSx for Windows File Server-Datensysteme erhöhen, wenn sich Ihre Speicheranforderungen weiterentwickeln. Weitere Informationen finden Sie unter [Verwalten der Speicherkapazität](#).

1. Juni 2020

[Unterstützung für Festplatten Speicher \(HDD\) hinzugefügt](#)

HDD-Speicher bietet Ihnen Preis- und Leistungsflexibilität bei der Verwendung von FSx für Windows File Server. Weitere Informationen finden Sie unter [Optimieren der Kosten mit Amazon FSx](#).

26. März 2020

[Unterstützung für die Dateiübertragung mit hinzugefügt AWS DataSync](#)

Sie können jetzt verwenden AWS DataSync , um Dateien zu und von Ihrem FSx for Windows File Server zu übertragen. Weitere Informationen finden Sie unter [Migrieren von Dateien zu Amazon FSx für Windows File Server mit AWS DataSync](#).

4. Februar 2020

[FSx for Windows File Server veröffentlicht Unterstützung für zusätzliche Verwaltungsaufgaben für das Windows-Dateisystem](#)

Sie können jetzt Dateifreigaben, Datenduplizierung, Speicherkontingente und Verschlüsselung während der Übertragung für Ihre Dateifreigaben mithilfe der Amazon FSx-CLI für die Remote-Verwaltung in PowerShell verwalten und weitere Informationen finden Sie unter [Verwalten von Dateisystemen](#).

20. November 2019

[FSx for Windows File Server veröffentlicht native Multi-AZ-Unterstützung](#)

Sie können die Multi-AZ-Bereitstellung für FSx for Windows File Server verwenden, um einfachere Dateisysteme mit hoher Verfügbarkeit zu erstellen, die sich über mehrere Availability Zones (AZs) erstrecken. Weitere Informationen finden Sie im Artikel über [Verfügbarkeit und Haltbarkeit: Einzel-AZ- und Multi-AZ-Dateisysteme](#).

20. November 2019

[FSx for Windows File Server veröffentlicht Unterstützung für die Verwaltung von Benutzersitzungen und geöffneten Dateien](#)

Sie können jetzt das in Microsoft Windows native Tool Shared Folders verwenden, um Benutzersitzungen zu verwalten und Dateien auf Ihren Dateisystemen von FSx für Windows File Server zu öffnen. Weitere Informationen finden Sie unter [Verwalten von Benutzersitzungen und offenen Dateien](#).

17. Oktober 2019

[Amazon FSx veröffentlicht Unterstützung für Microsoft Windows-Shadow-Kopien](#)

Sie können jetzt Windows-Shadow-Kopien auf Ihren Dateisystemen von FSx für Windows File Server konfigurieren. Schattenkopien ermöglichen es Ihren Benutzern, Änderungen an Dateien einfach rückgängig zu machen und Dateiversionen zu vergleichen, indem Dateien mit früheren Versionen wiederhergestellt werden. Weitere Informationen finden Sie unter [Arbeiten mit Schattenkopien](#).

31. Juli 2019

[Amazon FSx veröffentlicht gemeinsam genutzte Microsoft Active Directory-Unterstützung](#)

Sie können jetzt FSx for Windows File Server-Dateisysteme mit AWS Managed Microsoft AD Verzeichnissen verbinden, die sich in einer anderen VPC oder in einer anderen AWS-Konto als dem Dateisystem befinden. Weitere Informationen finden Sie unter [Active-Directory-Unterstützung](#).

25. Juni 2019



[Amazon FSx veröffentlicht erweiterten Microsoft Active Directory-Support](#)

Sie können jetzt FSx for Windows File Server-Datensysteme mit Ihren selbstverwalteten Microsoft Active Directory-Domains verbinden , entweder On-Premises oder in der Cloud. Weitere Informationen finden Sie unter [Active Directory Support](#).

24. Juni 2019

[Amazon FSx entspricht der SOC-Zertifizierung](#)

Amazon FSx wurde bewertet, um die SOC-Zertifizierung einzuhalten. Weitere Informationen finden Sie unter [Sicherheit und Datenschutz](#).

16. Mai 2019

[Verdeutlichender Hinweis zur Unterstützung von AWS Direct Connect, VPN und regionsübergreifenden VPC-Peering-Verbindungen hinzugefügt](#)

Amazon-FSx-Datensysteme, die nach dem 22. Februar 2019 erstellt wurden, sind über AWS Direct Connect, VPN und regionsübergreifendes VPC-Peering zugänglich. Weitere Informationen finden Sie unter [Unterstützte Zugriffsmethoden](#).

25. Februar 2019

[AWS Direct Connect Unterstützung für , VPN und regionsübergreifende VPC-Peering-Verbindungen hinzugefügt](#)

Sie können jetzt von On-Premises-Ressourcen und von Ressourcen in einer anderen Amazon VPC oder auf Datensysteme von Amazon FSx für Windows File Server zugreifen AWS-Konto. Weitere Informationen finden Sie unter [Unterstützte Zugriffsmethoden](#).

22. Februar 2019

## [Amazon FSx ist jetzt allgemein verfügbar](#)

Amazon FSx for Windows File Server bietet Microsoft -Windows-Dateiserver, die vollständig verwaltet werden und von einem vollständig nativen Windows-Dateisystem unterstützt werden. Amazon FSx for Windows File Server bietet die Funktionen, Leistung und Kompatibilität, um Unternehmensanwendungen einfach in zu verschieben AWS.

28. November 2018

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.