ONTAP-Benutzerhandbuch

FSx für ONTAP

FSx für ONTAP: ONTAP-Benutzerhandbuch

Table of Contents

Was ist Amazon FSx für NetApp ONTAP? ... 1
Funktionen von FSx für ONTAP ... 2
Sicherheit und Datenschutz ... 3
Preise für FSx für ONTAP ... 4
FSx-für-ONTAP-Foren ... 4
Verwenden Sie Amazon FSx zum ersten Mal? ... 4
Funktionsweise ... 6
Dateisysteme ... 6
Virtuelle Speichermaschinen ... 6
Datenträger ... 7
Speicherstufen ... 7
Daten-Tiering ... 8
Speichereffizienz ... 8
Zugriff auf Ihre Daten ... 8
Verwaltung von FSx for ONTAP-Ressourcen ... 8
Einrichtung ... 10
So melden Sie sich für ein AWS-Konto an ... 10
Erstellen eines Administratorbenutzers ... 11
Nächster Schritt ... 12
Erste Schritte ... 13
Erstellen Ihres FSx-für-ONTAP-Dateisystems ... 13
Schritt 2: Mounten Ihres Dateisystems ... 16
Schritt 3: Bereinigen von Ressourcen ... 19
Zugreifen auf Ihre Daten ... 21
Unterstützte Clients ... 21
Zugriff auf Daten aus dem heraus AWS ... 23
Zugreifen auf Daten aus derselben VPC ... 23
Zugreifen auf Daten aus einer anderen VPC ... 23
Zugriff auf Daten von On-Premises ... 29
Zugriff auf NFS-, SMB- oder ONTAP-CLI- oder REST-API-Endpunkte von On-Premises ... 29
Zugriff auf Cluster-übergreifende Endpunkte von On-Premises ... 32
Mounting von Volumes ... 32
Mounting auf Linux-Clients ... 34
Mounting auf Windows-Clients ... 38

Mounting auf macOS-Clients ... 40
Mounten von iSCSI-LUNs ... 42
Mounting von iSCSI LUNs an einen Linux-Client ... 43
Mounting von iSCSI LUNs an einen Windows-Client ... 54
Verwenden von FSx für ONTAP mit anderen AWS -Services ... 61
Benutzen WorkSpaces ... 61
Verwenden von Amazon ECS ... 67
Verwenden von VMware Cloud ... 71
Verfügbarkeit und Beständigkeit ... 72
Auswählen eines Dateisystem-Bereitstellungstyps ... 72
Single-AZ-Bereitstellungstyp ... 72
Multi-AZ-Bereitstellungstyp ... 73
Failover-Prozess für FSx für ONTAP ... 74
Testen des Failovers auf einem Dateisystem ... 75
Netzwerkressourcen ... 76
Subnetze ... 76
Elastic Network-Schnittstellen für Dateisysteme ... 76
Verwaltung der Speicherkapazität ... 79
Speicherstufen ... 79
Auswahl der Speicherkapazität des Dateisystems ... 81
Wie wird SSD-Speicher verwendet ... 81
Empfohlene SSD-Kapazitätsauslastung ... 82
Speichereffizienz ... 83
Speicherkapazität und IOPS des Dateisystems ... 84
Skalierung von SSD-Speicher und IOPS ... 85
Überwachung der SSD-Speichernutzung ... 87
Einen Alarm für die Speichernutzung einrichten ... 88
Einsparungen bei der Speichereffizienz anzeigen ... 92
Änderung des SSD-Speichers und der IOPS ... 94
Überwachung der Speicherkapazität und der IOPS-Updates ... 98
Dynamische Erhöhung der Speicherkapazität ... 101
Speicherkapazität des Volumens ... 106
Tiering von Volumendaten ... 107
Schnappschüsse und Speicherkapazität ... 111
Kapazität der Volumendatei ... 112
Die Speicherkapazität eines Volumes aktualisieren ... 113

Automatische Volumengrößenanpassung aktivieren 114
Überwachen Sie die Volumenspeicherkapazität 115
Festlegung der Tiering-Richtlinie für ein Volume 119
Einstellung der Kühltage 121
Richtlinie für den Cloud-Abruf festlegen 123
Die Dateikapazität eines Volumes anzeigen 124
Erhöhung der maximalen Anzahl von Dateien auf einem Volume 125
Cloud-Schreibmodus aktivieren 126
Schützen Ihrer Daten 129
Arbeiten mit Backups 129
Wie funktionieren Backups 131
Speicheranforderungen 131
Automatische tägliche Backups 131
Vom Benutzer initiierte Backups 132
Tags in Backups kopieren 133
Backup-Leistung 133
Verwendung AWS Backup mit Amazon FSx 134
Backups auf einem neuen Volume wiederherstellen 135
Löschen eines Backups 136
Backups und Offline-Volumes 136
Erstellen eines vom Benutzer initiierten Backups 137
Eine Sicherung auf einem neuen Volume wiederherstellen 137
Löschen einer Sicherung 140
Arbeiten mit Snapshots 141
Snapshot-Richtlinien 142
Wiederherstellen einzelner Dateien und Ordner 143
Wiederherstellen von Dateien aus Snapshots 143
Löschen von Snapshots 144
Erstellen einer Richtlinie zum automatischen Löschen von Snapshots 145
Snapshot löschen 145
Deaktivieren automatischer Snapshots 146
Snapshot-Reservierung 148
Aktualisieren der Snapshot-Reservierung 149
Geplante Replikation 150
Verwenden von NetApp BlueXP zum Planen der Replikation 150
Verwenden der NetApp ONTAP-CLI zum Planen der Replikation 151

Schützen von Daten mit SnapLock 151
Funktionsweise von SnapLock 151
SnapLock-Compliance 156
SnapLock Unternehmen 159
Aufbewahrungszeitraum 163
Übergeben von Dateien an WORM 165
Sichern von SnapLock Volumes 171
Löschen von SnapLock Volumes 171
Arbeiten mit Active Directory 173
Voraussetzungen für selbstverwaltetes Active Directory 174
Selbstverwaltete Active Directory-Anforderungen 174
Anforderungen an die Netzwerkkonfiguration 175
Anforderungen an Active-Directory-Servicekonten 176
Bewährte Methoden für selbstverwaltetes AD 178
Delegieren von Berechtigungen an Ihr Amazon FSx-Servicekonto 178
Halten Sie eine AD-Konfiguration auf dem neuesten Stand 179
Beschränken Sie den Verkehr innerhalb einer VPC mit Sicherheitsgruppen 180
Regeln für Sicherheitsgruppen für ausgehenden Datenverkehr erstellen 180
Verbinden von SVMs mit einem Active Directory 181
Erforderliche Active-Directory-Informationen 182
Verwalten von SVM-Active-Directory-Konfigurationen 183
Verbinden einer SVM mit Active Directory 184
Aktualisieren einer SVM-Active-Directory-Konfiguration mit AWS Konsole, CLI, API 187
Active-Directory-Konfiguration mit NetApp CLI verwalten 188
Leistung 195
Messung der Leistung 195
Latency 195
Durchsatz und IOPS 195
SMB-Multikanal- und NFS-nconnect-Unterstützung 196
Leistungsdetails 196
Auswirkungen des Bereitstellungstyps auf die Leistung 198
Auswirkungen der Speicherkapazität auf die Leistung 200
Auswirkungen der Durchsatzkapazität auf die Leistung 200
Beispiel: Speicherkapazität und Durchsatzkapazität 205
Verwaltung von Ressourcen 206
Verwalten von Dateisystemen 206

Ressourcen des Dateisystems 207
HA-Paare 209
FSx für ONTAP-Dateisysteme erstellen 210
Dateisysteme in gemeinsam genutzten Subnetzen erstellen 220
Aktualisierung eines Dateisystems 224
Löschen eines Dateisystems 227
Dateisystemdetails anzeigen 228
Status des Dateisystems 229
Verwalten von SVMs 230
Maximale Anzahl von SVMs pro Dateisystem 230
Erstellen einer SVM 231
Aktualisieren einer SVM 237
Löschen einer SVM 239
Anzeigen von SVM-Details 241
Verwaltung von Volumes 241
Lautstärkestile 243
Volume-Typen 244
Sicherheitsstil des Volumes 245
Volumen erstellen 246
Ein Volume aktualisieren 251
Löschen eines Volumes 253
Ein Volume anzeigen 255
Eine iSCSI-LUN erstellen 255
Nächste Schritte 257
Verwaltung von SMB-Aktien 257
Überwachen des Dateizugriffs 260
Überblick über die Dateizugriffsüberwachung 260
Überblick über die Aufgaben zur Einrichtung der Dateizugriffskontrolle 264
Speicherkapazität und IOPS 273
Durchsatzkapazität 273
Wann muss die Durchsatzkapazität geändert werden 274
Wie werden gleichzeitige Durchsatz- und Speicherskalierungsanforderungen behandelt 275
Wie ändert man die Durchsatzkapazität 275
Überwachung von Änderungen der Durchsatzkapazität 276
Wartungsfenster 279
Markieren Ihrer -Ressourcen mit Tags (Markierungen) 280

Grundlagen zu Tags (Markierungen) ... 281
Markieren Ihrer -Ressourcen ... 282
Kopieren von Tags in Backups ... 283
Tag (Markierung)-Einschränkungen ... 284
Berechtigungen und Tagging ... 284
Verwaltung mit Anwendungen NetApp ... 285
Eröffnen Sie ein Konto NetApp ... 285
Verwenden von NetApp BlueXP ... 286
Verwenden der NetApp ONTAP-CLI ... 287
Verwendung der ONTAP REST-API ... 291
Sicherheit ... 293
Datenschutz ... 294
Datenverschlüsselung in FSx für ONTAP ... 295
Verschlüsselung im Ruhezustand ... 295
Verschlüsseln von Daten während der Übertragung ... 297
Identity and Access Management ... 320
Zielgruppe ... 321
Authentifizierung mit Identitäten ... 321
Verwalten des Zugriffs mit Richtlinien ... 326
FSx für ONTAP und IAM ... 328
Beispiele für identitätsbasierte Richtlinien ... 335
Fehlerbehebung ... 339
Verwenden von Tags mit Amazon FSx ... 341
Verwenden von serviceverknüpften Rollen ... 347
AWS verwaltete Richtlinien ... 353
AmazonF SxServiceRolePolicy ... 354
AmazonF SxDeleteServiceLinkedRoleAccess ... 354
AmazonF SxFullAccess ... 354
AmazonF SxConsoleFullAccess ... 355
AmazonF SxConsoleReadOnlyAccess ... 356
AmazonF SxReadOnlyAccess ... 357
Richtlinienaktualisierungen ... 358
Dateisystem-Zugriffskontrolle mit Amazon VPC ... 368
Amazon VPC-Sicherheitsgruppen ... 368
Compliance-Validierung ... 371
Schnittstellen-VPC-Endpunkte ... 373

Überlegungen zu VPC-Endpunkten mit Amazon FSx-Schnittstelle ... 373
Erstellen eines VPC-Schnittstellen-Endpunkts für Amazon FSx API ... 374
Erstellen einer VPC-Endpunktrichtlinie für Amazon FSx ... 374
Ausfallsicherheit ... 375
Backup und Wiederherstellung ... 375
Snapshots ... 375
Availability Zones ... 376
Sicherheit der Infrastruktur ... 376
Verwenden Sie Antivirensoftware ... 377
ONTAP Rollen und Benutzer ... 377
Vordefinierte Rollen auf einer SVM ... 378
Neue Rollen oder Benutzer erstellen ... 381
Das Aktualisieren des `fsxadmin` Kontopassworts schlägt fehl ... 382
Neue Rollen für eine SVM mit der NetApp ONTAP CLI erstellen ... 384
Verwenden Sie Active Directory-Benutzerkonten mit Ihrem Dateisystem ... 385
Konfiguration der Authentifizierung mit öffentlichem Schlüssel ... 387
Migration zu Amazon FSx ... 389
Migrieren mit SnapMirror ... 389
Bevor Sie beginnen ... 391
Erstellen des Ziel-Volumes ... 393
Aufzeichnen der Quell- und Ziel-Cluster-übergreifenden LIFs ... 393
Einrichten von Cluster-Peering zwischen Quelle und Ziel ... 394
Erstellen einer SVM-Peering-Beziehung ... 395
Erstellen der SnapMirror Beziehung ... 396
Übertragen von Daten in Ihr FSx-für-ONTAP-Dateisystem ... 397
Umstellung auf Amazon FSx ... 398
Migrieren von Dateien mit AWS DataSync ... 399
Voraussetzungen ... 400
DataSync Grundlegende Schritte zur Migration ... 401
Überwachen von Dateisystemen ... 402
Überwachung mit CloudWatch ... 403
So verwenden Sie FSx für ONTAP CloudWatch-Metriken ... 404
Zugreifen auf CloudWatch Metriken ... 410
Dateisystemmetriken ... 413
Aufskalieren von Dateisystemmetriken ... 436
Volume-Metriken ... 456

Leistungswarnungen und Empfehlungen ... 465
Erstellen von Alarmen ... 468
Überwachen des Workload-Balance ... 471
Auslastungssaldo des primären Speichers ... 471
Ungleichgewicht bei der Dateiserver- und Festplattenleistung ... 472
Zuordnen von CloudWatch Dimensionen zu ONTAP-CLI- und REST-API-Ressourcen ... 473
Neuausgleich von Clients mit hohem Datenverkehr ... 474
Wiederherstellen des Gleichgewichts von stark ausgelasteten Volumes ... 476
Überwachen von ... 479
Übersicht über ... 479
Anzeigen von ... 480
Weiterleitung von an einen Syslog-Server ... 487
Überwachung mit Cloud Insights ... 489
Überwachung mit Bolvest und Grafana ... 490
Erste Schritte mitvest und Grafana ... 490
Unterstützte Bolvest-Dashboards ... 491
AWS CloudFormation-Vorlage ... 491
Amazon EC2-Instance-Typen ... 492
Bereitstellungsverfahren ... 492
Anmelden bei Grafana ... 496
Fehlerbehebungvest und Grafana ... 496
Protokollieren mit AWS CloudTrail ... 500
Amazon FSx Informationen in CloudTrail ... 500
Grundlagen zu Amazon FSx -Protokolldateieinträgen ... 501
Kontingente ... 504
Kontingente, die Sie erhöhen können ... 504
Ressourcenkontingente für jedes Dateisystem ... 506
Fehlerbehebung ... 509
Mein Multi-AZ-Dateisystem befindet sich in einem -MISCONFIGUREDZustand ... 509
Das VPC-Eigentümerkonto hat die Multi-AZ-VPC-Freigabe deaktiviert ... 509
Sie können keine neue SVM auf einem Multi-AZ-Dateisystem erstellen ... 510
Sie können nicht auf Ihr Dateisystem zugreifen ... 510
Die Elastic Network-Schnittstelle des Dateisystems wurde geändert oder gelöscht ... 511
Die Elastic IP-Adresse, die an die Elastic Network-Schnittstelle des Dateisystems angefügt ist, wurde gelöscht ... 511

Der VPC-Sicherheitsgruppe des Dateisystems fehlen die erforderlichen Regeln für eingehenden Datenverkehr 511
Der VPC-Sicherheitsgruppe der Datenverarbeitungs-Instance fehlen die erforderlichen Regeln für ausgehenden Datenverkehr 512
Das Subnetz der Datenverarbeitungs-Instance verwendet keine der Routing-Tabellen, die Ihrem Dateisystem zugeordnet sind 512
Amazon FSx kann die Routing-Tabelle für Multi-AZ-Dateisysteme, die mit erstellt wurden, nicht aktualisieren AWS CloudFormation 512
Kann nicht von einem Client in einer anderen VPC über iSCSI auf ein Dateisystem zugreifen 513
Das besitzende Konto hat die Freigabe des VPC-Subnetzes aufgehoben 513
Kann nicht über NFS, SMB, die ONTAP-CLI oder die ONTAP-REST-API von einem Client in einer anderen VPC oder On-Premises auf ein Dateisystem zugreifen 513
Sie können eine virtuelle Speichermaschine (SVM) nicht mit Active Directory verbinden 514
Der SVM-NetBIOS-Name entspricht dem NetBIOS-Namen für die Heimatdomäne. 514
Die SVM ist bereits mit einem anderen Active Directory verbunden 515
Amazon FSx kann keine Verbindung zu Ihren Active-Directory-Domain-Controllern herstellen, da der NetBIOS-Name der SVM bereits verwendet wird 515
Amazon FSx kann nicht mit Ihren Active-Directory-Domain-Controllern kommunizieren 516
Amazon FSx kann aufgrund nicht erfüllter Portanforderungen oder Servicekontoberechtigungen keine Verbindung zu Ihrem Active Directory herstellen 517
Amazon FSx kann keine Verbindung zu Ihren Active-Directory-Domain-Controllern herstellen, da die Anmeldeinformationen für das Servicekonto ungültig sind 517
Amazon FSx kann aufgrund unzureichender Servicekonto-Anmeldeinformationen keine Verbindung zu Ihren Active-Directory-Domain-Controllern herstellen 518
Amazon FSx kann nicht mit Ihren Active-Directory-DNS-Servern oder Domain-Controllern kommunizieren 519
Amazon FSx kann aufgrund eines ungültigen Active-Directory-Domänennamens nicht mit Ihrem Active Directory kommunizieren. 521
Das Servicekonto kann nicht auf die Administratorengruppe zugreifen, die in der SVM-Active-Directory-Konfiguration angegeben ist. 522
Amazon FSx kann keine Verbindung zu den Active-Directory-Domain-Controllern herstellen, da die angegebene Organisationseinheit nicht vorhanden ist oder nicht zugänglich ist 522
Sie können eine virtuelle Speichermaschine oder ein virtuelles Volume nicht löschen 523
Identifizieren fehlgeschlagener Löschungen 524
SVM-Löschung: Auf Routing-Tabellen kann nicht zugegriffen werden 524

SVM-Löschung: Peer-Beziehung 526
SVM- oder Volume-Löschung: SnapMirror 527
SVM-Löschung: Kerberos-fähiges LIF 528
SVM-Löschung: Anderer Grund 531
Volume-Löschung: FlexCache Beziehung 532
Automatische tägliche Backups schlagen aufgrund unzureichender Volume-Kapazität fehl 533
Sie verfügen über unzureichende Volume-Kapazität 534
Bestimmen, wie Ihre Volume-Speicherkapazität verwendet wird 534
Erhöhen der Speicherkapazität eines Volumes 534
Verwenden der automatischen Volume-Größe 534
Der primäre Speicher Ihres Dateisystems ist voll 535
Löschen von Snapshots 535
Erhöhen der maximalen Dateikapazität eines Volumes 535
Fehlerbehebung bei Netzwerkproblemen 536
Sie möchten eine Paketverfolgung erfassen 536
Dokumentverlauf 540
..... dlvi

Was ist Amazon FSx für NetApp ONTAP?

Amazon FSx für NetApp ONTAP ist ein vollständig verwalteter Service, der äußerst zuverlässigen, skalierbaren, leistungsstarken und funktionsreichen Dateispeicher bietet, der auf dem beliebten ONTAP-Dateisystem von NetAppaufbaut. FSx für ONTAP kombiniert die vertrauten Features, Leistung, Funktionen und API-Operationen von NetApp Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit einer vollständig verwalteten AWS-Service.

FSx für ONTAP bietet funktionsreichen, schnellen und flexiblen gemeinsamen Dateispeicher, auf den allgemein von Linux-, Windows- und macOS-Computing-Instances zugegriffen werden kann, die in AWS oder On-Premises ausgeführt werden. FSx für ONTAP bietet Hochleistungsspeicher für Solid-State-Laufwerke (SSD) mit Latenzen von unter einer Millisekunde. Mit FSx für ONTAP können Sie SSD-Leistung für Ihren Workload erreichen und gleichzeitig nur für einen kleinen Teil Ihrer Daten für SSD-Speicher bezahlen.

Die Verwaltung Ihrer Daten mit FSx für ONTAP ist einfacher, da Sie Ihre Dateien mit einem Klick auf eine Schaltfläche mit Snapshots, Klonen und Replizieren können. FSx für ONTAP stuft Ihre Daten außerdem automatisch auf kostengünstigeren, elastischen Speicher ein, sodass Sie weniger Kapazität bereitstellen oder verwalten müssen.

FSx für ONTAP bietet auch hochverfügbaren und dauerhaften Speicher mit vollständig verwalteten Backups und Unterstützung für regionsübergreifende Notfallwiederherstellung. Um den Schutz und die Sicherung Ihrer Daten zu vereinfachen, unterstützt FSx für ONTAP beliebte Datensicherheits- und Antivirenanwendungen.

Für Kunden, die NetApp ONTAP On-Premises verwenden, ist FSx für ONTAP eine ideale Lösung, um Ihre dateibasierten Anwendungen von On-Premises zu zu migrieren, zu sichern oder zu pushen, AWS ohne dass Sie Ihren Anwendungscode ändern oder Ihre Daten verwalten müssen.

Als vollständig verwalteter Service erleichtert FSx für ONTAP das Starten und Skalieren eines zuverlässigen, leistungsstarken und sicheren freigegebenen Dateispeichers in der Cloud. Mit FSx für ONTAP müssen Sie sich keine Gedanken mehr machen über:

- Einrichten und Bereitstellen von Dateiservern und Speicher-Volumes
- Replizieren von Daten
- Installieren und Patchen von Dateiserversoftware
- Erkennen und Beheben von Hardwarefehlern

- Verwalten von Failover und Failover
- Manuelles Ausführen von Backups

FSx für ONTAP bietet auch eine umfassende Integration mit anderen -AWSServices wie AWS Identity and Access Management (IAM), Amazon WorkSpaces, AWS Key Management Service (AWS KMS) und AWS CloudTrail.

Themen

- Funktionen von FSx für ONTAP
- Sicherheit und Datenschutz
- Preise für FSx für ONTAP
- FSx-für-ONTAP-Foren
- Verwenden Sie Amazon FSx zum ersten Mal?

Funktionen von FSx für ONTAP

Mit FSx für ONTAP erhalten Sie eine vollständig verwaltete Dateispeicherlösung mit:

- Unterstützung für Datensätze im Petabyte-Bereich in einem einzigen Namespace
- Bis zu zehn Gigabyte pro Sekunde (GBps) Durchsatz pro Dateisystem
- Multiprotokollzugriff auf Daten mithilfe der Protokolle Network File System (NFS), Server Message Block (SMB) und Internet Small Computer Systems Interface (iSCSI)
- Hochverfügbare und dauerhafte Multi-AZ- und Single-AZ-Bereitstellungsoptionen
- Automatisches Daten-Tiering, das die Speicherkosten senkt, indem Daten, auf die selten zugegriffen wird, basierend auf Ihren Zugriffsmustern automatisch in eine kostengünstigere Speicherebene überführt werden
- Datenkomprimierung, Deduplizierung und Verdichtung zur Reduzierung Ihres Speicherverbrauchs
- Unterstützung für NetAppdie SnapMirror Replikationsfunktion von
- Unterstützung für NetAppdie On-Premises-Caching-Lösungen von: NetApp Global File Cache und FlexCache
- Unterstützung für den Zugriff und die Verwaltung mit nativen AWS oder NetApp Tools und API-Operationen
  - AWS Management Console, AWS Command Line Interface (AWS CLI) und -SDKs

  - NetApp ONTAP-CLI, REST-API und BlueXP
- Unterstützung für die folgenden Datenschutz- und Sicherheitsfunktionen:
  - Verschlüsselung von Dateisystemdaten und Backups im Ruhezustand mit AWS KMS keys
  - Verschlüsselung von Daten während der Übertragung mit SMB-Kerberos-Sitzungsschlüsseln
  - On-Demand-Antivirenscan
  - Authentifizierung und Autorisierung mit Microsoft Active Directory
  - Prüfung des Dateizugriffs
  - NetApp's SnapLock -Funktion mit Unterstützung sowohl für Compliance- als auch für Enterprise-Volumes

Sicherheit und Datenschutz

Amazon FSx bietet mehrere Sicherheits- und Compliance-Stufen, um den Schutz Ihrer Daten zu erleichtern. Es verschlüsselt automatisch Daten im Ruhezustand in Dateisystemen und Backups mit Schlüsseln, die Sie in AWS Key Management Service () verwaltenAWS KMS. Sie können Daten auch während der Übertragung mit Kerberos für NFS- und SMB-Clients verschlüsseln.

Amazon FSx wurde bewertet, um die folgenden Standards zu erfüllen:

- International Standards Organization (ISO)
- Payment Card Industry Data Security Standard (PCI DSS)
- System and Organization Controls (SOC)-Zertifizierungen
- Der Health Insurance Portability and Accountability Act von 1996 (HIPAA)

Weitere Informationen finden Sie unter Datenschutz in Amazon FSx for NetApp ONTAP.

Amazon FSx bietet auch die folgenden Zugriffssteuerungsebenen:

- Auf Dateisystemebene bietet Amazon FSx die Zugriffskontrolle mithilfe von Amazon Virtual Private Cloud (Amazon VPC)-Sicherheitsgruppen.
- Auf API-Ebene bietet Amazon FSx Zugriffskontrolle mithilfe von AWS Identity and Access Management (IAM)-Zugriffsrichtlinien.
- Um die Zugriffskontrolle auf Datei- und Ordnerebene bereitzustellen, unterstützt Amazon FSx Unix-Berechtigungen, NFS-Zugriffskontrolllisten (ACLs) und NTFS-ACLs . Wenn Sie Amazon FSx mit

einem Active Directory verbinden, können sich Benutzer, die auf Dateisysteme zugreifen, mit ihren Active-Directory-Anmeldeinformationen authentifizieren.

Damit Sie die von Benutzern auf Ihren Amazon-FSx-Ressourcen durchgeführten Aktionen sehen können, lässt sich Amazon FSx in integrieren, AWS CloudTrail um Ihre Amazon-FSx-API-Aufrufe zu überwachen und zu protokollieren. Weitere Informationen finden Sie unter Protokollieren von FSx für ONTAP-API-Aufrufe mitAWS CloudTrail.

Darüber hinaus schützt Amazon FSx Ihre Daten mit äußerst dauerhaften Dateisystem-Backups. Amazon FSx führt automatische tägliche Backups durch, und Sie können jederzeit zusätzliche Backups erstellen. Weitere Informationen finden Sie unter Schützen Ihrer Daten.

Preise für FSx für ONTAP

Dateisysteme, die auf den folgenden Kategorien basieren, werden Ihnen in Rechnung gestellt:

- SSD-Speicherkapazität (pro Gigabyte-Monat oder GB-Monat)
- SSD-IOPS, die Sie über drei IOPS/GB bereitstellen (pro IOPS-Monat)
- Durchsatzkapazität (pro Megabyte pro Sekunde [MBps-Monat)
- Kapazitätspool-Speicherverbrauch (pro GB-Monat)
- Kapazitätspool-Anforderungen (pro Lese- und Schreibvorgang)
- Backup-Speicherverbrauch (pro GB-Monat)

Weitere Informationen zu Preisen und Gebühren für den Service finden Sie unter Amazon FSx für NetApp ONTAP – Preise.

FSx-für-ONTAP-Foren

Wenn bei der Verwendung von Amazon FSx Probleme auftreten, verwenden Sie die FSx-für-ONTAP-Diskussionsforen, um Antworten zu erhalten.

Verwenden Sie Amazon FSx zum ersten Mal?

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

1. Wenn Sie noch nicht mit vertraut sindAWS, finden Sie weitere Informationen unter , Einrichten von FSx für ONTAP um ein einzurichtenAWS-Konto.
2. Wenn Sie bereit sind, Ihr erstes Amazon-FSx-Dateisystem zu erstellen, folgen Sie den Anweisungen unter Erste Schritte mit Amazon FSx für NetApp ONTAP.
3. Informationen zur Leistung finden Sie unter Leistung von Amazon FSx für NetApp ONTAP.
4. Details zur Amazon-FSx-Sicherheit finden Sie unter Sicherheit in Amazon FSx für ONTAP NetApp .
5. Weitere Informationen zur Amazon-FSx-API finden Sie in der Amazon-FSx-API-Referenz.

So funktioniert Amazon FSx for NetApp ONTAP

In diesem Thema werden die wichtigsten Funktionen von Amazon FSx für NetApp ONTAP-Dateisysteme und deren Funktionsweise vorgestellt. Es enthält Links zu Abschnitten mit ausführlichen Beschreibungen, wichtigen Implementierungsdetails und step-by-step Konfigurationsverfahren.

Themen

- FSx-für-ONTAP-Dateisysteme
- Virtuelle Speichermaschinen
- Datenträger
- Speicherstufen
- Speichereffizienz
- Zugreifen auf Daten, die auf FSx für ONTAP-Dateisysteme gespeichert sind
- Verwaltung von FSx for ONTAP-Ressourcen

FSx-für-ONTAP-Dateisysteme

Ein Dateisystem ist die primäre FSx-Ressource für ONTAP, analog zu einem lokalen NetApp ONTAP-Cluster. Sie geben die Solid-State-Drive-Speicherkapazität (SSD) und die Durchsatzkapazität für Ihr Dateisystem an und wählen eine Amazon Virtual Private Cloud (VPC), in der Ihr Dateisystem erstellt wird. Weitere Informationen finden Sie unter Verwaltung von FSx für ONTAP-Dateisysteme.

Ihr Dateisystem kann je nach Konfiguration aus einem bis zwölf Hochverfügbarkeitspaaren (HA) bestehen. Ein HA-Paar besteht aus zwei Dateiservern in einer Active-Standby-Konfiguration. Dateisysteme mit einem einzigen HA-Paar werden als Scale-up-Dateisysteme bezeichnet. Dateisysteme mit mehreren HA-Paaren werden als Scale-Out-Dateisysteme bezeichnet. Weitere Informationen finden Sie unter Paare mit hoher Verfügbarkeit (HA).

Virtuelle Speichermaschinen

Eine virtuelle Speichermaschine (SVM) ist ein isolierter Dateiserver mit eigenen Verwaltungs- und Datenzugriffsendpunkten für die Verwaltung und den Zugriff auf Daten. Wenn Sie auf Daten in Ihrem

FSx for ONTAP-Dateisystem zugreifen, stellen Ihre Clients und Workstations über die Endpunkt-IP-Adresse der SVM eine Verbindung zu einer SVM her. Weitere Informationen finden Sie unter Verwalten von SVMs.

Sie können SVMs einem Microsoft Active Directory hinzufügen, um den Dateizugriff zu authentifizieren und zu autorisieren. Weitere Informationen finden Sie unter Arbeiten mit Microsoft Active Directory in FSx für ONTAP.

Datenträger

FSx for ONTAP-Volumes sind virtuelle Ressourcen, die Sie für die Organisation und Gruppierung Ihrer Daten verwenden. Volumes sind logische Container, die auf SVMs gehostet werden, und die darin gespeicherten Daten verbrauchen physische Speicherkapazität auf Ihrem Dateisystem.

Wenn Sie ein Volume erstellen, legen Sie dessen Größe fest, wodurch die Menge der physischen Daten bestimmt wird, die Sie darauf speichern können, unabhängig davon, auf welcher Speicherebene die Daten gespeichert werden. Sie legen auch den Volumetyp fest, entweder RW (lesbar) oder DP (Datenschutz). Ein DP-Volume ist schreibgeschützt und kann als Ziel in einer Oder-Beziehung verwendet werden. NetApp SnapMirror SnapVault

FSx for ONTAP-Volumes sind Thin Provisioning, was bedeutet, dass sie nur Speicherkapazität für die darin gespeicherten Daten verbrauchen. Bei Volumes mit Thin-Provisioning wird Speicherkapazität nicht im Voraus reserviert. Stattdessen wird der Speicher dynamisch zugewiesen, wenn er benötigt wird. Freier Speicherplatz wird wieder für das Dateisystem freigegeben, wenn Daten auf dem Volume oder der LUN gelöscht werden. Sie können beispielsweise drei 10-TiB-Volumes in einem Dateisystem erstellen, das mit 10 TiB freier Speicherkapazität konfiguriert ist, sofern die Gesamtmenge der auf den drei Volumes gespeicherten Daten zu keinem Zeitpunkt 10 TiB überschreitet. Die Menge der physisch auf einem Volume gespeicherten Daten wird auf Ihren Gesamtverbrauch an Speicherkapazität angerechnet. Weitere Informationen finden Sie unter Verwaltung von FSx für ONTAP-Volumes.

Speicherstufen

Ein FSx for ONTAP-Dateisystem hat zwei Speicherstufen: Primärspeicher und Kapazitätspoolspeicher. Primärspeicher ist ein bereitgestellter, skalierbarer, leistungsstarker SSD-Speicher, der speziell für den aktiven Teil Ihres Datensatzes entwickelt wurde. Beim Kapazitätspoolspeicher handelt es sich um eine vollständig elastische Speicherebene, die auf Petabyte skaliert werden kann und für Daten, auf die selten zugegriffen wird, kostenoptimiert ist.

Daten, die Sie auf Ihre Volumes schreiben, verbrauchen Kapazität auf Ihren Speicherebenen. Weitere Informationen finden Sie unter FSx für ONTAP Speicherstufen.

Daten-Tiering

Data Tiering ist der Prozess, bei dem Amazon FSx for NetApp ONTAP automatisch Daten zwischen der SSD und den Speicherstufen des Kapazitätspools verschiebt. Jedes Volume verfügt über eine Tiering-Richtlinie, die steuert, ob Daten auf die Kapazitätsstufe verschoben werden, wenn sie inaktiv (kalt) werden. Die Kühlperiode eines Volumes bestimmt, wann Daten inaktiv (kalt) werden. Weitere Informationen finden Sie unter Tiering von Volumendaten.

Speichereffizienz

Amazon FSx for NetApp ONTAP unterstützt die Speichereffizienzfunktionen von ONTAP auf Blockebene — Komprimierung, Komprimierung und Deduplizierung —, um die Speicherkapazität zu reduzieren, die Ihre Daten verbrauchen. Funktionen zur Speichereffizienz können den Platzbedarf Ihrer Daten im SSD-Speicher, im Kapazitätspool-Speicher und in Backups reduzieren. Die typischen Einsparungen an Speicherkapazität bei allgemeinen Filesharing-Workloads ohne Leistungseinbußen betragen 65% durch Komprimierung, Deduplizierung und Verdichtung, und zwar sowohl auf der SSD- als auch auf der Speicherebene des Kapazitätspools. Weitere Informationen finden Sie unter FSx für ONTAP-Speichereffizienz.

Zugreifen auf Daten, die auf FSx für ONTAP-Dateisysteme gespeichert sind

Sie können auf Ihre Daten auf FSx for ONTAP-Volumes von mehreren Linux-, Windows- oder macOS-Clients gleichzeitig über die Protokolle NFS (v3, v4, v4.1, v4.2) und SMB zugreifen. Sie können auch mit dem iSCSI-Protokoll (Block) auf Daten zugreifen. Weitere Informationen finden Sie unter Zugriff auf -Daten.

Verwaltung von FSx for ONTAP-Ressourcen

Es gibt mehrere Möglichkeiten, mit Ihrem FSx for ONTAP-Dateisystem zu interagieren und dessen Ressourcen zu verwalten. Sie können Ihre FSx for ONTAP-Ressourcen sowohl mit den ONTAP-Management-Tools als auch mit den AWS NetApp ONTAP-Management-Tools verwalten:

- AWS Verwaltungstools

  - Die AWS Management Console
  - Das AWS Command Line Interface (AWS CLI)
  - Die Amazon FSx-API und die SDKs
  - AWS CloudFormation
- NetApp Verwaltungstools:
  - NetApp BlueXP
  - Die NetApp ONTAP CLI
  - Die NetApp ONTAP REST API

Weitere Informationen finden Sie unter Verwaltung von Ressourcen.

Einrichten von FSx für ONTAP

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

1. So melden Sie sich für ein AWS-Konto an
2. Erstellen eines Administratorbenutzers

Themen

- So melden Sie sich für ein AWS-Konto an
- Erstellen eines Administratorbenutzers
- Nächster Schritt

So melden Sie sich für ein AWS-Konto an

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Anmeldung für ein 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 ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen eine Bestätigungs-E-Mail, sobald die Anmeldung abgeschlossen ist. 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 eines Administratorbenutzers

Nachdem Sie sich für ein AWS-Kontoangemeldet haben, sichern Sie Ihr Root-Benutzer des AWS-Kontos, aktivieren Sie AWS IAM Identity Centerund erstellen Sie einen administrativen Benutzer, damit Sie nicht den Root-Benutzer für alltägliche Aufgaben verwenden.

Schützen Ihres Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei der AWS Management Console als Kontobesitzer 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-AnmeldungBenutzerhandbuch zu .
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen dazu finden Sie unter Aktivieren eines virtuellen MFA-Geräts für den Root-Benutzer Ihres AWS-Konto (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Administratorbenutzers

1. Aktivieren von IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Im IAM Identity Center gewähren Sie einem administrativen Benutzer administrativen Zugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit dem standardmäßigen IAM-Identity-Center-Verzeichnis konfigurieren im AWS IAM Identity Center-Benutzerhandbuch.

Anmelden als Administratorbenutzer

- 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 unter Anmelden beim AWS-Zugangsportal im AWS-Anmeldung Benutzerhandbuch zu.

Nächster Schritt

Anweisungen zum Erstellen Ihrer Amazon-FSx-Ressourcen Erste Schritte mit Amazon FSx für NetApp ONTAP finden Sie unter FSx für ONTAP.

Erste Schritte mit Amazon FSx für NetApp ONTAP

Erfahren Sie, wie Sie mit der Verwendung von Amazon FSx für NetApp ONTAP beginnen. Diese Übung „Erste Schritte“ umfasst die folgenden Schritte.

Themen

- Schritt 1: Erstellen eines Dateisystems von Amazon FSx für NetApp ONTAP
- Schritt 2: Mounten Ihres Dateisystems von einer Amazon EC2-Linux-Instance
- Schritt 3: Bereinigen von Ressourcen

Schritt 1: Erstellen eines Dateisystems von Amazon FSx für NetApp ONTAP

Die Amazon-FSx-Konsole bietet zwei Optionen zum Erstellen eines Dateisystems: eine Option Schnellerstellung und eine Option Standarderstellung. Verwenden Sie die Option Schnellerstellung, um schnell und einfach ein Dateisystem von Amazon FSx für NetApp ONTAP mit der vom Service empfohlenen Konfiguration zu erstellen.

Die Option Schnellerstellung erstellt ein Dateisystem mit einem einzigen Hochverfügbarkeitspaar (HA), einer virtuellen Einzelspeichermaschine (SVM) und einem einzigen Volume. Mit der Option Schnellerstellung wird dieses Dateisystem so konfiguriert, dass der Datenzugriff von Linux-Instances über das Network File System (NFS)-Protokoll ermöglicht wird. Nachdem Ihr Dateisystem erstellt wurde, können Sie nach Bedarf zusätzliche SVMs und Volumes erstellen, einschließlich einer SVM, die mit einem Active Directory verbunden ist, um den Zugriff von Windows- und macOS-Clients über das Server Message Block (SMB)-Protokoll zu ermöglichen.

Informationen zur Verwendung der Standarderstellungsoption zum Erstellen eines Dateisystems mit einer benutzerdefinierten Konfiguration und zur Verwendung der AWS CLI und API finden Sie unter FSx für ONTAP-Dateisysteme erstellen.

So erstellen Sie Ihr -Dateisystem:

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 Dateisystemtyp auswählen Amazon FSx für NetApp ONTAP und dann Weiter aus. Die Seite ONTAP-Dateisystem erstellen wird angezeigt.
4. Wählen Sie für Erstellungsmethode die Option Schnellerstellung aus.
5. Geben Sie im Abschnitt Schnellkonfiguration für Dateisystemname – optional einen Namen für Ihr Dateisystem ein. 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 folgenden Sonderzeichen verwenden: + - (Bindestrich) = . _ (Unterstrich): /
6. Wählen Sie für Bereitstellungstyp Multi-AZ oder Single-AZ aus.

   - Multi-AZ-Dateisysteme replizieren Ihre Daten und unterstützen Failover über mehrere Availability Zones in derselben AWS-Region.
   - Single-AZ-Dateisysteme replizieren Ihre Daten und bieten ein automatisches Failover innerhalb einer einzigen Availability Zone.

   Weitere Informationen finden Sie unter Verfügbarkeit und Beständigkeit.
7. Geben Sie für SSD-Speicherkapazität die Speicherkapazität Ihres Dateisystems in Gibibyte () anGiBs. Geben Sie eine ganze Zahl im Bereich von 1.024 bis 196.608 ein. Wenn Sie mehr SSD-Speicherkapazität benötigen, können Sie Standarderstellung verwenden. Weitere Informationen finden Sie unter Um ein Dateisystem (Konsole) zu erstellen.

   Sie können die Speicherkapazität jederzeit nach Bedarf erhöhen, nachdem Sie das Dateisystem erstellt haben. Weitere Informationen finden Sie unter Verwaltung der Speicherkapazität.
8. Für die Durchsatzkapazität stellt Amazon FSx automatisch eine empfohlene Durchsatzkapazität bereit, die auf Ihrem SSD-Speicher basiert. Sie können auch den Durchsatz Ihres Dateisystems (bis zu 4 096 MBps auswählen. Wenn Sie mehr Durchsatzkapazität benötigen, können Sie Standarderstellung verwenden.
9. Wählen Sie für Virtual Private Cloud (VPC) die Amazon VPC aus, die Sie Ihrem Dateisystem zuordnen möchten.
10. Wählen Sie für Speichereffizienz die Option Aktiviert aus, um die ONTAP-Speichereffizienzfunktionen (Komprimierung, Deduplizierung und Verdichtung) zu aktivieren, oder Deaktiviert, um sie auszuschalten.
11. (Nur Multi-AZ) Der Endpunkt-IP-Adressbereich gibt den IP-Adressbereich an, in dem die Endpunkte für den Zugriff auf Ihr Dateisystem erstellt werden.

    Wählen Sie eine Option Schnellerstellung für den Endpunkt-IP-Adressbereich aus:

- Nicht zugewiesener IP-Adressbereich aus Ihrer VPC – Wählen Sie diese Option, damit Amazon FSx die letzten 64 IP-Adressen aus dem primären CIDR-Bereich der VPC als Endpunkt-IP-Adressbereich für das Dateisystem verwendet. Beachten Sie, dass dieser Bereich für mehrere Dateisysteme gemeinsam genutzt wird, wenn Sie diese Option mehrmals auswählen.

  > **Note**
  >
  > - Jedes Dateisystem, das Sie erstellen, verbraucht zwei IP-Adressen aus diesem Bereich – eine für den Cluster und eine für die erste SVM. Die erste und letzte IP-Adresse sind ebenfalls reserviert. Für jede zusätzliche SVM verwendet das Dateisystem eine weitere IP-Adresse. Beispielsweise verwendet ein Dateisystem, das 10 SVMs hostet, 11 IP-Adressen. Zusätzliche Dateisysteme funktionieren auf die gleiche Weise. Sie verbrauchen die beiden anfänglichen IP-Adressen plus eine für jede zusätzliche SVM. Die maximale Anzahl von Dateisystemen, die denselben IP-Adressbereich verwenden, jedes mit einer einzelnen SVM, beträgt 31.
  > - Diese Option ist ausgegraut, wenn eine der letzten 64 IP-Adressen im primären CIDR-Bereich einer VPC von einem Subnetz verwendet wird.

- Gleitender IP-Adressbereich außerhalb Ihrer VPC – Wählen Sie diese Option, damit Amazon FSx einen 198.19.x.0/24-Adressbereich verwendet, der noch nicht von anderen Dateisystemen mit derselben VPC und denselben Routing-Tabellen verwendet wird.

Sie können auch Ihren eigenen IP-Adressbereich in der Option Standarderstellung angeben.

12. Wählen Sie Weiter und überprüfen Sie die Dateisystemkonfiguration auf der Seite ONTAP-Dateisystem erstellen. Beachten Sie, welche Dateisystemeinstellungen Sie ändern können, nachdem das Dateisystem erstellt wurde.
13. Wählen Sie Create file system (Dateisystem erstellen) aus.

Quick Create erstellt ein Dateisystem mit einer SVM (benannt `fsx`) und einem Volume (benannt `vol1`). Das Volume verfügt über einen Verbindungspfad von `/vol1` und eine Kapazitätspool-Tiering-Richtlinie von Auto (die automatisch alle Daten, auf die 31 Tage lang nicht zugegriffen wurde, auf einen kostengünstigeren Kapazitätspoolspeicher abstuft). Die Standard-Snapshot-Richtlinie wird dem Standard-Volume zugewiesen. Die Dateisystemdaten werden im Ruhezustand mit Ihrem standardmäßigen serviceverwalteten AWS KMS Schlüssel verschlüsselt.

Schritt 2: Mounten Ihres Dateisystems von einer Amazon EC2-Linux-Instance

Sie können Ihr Dateisystem von einer Amazon Elastic Compute Cloud (Amazon EC2)-Instance mounten. Bei diesem Verfahren wird eine Instance verwendet, auf der Amazon Linux 2 ausgeführt wird.

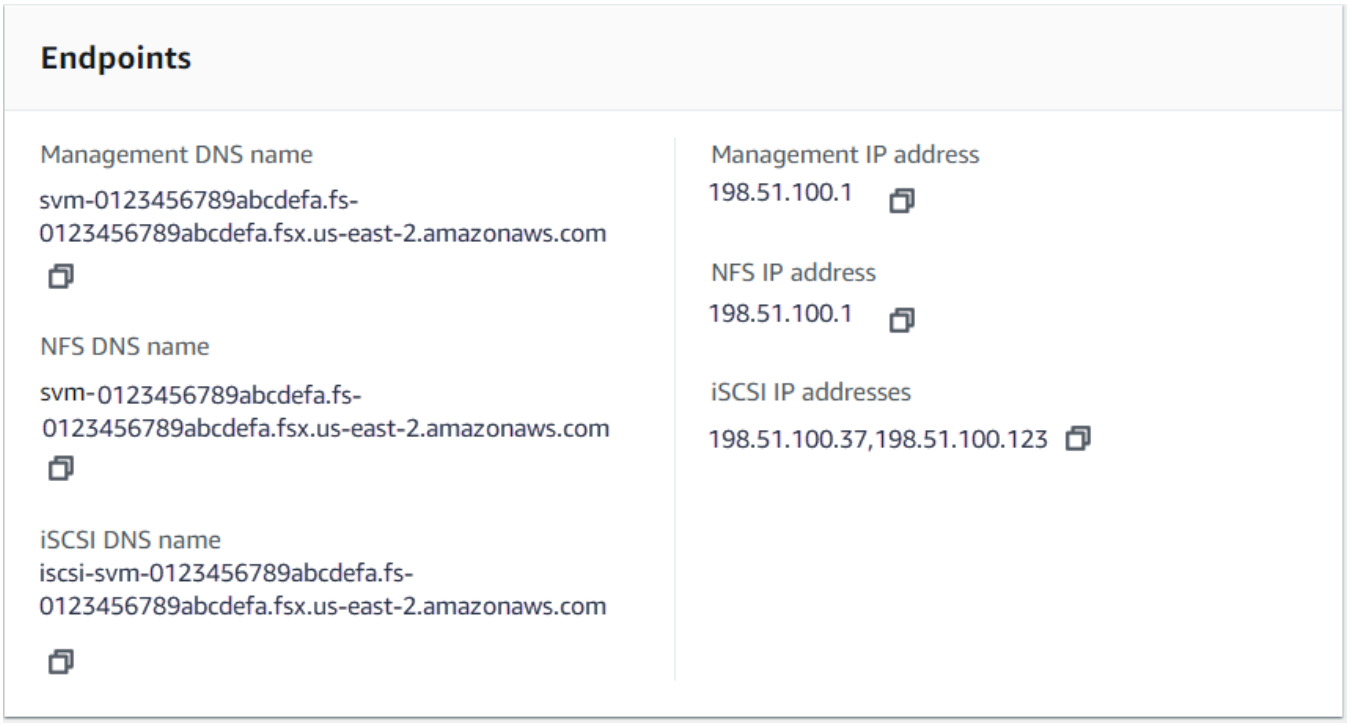
So mounten Sie Ihr Dateisystem von Amazon EC2 aus

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Erstellen oder wählen Sie eine Amazon EC2-Instance mit Amazon Linux 2 aus, die sich in derselben Virtual Private Cloud (VPC) wie Ihr Dateisystem befindet. Weitere Informationen zum Starten einer Instance finden Sie unter Schritt 1: Starten einer Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances.
3. Stellen Sie eine Verbindung zu Ihrer Amazon EC2 Linux-Instance her. Weitere Informationen finden Sie unter Verbinden Sie sich mit Ihrer Linux-Instance im Benutzerhandbuch zu Amazon EC2 für Linux-Instances.
4. Öffnen Sie ein Terminal auf Ihrer Amazon EC2-Instance mit Secure Shell (SSH) und melden Sie sich mit den entsprechenden Anmeldeinformationen an.
5. Erstellen Sie ein Verzeichnis auf Ihrer Amazon EC2-Instance, das Sie als Mountingpunkt des Volumes mit dem folgenden Befehl verwenden können. Ersetzen Sie im folgenden Beispiel *mount-point* durch Ihre eigenen Informationen.

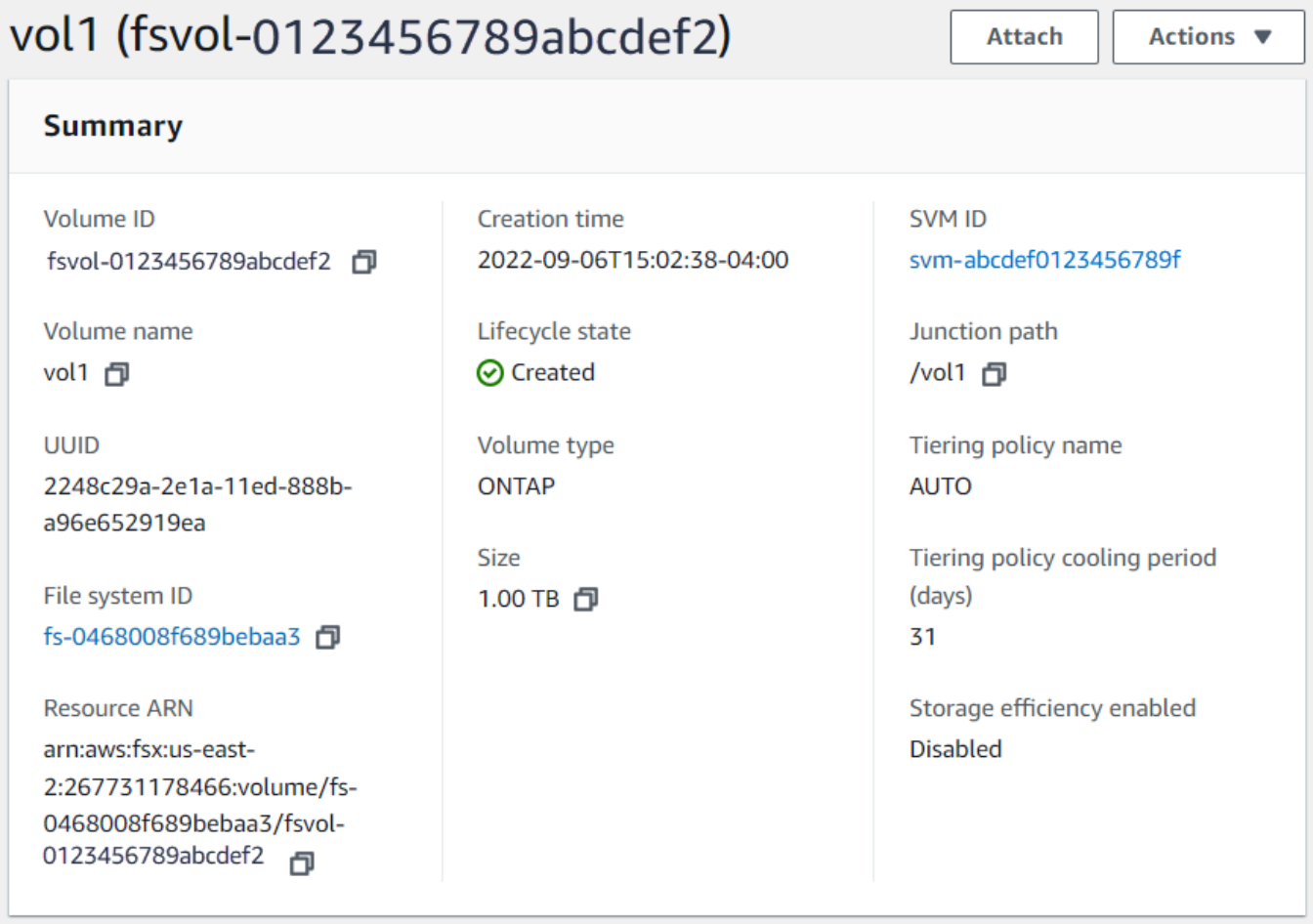
   ```
   $ sudo mkdir /mount-point
   ```

6. Mounten Sie Ihr Dateisystem von Amazon FSx für NetApp ONTAP in das von Ihnen erstellte Verzeichnis. Verwenden Sie einen `mount` Befehl ähnlich dem folgenden Beispiel. Ersetzen Sie im folgenden Beispiel die folgenden Platzhalterwerte durch Ihre eigenen Informationen.

   - *nfs_version* – Die NFS-Version, die Sie verwenden; FSx für ONTAP unterstützt die Versionen 3, 4.0, 4.1 und 4.2.
   - *nfs-dns-name* – Der NFS-DNS-Name der virtuellen Speichermaschine (SVM), in der sich das Volume befindet, das Sie mounten. Sie finden den NFS-DNS-Namen in der Amazon-FSx-Konsole, indem Sie Virtuelle Speichermaschinen und dann die SVM auswählen, auf der das Volume gemountet wird. Der NFS-DNS-Name befindet sich im Bereich Endpunkte, wie in der folgenden Abbildung dargestellt.



- *`volume-junction-path`* – Der Verbindungspfad des Volumes, das Sie mounten. Sie finden den Verbindungspfad eines Volumes in der Amazon-FSx-Konsole im Bereich Zusammenfassung der Seite Volume-Details, wie in der folgenden Abbildung dargestellt.



- *`mount-point`* – Der Name des Verzeichnisses, das Sie auf Ihrer EC2-Instance für den Mountingpunkt des Volumes erstellt haben.

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

Der folgende Befehl verwendet Beispielwerte.

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

Wenn Sie Probleme mit Ihrer Amazon EC2-Instance haben (z. B. Verbindungs-Timeout), finden Sie weitere Informationen unter Fehlerbehebung bei EC2-Instances im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Schritt 3: Bereinigen von Ressourcen

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

So bereinigen Sie Ressourcen

1. Beenden Sie in der Amazon EC2-Konsole Ihre Instance. Weitere Informationen finden Sie unter Beenden Ihrer Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances.
2. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
3. Löschen Sie in der Amazon-FSx-Konsole alle Ihre FSx-für-ONTAP-Volumes, die keine Root-Volumes Ihrer SVM sind. Weitere Informationen finden Sie unter Löschen eines Volumes.
4. Löschen Sie alle Ihre FSx-für-ONTAP-SVMs. Weitere Informationen finden Sie unter Löschen einer virtuellen Speichermaschine (SVM).
5. Löschen Sie in der Amazon-FSx-Konsole Ihr Dateisystem. Wenn Sie ein Dateisystem löschen, werden alle automatischen Backups automatisch gelöscht. Sie müssen jedoch weiterhin manuell erstellte Backups löschen. In den folgenden Schritten wird dieser Prozess beschrieben.

    a. Wählen Sie im Dashboard der Konsole den Namen des Dateisystems aus, das Sie für diese Übung erstellt haben.

    b. Klicken Sie bei Aktionen auf Dateisystem löschen.

    c. Geben Sie im Dialogfeld Dateisystem löschen die ID des Dateisystems, das Sie löschen möchten, in das Feld Dateisystem-ID ein.

    d. Wählen Sie Dateisystem löschen aus.

    e. Während Amazon FSx das Dateisystem löscht, ändert sich sein Status im Dashboard in DELETING . Sobald das Dateisystem gelöscht wurde, wird es nicht mehr im Dashboard angezeigt. Alle automatischen Backups werden zusammen mit dem Dateisystem gelöscht.

    f. Jetzt können Sie alle manuell erstellten Backups für Ihr Dateisystem löschen. Wählen Sie in der linken Navigation Backups aus.

    g. Wählen Sie im Dashboard alle Backups aus, die dieselbe Dateisystem-ID wie das Dateisystem haben, das Sie gelöscht haben, und wählen Sie Sicherung löschen aus. Stellen Sie sicher, dass Sie das endgültige Backup aufbewahren, falls Sie eines erstellt haben.

    h. Das Dialogfeld Backups löschen wird geöffnet. Lassen Sie das Kontrollkästchen für die IDs der Backups aktiviert, die Sie löschen möchten, und wählen Sie dann Backups löschen aus.

Ihr Amazon-FSx-Dateisystem und alle zugehörigen automatischen Backups werden jetzt zusammen mit allen manuellen Backups gelöscht, die Sie ebenfalls löschen möchten.

Zugriff auf -Daten

Sie können auf Ihre Amazon-FSx-Dateisysteme zugreifen, indem Sie eine Vielzahl von unterstützten Clients und Methoden sowohl in der - AWS Cloud als auch in der On-Premises-Umgebung verwenden.

Jede SVM verfügt über vier Endpunkte, die für den Zugriff auf Daten oder die Verwaltung der SVM mithilfe der NetApp ONTAP-CLI oder REST-API verwendet werden:

- `Nfs` – Zum Herstellen einer Verbindung über das Network File System (NFS)-Protokoll
- `Smb` – Zum Herstellen einer Verbindung über das Service Message Block (SMB)-Protokoll (Wenn Ihre SVM mit einem Active Directory verbunden ist oder Sie eine Arbeitsgruppe verwenden).
- `Iscsi` – Zum Herstellen einer Verbindung über das Internet Small Computer Systems Interface (iSCSI)-Protokoll (nur für Scale-up-Dateisysteme).
- `Management` – Zur Verwaltung von SVMs mit der NetApp ONTAP-CLI oder -API oder NetApp BlueXP

Themen

- Unterstützte Clients
- Zugriff auf Daten aus dem heraus AWS
- Zugriff auf Daten von On-Premises
- Mounting von Volumes
- Mounten von iSCSI-LUNs
- Verwenden von FSx für ONTAP mit anderen AWS -Services

Unterstützte Clients

Dateisysteme von FSx für ONTAP unterstützen den Zugriff auf Daten von einer Vielzahl von Datenverarbeitungs-Instances und Betriebssystemen. Dies geschieht, indem der Zugriff über das Network File System (NFS)-Protokoll (v3, v4.0, v4.1 und v4.2), alle Versionen des Server Message Block (SMB)-Protokolls (einschließlich 2.0, 3.0 und 3.1.1) und das Internet Small Computer Systems Interface (iSCSI)-Protokoll unterstützt wird.

> **Important**
>
> Amazon FSx unterstützt nicht den Zugriff auf Dateisysteme aus dem öffentlichen Internet. Amazon FSx trennt automatisch jede Elastic IP-Adresse, bei der es sich um eine öffentliche IP-Adresse handelt, die vom Internet erreichbar ist und an die Elastic Network-Schnittstelle eines Dateisystems angehängt wird.

Die folgenden AWS Rechen-Instances werden für die Verwendung mit FSx für ONTAP unterstützt:

- Amazon Elastic Compute Cloud (Amazon EC2)-Instances, auf denen Linux mit NFS- oder SMB-Unterstützung, Microsoft Windows und MacOS ausgeführt wird. Weitere Informationen finden Sie unter Mounting von Volumes.
- Amazon Elastic Container Service (Amazon ECS) Docker-Container auf Amazon EC2 Windows- und Linux-Instances. Weitere Informationen finden Sie unter Verwenden von Amazon Elastic Container Service mit FSx für ONTAP.
- Amazon Elastic Kubernetes Service – Weitere Informationen finden Sie unter Amazon-FSx-für-NetApp ONTAP-CSI-Treiber im Amazon-EKS-Benutzerhandbuch.
- Red Hat OpenShift Service in AWS (ROSA) – Weitere Informationen finden Sie unter Was ist Red Hat OpenShift Service in AWS? im Red Hat OpenShift Service in AWS Benutzerhandbuch.
- Amazon- WorkSpaces Instances. Weitere Informationen finden Sie unter Amazon WorkSpaces mit FSx für ONTAP verwenden.
- Amazon- AppStream 2.0-Instances.
- AWS Lambda – Weitere Informationen finden Sie im AWS Blogbeitrag Enabling SMB access for serverless workloads with Amazon FSx.
- Virtuelle Maschinen (VMs), die in Umgebungen von VMware Cloud in ausgeführt AWS werden. Weitere Informationen finden Sie unter Konfigurieren von Amazon FSx für NetApp ONTAP als externen Speicher und VMware Cloud in AWS mit Amazon FSx für NetApp ONTAP-Bereitstellungshandbuch.

Nach dem Mounten werden FSx-für-ONTAP-Dateisysteme als lokales Verzeichnis oder Laufwerkbuchstabe über NFS und SMB angezeigt, was einen vollständig verwalteten, gemeinsam genutzten Netzwerkdateispeicher bereitstellt, auf den bis zu Tausende von Clients gleichzeitig zugreifen können. iSCSI LUNS sind als Blockgeräte zugänglich, wenn es über iSCSI gemountet wird.

Zugriff auf Daten aus dem heraus AWS

Jedes Amazon-FSx-Dateisystem ist einer Virtual Private Cloud (VPC) zugeordnet. Sie können unabhängig von der Availability Zone von überall in der VPC des Dateisystems auf Ihr FSx-für-ONTAP-Dateisystem zugreifen. Sie können auch von anderen VPCs aus auf Ihr Dateisystem zugreifen, die sich in verschiedenen AWS Konten oder befinden können AWS-Regionen. Zusätzlich zu den in den folgenden Abschnitten beschriebenen Anforderungen für den Zugriff auf FSx-für-ONTAP-Ressourcen müssen Sie auch sicherstellen, dass die VPC-Sicherheitsgruppe Ihres Dateisystems so konfiguriert ist, dass Daten- und Verwaltungsdatenverkehr zwischen Ihrem Dateisystem und Clients fließen kann. Weitere Informationen zum Konfigurieren von Sicherheitsgruppen mit den erforderlichen Ports finden Sie unter Amazon VPC-Sicherheitsgruppen.

Themen

- Zugreifen auf Daten aus derselben VPC
- Zugriff auf Daten von außerhalb der Bereitstellungs-VPC

Zugreifen auf Daten aus derselben VPC

Wenn Sie Ihr Dateisystem von Amazon FSx für NetApp ONTAP erstellen, wählen Sie die Amazon VPC aus, in der es sich befindet. Alle SVMs und Volumes, die dem Dateisystem von Amazon FSx für NetApp ONTAP zugeordnet sind, befinden sich ebenfalls in derselben VPC. Wenn sich das Dateisystem und der Client, die das Volume mounten, beim Mounten eines Volumes in derselben VPC und in derselben befinden AWS-Konto, können Sie je nach Client den DNS-Namen und die Volume-Verbindung oder die SMB-Freigabe der SVM verwenden. Weitere Informationen finden Sie unter Mounting von Volumes.

Sie können eine optimale Leistung erzielen, wenn sich der Client und das Volume in derselben Availability Zone wie das Subnetz des Dateisystems oder in einem bevorzugten Subnetz für Multi-AZ-Dateisysteme befinden. Um das Subnetz oder das bevorzugte Subnetz eines Dateisystems zu identifizieren, wählen Sie in der Amazon-FSx-Konsole Dateisysteme und dann das ONTAP-Dateisystem aus, dessen Volume Sie mounten, und das Subnetz oder das bevorzugte Subnetz (Multi-AZ) wird im Bereich Subnet zoder Bevorzugtes Subnetz angezeigt.

Zugriff auf Daten von außerhalb der Bereitstellungs-VPC

In diesem Abschnitt wird beschrieben, wie Sie von AWS Speicherorten außerhalb der Bereitstellungs-VPC des Dateisystems auf die Endpunkte eines FSx-für-ONTAP-Dateisystems zugreifen.

Zugriff auf NFS-, SMB- und ONTAP-Verwaltungsendpunkte auf Multi-AZ-Dateisystemen

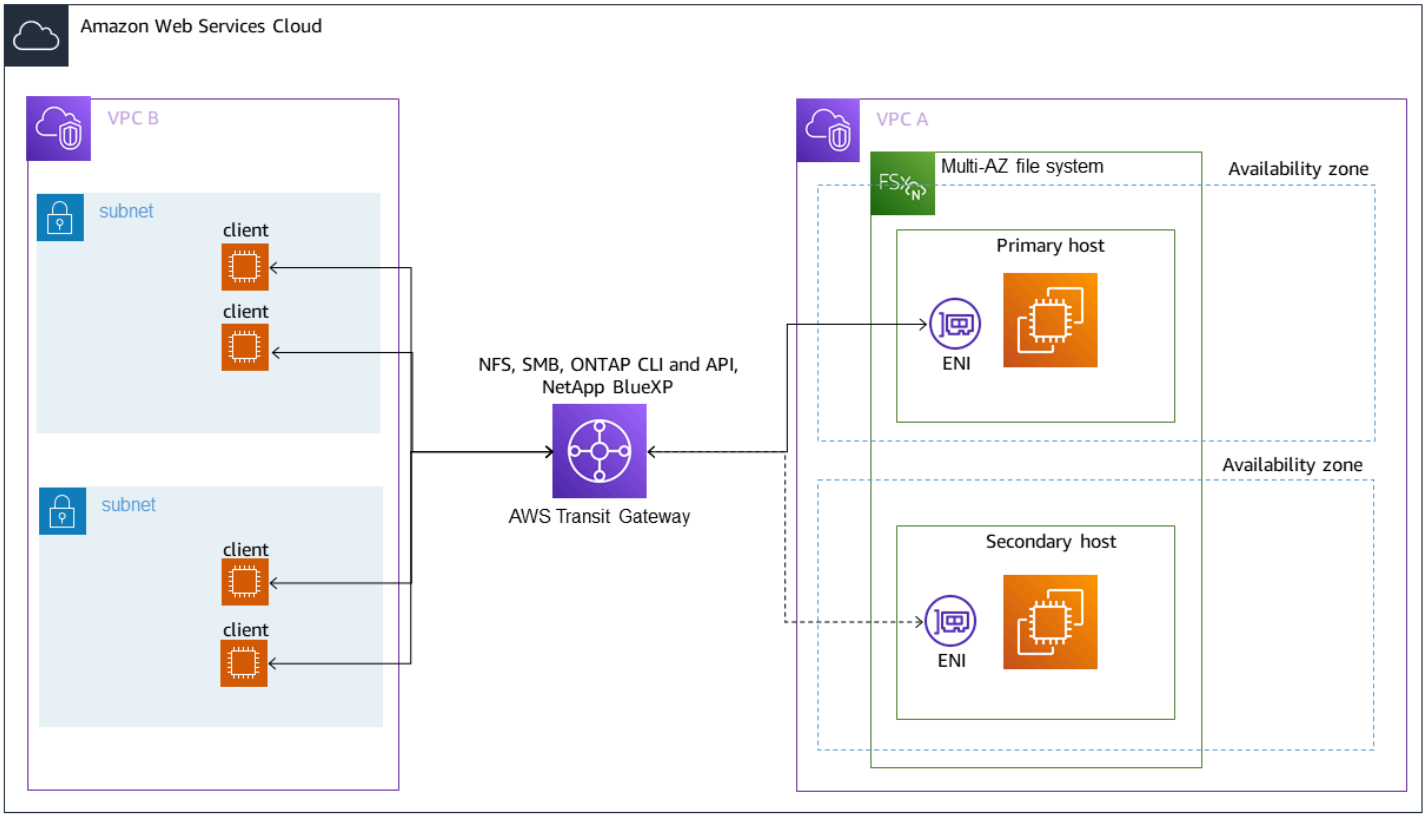
Die NFS-, SMB- und ONTAP-Verwaltungsendpunkte auf Amazon-FSx-für- NetApp ONTAP-Multi-AZ-Dateisystemen verwenden Floating Internet Protocol (IP)-Adressen, sodass verbundene Clients während eines Failover-Ereignisses nahtlos zwischen den bevorzugten und Standby-Dateiservern wechseln können. Weitere Informationen zu Failovers finden Sie unter Failover-Prozess für FSx für ONTAP.

Diese schwebenden IP-Adressen werden in den VPC-Routing-Tabellen erstellt, die Sie Ihrem Dateisystem zuordnen, und befinden sich innerhalb des Dateisystems`EndpointIpAddressRange`, das Sie bei der Erstellung angeben können. Die `EndpointIpAddressRange` verwendet die folgenden Adressbereiche, je nachdem, wie ein Dateisystem erstellt wird:

- Multi-AZ-Dateisysteme, die mit der Amazon-FSx-Konsole erstellt wurden, verwenden `EndpointIpAddressRange` standardmäßig die letzten 64 IP-Adressen im primären CIDR-Bereich der VPC für das Dateisystem.
- Multi-AZ-Dateisysteme, die mit der AWS CLI oder Amazon-FSx-API erstellt wurden, verwenden `EndpointIpAddressRange` standardmäßig einen IP-Adressbereich innerhalb des `198.19.0.0/16` Adressblocks für die .

AWS Transit Gateway Unterstützt nur das Routing zu schwebenden IP-Adressen, die auch als transitives Peering bezeichnet werden. VPC Peering AWS Direct Connect und unterstützen AWS VPN kein transitives Peering. Daher müssen Sie Transit Gateway verwenden, um von Netzwerken aus auf diese Schnittstellen zuzugreifen, die sich außerhalb der VPC Ihres Dateisystems befinden.

Das folgende Diagramm veranschaulicht die Verwendung von Transit Gateway für NFS-, SMB- oder Verwaltungszugriff auf ein Multi-AZ-Dateisystem, das sich in einer anderen VPC befindet als die Clients, die darauf zugreifen.



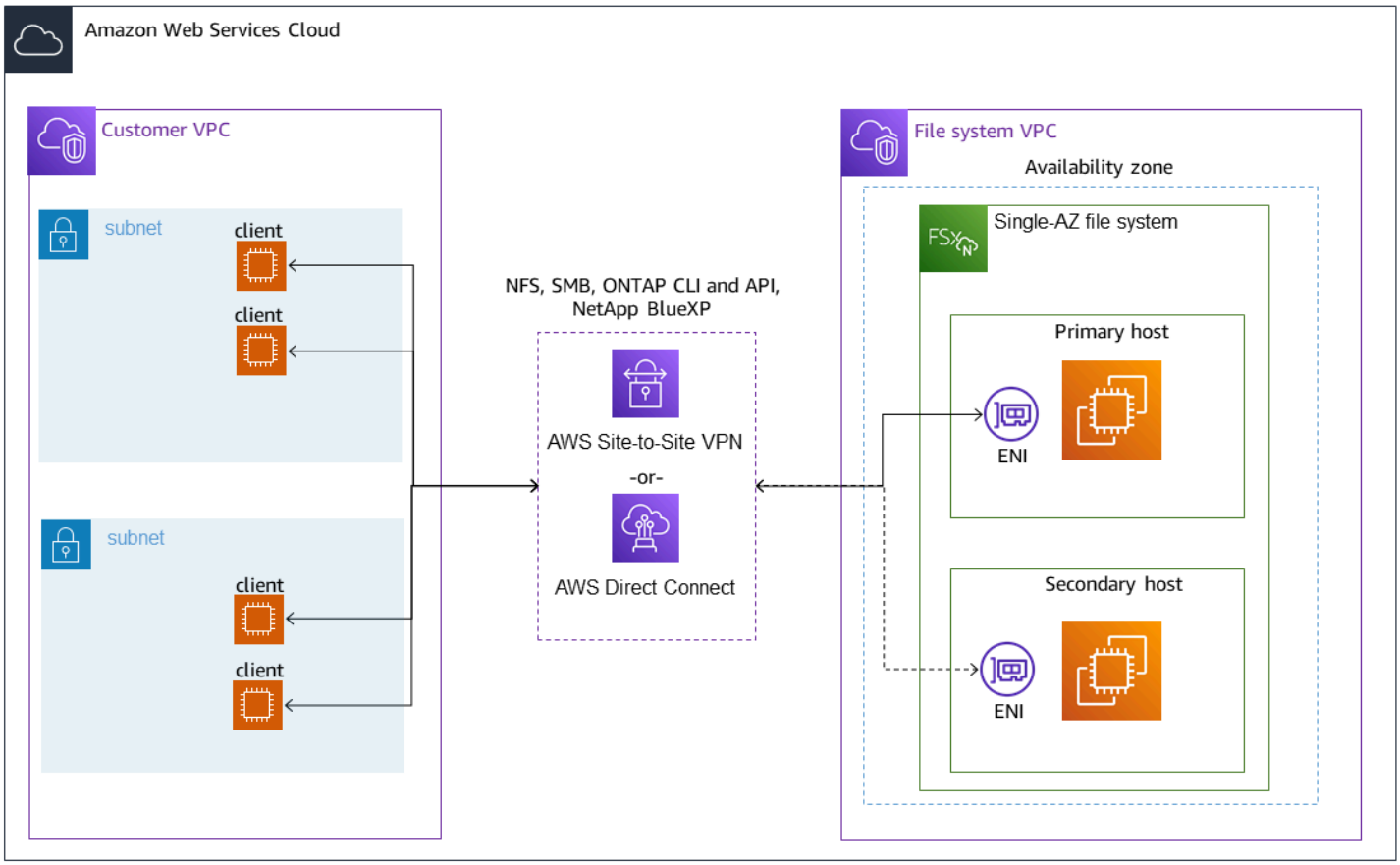
> **Note**
>
> Stellen Sie sicher, dass alle von Ihnen verwendeten Routing-Tabellen Ihrem Multi-AZ-Dateisystem zugeordnet sind. Dies trägt dazu bei, die Nichtverfügbarkeit während eines Failovers zu verhindern. Informationen zum Zuordnen Ihrer Amazon-VPC-Routing-Tabellen zu Ihrem Dateisystem finden Sie unter Aktualisierung eines Dateisystems.

Informationen darüber, wann Sie Transit Gateway für den Zugriff auf Ihr FSx-für-ONTAP-Dateisystem verwenden müssen, finden Sie unter Wann ist Transit Gateway erforderlich?.

Zugriff auf NFS, SMB oder die ONTAP-CLI und -API für Single-AZ-Dateisysteme

Die Endpunkte, die für den Zugriff auf Single-AZ-Dateisysteme von FSx für ONTAP über NFS oder SMB und für die Verwaltung von Dateisystemen mit der ONTAP-CLI oder REST-API verwendet werden, sind sekundäre IP-Adressen auf der ENI des aktiven Dateiservers. Die sekundären IP-Adressen befinden sich im CIDR-Bereich der VPC, sodass Clients mit VPC Peering oder auf Daten- und Verwaltungsports zugreifen können AWS Direct Connect, AWS VPN ohne dass erforderlich ist AWS Transit Gateway.

Das folgende Diagramm veranschaulicht die Verwendung von AWS VPN oder AWS Direct Connect für den NFS-, SMB- oder Verwaltungszugriff auf ein Single-AZ-Dateisystem, das sich in einer anderen VPC befindet als die Clients, die darauf zugreifen.



Wann ist Transit Gateway erforderlich?

Ob Transit Gateway für Ihre Multi-AZ-Dateisysteme erforderlich ist oder nicht, hängt von der Methode ab, mit der Sie auf Ihre Dateisystemdaten zugreifen. Single-AZ-Dateisysteme erfordern kein Transit Gateway. In der folgenden Tabelle wird beschrieben, wann Sie verwenden AWS Transit Gateway müssen, um auf Multi-AZ-Dateisysteme zuzugreifen.

Datenzugriff	Benötigt Transit Gateway?
Zugreifen auf FSx über NFS, SMB oder die NetApp ONTAP-REST-API, -CLI oder BlueXP	Nur wenn: • Zugreifen auf von einem per Peering verbundenen (z. B. On-Premises) Netzwerk und

Datenzugriff	Benötigt Transit Gateway?
	• Sie greifen nicht über eine NetApp FlexCache oder eine Global File Cache-Instance auf FSx zu
Zugreifen auf Daten über iSCSI	Nein
Verbinden einer SVM mit einem Active Directory	Nein
SnapMirror	Nein
FlexCache Zwischenspeichern	Nein
Globaler Datei-Cache	Nein

Konfigurieren des Routings mit AWS Transit Gateway

Wenn Sie über ein Multi-AZ-Dateisystem mit einem verfügen`EndpointIPAddressRange`, das sich außerhalb des CIDR-Bereichs Ihrer VPC befindet, müssen Sie zusätzliches Routing in Ihrem einrichten, AWS Transit Gateway um von Peer- oder On-Premises-Netzwerken aus auf Ihr Dateisystem zuzugreifen.

Important

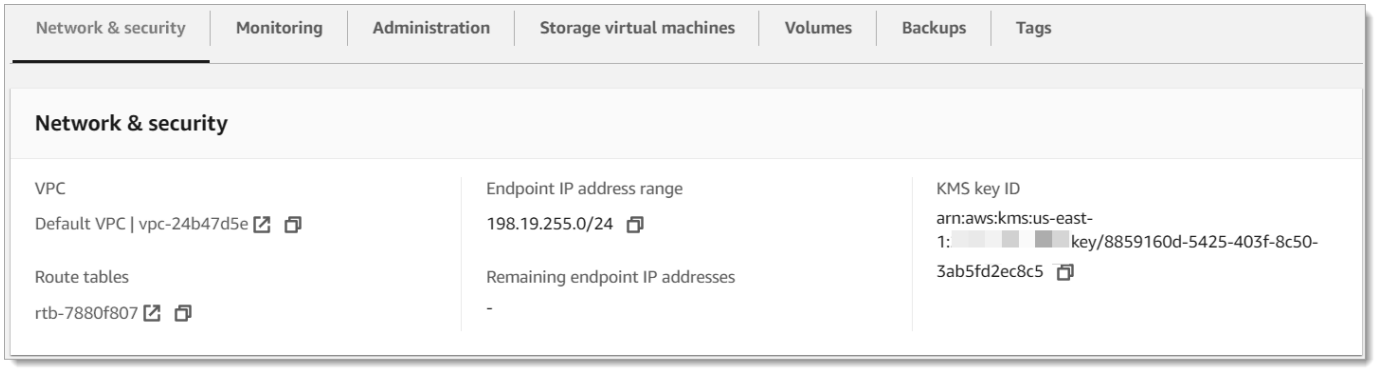
Um über ein Transit Gateway auf ein Multi-AZ-Dateisystem zuzugreifen, muss jeder der Anhänge des Transit Gateways in einem Subnetz erstellt werden, dessen Routing-Tabelle Ihrem Dateisystem zugeordnet ist.

Note

Für Single-AZ-Dateisysteme oder Multi-AZ-Dateisysteme mit einem `EndpointIPAddressRange`, das sich innerhalb des IP-Adressbereichs Ihrer VPC befindet, ist keine zusätzliche Transit-Gateway-Konfiguration erforderlich.

So konfigurieren Sie das Routing mit AWS Transit Gateway

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie das FSx-für-ONTAP-Dateisystem aus, für das Sie den Zugriff von einem Peer-Netzwerk aus konfigurieren.
3. Kopieren Sie unter Netzwerk und Sicherheit den Endpunkt-IP-Adressbereich .



4. Fügen Sie eine Route zu Transit Gateway hinzu, die den für diesen IP-Adressbereich bestimmten Datenverkehr an die VPC Ihres Dateisystems weiterleitet. Weitere Informationen finden Sie unter Arbeiten mit Transit Gateways im Amazon VPC Transit Gateways .
5. Vergewissern Sie sich, dass Sie über das per Peering verbundene Netzwerk auf Ihr FSx-für-ONTAP-Dateisystem zugreifen können.

Informationen zum Hinzufügen der Routing-Tabelle zu Ihrem Dateisystem finden Sie unter Aktualisierung eines Dateisystems.

> **Note**
>
> DNS-Datensätze für die Verwaltungs-, NFS- und SMB-Endpunkte können nur innerhalb derselben VPC wie das Dateisystem aufgelöst werden. Um ein Volume zu mounten oder von einem anderen Netzwerk aus eine Verbindung zu einem Verwaltungsport herzustellen, müssen Sie die IP-Adresse des Endpunkts verwenden. Diese IP-Adressen ändern sich im Laufe der Zeit nicht.

Zugriff auf iSCSI- oder Cluster-übergreifende Endpunkte außerhalb der Bereitstellungs-VPC

Sie können entweder VPC Peering oder verwenden AWS Transit Gateway , um von außerhalb der Bereitstellungs-VPC des Dateisystems auf den iSCSI- oder Cluster-übergreifenden Endpunkt Ihres Dateisystems zuzugreifen. Sie können VPC Peering verwenden, um iSCSI- und clusterübergreifenden Datenverkehr zwischen VPCs weiterzuleiten. Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs und wird verwendet, um den Datenverkehr zwischen ihnen über private IPv4-Adressen weiterzuleiten. Sie können VPC-Peering verwenden, um VPCs innerhalb derselben AWS-Region oder zwischen verschiedenen zu verbinden AWS-Regionen. Weitere Informationen zu VPC Peering finden Sie unter Was ist VPC Peering? im Amazon-VPC-Peering-Handbuch.

Zugriff auf Daten von On-Premises

Sie können von On-Premises mit AWS VPN und auf Ihre FSx-für-ONTAP-Dateisysteme zugreifenAWS Direct Connect. Spezifischere Anwendungsfallrichtlinien finden Sie in den folgenden Abschnitten. Zusätzlich zu den unten aufgeführten Anforderungen für den Zugriff auf verschiedene FSx-für-ONTAP-Ressourcen von On-Premises müssen Sie auch sicherstellen, dass die VPC-Sicherheitsgruppe Ihres Dateisystems den Datenfluss zwischen Ihrem Dateisystem und Clients zulässt. Eine Liste der erforderlichen Ports finden Sie unter Amazon-VPC-Sicherheitsgruppen.

Zugriff auf NFS-, SMB- oder ONTAP-CLI- oder REST-API-Endpunkte von On-Premises

In diesem Abschnitt wird beschrieben, wie Sie von On-Premises-Netzwerken aus auf die NFS-, SMB- und ONTAP-Verwaltungsports auf FSx-für-ONTAP-Dateisystemen zugreifen.

Zugriff auf Multi-AZ-Dateisysteme

Amazon FSx erfordert, dass Sie AWS Transit Gateway oder verwenden, den globalen Remote NetApp-Dateicache konfigurieren oder NetApp FlexCache Multi-AZ-Dateisysteme von einem On-Premises-Netzwerk aus aufrufen. Um ein Failover über AZs hinweg für Multi-AZ-Dateisysteme zu unterstützen, verwendet Amazon FSx schwebende IP-Adressen für die Schnittstellen, die für NFS-, SMB- und ONTAP-Verwaltungsendpunkte verwendet werden. Da die NFS-, SMBIPs und Verwaltungsendpunkte Gleitkommazahlen verwenden, müssen Sie AWS Transit Gateway in Verbindung mit AWS Direct Connect oder verwenden, AWS VPN um von einem On-Premises-

Netzwerk aus auf diese Schnittstellen zuzugreifen. Die für diese Schnittstellen verwendeten schwebenden IP-Adressen befinden sich innerhalb der , die `EndpointIpAddressRange` Sie beim Erstellen Ihres Multi-AZ-Dateisystems angeben. Wenn Sie Ihr Dateisystem über die Amazon-FSx-Konsole erstellen, wählt Amazon FSx standardmäßig die letzten 64 IP-Adressen aus dem primären CIDR-Bereich der VPC aus, die als Endpunkt-IP-Adressbereich für das Dateisystem verwendet werden sollen. Wenn Sie Ihr Dateisystem über die AWS CLI oder die Amazon-FSx-API erstellen, wählt Amazon FSx standardmäßig einen IP-Adressbereich aus dem `198.19.0.0/16` IP-Adressbereich aus. Die schwebenden IP-Adressen werden verwendet, um einen nahtlosen Übergang Ihrer Clients in das Standby-Dateisystem zu ermöglichen, falls ein Failover erforderlich ist. Weitere Informationen finden Sie unter Failover-Prozess für FSx für ONTAP.

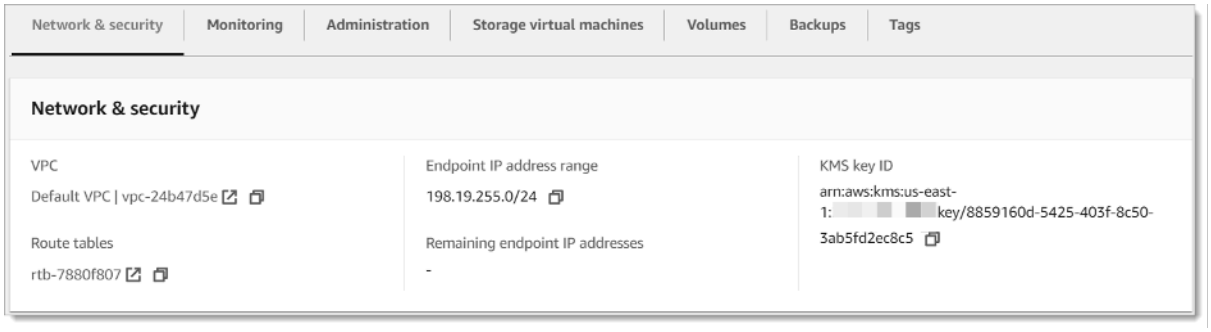
> **Important**
>
> Um über ein Transit Gateway auf ein Multi-AZ-Dateisystem zuzugreifen, muss jeder der Anhänge des Transit Gateways in einem Subnetz erstellt werden, dessen Routing-Tabelle Ihrem Dateisystem zugeordnet ist.

So konfigurieren Sie AWS Transit Gateway für den Zugriff von außerhalb Ihrer VPC

Wenn Sie ein Multi-AZ-Dateisystem mit einem haben`EndpointIPAddressRange`, das sich außerhalb des CIDR-Bereichs Ihrer VPC befindet, müssen Sie zusätzliches Routing in Ihrem einrichten, AWS Transit Gateway um von Peer- oder On-Premises-Netzwerken aus auf Ihr Dateisystem zuzugreifen.

> **Note**
>
> Für Single-AZ-Dateisysteme oder Multi-AZ-Dateisysteme mit einem `EndpointIPAddressRange`, das sich innerhalb des IP-Adressbereichs Ihrer VPC befindet, ist keine zusätzliche Transit-Gateway-Konfiguration erforderlich.

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie das FSx-für-ONTAP-Dateisystem aus, für das Sie den Zugriff von einem Peer-Netzwerk aus konfigurieren.
3. Kopieren Sie unter Netzwerk und Sicherheit den Endpunkt-IP-Adressbereich .



4. Fügen Sie dem Transit Gateway eine Route hinzu, die den für diesen IP-Adressbereich bestimmten Datenverkehr an die VPC Ihres Dateisystems weiterleitet. Weitere Informationen finden Sie unter Arbeiten mit Transit-Gateways im Benutzerhandbuch für Amazon VPC Transit Gateway.
5. Vergewissern Sie sich, dass Sie vom Peer-Netzwerk aus auf Ihr FSx-für-ONTAP-Dateisystem zugreifen können.

> **Important**
>
> Um über ein Transit Gateway auf ein Multi-AZ-Dateisystem zuzugreifen, muss jeder der Anhänge des Transit Gateways in einem Subnetz erstellt werden, dessen Routing-Tabelle Ihrem Dateisystem zugeordnet ist.

Informationen zum Hinzufügen einer Routing-Tabelle zu Ihrem Dateisystem finden Sie unter Aktualisierung eines Dateisystems.

Zugriff auf Single-AZ-Dateisysteme

Für Single-AZ-Dateisysteme besteht keine Anforderung, für AWS Transit Gateway den Zugriff auf Daten aus einem On-Premises-Netzwerk zu verwenden. Single-AZ-Dateisysteme werden in einem einzigen Subnetz bereitgestellt, und eine schwebende IP-Adresse ist nicht erforderlich, um ein Failover zwischen Knoten bereitzustellen. Stattdessen werden die IP-Adressen, auf die Sie auf Single-AZ-Dateisystemen zugreifen, als sekundäre IP-Adressen innerhalb des VPC-CIDR-Bereichs des Dateisystems implementiert, sodass Sie von einem anderen Netzwerk aus auf Ihre Daten zugreifen können, ohne dass erforderlich ist AWS Transit Gateway.

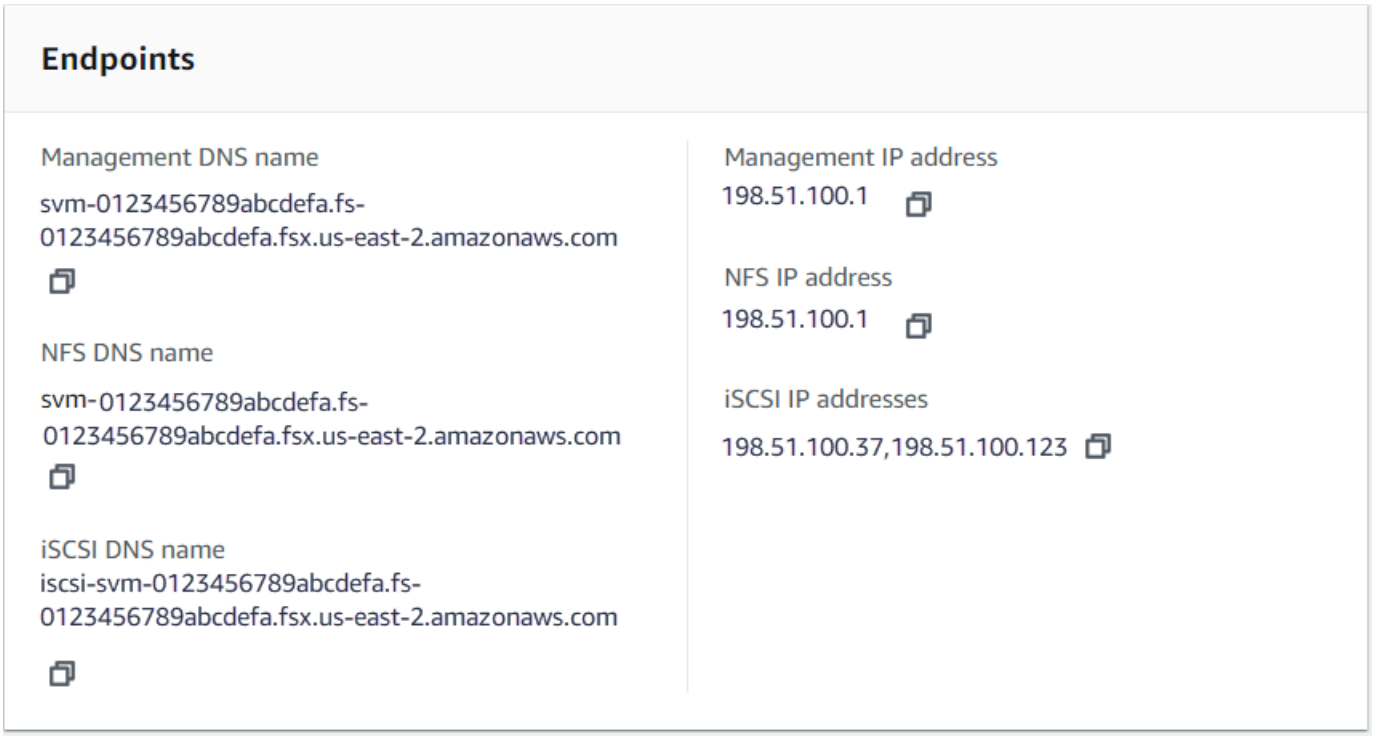
Zugriff auf Cluster-übergreifende Endpunkte von On-Premises

Die Cluster-übergreifenden Endpunkte von FSx für ONTAP sind für den Replikationsverkehr zwischen NetApp ONTAP-Dateisystemen vorgesehen, einschließlich zwischen On-Premises- NetApp Bereitstellungen und FSx für ONTAP. Der Replikationsverkehr umfasst SnapMirror FlexCache, und FlexClone Beziehungen zwischen virtuellen Speichermaschinen (SVMs) und Volumes über verschiedene Dateisysteme hinweg sowie NetApp Global File Cache. Die Cluster-übergreifenden Endpunkte werden auch für Active-Directory-Datenverkehr verwendet.

Da die Cluster-übergreifenden Endpunkte eines Dateisystems IP-Adressen verwenden, die innerhalb des CIDR-Bereichs der VPC liegen, die Sie beim Erstellen Ihres FSx-für-ONTAP-Dateisystems angeben, müssen Sie kein Transit Gateway für das Routing von Cluster-übergreifendem Datenverkehr zwischen On-Premises und verwenden AWS Cloud. On-Premises-Clients müssen jedoch weiterhin AWS VPN oder verwenden, AWS Direct Connect um eine sichere Verbindung zu Ihrer VPC herzustellen.

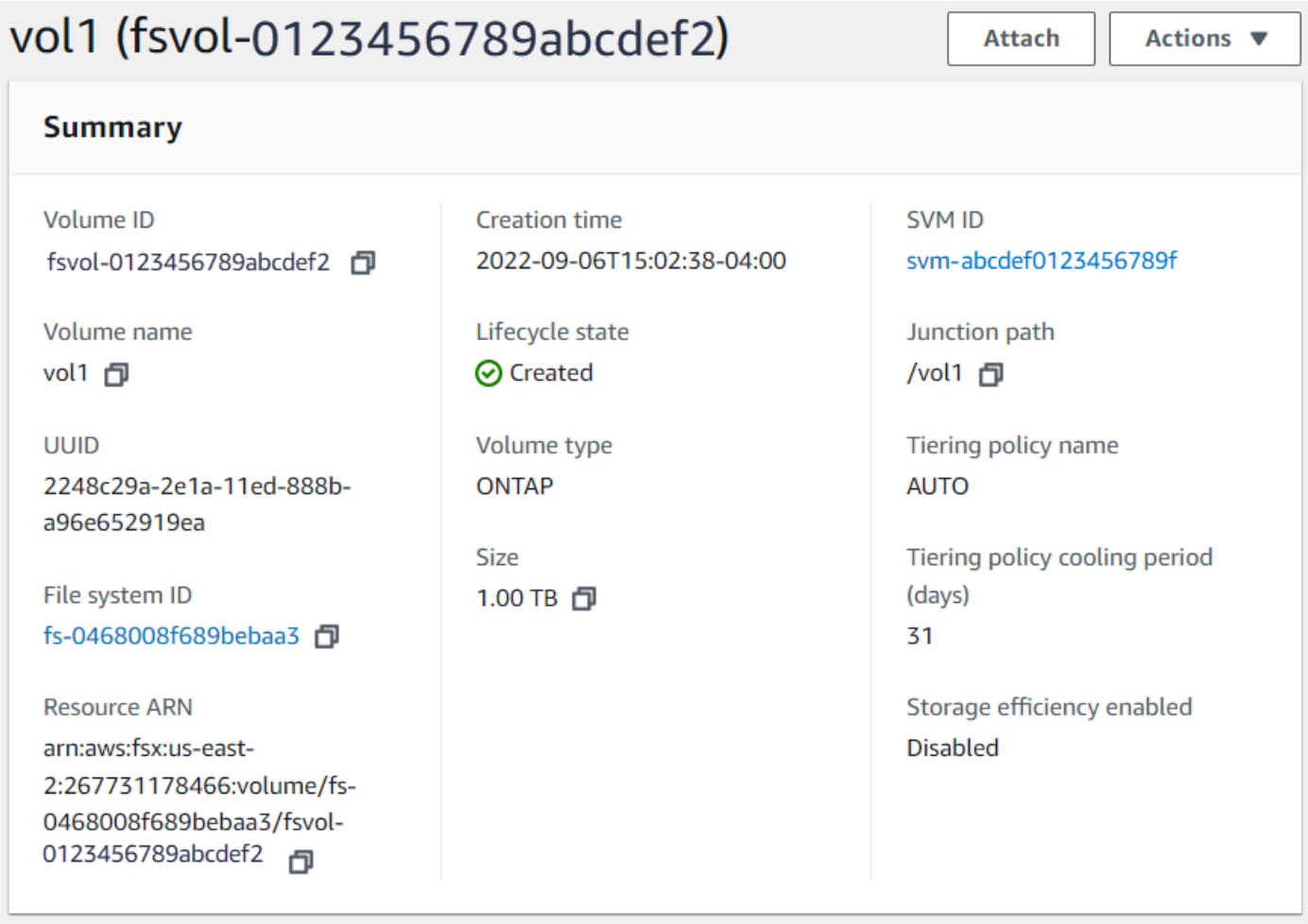
Mounting von Volumes

Sie greifen auf die Daten in FSx für ONTAP zu, indem Sie ein Volume auf Ihrem Client mounten. Die Befehle in diesem Abschnitt verwenden den DNS-Namen oder die IP-Adresse der SVM, in der das Volume erstellt wird, um ein Volume zu mounten oder anzuhängen. Sie finden den DNS-Namen und die IP-Adresse der SVM in der Amazon-FSx-Konsole, indem Sie ONTAP **>** Virtuelle Speichermaschinen oder auf der Registerkarte Virtuelle Speichermaschine auf der Seite Dateisystemdetails für das Dateisystem auswählen, wie in der folgenden Abbildung dargestellt.



Oder Sie finden sie in der Antwort des DescribeStorageVirtualMachines -API-Vorgangs.

Sie finden den Verbindungspfad eines Volumes in der Amazon-FSx-Konsole im Bereich Zusammenfassung der Seite mit den Volume-Details, wie in der folgenden Abbildung dargestellt.



Themen

- Mounting auf Linux-Clients
- Mounting auf Microsoft-Windows-Clients
- Mounting auf macOS-Clients

Mounting auf Linux-Clients

Wir empfehlen, dass die SVM-Volumes, an die Sie Linux-Clients anfügen, die Sicherheitseinstellung `UNIX` oder haben`mixed`. Weitere Informationen finden Sie unter Verwaltung von FSx für ONTAP-Volumes.

> **Note**
>
> Standardmäßig sind FSx-für-ONTAP-NFS-Mounts `hard` Mounts. Um ein reibungsloses Failover für den Fall eines solchen Falls zu gewährleisten, empfehlen wir Ihnen, die Standard-`hard`Mounting-Option zu verwenden.

So mounten Sie ein ONTAP-Volume auf einem Linux-Client

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Erstellen oder wählen Sie eine Amazon EC2-Instance mit Amazon Linux 2 aus, die sich in derselben VPC wie das Dateisystem befindet.

   Weitere Informationen zum Starten einer EC2-Linux-Instance finden Sie unter Schritt 1: Starten einer Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances.
3. Stellen Sie eine Verbindung zu Ihrer Amazon EC2 Linux-Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux-Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances.
4. Öffnen Sie ein Terminal auf Ihrer EC2-Instance mit Secure Shell (SSH) und melden Sie sich mit den entsprechenden Anmeldeinformationen an.
5. Erstellen Sie auf der EC2-Instance wie folgt ein Verzeichnis zum Mounten des SVM-Volumes:

   ```
   sudo mkdir /fsx
   ```
6. Mounten Sie das Volume mit dem folgenden Befehl in das Verzeichnis, das Sie gerade erstellt haben:

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

   Im folgenden Beispiel werden Beispielwerte verwendet.

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

   Sie können auch die IP-Adresse SVM der SVM anstelle ihres DNS-Namens verwenden. Wir empfehlen, den DNS-Namen zum Mounten von Clients an Scale-Out-Dateisysteme zu

verwenden, da dadurch sichergestellt wird, dass Ihre Clients über die High-Availability (HA)-Paare Ihres Dateisystems verteilt sind.

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

> **Note**
>
> Bei Scale-Out-Dateisystemen ist das parallele NFS-Protokoll (pNFS) standardmäßig aktiviert und wird standardmäßig für alle Clients verwendet, die Volumes mit NFS v4.1 oder höher mounten.

Verwenden von /etc/fstab zum automatischen Mounten beim Neustart der Instance

Verwenden Sie die -`/etc/fstab`Datei, um Ihr FSx-für-ONTAP-Volume automatisch neu zu mounten, wenn eine Amazon EC2-Linux-Instance neu gestartet wird. Die `/etc/fstab`-Datei enthält Informationen zu Dateisystemen. Der Befehl `mount -a`, der während des Instance-Starts ausgeführt wird, mountet die in aufgeführten Dateisysteme`/etc/fstab`.

> **Note**
>
> Dateisysteme von FSx für ONTAP unterstützen kein automatisches Mounting mit `/etc/fstab` auf Amazon EC2-Mac-Instances.

> **Note**
>
> Bevor Sie die `/etc/fstab` Datei Ihrer EC2-Instance aktualisieren können, stellen Sie sicher, dass Sie Ihr FSx-für-ONTAP-Dateisystem bereits erstellt haben. Weitere Informationen finden Sie unter FSx für ONTAP-Dateisysteme erstellen.

So aktualisieren Sie die /etc/fstab-Datei in Ihrer EC2-Instance

1. Stellen Sie eine Verbindung mit der EC2-Instance her:

- Wenn Sie von einem Computer unter macOS oder Linux eine Verbindung mit Ihrer Instance herzustellen möchten, geben Sie die PEM-Datei für den SSH-Befehl an. Verwenden Sie dazu die `-i`-Option und den Pfad zu Ihrem privaten Schlüssel.
- Um von einem Computer, auf dem Windows ausgeführt wird, eine Verbindung zu Ihrer Instance herzustellen, können Sie entweder MindTerm oder PuTTY verwenden. Zur Verwendung von PuTTY installieren Sie es und konvertieren Sie die PEM-Datei in eine PPK-Datei.

Weitere Informationen finden Sie in den folgenden Themen im Amazon EC2-Benutzerhandbuch für Linux-Instances:

- Herstellen einer Verbindung zu Ihrer Linux-Instance über SSH
- Herstellen einer Verbindung zu Ihrer Linux-Instance von Windows über PuTTY

2. Erstellen Sie ein lokales Verzeichnis, das zum Mounten des SVM-Volumes verwendet wird.

```
sudo mkdir /fsx
```

3. Öffnen Sie die `/etc/fstab` Datei in einem Editor Ihrer Wahl.
4. Fügen Sie der Datei `/etc/fstab` die folgende Zeile hinzu. Fügen Sie zwischen jedem Parameter ein Tabulatorzeichen ein. Er sollte als eine Zeile ohne Zeilenumbrüche erscheinen.

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

Sie können auch die IP-Adresse der SVM des Volumes verwenden. Die letzten drei Parameter weisen auf NFS-Optionen (die wir auf Standard festlegen), das Dumping des Dateisystems und die Dateisystemprüfung hin (diese werden normalerweise nicht verwendet, daher setzen wir sie auf 0).

5. Speichern Sie die Änderungen an der Datei.
6. Mounten Sie nun die Dateifreigabe mit dem folgenden Befehl. Beim nächsten Start des Systems wird der Ordner automatisch gemountet.

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

Ihre EC2-Instance ist jetzt so konfiguriert, dass das ONTAP-Volume bei jedem Neustart gemountet wird.

Mounting auf Microsoft-Windows-Clients

In diesem Abschnitt wird beschrieben, wie Sie auf Daten in Ihrem FSx-für-ONTAP-Dateisystem mit Clients zugreifen, auf denen das Microsoft-Windows-Betriebssystem ausgeführt wird. Überprüfen Sie die folgenden Anforderungen, unabhängig von der Art des Clients, den Sie verwenden.

Bei diesem Verfahren wird davon ausgegangen, dass sich der Client und das Dateisystem in derselben VPC und in derselben befinden AWS-Konto. Wenn sich der Client On-Premise oder in einer anderen VPC, oder befindet AWS-Region, geht dieses Verfahren auch davon aus AWS-Konto, dass Sie AWS Transit Gateway oder eine dedizierte Netzwerkverbindung mit AWS Direct Connect oder einem privaten, sicheren Tunnel mit eingerichtet haben AWS Virtual Private Network. Weitere Informationen finden Sie unter Zugriff auf Daten von außerhalb der Bereitstellungs-VPC.

Wir empfehlen, Volumes mithilfe des SMB-Protokolls an Ihre Windows-Clients anzufügen.

Voraussetzungen

Um mit einem Microsoft Windows-Client auf ein ONTAP-Speicher-Volume zuzugreifen, müssen Sie die folgenden Voraussetzungen erfüllen:

- Die SVM des Volumes, das Sie anfügen, muss mit dem Active Directory Ihrer Organisation verbunden sein, oder Sie müssen eine Arbeitsgruppe verwenden. Weitere Informationen zum Verbinden Ihrer SVM mit einem Active Directory finden Sie unter Verwalten virtueller FSx-für-ONTAP-Speichermaschinen. Weitere Informationen zur Verwendung von Arbeitsgruppen finden Sie unter Einrichten eines SMB-Servers in einer Arbeitsgruppenübersicht im NetApp - Dokumentationszentrum.
- Das Volume, das Sie anfügen, hat die Sicherheitsstileinstellung `NTFS` oder `mixed`. Weitere Informationen finden Sie unter Verwaltung von FSx für ONTAP-Volumes.

So fügen Sie ein ONTAP-Volume auf einem Windows-Client mithilfe von SMB und Active Directory an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Erstellen oder wählen Sie eine Amazon EC2-Instance mit Microsoft Windows aus, die sich in derselben VPC wie das Dateisystem befindet und mit demselben Microsoft Active Directory wie die SVM des Volumes verbunden ist.

Weitere Informationen zum Starten einer Instance finden Sie unter Schritt 1: Starten einer Instance im Amazon EC2-Benutzerhandbuch für Windows-Instances.

Weitere Informationen zum Verbinden einer SVM mit einem Active Directory finden Sie unter Verwalten virtueller FSx-für-ONTAP-Speichermaschinen.

3. Stellen Sie eine Verbindung zu Ihrer Amazon EC2 Windows-Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance im Amazon-EC2-Benutzerhandbuch für Windows-Instances.
4. Öffnen Sie eine Befehlszeile.
5. Führen Sie den folgenden Befehl aus. Ersetzen Sie Folgendes:

   - Ersetzen Sie `Z:` durch einen beliebigen verfügbaren Laufwerkbuchstaben.
   - Ersetzen Sie `DNS_NAME` durch den DNS-Namen oder die IP-Adresse des SMB-Endpunkts für die SVM des Volumes.
   - Ersetzen Sie durch `SHARE_NAME` den Namen einer SMB-Freigabe. `C$` ist die Standard-SMB-Freigabe im Stammverzeichnis des Namespace der SVM, aber Sie sollten sie nicht mounten, da Speicher für das Stamm-Volume verfügbar macht und zu Sicherheits- und Serviceunterbrechungen führen kann. Sie sollten anstelle von einen SMB-Freigabenamen für das Mounten angeben`C$`. Weitere Informationen zum Erstellen von SMB-Freigaben finden Sie unter Verwaltung von SMB-Aktien.

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

Im folgenden Beispiel werden Beispielwerte verwendet.

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

Sie können auch die IP-Adresse der SVM anstelle ihres DNS-Namens verwenden. Wir empfehlen, den DNS-Namen zum Mounten von Clients an Scale-Out-Dateisysteme zu verwenden, da dadurch sichergestellt wird, dass Ihre Clients über die High-Availability (HA)-Paare Ihres Dateisystems verteilt sind.

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

Mounting auf macOS-Clients

In diesem Abschnitt wird beschrieben, wie Sie auf Daten in Ihrem FSx-für-ONTAP-Dateisystem mit Clients zugreifen, auf denen das macOS-Betriebssystem ausgeführt wird. Überprüfen Sie die folgenden Anforderungen, unabhängig von der Art des Clients, den Sie verwenden.

Bei diesem Verfahren wird davon ausgegangen, dass sich der Client und das Dateisystem in derselben VPC und in derselben befinden AWS-Konto. Wenn sich der Client On-Premise oder in einer anderen VPC AWS-Konto oder befindet, haben AWS-Region Sie AWS Transit Gateway eine dedizierte Netzwerkverbindung mit AWS Direct Connect oder einem privaten, sicheren Tunnel mit eingerichtet AWS Virtual Private Network. Weitere Informationen finden Sie unter Zugriff auf Daten von außerhalb der Bereitstellungs-VPC.

Wir empfehlen Ihnen, Volumes mithilfe des SMB-Protokolls an Ihre Mac-Clients anzufügen.

So mounten Sie ein ONTAP-Volume auf einem macOS-Client mit SMB

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Erstellen oder wählen Sie eine Amazon EC2-Mac-Instance aus, auf der das macOS ausgeführt wird, das sich in derselben VPC wie das Dateisystem befindet.

   Weitere Informationen zum Starten einer Instance finden Sie unter Schritt 1: Starten einer Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances.
3. Stellen Sie eine Verbindung zu Ihrer Amazon EC2-Mac-Instance her. Weitere Informationen finden Sie unter Verbinden Sie sich mit Ihrer Linux-Instance im Benutzerhandbuch zu Amazon EC2 für Linux-Instances.
4. Öffnen Sie ein Terminal auf Ihrer EC2-Instance mit Secure Shell (SSH) und melden Sie sich mit den entsprechenden Anmeldeinformationen an.
5. Erstellen Sie auf der EC2-Instance wie folgt ein Verzeichnis zum Mounten des Volumes:

   ```
   sudo mkdir /fsx
   ```
6. Mounten Sie das Volume mit dem folgenden Befehl.

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

   Im folgenden Beispiel werden Beispielwerte verwendet.

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

Sie können auch die IP-Adresse der SVM anstelle ihres DNS-Namens verwenden. Wir empfehlen, den DNS-Namen zum Mounten von Clients an Scale-Out-Dateisysteme zu verwenden, da dadurch sichergestellt wird, dass Ihre Clients über die High-Availability (HA)-Paare Ihres Dateisystems verteilt sind.

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

`C$` ist die standardmäßige SMB-Freigabe, die Sie mounten können, um den Stamm des Namespace der SVM anzuzeigen. Wenn Sie Server Message Block (SMB)-Freigaben in Ihrer SVM erstellt haben, geben Sie die SMB-Freigabenamen anstelle von an`C$`. Weitere Informationen zum Erstellen von SMB-Freigaben finden Sie unter Verwaltung von SMB-Aktien.

So mounten Sie ein ONTAP-Volume auf einem macOS-Client mit NFS

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Erstellen oder wählen Sie eine Amazon EC2-Instance mit Amazon Linux 2 aus, die sich in derselben VPC wie das Dateisystem befindet.

   Weitere Informationen zum Starten einer EC2-Linux-Instance finden Sie unter Schritt 1: Starten einer Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances.
3. Stellen Sie eine Verbindung zu Ihrer Amazon EC2 Linux-Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux-Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances.
4. Mounten Sie Ihr FSx-für-ONTAP-Volume auf der Linux-EC2-Instance, indem Sie entweder beim Start der Instance ein Benutzerdatenskript verwenden oder die folgenden Befehle ausführen:

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

   Im folgenden Beispiel werden Beispielwerte verwendet.

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

Sie können auch die IP-Adresse SVM der SVM anstelle ihres DNS-Namens verwenden. Wir empfehlen, den DNS-Namen zum Mounten von Clients an Scale-Out-Dateisysteme zu verwenden, da dadurch sichergestellt wird, dass Ihre Clients auf die HA-Paare Ihres Dateisystems verteilt sind.

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

5. Mounten Sie das Volume mit dem folgenden Befehl in das Verzeichnis, das Sie gerade erstellt haben.

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

Im folgenden Beispiel werden Beispielwerte verwendet.

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

Sie können auch die IP-Adresse SVM der SVM anstelle ihres DNS-Namens verwenden. Wir empfehlen, den DNS-Namen zum Mounten von Clients an Scale-Out-Dateisysteme zu verwenden, da dadurch sichergestellt wird, dass Ihre Clients über die High-Availability (HA)-Paare Ihres Dateisystems verteilt sind.

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

Mounten von iSCSI-LUNs

Amazon FSx für NetApp ONTAP bietet gemeinsam genutzte Blockspeicherunterstützung über das iSCSI-Protokoll (Internet Small Computer Systems Interface). Sie können den iSCSI-Speicher aktivieren, indem Sie LUNs (Logical Unit Number) bereitstellen und sie Initiatorgruppen (igroups) zuordnen, wodurch Blockspeicher für Ihre Linux- und Windows-Hosts verfügbar gemacht wird.

> **Note**
>
> Das iSCSI-Protokoll wird für FSx-für-ONTAP-Scale-Out-Dateisysteme nicht unterstützt. Dabei handelt es sich um Dateisysteme mit mehr als einem Hochverfügbarkeitspaar (HA) von Dateiservern.

Themen

- Mounting von iSCSI LUNs an einen Linux-Client
- Mounting von iSCSI LUNs an einen Windows-Client

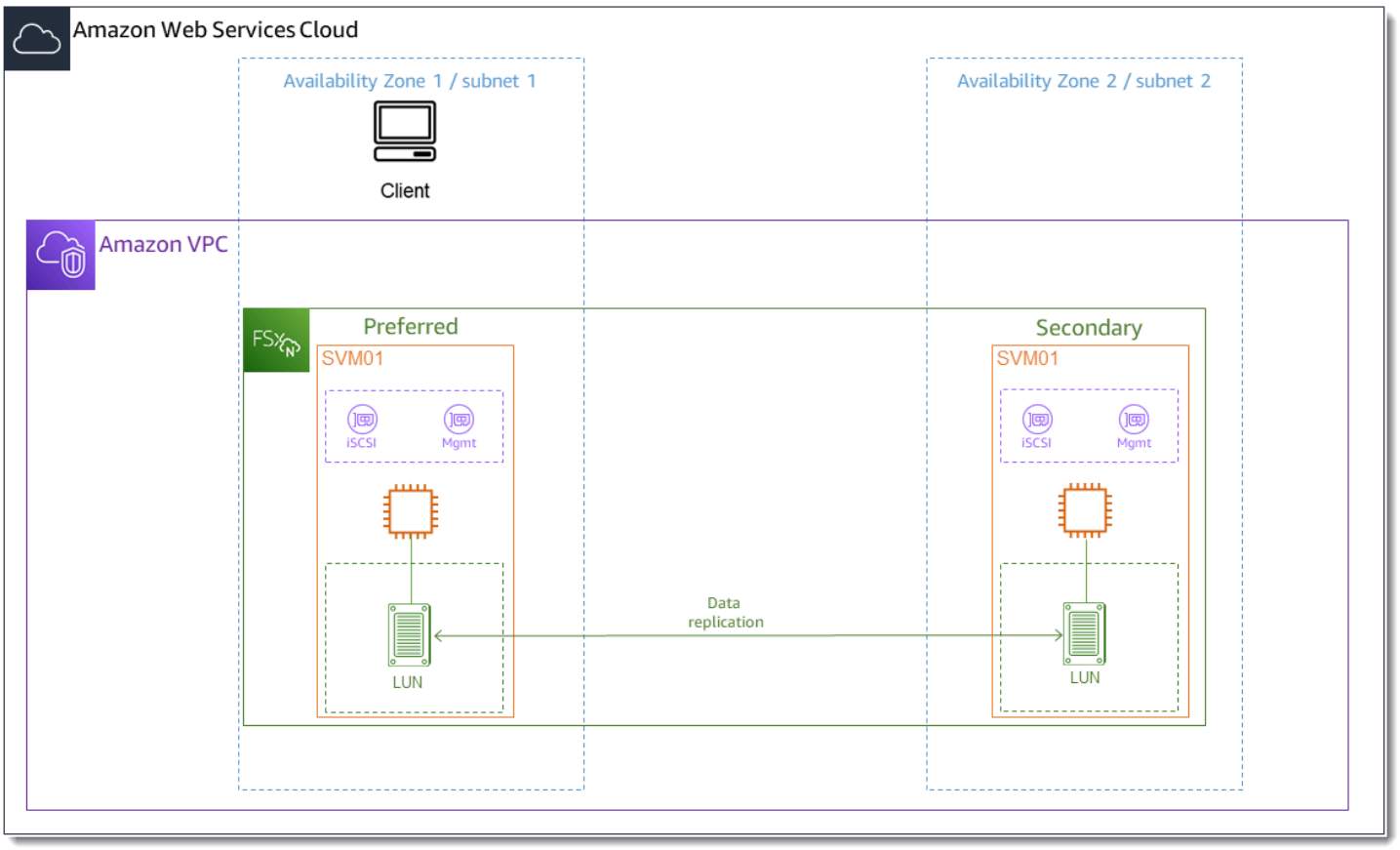
Mounting von iSCSI LUNs an einen Linux-Client

Die in diesen Verfahren vorgestellten Beispiele verwenden die folgende Einrichtung:

- Das iSCSI LUN, das auf dem Linux-Host bereitgestellt wird, wurde bereits erstellt. Weitere Informationen finden Sie unter Eine iSCSI-LUN erstellen.
- Der Linux-Host, der den iSCSI LUN mountet, ist eine Amazon EC2-Instance, auf der das Amazon Machine Image (AMI) von Amazon Linux 2 ausgeführt wird. Es sind VPC-Sicherheitsgruppen so konfiguriert, dass ein- und ausgehender Datenverkehr zugelassen wird, wie unter beschriebenDateisystem-Zugriffskontrolle mit Amazon VPC.
- Der Linux-Host und das FSx-für-ONTAP-Dateisystem befinden sich in derselben VPC und AWS-Konto. Wenn sich der Host in einer anderen VPC befindet, können Sie VPC-Peering oder verwenden, AWS Transit Gateway um anderen VPCs Zugriff auf die iSCSI-Endpunkte des Volumes zu gewähren. Weitere Informationen finden Sie unter Zugriff auf Daten von außerhalb der Bereitstellungs-VPC.

  Wenn Sie eine EC2-Instance verwenden, auf der ein anderes Linux-AMI ausgeführt wird, sind einige der Dienstprogramme, die auf dem Host installiert werden, möglicherweise vorinstalliert, und Sie verwenden möglicherweise andere Befehle, um die erforderlichen Pakete zu installieren. Neben der Installation von Paketen sind die in diesem Abschnitt verwendeten Befehle auch für andere EC2-Linux-AMIs gültig.

  Wir empfehlen, dass sich die EC2-Instance in derselben Availability Zone wie das bevorzugte Subnetz Ihres Dateisystems befindet, wie in der folgenden Grafik dargestellt.



Themen

- Installieren und Konfigurieren von iSCSI auf dem Linux-Client
- Konfigurieren von iSCSI auf dem FSx-für-ONTAP-Dateisystem
- Mounten eines iSCSI LUN auf Ihrem Linux-Client

Installieren und Konfigurieren von iSCSI auf dem Linux-Client

So installieren Sie den iSCSI-Client

1. Vergewissern Sie sich, dass `iscsi-initiator-utils` und auf Ihrem Linux-Gerät installiert `device-mapper-multipath` sind. Stellen Sie über einen SSH-Client eine Verbindung zu Ihrer Linux-Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux-Instance über SSH.
2. Installieren Sie `multipath` und den iSCSI-Client mit dem folgenden Befehl. Die Installation `multipath` von ist erforderlich, wenn Sie ein automatisches Failover zwischen Ihren Dateiservern durchführen möchten.

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

3. Um eine schnellere Reaktion beim automatischen Failover zwischen Dateiservern bei Verwendung von zu ermöglichen`multipath`, legen Sie den Ersatz-Timeout-Wert in der `/etc/iscsi/iscsid.conf` Datei auf einen Wert von fest, `5` anstatt den Standardwert von zu verwenden`120`.

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

4. Starten Sie den iSCSI-Service.

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

Beachten Sie, dass Sie je nach Linux-Version möglicherweise stattdessen diesen Befehl verwenden müssen:

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

5. Bestätigen Sie mit dem folgenden Befehl, dass der Service ausgeführt wird.

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

Das System antwortet mit der folgenden Ausgabe:

```
iscsid.service - Open-iSCSI
    Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor
 preset: disabled)
    Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
    Docs: man:iscsid(8)
    man:iscsiadm(8)
    Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
    CGroup: /system.slice/iscsid.service
    ##14659 /usr/sbin/iscsid
    ##14660 /usr/sbin/iscsid
```

So konfigurieren Sie iSCSI auf Ihrem Linux-Client

1. Damit Ihre Clients automatisch ein Failover zwischen Ihren Dateiservern durchführen können, müssen Sie Multipath konfigurieren. Verwenden Sie den folgenden Befehl:

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

2. Bestimmen Sie den Initiatornamen Ihres Linux-Hosts mit dem folgenden Befehl. Der Speicherort des Initiatornamens hängt von Ihrem iSCSI-Dienstprogramm ab. Wenn Sie verwenden`iscsi-initiator-utils`, befindet sich der Initiatorname in der Datei `/etc/iscsi/initiatorname.iscsi`.

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

   Das System antwortet mit dem Namen des Initiators.

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

Konfigurieren von iSCSI auf dem FSx-für-ONTAP-Dateisystem

1. Stellen Sie mit dem folgenden Befehl eine Verbindung mit der NetApp ONTAP-CLI auf dem FSx-für-ONTAP-Dateisystem her, auf dem Sie die iSCSI LUN erstellt haben. Weitere Informationen finden Sie unter Verwenden der NetApp ONTAP-CLI.

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

2. Erstellen Sie die Initiatorgruppe (`igroup`) mit dem NetApp ONTAP-CLI-lun igroup createBefehl. Eine Initiatorgruppe wird iSCSI LUNs zugeordnet und steuert, welche Initiatoren (Clients) Zugriff auf LUNs haben. Ersetzen Sie durch `host_initiator_name` den Initiatornamen von Ihrem Linux-Host, den Sie im vorherigen Verfahren abgerufen haben.

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

   Wenn Sie die dieser igroup zugeordneten LUNs für mehrere Hosts verfügbar machen möchten, können Sie mehrere Initiatornamen durch Kommas getrennt angeben. Weitere Informationen finden Sie unter lun igroup create im NetApp ONTAP-Dokumentationscenter.

3. Bestätigen Sie mit dem lun igroup show Befehl , dass vorhanden `igroup` ist:

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

Das System antwortet mit der folgenden Ausgabe:

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

4. In diesem Schritt wird davon ausgegangen, dass Sie bereits eine iSCSI-LUN erstellt haben. Wenn Sie dies nicht getan haben, Eine iSCSI-LUN erstellen finden Sie step-by-step Anweisungen dazu unter .

Erstellen Sie mithilfe der eine Zuordnung aus der von Ihnen erstellten LUN zu der von Ihnen erstellten igroup lun mapping createund geben Sie dabei die folgenden Attribute an:

- *svm_name* – Der Name der virtuellen Speichermaschine, die das iSCSI-Ziel bereitstellt. Der Host verwendet diesen Wert, um die LUN zu erreichen.
- *vol_name* – Der Name des Volumes, das die LUN hostet.
- *lun_name* – Der Name, den Sie der LUN zugewiesen haben.
- *igroup_name* – Der Name der Initiatorgruppe.
- *lun_id* – Die LUN-ID-Ganzzahl ist spezifisch für die Zuordnung, nicht für die LUN selbst. Dies wird von den Initiatoren in der igroup verwendet, da die Logische Einheitennummer diesen Wert für den Initiator beim Zugriff auf den Speicher verwendet.

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

5. Verwenden Sie den `lun show -path` Befehl , um zu bestätigen, dass die LUN erstellt, online und zugeordnet wurde.

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

Das System antwortet mit der folgenden Ausgabe:

```
 Vserver    Path                            serial-hex              state    mapped
```

```
--------- ------------------------------ ---------------------- --------
--------
svm_name  /vol/vol_name/lun_name         6c5742314e5d52766e796150 online   mapped
```

Speichern Sie den `serial_hex` Wert (in diesem Beispiel ist er `6c5742314e5d52766e796150`). Sie werden ihn in einem späteren Schritt verwenden, um einen Anzeigenamen für das Blockgerät zu erstellen.

6. Verwenden Sie den `network interface show -vserver` Befehl , um die Adressen der `iscsi_2` Schnittstellen `iscsi_1` und für die SVM abzurufen, in der Sie Ihre iSCSI LUN erstellt haben.

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

Das System antwortet mit der folgenden Ausgabe:

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

In diesem Beispiel `iscsi_1` lautet die IP-Adresse von `172.31.0.143` und `iscsi_2` `172.31.21.81`.

Mounten eines iSCSI LUN auf Ihrem Linux-Client

1. Verwenden Sie auf Ihrem Linux-Client den folgenden Befehl, um die Ziel-iSCSI-Knoten mithilfe `iscsi_1`der IP-Adresse von *`iscsi_1_IP`* zu ermitteln.

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

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

In diesem Beispiel `iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3` entspricht dem `target_initiator` für iSCSI LUN in der bevorzugten Availability Zone.

2. (Optional) Sie können zusätzliche Sitzungen mit der einrichten`target_initiator`. Amazon EC2 hat ein Bandbreitenlimit von 5 GB/s (~625 MB/s) für Single-Flow-Datenverkehr, aber Sie können mehrere Sitzungen erstellen, um von einem einzigen Client aus einen höheren Durchsatz zu Ihrem Dateisystem zu erreichen. Weitere Informationen finden Sie unter Netzwerkbandbreite für Amazon EC2-Instances im Amazon-Elastic-Compute-Cloud-Benutzerhandbuch für Linux-Instances.

   Der folgende Befehl richtet 8 Sitzungen pro Initiator pro ONTAP-Knoten in jeder Availability Zone ein, sodass der Client bis zu 40 Gb/s (5 000 MB/s) Gesamtdurchsatz an den iSCSI LUN senden kann.

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

3. Melden Sie sich bei den Zielinitiatoren an. Ihre iSCSI LUNs werden als verfügbare Datenträger angezeigt.

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

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

Die obige Ausgabe ist gekürzt. Sie sollten eine `Logging in` und eine `Login successful` Antwort für jede Sitzung auf jedem Dateiserver sehen. Bei 4 Sitzungen pro Knoten gibt es 8 `Logging in` und 8 `Login successful` Antworten.

4. Verwenden Sie den folgenden Befehl, um zu überprüfen, ob die iSCSI-Sitzungen identifiziert und zusammengeführt `dm-multipath` hat, indem Sie eine einzelne LUN mit mehreren Richtlinien anzeigen. Es sollte eine gleiche Anzahl von Geräten geben, die als aufgeführt sind, `active` und solche, die als aufgeführt sind`enabled`.

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

In der Ausgabe ist der Datenträgername als formatiert`dm-xyz`, wobei eine Ganzzahl `xyz` ist. Wenn es keine anderen Multipath-Festplatten gibt, ist dieser Wert `dm-0`.

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

Ihr Blockgerät ist jetzt mit Ihrem Linux-Client verbunden. Sie befindet sich unter dem Pfad `/dev/`*`dm-xyz`*. Sie sollten diesen Pfad nicht für administrative Zwecke verwenden. Verwenden Sie stattdessen den symbolischen Link unter dem Pfad `/dev/mapper/`*`wwid`*, wobei eine eindeutige Kennung für Ihre LUN *`wwid`* ist, die geräteübergreifend konsistent ist. Im nächsten Schritt geben Sie einen benutzerfreundlichen Namen für die an, *`wwid`* damit Sie sie von anderen Festplatten mit mehreren Pfaden unterscheiden können.

So geben Sie Ihrem Blockgerät einen benutzerfreundlichen Namen

1. Um Ihrem Gerät einen benutzerfreundlichen Namen zu geben, erstellen Sie einen Alias in der `-/etc/multipath.conf`Datei. Fügen Sie dazu der Datei mit Ihrem bevorzugten Texteditor den folgenden Eintrag hinzu und ersetzen Sie die folgenden Platzhalter:

   - Ersetzen Sie durch `serial_hex` den Wert, den Sie in der Konfigurieren von iSCSI auf dem FSx-für-ONTAP-DateisystemProzedur gespeichert haben.
   - Fügen Sie dem `serial_hex` Wert `3600a0980` das Präfix hinzu, wie im Beispiel gezeigt. Dies ist eine eindeutige Präambel für die NetApp ONTAP-Verteilung, die Amazon FSx für NetApp ONTAP verwendet.
   - Ersetzen Sie durch `device_name` den Anzeigenamen, den Sie für Ihr Gerät verwenden möchten.

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

Alternativ können Sie das folgende Skript kopieren und als Bash-Datei speichern, z. B. `multipath_alias.sh`. Sie können das Skript mit Sudo-Berechtigungen ausführen und *`serial_hex`* (ohne das Präfix 3600a0980) und *`device_name`* durch Ihre jeweilige Seriennummer und den gewünschten Anzeigenamen ersetzen. Dieses Skript sucht in `multipaths` der `/etc/multipath.conf` Datei nach einem Abschnitt ohne Kommentar. Wenn einer vorhanden ist, wird ein `multipath` Eintrag an diesen Abschnitt angehängt. Andernfalls wird ein neuer `multipaths` Abschnitt mit einem `multipath` Eintrag für Ihr Blockgerät erstellt.

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

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

2. Starten Sie den `multipathd` Service neu, damit die Änderungen wirksam `/etc/multipathd.conf` werden.

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

So partitionieren Sie die LUN

Der nächste Schritt besteht darin, Ihre LUN mit zu formatieren und zu partitionieren`fdisk`.

1. Verwenden Sie den folgenden Befehl, um zu überprüfen, ob der Pfad zu Ihrem vorhanden `device_name` ist.

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

```
/dev/device_name
```

2. Partitionieren Sie den Datenträger mit `fdisk`. Sie geben eine interaktive Eingabeaufforderung ein. Geben Sie die Optionen in der angezeigten Reihenfolge ein. Beachten Sie, dass der `Last sector` Wert je nach Größe Ihrer iSCSI LUN variiert (in diesem Beispiel 10 GB). Sie können mehrere Partitionen erstellen, indem Sie einen Wert verwenden, der kleiner ist als der letzte Sektor (`20971519` in diesem Beispiel).

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

Die `fsdisk` interaktive Eingabeaufforderung wird gestartet.

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

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

Device does not contain a recognized partition table.
```

```
Created a new DOS disklabel with disk identifier 0x66595cb0.

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

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

Nach der Eingabe von `/dev/mapper/`*`partition_name`* wird wIhre neue Partition verfügbar. Der *`partition_name`* hat das Format *`<device_name><partition_number>`*. 1 wurde als Partitionsnummer verwendet, die im `fdisk` Befehl im vorherigen Schritt verwendet wurde.

3. Erstellen Sie Ihr Dateisystem mit `/dev/mapper/`*`partition_name`* als Pfad.

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

Das System antwortet mit der folgenden Ausgabe:

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

```
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

So mounten Sie die LUN auf dem Linux-Client

1. Erstellen Sie ein Verzeichnis *directory_path* als Mountingpunkt für Ihr Dateisystem.

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

2. Mounten Sie das Dateisystem mit dem folgenden Befehl.

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

3. (Optional) Sie können die Eigentümerschaft des Mount-Verzeichnisses an Ihren Benutzer ändern. Ersetzen Sie *username* durch Ihren Benutzernamen.

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

4. (Optional) Stellen Sie sicher, dass Sie Daten aus dem Dateisystem lesen und in das Dateisystem schreiben können.

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

   Sie haben erfolgreich eine iSCSI LUN auf Ihrem Linux-Client erstellt und gemountet.

Mounting von iSCSI LUNs an einen Windows-Client

Die in diesen Verfahren vorgestellten Beispiele verwenden die folgende Einrichtung:

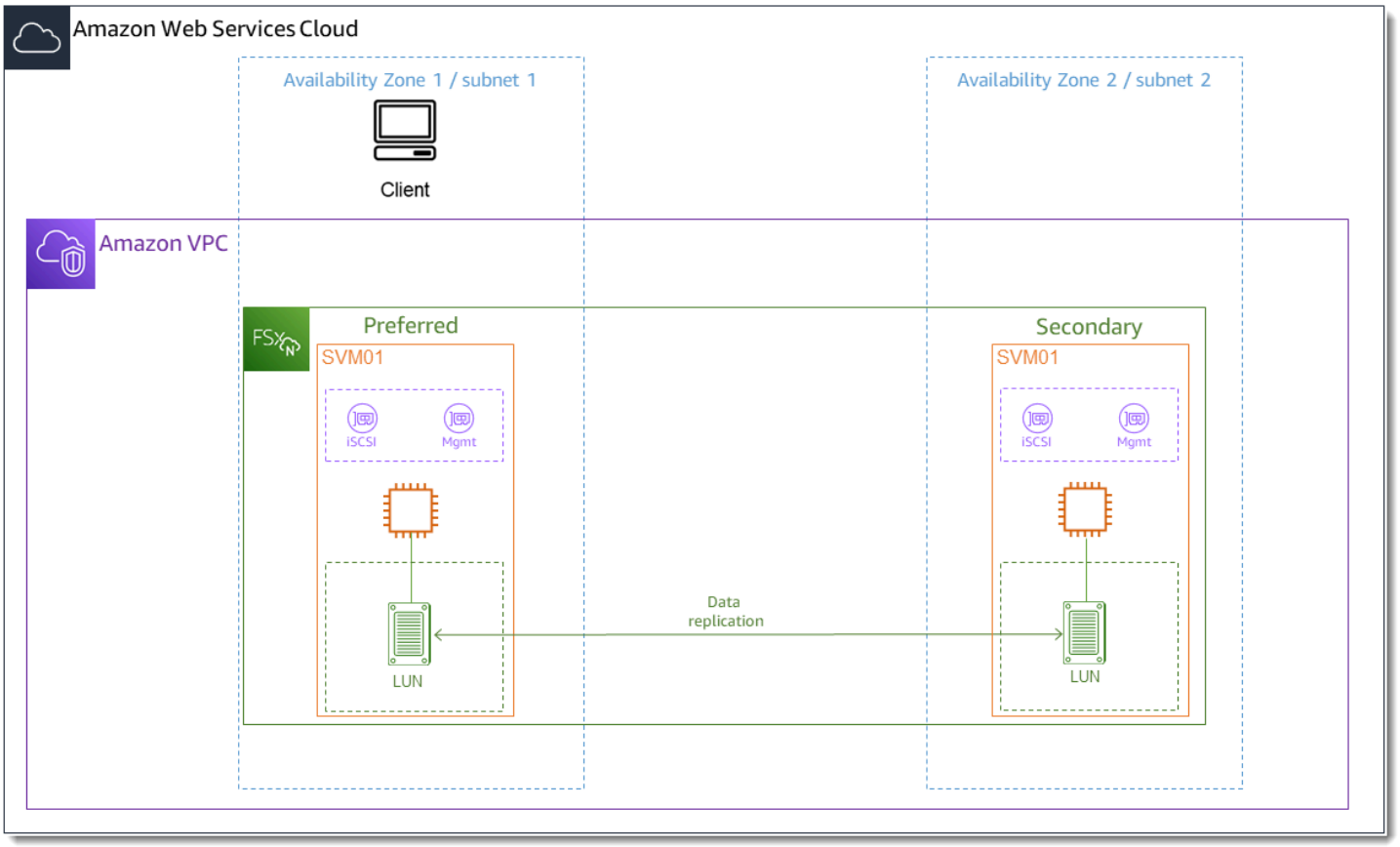
- Das iSCSI LUN, das auf einem Windows-Host bereitgestellt wird, ist bereits erstellt. Weitere Informationen finden Sie unter Eine iSCSI-LUN erstellen.
- Der Microsoft Windows-Host, der den iSCSI LUN mountet, ist eine Amazon EC2-Instance, auf der ein Microsoft Windows Server 2019 Amazon Machine Image (AMI) ausgeführt wird. Es sind VPC-

Sicherheitsgruppen so konfiguriert, dass ein- und ausgehender Datenverkehr zugelassen wird, wie unter beschriebenDateisystem-Zugriffskontrolle mit Amazon VPC.

Möglicherweise verwenden Sie in Ihrer Einrichtung ein anderes Microsoft Windows-AMI.

- Der Client und das Dateisystem befinden sich in derselben VPC und AWS-Konto. Wenn sich der Client in einer anderen VPC befindet, können Sie VPC-Peering oder verwenden, AWS Transit Gateway um anderen VPCs Zugriff auf die iSCSI-Endpunkte zu gewähren. Weitere Informationen finden Sie unter Zugriff auf Daten von außerhalb der Bereitstellungs-VPC.

  Wir empfehlen, dass sich die EC2-Instance in derselben Availability Zone wie das bevorzugte Subnetz Ihres Dateisystems befindet, wie in der folgenden Grafik dargestellt.



Themen

- Konfigurieren von iSCSI auf dem Windows-Client
- Konfigurieren von iSCSI auf dem FSx-für-ONTAP-Dateisystem
- Mounten eines iSCSI LUN auf dem Windows-Client

Konfigurieren von iSCSI auf dem Windows-Client

1. Verwenden Sie Windows Remote Desktop, um eine Verbindung mit dem Windows-Client herzustellen, auf dem Sie die iSCSI LUN mounten möchten. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance über RDP im Amazon Elastic Compute Cloud-Benutzerhandbuch.
2. Öffnen Sie ein Windows PowerShell als Administrator. Verwenden Sie die folgenden Befehle, um iSCSI auf Ihrer Windows-Instance zu aktivieren und den iSCSI-Service so zu konfigurieren, dass er automatisch gestartet wird.

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

3. Rufen Sie den Initiatornamen Ihrer Windows-Instance ab. Sie verwenden diesen Wert bei der Konfiguration von iSCSI auf Ihrem FSx-für-ONTAP-Dateisystem mithilfe der NetApp ONTAP-CLI.

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

   Das System antwortet mit dem Initiator-Port:

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

4. Damit Ihre Clients automatisch ein Failover zwischen Ihren Dateiservern durchführen können, müssen Sie `Multipath-IO` (MPIO) auf Ihrer Windows-Instance installieren. Verwenden Sie den folgenden Befehl:

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

5. Starten Sie Ihre Windows-Instance neu, nachdem die `Multipath-IO` Installation abgeschlossen ist. Halten Sie Ihre Windows-Instance geöffnet, um Schritte zum Mounten der iSCSI LUN in einem folgenden Abschnitt auszuführen.

Konfigurieren von iSCSI auf dem FSx-für-ONTAP-Dateisystem

1. Stellen Sie mit dem folgenden Befehl eine Verbindung mit der NetApp ONTAP-CLI auf dem FSx-für-ONTAP-Dateisystem her, auf dem Sie die iSCSI LUN erstellt haben. Weitere Informationen finden Sie unter Verwenden der NetApp ONTAP-CLI.

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

2. lun igroup createErstellen Sie mithilfe der NetApp ONTAP-CLI die Initiatorgruppe oder `igroup`. Eine Initiatorgruppe wird iSCSI LUNs zugeordnet und steuert, welche Initiatoren (Clients) Zugriff auf LUNs haben. Ersetzen Sie durch `host_initiator_name` den Initiatornamen von Ihrem Windows-Host, den Sie im vorherigen Verfahren abgerufen haben.

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

Wenn Sie die diesem zugeordneten LUNs mehreren Hosts zur `igroup` Verfügung stellen möchten, können Sie mehrere kommagetrennte Initiatornamen angeben. Weitere Informationen finden Sie unter `lun igroup create` im NetApp ONTAP-Dokumentationscenter.

3. Bestätigen Sie mit dem folgenden Befehl, dass erfolgreich erstellt `igroup` wurde:

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

Das System antwortet mit der folgenden Ausgabe:

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

Wenn das `igroup` erstellt wurde, können Sie LUNs erstellen und sie dem zuordnen`igroup`.

4. In diesem Schritt wird davon ausgegangen, dass Sie bereits eine iSCSI-LUN erstellt haben. Wenn Sie dies nicht getan haben, Eine iSCSI-LUN erstellen finden Sie step-by-step Anweisungen dazu unter .

Erstellen Sie eine LUN-Zuweisung aus der LUN zu Ihrem neuen `igroup`.

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

5. Bestätigen Sie mit dem folgenden Befehl, dass die LUN erstellt, online und zugeordnet wurde:

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
```

```
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

Sie können nun das iSCSI-Ziel auf Ihrer Windows-Instance hinzufügen.

6. Rufen Sie die IP-Adressen der `iscsi_2` Schnittstellen `iscsi_1` und für Ihre SVM mit dem folgenden Befehl ab:

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

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

In diesem Beispiel `iscsi_1` lautet die IP-Adresse von `172.31.0.143` und `iscsi_2` `172.31.21.81`.

Mounten eines iSCSI LUN auf dem Windows-Client

1. Öffnen Sie auf Ihrer Windows-Instance ein PowerShell Terminal als Administrator.
2. Sie erstellen ein `.ps1`Skript, das Folgendes tut:
   - Stellt eine Verbindung zu jeder der iSCSI-Schnittstellen Ihres Dateisystems her.
   - Fügt MPIO für iSCSI hinzu und konfiguriert es.
   - Stellt 8 Sitzungen für jede iSCSI-Verbindung her, wodurch der Client bis zu 40 Gb/s (5 000 MB/s) Gesamtdurchsatz an die iSCSI LUN weiterleiten kann. 8 Sitzungen stellen sicher, dass ein einzelner Client die volle Durchsatzkapazität von 4 000 MB/s für die höchste Durchsatzkapazität von FSx für ONTAP erreichen kann. Sie können optional die Anzahl der Sitzungen in eine höhere oder niedrigere Anzahl von Sitzungen ändern (jede Sitzung bietet einen Durchsatz von bis zu 625 MB/s), indem Sie den for-loop des Skripts im `#Establish`

`iSCSI connection` Schritt von `1..8` in einen anderen oberen Grenzwert ändern. Weitere Informationen finden Sie unter Netzwerkbandbreite der Amazon EC2-Instance im Amazon-Elastic-Compute-Cloud-Benutzerhandbuch für Windows-Instances.

Kopieren Sie den folgenden Satz von Befehlen in eine Datei, um das `.psl`Skript zu erstellen.

- Ersetzen Sie `iscsi_1` und `iscsi_2` durch die IP-Adressen, die Sie im vorherigen Schritt abgerufen haben.
- Ersetzen Sie durch `ec2_ip` die IP-Adresse Ihrer Windows-Instance.

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

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

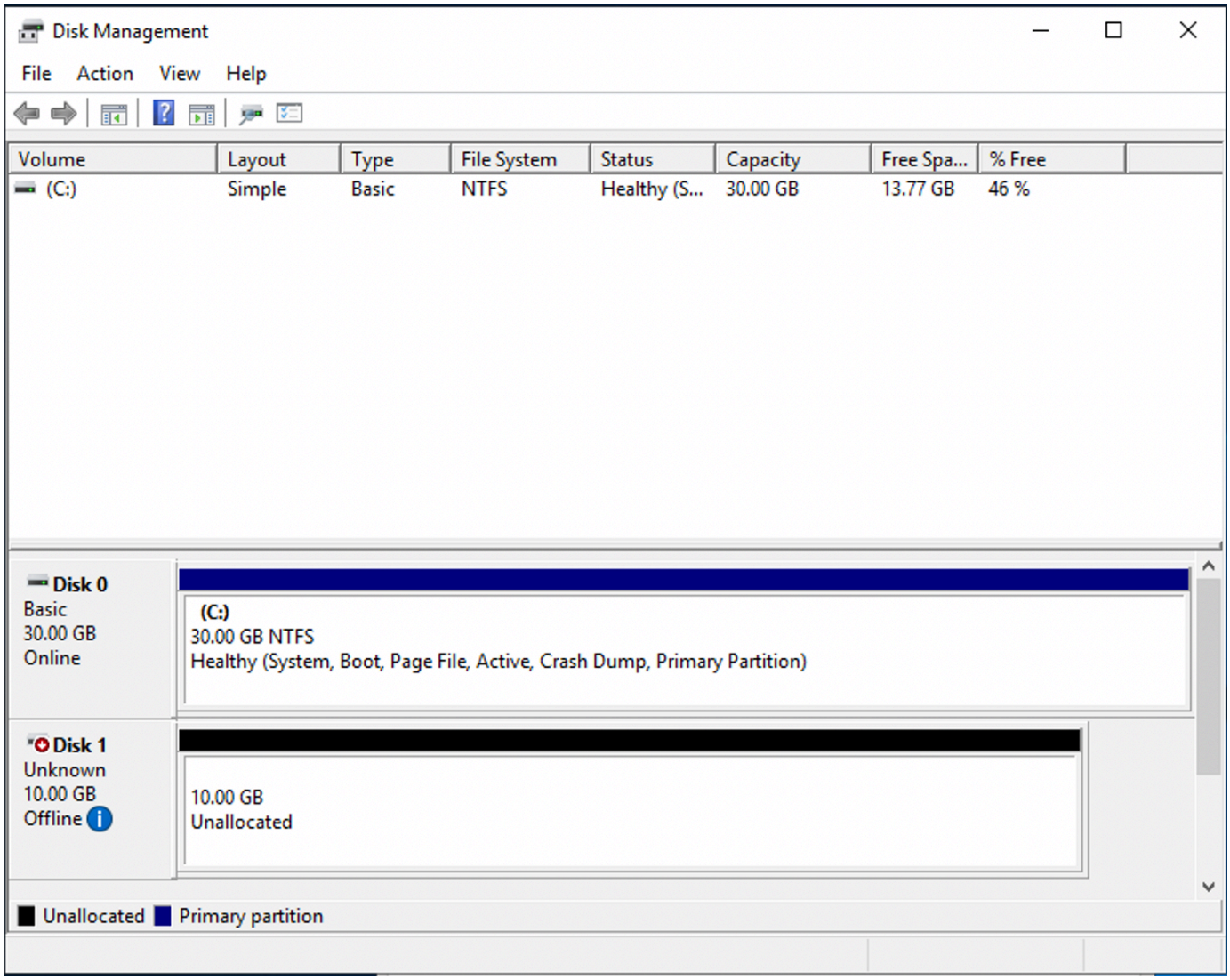
#Connect to FSx for NetApp ONTAP file system
Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

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

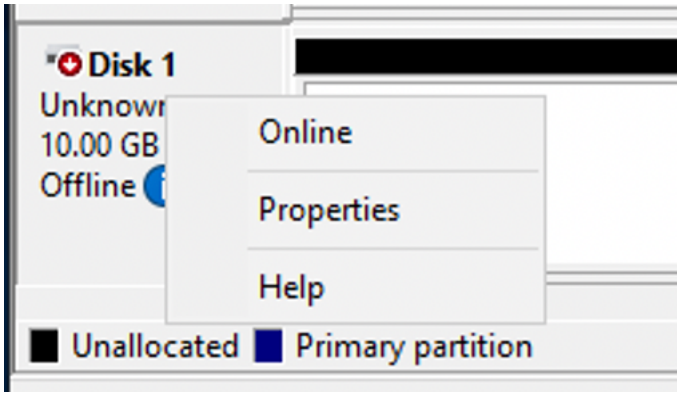
#Establish iSCSI connection
1..8 | %{Foreach($TargetPortalAddress in $TargetPortalAddresses)
{Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true}}

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

3. Starten Sie die Windows-Datenträgerverwaltungsanwendung. Öffnen Sie das Dialogfeld Windows ausführen und geben Sie ein `diskmgmt.msc` und drücken Sie die Eingabetaste. Die Datenträgerverwaltungsanwendung wird geöffnet.



4. Suchen Sie die nicht zugewiesene Festplatte Dies ist die iSCSI LUN. Im Beispiel ist Festplatte 1 der iSCSI-Datenträger. Sie ist offline.



Bringen Sie das Volume online, indem Sie den Cursor über Datenträger 1 platzieren und mit der rechten Maustaste klicken und dann Online auswählen.

> **Note**
>
> Sie können die Richtlinie für das Storage Area Network (SAN) ändern, sodass neue Volumes automatisch online geschaltet werden. Weitere Informationen finden Sie unter SAN-Richtlinien in der Microsoft Windows Server-Befehlsreferenz .

5. Um den Datenträger zu initialisieren, platzieren Sie den Cursor über Datenträger 1 und wählen Sie Initialisieren aus. Das Dialogfeld Initialisieren wird angezeigt. Wählen Sie OK, um den Datenträger zu initialisieren.
6. Formatieren Sie den Datenträger wie gewohnt. Nach Abschluss der Formatierung wird das iSCSI-Laufwerk als verwendbares Laufwerk auf dem Windows-Client angezeigt.

Verwenden von FSx für ONTAP mit anderen AWS -Services

Zusätzlich zu Amazon EC2 können Sie andere - AWS Services mit Ihren Volumes verwenden, um auf Ihre Daten zuzugreifen.

Themen

- Amazon WorkSpaces mit FSx für ONTAP verwenden
- Verwenden von Amazon Elastic Container Service mit FSx für ONTAP
- Verwenden von VMware Cloud mit FSx für ONTAP

Amazon WorkSpaces mit FSx für ONTAP verwenden

FSx for ONTAP kann mit Amazon verwendet werden WorkSpaces , um gemeinsam genutzten Netzwerkspeicher (NAS) bereitzustellen oder Roaming-Profile für Amazon-Konten zu speichern. WorkSpaces Nachdem der Benutzer mit einer WorkSpaces Instance eine Verbindung zu einer SMB-Dateifreigabe hergestellt hat, kann er Dateien auf der Dateifreigabe erstellen und bearbeiten.

Die folgenden Verfahren zeigen, wie Sie Amazon FSx mit Amazon verwenden, WorkSpaces um den Zugriff auf Roaming-Profile und Home-Ordner einheitlich zu gestalten und einen gemeinsamen Team-Ordner für Windows- und WorkSpaces Linux-Benutzer bereitzustellen. Wenn Sie neu bei Amazon sind WorkSpaces, können Sie Ihre erste WorkSpaces Amazon-Umgebung mithilfe der Anweisungen unter Erste Schritte mit der WorkSpaces Schnellinstallation im WorkSpaces Amazon-Administratorhandbuch erstellen.

Themen

- Bieten Sie Unterstützung für Roaming-Profile
- Stellen Sie einen gemeinsamen Ordner für den Zugriff auf häufig verwendete Dateien bereit

Bieten Sie Unterstützung für Roaming-Profile

Sie können Amazon FSx verwenden, um Benutzern in Ihrer Organisation Unterstützung für Roaming-Profile zu bieten. Ein Benutzer wird berechtigt sein, nur auf sein Roaming-Profil zuzugreifen. Der Ordner wird automatisch mithilfe der Active Directory-Gruppenrichtlinien verbunden. Mit einem Roaming-Profil werden die Daten und Desktop-Einstellungen der Benutzer gespeichert, wenn sie sich von einer Amazon FSx-Dateifreigabe abmelden, sodass Dokumente und Einstellungen zwischen verschiedenen WorkSpaces Instanzen gemeinsam genutzt und mithilfe der täglichen automatischen Backups von Amazon FSx automatisch gesichert werden können.

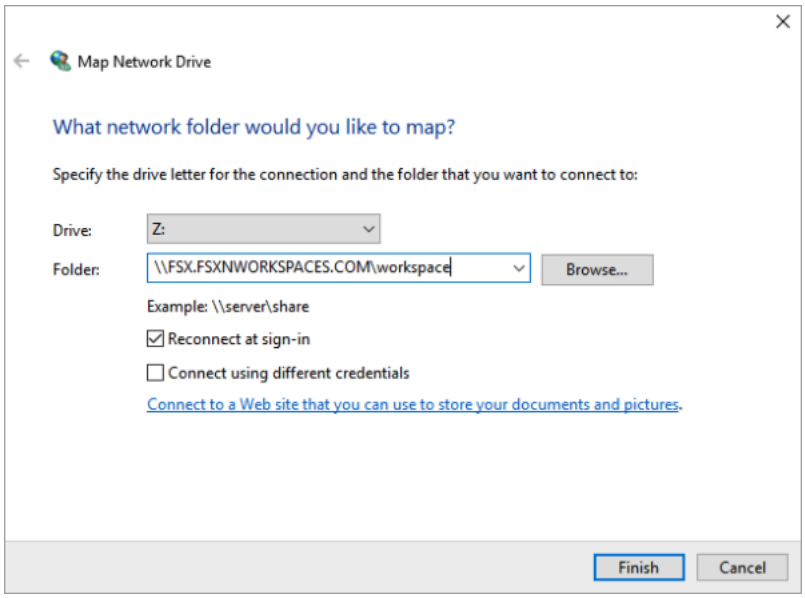
Schritt 1: Erstellen Sie einen Speicherort für einen Profilordner für Domain-Benutzer, die Amazon FSx verwenden

1. Erstellen Sie mit der Amazon FSx-Konsole ein FSx for ONTAP-Dateisystem. Weitere Informationen finden Sie unter Um ein Dateisystem (Konsole) zu erstellen.

   > **Important**
   >
   > Jedes FSx for ONTAP-Dateisystem hat einen Endpunkt-IP-Adressbereich, aus dem die mit dem Dateisystem verknüpften Endpunkte erstellt werden. Für Multi-AZ-Dateisysteme wählt FSx for ONTAP einen standardmäßigen ungenutzten IP-Adressbereich von 198.19.0.0/16 als Endpunkt-IP-Adressbereich. Dieser IP-Adressbereich wird auch von WorkSpaces für die Verwaltung des Datenverkehrsbereichs verwendet, wie unter IP-Adressen und Portanforderungen für WorkSpaces im Amazon WorkSpaces Administration Guide beschrieben. Um von Ihrem Multi-AZ FSx for ONTAP-Dateisystem aus auf Ihr Multi-AZ FSx for ONTAP-Dateisystem zuzugreifen WorkSpaces, müssen Sie daher einen Endpunkt-IP-Adressbereich auswählen, der sich nicht mit 198.19.0.0/16 überschneidet.

2. Wenn Sie noch keine virtuelle Speichermaschine (SVM) mit einem Active Directory verknüpft haben, erstellen Sie jetzt eine. Sie können beispielsweise eine SVM mit dem Namen `fsx` und dem Sicherheitsstil auf bereitstellen. `NTFS` Weitere Informationen finden Sie unter So erstellen Sie eine virtuelle Speichermaschine (Konsole).

3. Erstellen Sie ein Volume für Ihre SVM. Sie können beispielsweise ein Volume mit dem Namen erstellen`fsx-vol`, das den Sicherheitsstil des Root-Volumes Ihrer SVM übernimmt. Weitere Informationen finden Sie unter Um ein Volume (Konsole) zu erstellen FlexVol.
4. Erstellen Sie eine SMB-Freigabe auf Ihrem Volume. Sie können beispielsweise eine Freigabe mit `workspace` dem Namen auf Ihrem Volume erstellen`fsx-vol`, in der Sie einen Ordner mit dem Namen `profiles` erstellen. Weitere Informationen finden Sie unter Verwaltung von SMB-Aktien.
5. Greifen Sie auf Ihre Amazon FSx SVM von einer Amazon EC2 EC2-Instance aus zu, auf der Windows Server ausgeführt wird, oder von einer. WorkSpace Weitere Informationen finden Sie unter Zugriff auf -Daten.
6. Sie ordnen Ihren Anteil `Z:\` auf Ihrer Windows-Instance zu: WorkSpaces



Schritt 2: Die Dateifreigabe FSx for ONTAP mit Benutzerkonten verknüpfen

1. Wählen Sie auf dem Computer Ihres Testbenutzers WorkSpace Windows > System > Erweiterte Systemeinstellungen.
2. Wählen Sie in den Systemeigenschaften die Registerkarte „Erweitert“ und klicken Sie im Bereich „Benutzerprofile“ auf die Schaltfläche „Einstellungen“. Der angemeldete Benutzer hat den Profiltyp. `Local`
3. Melden Sie den Testbenutzer vom ab. WorkSpace
4. Stellen Sie für den Testbenutzer ein, dass sich ein Roaming-Profil in Ihrem Amazon FSx-Dateisystem befindet. Öffnen Sie in Ihrem Administrator WorkSpaces eine PowerShell Konsole

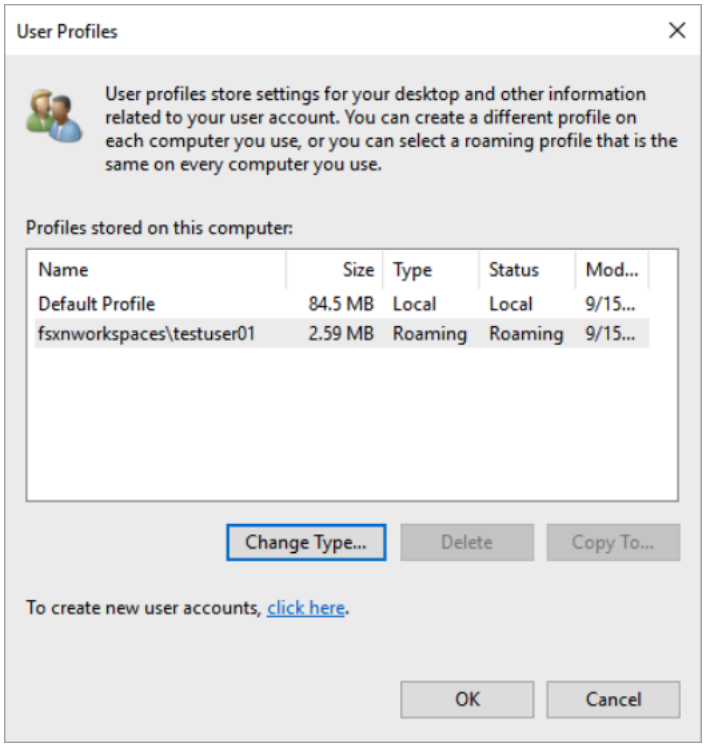
und verwenden Sie einen Befehl ähnlich dem folgenden Beispiel (der den `profiles` Ordner verwendet, den Sie zuvor in Schritt 1 erstellt haben):

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

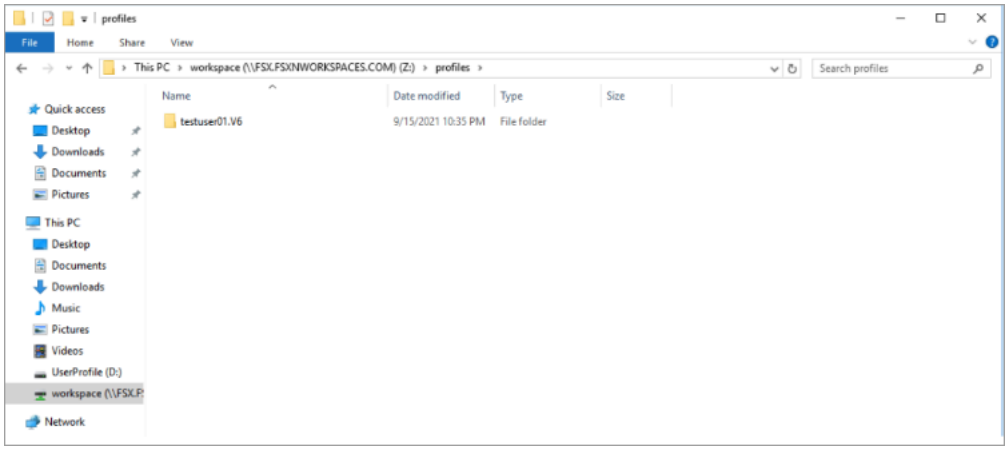
Beispiel:

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

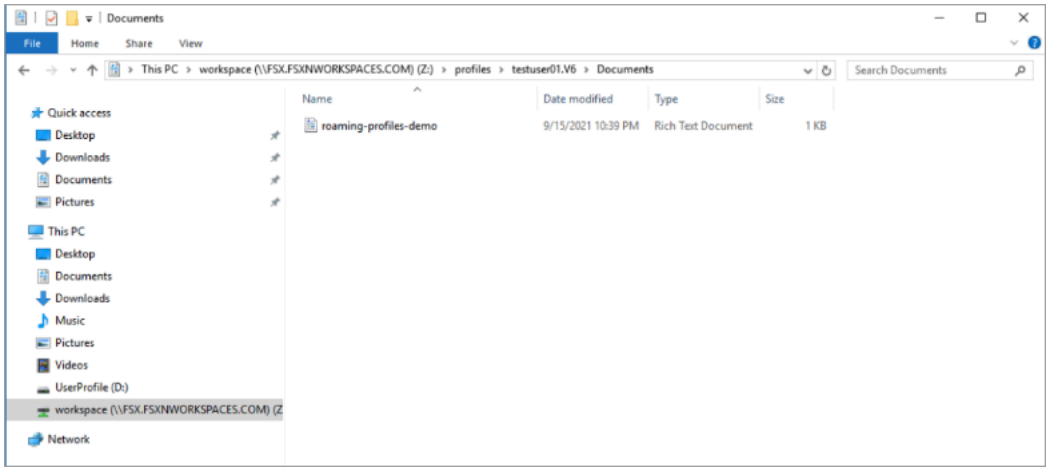
5. Melden Sie sich beim Testbenutzer an WorkSpace.
6. Wählen Sie in den Systemeigenschaften die Registerkarte Erweitert und klicken Sie im Bereich Benutzerprofile auf die Schaltfläche Einstellungen. Der angemeldete Benutzer hat den Profiltyp. `Roaming`



7. Durchsuchen Sie den freigegebenen Ordner FSx for ONTAP. In dem `profiles` Ordner sehen Sie einen Ordner für den Benutzer.



8. Erstellen Sie ein Dokument im `Documents` Ordner des Testbenutzers
9. Melden Sie den Testbenutzer von seinem ab WorkSpace.
10. Wenn Sie sich erneut als Testbenutzer anmelden und zu seinem Profilspeicher wechseln, wird das von Ihnen erstellte Dokument angezeigt.



Stellen Sie einen gemeinsamen Ordner für den Zugriff auf häufig verwendete Dateien bereit

Sie können Amazon FSx verwenden, um Benutzern in Ihrer Organisation einen gemeinsamen Ordner zur Verfügung zu stellen. In einem gemeinsamen Ordner können Dateien gespeichert werden, die von Ihrer Benutzergemeinschaft verwendet werden, z. B. Demo-Dateien, Codebeispiele und Anleitungen, die von allen Benutzern benötigt werden. In der Regel haben Sie Laufwerke für gemeinsam genutzte Ordner zugeordnet. Da zugeordnete Laufwerke jedoch Buchstaben verwenden, ist die Anzahl der Freigaben, die Sie haben können, begrenzt. Durch dieses Verfahren wird ein freigegebener Amazon FSx-Ordner erstellt, der ohne Laufwerksbuchstaben verfügbar ist. Dadurch erhalten Sie mehr Flexibilität bei der Zuweisung von Freigaben an Teams.

Um einen gemeinsamen Ordner für den plattformübergreifenden Zugriff von Linux und Windows aus bereitzustellen WorkSpaces

1. Wählen Sie in der Taskleiste „Orte“ > „Mit Server Connect“.

   a. Geben Sie *`file-system-dns-name`*für Server ein.

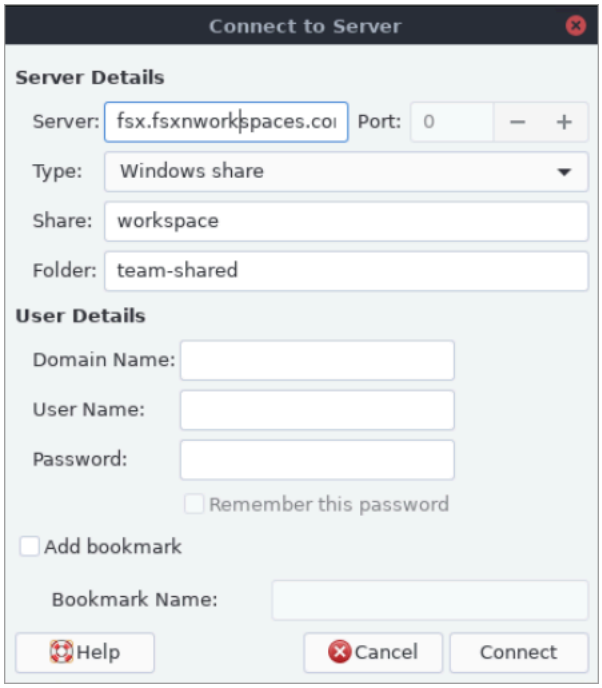
   b. Stellen Sie Typ auf ein`Windows share`.

   c. Stellen Sie Share auf den Namen der SMB-Freigabe ein, z. B. `workspace`

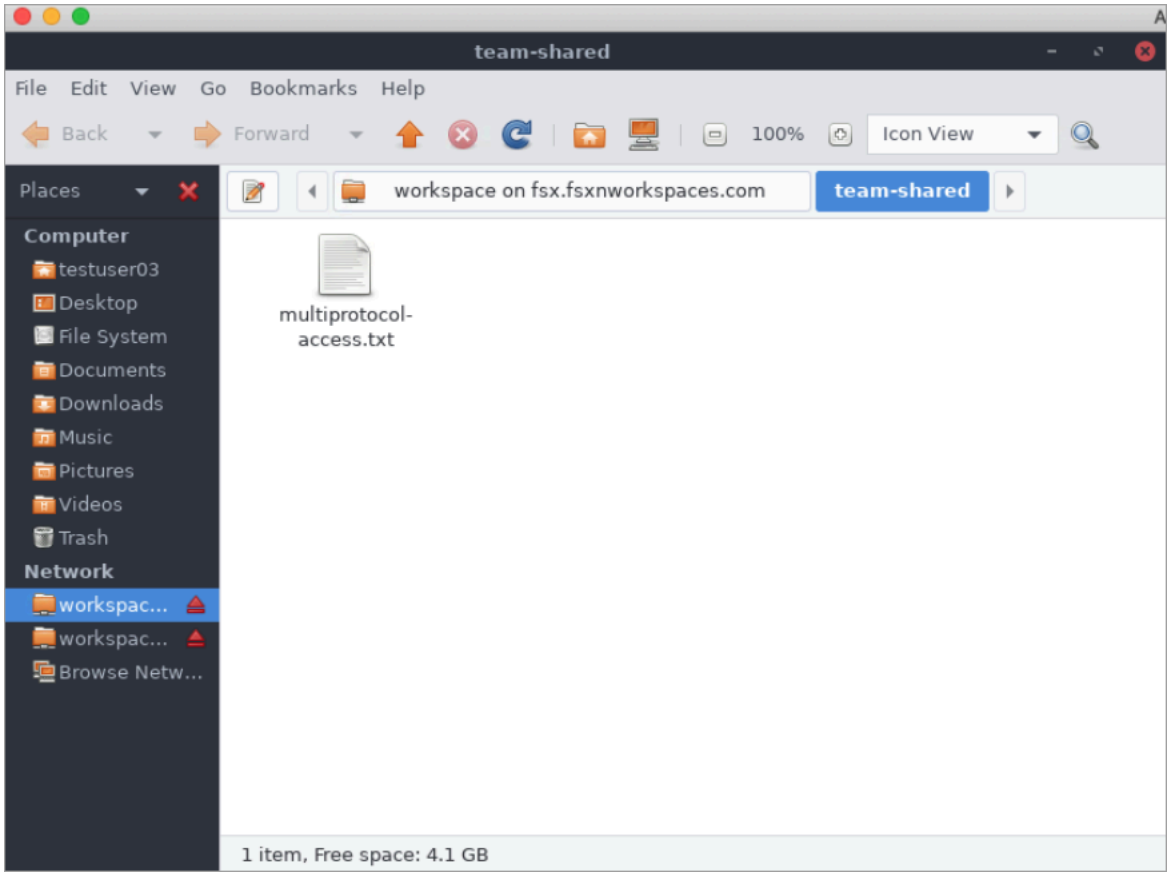
   d. Sie können Ordner unverändert lassen `/` oder ihn auf einen Ordner festlegen, z. B. einen Ordner mit dem Name`team-shared`.

   e. Für ein Linux müssen Sie Ihre Benutzerdaten nicht eingeben WorkSpace, wenn sich Ihr Linux in derselben Domain wie die Amazon FSx-Freigabe WorkSpace befindet.

   f. Wählen Sie Connect aus.



2. Nachdem die Verbindung hergestellt wurde, können Sie den geteilten Ordner (`team-shared`in diesem Beispiel benannt) in der SMB-Freigabe mit dem Namen sehen. `workspace`



Verwenden von Amazon Elastic Container Service mit FSx für ONTAP

Sie können auf Ihre Dateisysteme von Amazon FSx für NetApp ONTAP von einem Amazon Elastic Container Service (Amazon ECS) Docker-Container auf einer Amazon EC2 Linux- oder Windows-Instance zugreifen.

Mounting auf einem Amazon-ECS-Linux-Container

1. Erstellen Sie einen ECS-Cluster mit der EC2-Linux- + Networking-Clustervorlage für Ihre Linux-Container. Weitere Informationen finden Sie unter Erstellen eines Clusters im Amazon Elastic Container Service-Entwicklerhandbuch.
2. Erstellen Sie auf der EC2-Instance wie folgt ein Verzeichnis zum Mounten des SVM-Volumes:

```
sudo mkdir /fsxontap
```

3. Mounten Sie Ihr FSx-für-ONTAP-Volume auf der Linux-EC2-Instance, indem Sie entweder beim Start der Instance ein Benutzerdatenskript verwenden oder die folgenden Befehle ausführen:

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

4. Mounten Sie das Volume mit dem folgenden Befehl:

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

Im folgenden Beispiel werden Beispielwerte verwendet.

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

Sie können auch die IP-Adresse der SVM anstelle des DNS-Namens verwenden.

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

5. Wenn Sie Ihre Amazon-ECS-Aufgabendefinitionen erstellen, fügen Sie der JSON-Containerdefinition die folgenden - `volumes` und -`mountPoints`Containereigenschaften hinzu. Ersetzen Sie die `sourcePath` durch den Mountingpunkt und das Verzeichnis in Ihrem FSx-für-ONTAP-Dateisystem.

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

```
}
```

Mounting auf einem Amazon-ECS-Windows-Container

1. Erstellen Sie einen ECS-Cluster mit der EC2-Windows + Networking-Clustervorlage für Ihre Windows-Container. Weitere Informationen finden Sie unter Erstellen eines Clusters im Amazon Elastic Container Service-Entwicklerhandbuch.
2. Fügen Sie dem ECS-Windows-Cluster eine mit der Domain verbundene Windows-EC2-Instance hinzu und ordnen Sie eine SMB-Freigabe zu.

   Starten Sie eine ECS-optimierte Windows-EC2-Instance, die mit Ihrer Active-Directory-Domain verbunden ist, und initialisieren Sie den ECS-Agenten, indem Sie den folgenden Befehl ausführen.

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

   Sie können die Informationen auch wie folgt in einem Skript an das Textfeld Benutzerdaten übergeben.

   ```
   <powershell>
   Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
   </powershell>
   ```

3. Erstellen Sie ein globales SMB-Mapping auf der EC2-Instance, damit Sie Ihre SMB-Freigabe einem Laufwerk zuordnen können. Ersetzen Sie die Werte unter netbios oder DNS-Name für Ihr FSx-Dateisystem und geben Sie den Namen frei. Das NFS-Volume vol1, das auf der Linux-EC2-Instance gemountet wurde, ist als CIFS-Freigabe fsxontap auf dem FSx-Dateisystem konfiguriert.

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


                                   Vserver: svm08
                                     Share: fsxontap
                   CIFS Server NetBIOS Name: FSXONTAPDEMO
                                      Path: /vol1
                            Share Properties: oplocks
                                              browsable
   ```

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

4. Erstellen Sie das globale SMB-Mapping auf der EC2-Instance mit dem folgenden Befehl:

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

5. Wenn Sie Ihre Amazon-ECS-Aufgabendefinitionen erstellen, fügen Sie der JSON-Containerdefinition die folgenden - `volumes` und -`mountPoints`Containereigenschaften hinzu. Ersetzen Sie die `sourcePath` durch den Mountingpunkt und das Verzeichnis in Ihrem FSx-für-ONTAP-Dateisystem.

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

Verwenden von VMware Cloud mit FSx für ONTAP

Sie können FSx für ONTAP als externen Datenspeicher für AWS Software-Defined Data Centers (SDDCs) von VMware Cloud in verwenden. Weitere Informationen finden Sie unter Konfigurieren von Amazon FSx für NetApp ONTAP als externen Speicher und VMware Cloud in AWS mit Amazon FSx für NetApp ONTAP-Bereitstellungshandbuch.

Verfügbarkeit und Beständigkeit

Amazon FSx für NetApp ONTAP verwendet zwei Bereitstellungstypen, Single-AZ und Multi-AZ, die unterschiedliche Verfügbarkeits- und Haltbarkeitsstufen bieten. In diesem Thema werden die Verfügbarkeits- und Haltbarkeitsfunktionen der einzelnen Bereitstellungstypen beschrieben, damit Sie die für Ihre Workloads am besten geeignete auswählen können. Informationen zur Verfügbarkeits-SLA des Services (Service Level Agreement) finden Sie unter Amazon FSx Service Level Agreement.

Themen

- Auswählen eines Dateisystem-Bereitstellungstyps
- Failover-Prozess für FSx für ONTAP
- Netzwerkressourcen

Auswählen eines Dateisystem-Bereitstellungstyps

Die Verfügbarkeits- und Haltbarkeitsfunktionen von Single-AZ- und Multi-AZ-Dateisystem-Bereitstellungstypen werden in den folgenden Abschnitten beschrieben.

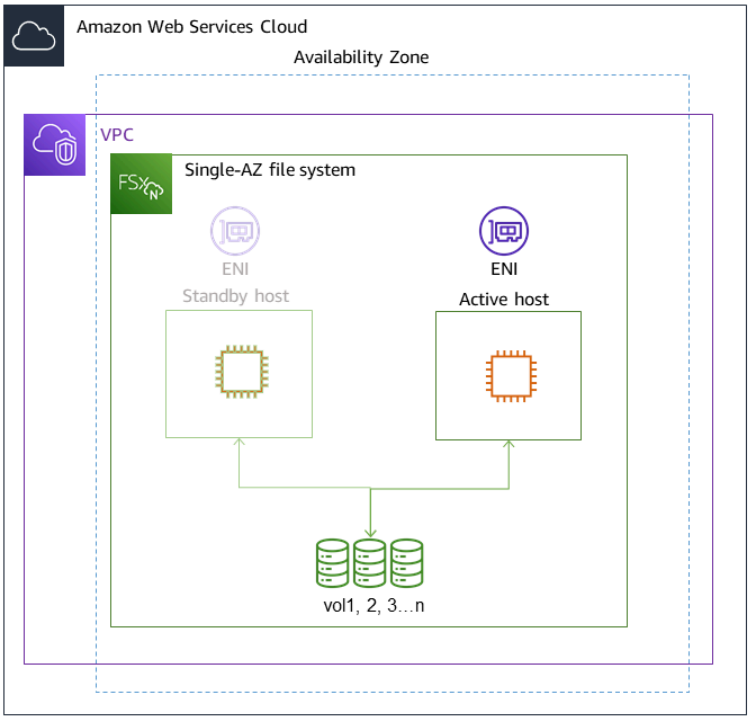
Single-AZ-Bereitstellungstyp

Wenn Sie ein Single-AZ-Dateisystem erstellen, stellt Amazon FSx automatisch ein bis zwölf Paare von Dateiservern in einer Aktiv-Standby-Konfiguration bereit, wobei sich die aktiven und Standby-Dateiserver in jedem Paar in separaten Fehlerdomänen innerhalb einer einzigen Availability Zone in der befinden AWS-Region. Während der geplanten Dateisystemwartung oder einer ungeplanten Serviceunterbrechung eines aktiven Dateiservers führt Amazon FSx automatisch und unabhängig ein Failover dieses Hochverfügbarkeitspaars (HA) zum Standby-Dateiserver durch, in der Regel innerhalb weniger Sekunden. Während eines Failovers haben Sie weiterhin ohne manuellen Eingriff Zugriff auf Ihre Daten.

Um eine hohe Verfügbarkeit zu gewährleisten, überwacht Amazon FSx kontinuierlich auf Hardwareausfälle und ersetzt automatisch Infrastrukturkomponenten im Falle eines Ausfalls. Um eine hohe Haltbarkeit zu erreichen, repliziert Amazon FSx Ihre Daten automatisch innerhalb einer Availability Zone, um sie vor Komponentenausfällen zu schützen. Darüber hinaus haben Sie die Möglichkeit, automatische tägliche Backups Ihrer Dateisystemdaten zu konfigurieren. Diese Backups werden in mehreren Availability Zones gespeichert, um Multi-AZ-Ausfallsicherheit für alle Backup-Daten zu gewährleisten.

Single-AZ-Dateisysteme sind für Anwendungsfälle konzipiert, für die das Datenausfallsicherheitsmodell eines Multi-AZ-Dateisystems nicht erforderlich ist. Sie bieten eine kostenoptimierte Lösung für Anwendungsfälle wie Entwicklungs- und Testumgebungen oder das Speichern sekundärer Kopien von Daten, die bereits On-Premises oder in anderen gespeichert sind AWS-Regionen, indem sie Daten nur innerhalb einer einzigen Availability Zone replizieren.

Das folgende Diagramm veranschaulicht die Architektur für ein Single-AZ-Dateisystem von FSx für ONTAP.

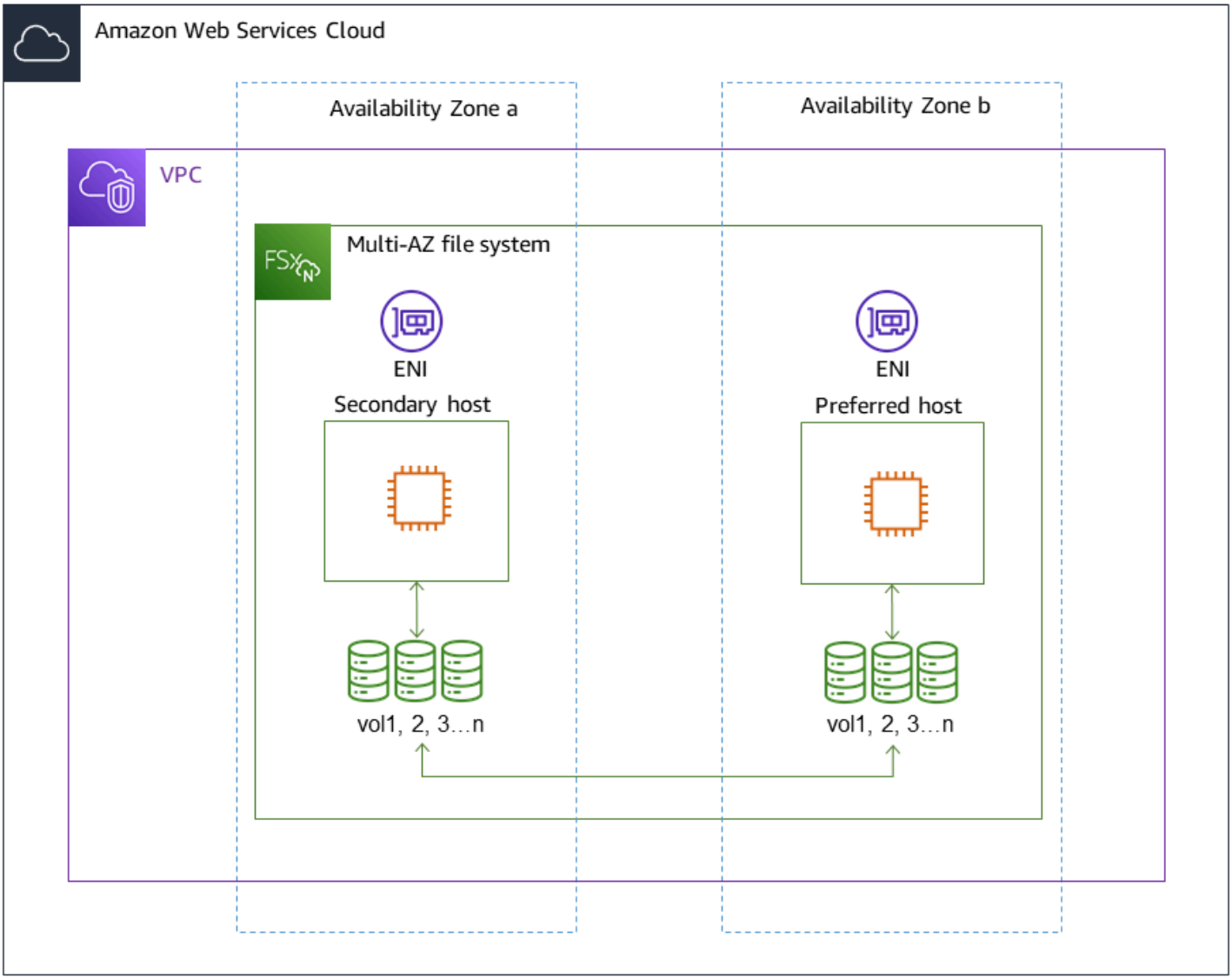


Multi-AZ-Bereitstellungstyp

Multi-AZ-Dateisysteme unterstützen alle Verfügbarkeits- und Haltbarkeitsfunktionen von Single-AZ-Dateisystemen. Darüber hinaus sind sie darauf ausgelegt, Daten kontinuierlich verfügbar zu machen, auch wenn eine Availability Zone nicht verfügbar ist. Multi-AZ-Bereitstellungen verfügen über ein einziges HA-Paar von Dateiservern. Der Standby-Dateiserver wird in einer anderen Availability Zone als der aktive Dateiserver in derselben bereitgestellt AWS-Region. Alle in Ihr Dateisystem geschriebenen Änderungen werden synchron über Availability Zones in den Standby-Modus repliziert.

Multi-AZ-Dateisysteme sind für Anwendungsfälle wie geschäftskritische Produktions-Workloads konzipiert, die eine hohe Verfügbarkeit für gemeinsam genutzte ONTAP-Dateidaten und Speicher

mit integrierter Replikation über Availability Zones hinweg erfordern. Das folgende Diagramm veranschaulicht die Architektur für ein FSx-für-ONTAP-Multi-AZ-Dateisystem.



Failover-Prozess für FSx für ONTAP

Single-AZ- und Multi-AZ-Dateisysteme führen automatisch ein Failover für ein bestimmtes HA-Paar vom bevorzugten oder aktiven Dateiserver zum Standby-Dateiserver durch, wenn eine der folgenden Bedingungen eintritt:

- Der bevorzugte oder aktive Dateiserver ist nicht verfügbar
- Die Durchsatzkapazität des Dateisystems wird geändert
- Der bevorzugte oder aktive Dateiserver wird einer geplanten Wartung unterzogen

- Es kommt zu einem Ausfall der Availability Zone (nur Multi-AZ-Dateisysteme)

> **Note**
>
> Bei Scale-Out-Dateisystemen ist das Failover-Verhalten jedes HA-Paares unabhängig. Wenn der bevorzugte Dateiserver für ein HA-Paar nicht verfügbar ist, führt nur dieses HA-Paar ein Failover auf seinen Standby-Dateiserver durch.

Beim Failover von einem Dateiserver zu einem anderen beginnt der neue aktive Dateiserver automatisch mit der Verarbeitung aller Lese- und Schreibanforderungen des Dateisystems an dieses HA-Paar. Wenn bei Multi-AZ-Dateisystemen der bevorzugte Dateiserver vollständig wiederhergestellt ist und verfügbar wird, schlägt Amazon FSx automatisch zurück, wobei das Failback normalerweise in weniger als 60 Sekunden abgeschlossen wird. Bei Single-AZ- und Multi-AZ-Dateisystemen wird ein Failover in der Regel in weniger als 60 Sekunden abgeschlossen, von der Erkennung des Fehlers auf dem aktiven Dateiserver bis zur Heraufstufung des Standby-Dateiservers in den aktiven Status. Da die Endpunkt-IP-Adresse, die Clients für den Zugriff auf Daten über NFS oder SMB verwenden, gleich bleibt, sind Failovers für Linux-, Windows- und macOS-Anwendungen transparent, die den Dateisystembetrieb ohne manuellen Eingriff fortsetzen.

Informationen dazu, wie Sie sicherstellen, dass Failovers für Clients transparent sind, die mit Ihren Single-AZ- und Multi-AZ-Dateisystemen von FSx für ONTAP verbunden sind, finden Sie unter Zugriff auf Daten aus dem heraus AWS.

Testen des Failovers auf einem Dateisystem

Sie können Failover auf Ihrem Scale-up-Dateisystem testen, indem Sie dessen Durchsatzkapazität ändern. Wenn Sie die Durchsatzkapazität Ihres Dateisystems ändern, schaltet Amazon FSx die Dateiserver des Dateisystems seriell aus. Dateisysteme führen automatisch ein Failover auf den sekundären Server durch, während Amazon FSx zuerst den bevorzugten Dateiserver ersetzt. Nach der Aktualisierung schlägt das Dateisystem automatisch auf den neuen primären Server zurück und Amazon FSx ersetzt den sekundären Dateiserver.

Sie können den Fortschritt der Aktualisierungsanforderung für die Durchsatzkapazität in der Amazon-FSx-Konsole, der CLI und der API überwachen. Weitere Informationen zum Ändern der Durchsatzkapazität Ihres Dateisystems und zur Überwachung des Fortschritts der Anforderung finden Sie unter Verwaltung der Durchsatzkapazität.

Netzwerkressourcen

In diesem Abschnitt werden die Netzwerkressourcen beschrieben, die von Single-AZ- und Multi-AZ-Dateisystemen verbraucht werden.

Subnetze

Wenn Sie ein Single-AZ-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 von Ihnen ausgewählten Subnetze müssen sich in verschiedenen Availability Zones innerhalb derselben befinden AWS-Region. Weitere Informationen zu Amazon VPC finden Sie unter Was ist Amazon VPC? im Amazon Virtual Private Cloud-Benutzerhandbuch.

> **Note**
>
> Unabhängig vom angegebenen Subnetz können Sie von jedem Subnetz innerhalb der VPC des Dateisystems aus auf Ihr Dateisystem zugreifen.

Elastic Network-Schnittstellen für Dateisysteme

Für Single-AZ-Dateisysteme stellt Amazon FSx zwei Elastic Network-Schnittstellen (ENI) in dem Subnetz bereit, das Sie Ihrem Dateisystem zuordnen. Für Multi-AZ-Dateisysteme stellt Amazon FSx auch zwei ENIs bereit, eine in jedem der Subnetze, die Sie Ihrem Dateisystem zuordnen. Clients kommunizieren über die Elastic-Network-Schnittstelle mit Ihrem Amazon-FSx-Dateisystem. Die Netzwerkschnittstellen gelten als im Servicebereich von Amazon FSx , obwohl sie Teil der VPC Ihres Kontos sind. Multi-AZ-Dateisysteme verwenden Floating Internet Protocol (IP)-Adressen, sodass verbundene Clients während eines Failover-Ereignisses nahtlos zwischen den bevorzugten und Standby-Dateiservern wechseln können.

> **Warning**
>
> - Sie dürfen die Ihrem Dateisystem zugeordneten 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.

- Bei den Elastic Network-Schnittstellen, die Ihrem Dateisystem zugeordnet sind, werden Routen automatisch erstellt und zu Ihren Standard-VPC- und Subnetz-Routing-Tabellen hinzugefügt. Das Ändern oder Löschen dieser Routen kann zu einem vorübergehenden oder dauerhaften Verlust der Konnektivität für Ihre Dateisystem-Clients führen.

In der folgenden Tabelle sind die Subnetz-, Elastic-Network-Schnittstellen- und IP-Adressressourcen für die einzelnen Bereitstellungstypen des FSx-für-ONTAP-Dateisystems zusammengefasst:

	Single-AZ (hochskalieren)	Single-AZ (Skalierung)	Multi-AZ (hochskalieren)
Anzahl der Subnetze	1	1	2
Anzahl der Elastic Network-Schnittstellen	2	2 pro HA-Paar	2
Anzahl der IP-Adressen pro ENI	1 + die Anzahl der SVMs im Dateisystem	Anzahl der HA-Paare + Anzahl der HA-Paare multipliziert mit der Anzahl der SVMs im Dateisystem	1 + die Anzahl der SVMs im Dateisystem
Anzahl der Routen der VPC-Routing-Tabelle	N/A	N/A	1 + die Anzahl der SVMs im Dateisystem

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

Important

Amazon FSx unterstützt nicht den Zugriff auf Dateisysteme aus dem öffentlichen Internet oder die Offenlegung von Dateisystemen im öffentlichen Internet. Amazon FSx trennt automatisch jede Elastic IP-Adresse, bei der es sich um eine öffentliche IP-Adresse handelt, die vom Internet erreichbar ist, die an die Elastic Network-Schnittstelle eines Dateisystems angehängt wird.

Verwaltung der Speicherkapazität

Amazon FSx for NetApp ONTAP bietet eine Reihe von speicherbezogenen Funktionen, mit denen Sie die Speicherkapazität in Ihrem Dateisystem verwalten können.

Themen

- FSx für ONTAP Speicherstufen
- Auswahl der richtigen Menge an SSD-Speicher für das Dateisystem
- Speicherkapazität und IOPS des Dateisystems
- Speicherkapazität des Volumens

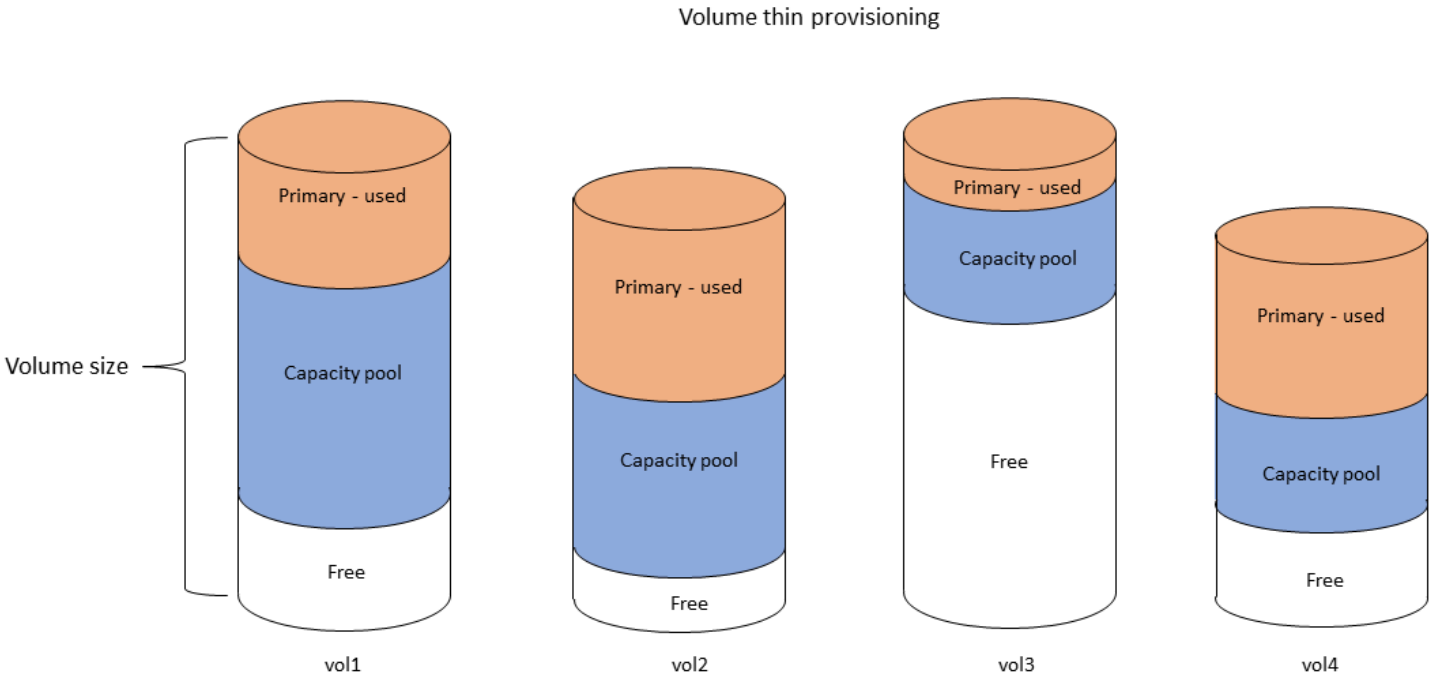
FSx für ONTAP Speicherstufen

Speicherstufen sind die physischen Speichermedien für ein Amazon FSx for NetApp ONTAP-Dateisystem. FSx for ONTAP bietet die folgenden Speicherstufen:

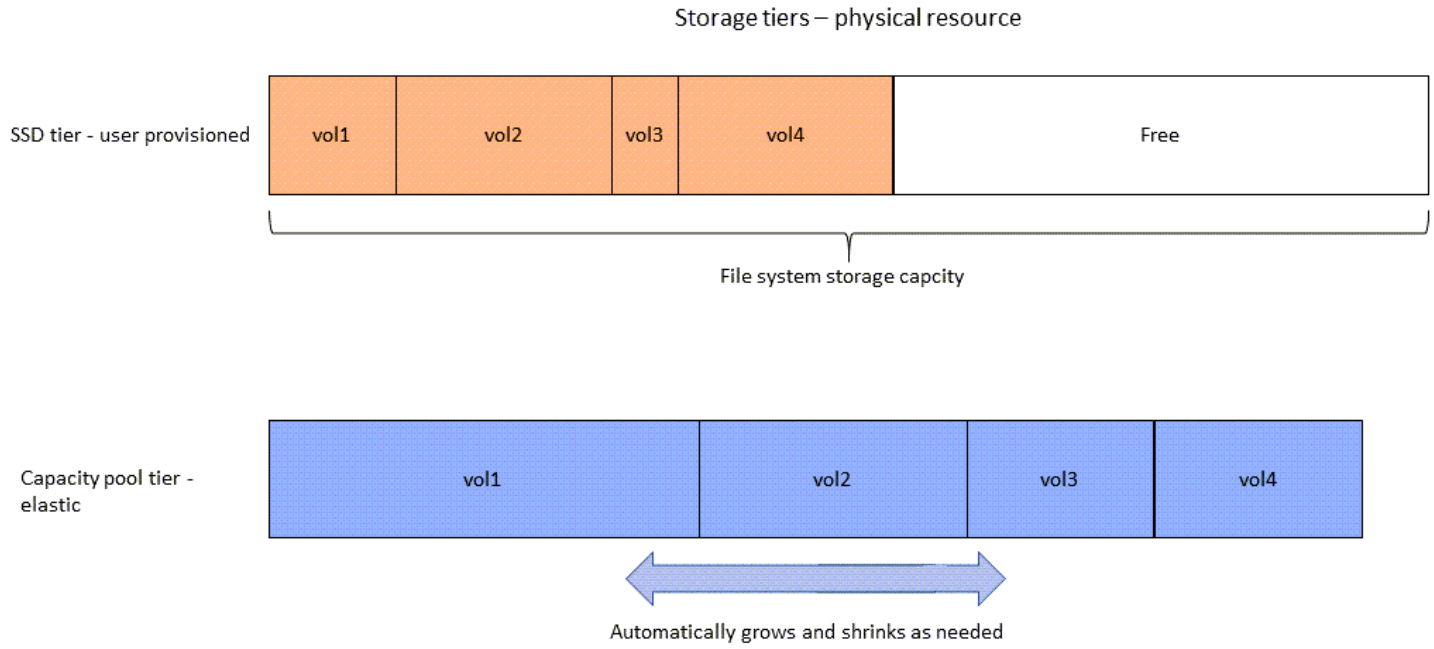
- SSD-Stufe — Der vom Benutzer bereitgestellte, leistungsstarke Solid-State-Drive-Speicher (SSD), der speziell für den aktiven Teil Ihres Datensatzes entwickelt wurde.
- Kapazitätspool-Tier — Vollständig elastischer Speicher, der automatisch auf Petabyte skaliert wird und kostenoptimiert für Ihre Daten ist, auf die Sie selten zugreifen.

Ein FSx for ONTAP-Volume ist eine virtuelle Ressource, die, ähnlich wie Ordner, keine Speicherkapazität verbraucht. Die Daten, die Sie speichern — und die physischen Speicherplatz beanspruchen — befinden sich in Volumes. Wenn Sie ein Volume erstellen, geben Sie dessen Größe an, die Sie nach der Erstellung ändern können. FSx for ONTAP-Volumes sind Thin Provisioning, und der Dateisystemspeicher wird nicht im Voraus reserviert. Stattdessen werden SSD- und Kapazitätspoolspeicher nach Bedarf dynamisch zugewiesen. Eine Tiering-Richtlinie, die Sie auf Volume-Ebene konfigurieren, bestimmt, ob und wann Daten, die auf der SSD-Stufe gespeichert sind, in die Kapazitätspoolebene übergehen.

Das folgende Diagramm zeigt ein Beispiel für Daten, die auf mehreren FSx for ONTAP-Volumes in einem Dateisystem angeordnet sind.



Das folgende Diagramm zeigt, wie die physische Speicherkapazität des Dateisystems durch die Daten in den vier Volumes im vorherigen Diagramm verbraucht wird.



Sie können Ihre Speicherkosten senken, indem Sie die Tiering-Richtlinie wählen, die den Anforderungen für jedes Volume in Ihrem Dateisystem am besten entspricht. Weitere Informationen finden Sie unter Tiering von Volumendaten.

Auswahl der richtigen Menge an SSD-Speicher für das Dateisystem

Bei der Auswahl der SSD-Speicherkapazität für Ihr FSx for ONTAP-Dateisystem müssen Sie die folgenden Punkte berücksichtigen, die sich auf die Menge des für die Speicherung Ihrer Daten verfügbaren SSD-Speichers auswirken:

- Speicherkapazität, die für den Overhead der NetApp ONTAP-Software reserviert ist.
- Datei-Metadaten
- Kürzlich geschriebene Daten
- Dateien, die Sie auf SSD-Speicher speichern möchten, unabhängig davon, ob es sich um Daten handelt, deren Kühlzeit noch nicht erreicht wurde, oder um Daten, die Sie kürzlich gelesen haben und die wieder auf die SSD abgerufen wurden.

Wie wird SSD-Speicher verwendet

Der SSD-Speicher Ihres Dateisystems wird für eine Kombination aus NetApp ONTAP-Software (Overhead), Dateimetadaten und Ihren Daten verwendet.

NetApp Mehraufwand für die ONTAP-Software

Wie bei anderen NetApp ONTAP-Dateisystemen sind bis zu 16% der SSD-Speicherkapazität eines Dateisystems für ONTAP-Overhead reserviert, was bedeutet, dass sie nicht zum Speichern Ihrer Dateien verfügbar sind. Der ONTAP-Overhead wird wie folgt zugewiesen:

- 11% sind für NetApp ONTAP-Software reserviert. Für Dateisysteme mit über 30 Tebibyte (TiB) SSD-Speicherkapazität sind 6% reserviert.
- 5% sind für aggregierte Snapshots reserviert, die zur Synchronisation von Daten zwischen den beiden Dateiservern eines Dateisystems erforderlich sind.

Datei-Metadaten

Dateimetadaten belegen in der Regel 3-7% der Speicherkapazität, die von den Dateien belegt wird. Dieser Prozentsatz hängt von der durchschnittlichen Dateigröße (eine geringere durchschnittliche Dateigröße erfordert mehr Metadaten) und der Höhe der Einsparungen bei der Speichereffizienz Ihrer Dateien ab. Beachten Sie, dass Dateimetadaten nicht von Einsparungen bei der Speichereffizienz

profitieren. Sie können die folgenden Richtlinien verwenden, um abzuschätzen, wie viel SSD-Speicher für Metadaten in Ihrem Dateisystem verwendet wird.

Durchschnittliche Dateigröße	Größe der Metadaten als Prozentsatz der Dateidaten
4 KB	7%
8 KB	3,5%
32 KB oder mehr	1-3%

Bei der Bemessung der SSD-Speicherkapazität, die Sie für die Metadaten von Dateien benötigen, die Sie auf der Kapazitätspoolebene speichern möchten, empfehlen wir, ein konservatives Verhältnis von 1 GiB SSD-Speicher pro 10 GiB an Daten zu verwenden, die Sie auf der Kapazitätspoolebene speichern möchten.

Dateidaten, die auf Ihrer SSD-Stufe gespeichert sind

Zusätzlich zu Ihrem aktiven Datensatz und allen Dateimetadaten werden alle in Ihr Dateisystem geschriebenen Daten zunächst auf die SSD-Ebene geschrieben, bevor sie auf den Kapazitätspoolspeicher abgestuft werden. Dies gilt unabhängig von der Tiering-Richtlinie des Volumes, mit Ausnahme der Übertragung von Daten auf ein Volume, für das SnapMirror die Tiering-Richtlinie „Alle Daten“ konfiguriert wurde.

Zufällige Lesevorgänge aus der Kapazitätspoolebene werden in der SSD-Stufe zwischengespeichert, sofern die SSD-Stufe zu weniger als 90% ausgelastet ist. Weitere Informationen finden Sie unter Tiering von Volumendaten.

Empfohlene SSD-Kapazitätsauslastung

Wir empfehlen, dass Sie Ihre SSD-Speicherebene nicht kontinuierlich zu mehr als 80% nutzen. Bei Dateisystemen mit horizontaler Skalierung empfehlen wir außerdem, die Gesamtauslastung der Aggregate Ihres Dateisystems nicht kontinuierlich zu überschreiten. Diese Empfehlungen entsprechen der Empfehlung für NetApp ONTAP. Da die SSD-Stufe Ihres Dateisystems auch für das Staging von Schreibvorgängen und für zufällige Lesevorgänge auf der Ebene des Kapazitätspools verwendet wird, können plötzliche Änderungen der Zugriffsmuster schnell zu einer erhöhten Auslastung Ihrer SSD-Stufe führen.

Bei einer SSD-Auslastung von 90% werden die aus der Kapazitätspoolebene gelesenen Daten nicht mehr auf der SSD-Ebene zwischengespeichert, sodass die verbleibende SSD-Kapazität für alle neuen Daten, die in das Dateisystem geschrieben werden, erhalten bleibt. Dies führt dazu, dass wiederholte Lesevorgänge derselben Daten aus der Kapazitätspoolebene aus dem Kapazitätspoolspeicher gelesen werden, anstatt zwischengespeichert und aus der SSD-Ebene gelesen zu werden, was sich auf die Durchsatzkapazität Ihres Dateisystems auswirken kann.

Alle Tiering-Funktionen werden beendet, wenn die SSD-Stufe zu 98% oder mehr ausgelastet ist. Weitere Informationen finden Sie unter Schwellenwerte für die Staffelung.

FSx für ONTAP-Speichereffizienz

NetApp ONTAP bietet Funktionen zur Speichereffizienz auf Blockebene, darunter Komprimierung, Komprimierung und Deduplizierung, mit denen Sie bis zu 65% an Speicherkapazität für allgemeine Dateifreigaben sparen können, ohne die Leistung zu beeinträchtigen.

Amazon FSx for NetApp ONTAP unterstützt auch andere ONTAP-Funktionen, mit denen Sie Speicherplatz sparen, darunter Snapshots, Thin Provisioning und Volumes. FlexClone

Funktionen zur Speichereffizienz sind standardmäßig nicht aktiviert. Sie können sie wie folgt aktivieren:

- Auf dem Root-Volume einer SVM, wenn Sie ein Dateisystem erstellen.
- Wenn Sie ein neues Volume erstellen.
- Wenn Sie ein vorhandenes Volume ändern.

Informationen zum Umfang der Speichereinsparungen in einem Dateisystem mit aktivierter Speichereffizienz finden Sie unterEinsparungen bei der Speichereffizienz anzeigen.

Berechnung der Einsparungen bei der Speichereffizienz

Sie können die CloudWatch Dateisystemmetriken `LogicalDataStored` und `StorageUsed` FSx for ONTAP verwenden, um Speichereinsparungen durch Komprimierung, Deduplizierung, Komprimierung, Snapshots und zu berechnen. FlexClones Diese Metriken haben eine einzige Dimension,. `FileSystemId` Weitere Informationen finden Sie unter Dateisystemmetriken.

- Um die Einsparungen bei der Speichereffizienz in Byte zu berechnen, nehmen Sie den Durchschnitt von `StorageUsed` über einen bestimmten Zeitraum und subtrahieren Sie ihn vom Durchschnitt für denselben `LogicalDataStored` Zeitraum.

- Um die Einsparungen bei der Speichereffizienz als Prozentsatz der gesamten logischen Datengröße zu berechnen, nehmen Sie den Wert `Average` von `StorageUsed` über einen bestimmten Zeitraum und subtrahieren ihn vom Wert von von im `Average` gleichen Zeitraum. `LogicalDataStored` Dann dividieren Sie die Differenz durch den Wert `Average` von `LogicalDataStored` im gleichen Zeitraum.

Beispiel für die SSD-Größe

Angenommen, Sie möchten 100 TiB an Daten für eine Anwendung speichern, bei der auf 80% der Daten selten zugegriffen wird. In diesem Szenario werden 80% (80 TB) Ihrer Daten automatisch auf die Ebene des Kapazitätspools aufgeteilt, und die restlichen 20% (20 TB) verbleiben im SSD-Speicher. Basierend auf den typischen Einsparungen bei der Speichereffizienz von 65% für allgemeine Filesharing-Workloads entspricht das einer Datenmenge von 7 TiB. Um eine SSD-Nutzungsrate von 80% aufrechtzuerhalten, benötigen Sie 8,75 TiB SSD-Speicherkapazität für die 20 TiB an aktiv abgerufenen Daten. Die Menge an SSD-Speicher, die Sie bereitstellen, muss auch den Speicheraufwand der ONTAP-Software in Höhe von 16% berücksichtigen, wie aus der folgenden Berechnung hervorgeht.

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

In diesem Beispiel müssen Sie also mindestens 10,42 TiB SSD-Speicher bereitstellen. Sie verwenden außerdem 28 TiB Kapazitätspoolspeicher für die verbleibenden 80 TiB an selten abgerufenen Daten.

Speicherkapazität und IOPS des Dateisystems

Wenn Sie ein FSx for ONTAP-Dateisystem erstellen, geben Sie die Speicherkapazität der SSD-Stufe an. Bei Dateisystemen mit horizontaler Skalierung wird die von Ihnen angegebene Speicherkapazität gleichmäßig auf die Speicherpools der einzelnen Hochverfügbarkeitspaare (HA) verteilt. Diese Speicherpools werden als Aggregate bezeichnet.

Für jedes GiB SSD-Speicher, den Sie bereitstellen, stellt Amazon FSx automatisch 3 SSD-Eingabe-/Ausgabeoperationen pro Sekunde (IOPS) für das Dateisystem bereit, bis zu einem Maximum von 160.000 SSD-IOPS pro Dateisystem. Bei Scale-Out-Dateisystemen werden Ihre SSD-IOPS gleichmäßig auf alle Aggregate Ihres Dateisystems verteilt. Sie haben die Möglichkeit, einen Wert

für bereitgestellte SSD-IOPS anzugeben, der über den automatischen 3 SSD-IOPS pro GiB liegt. Weitere Informationen zur maximalen Anzahl von SSD-IOPS, die Sie für Ihr FSx for ONTAP-Dateisystem bereitstellen können, finden Sie unter. Auswirkungen der Durchsatzkapazität auf die Leistung

Themen

- Aktualisierung des Dateisystems, des SSD-Speichers und der IOPS
- Überwachung der SSD-Speichernutzung
- Einen Alarm für die Speichernutzung einrichten
- Einsparungen bei der Speichereffizienz anzeigen
- Änderung der SSD-Speicherkapazität und der bereitgestellten IOPS
- Überwachung der Speicherkapazität und der IOPS-Updates
- Dynamisches Erhöhen der SSD-Speicherkapazität

Aktualisierung des Dateisystems, des SSD-Speichers und der IOPS

Wenn Sie zusätzlichen Speicherplatz für den aktiven Teil Ihres Datensatzes benötigen, können Sie die SSD-Speicherkapazität Ihres Amazon FSx for NetApp ONTAP-Dateisystems erhöhen. Verwenden Sie die Amazon FSx-Konsole, die Amazon FSx-API oder AWS Command Line Interface (AWS CLI), um die SSD-Speicherkapazität zu erhöhen. Weitere Informationen finden Sie unter Änderung der SSD-Speicherkapazität und der bereitgestellten IOPS.

Wenn Sie die SSD-Speicherkapazität Ihres Amazon FSx-Dateisystems erhöhen, ist die neue Kapazität in der Regel innerhalb weniger Minuten einsatzbereit. Die neue SSD-Speicherkapazität wird Ihnen in Rechnung gestellt, sobald sie Ihnen zur Verfügung steht. Weitere Informationen zur Preisgestaltung finden Sie unter Amazon FSx for NetApp ONTAP Pricing.

Nachdem Sie Ihre Speicherkapazität erhöht haben, führt Amazon FSx im Hintergrund einen Speicheroptimierungsprozess durch, um Ihre Daten neu auszubalancieren. Bei den meisten Dateisystemen dauert die Speicheroptimierung einige Stunden, ohne dass sich dies merklich auf Ihre Workload-Leistung auswirkt.

Sie können den Fortschritt des Speicheroptimierungsprozesses jederzeit mithilfe der Amazon FSx-Konsole, CLI und API verfolgen. Weitere Informationen finden Sie unter Überwachung der Speicherkapazität und der IOPS-Updates.

Überlegungen

Hier sind einige wichtige Punkte, die Sie bei der Änderung der SSD-Speicherkapazität und der bereitgestellten IOPS eines Dateisystems berücksichtigen sollten:

- Nur Erhöhung der Speicherkapazität — Sie können nur die Menge der SSD-Speicherkapazität für ein Dateisystem erhöhen; Sie können die Speicherkapazität nicht verringern.
- Minimale Erhöhung der Speicherkapazität — Jede Erhöhung der SSD-Speicherkapazität muss mindestens 10 Prozent der aktuellen SSD-Speicherkapazität des Dateisystems bis zur maximalen SSD-Speicherkapazität für die Konfiguration Ihres Dateisystems betragen.
- (Nur Scale-out) Verteilung der Speicherkapazität — Die neue Speicherkapazität oder SSD-IOPS, die Sie für Ihr Dateisystem auswählen, wird gleichmäßig auf alle Aggregate Ihres Dateisystems verteilt.
- Zeit zwischen Erhöhungen — Nachdem Sie die SSD-Speicherkapazität, die bereitgestellten IOPS oder die Durchsatzkapazität in einem Dateisystem geändert haben, müssen Sie mindestens sechs Stunden warten, bevor Sie eine dieser Konfigurationen auf demselben Dateisystem erneut ändern können. Dies wird manchmal auch als Ruhephase bezeichnet.
- Bereitgestellte IOPS-Modi — Für eine Änderung bereitgestellter IOPS müssen Sie einen der beiden IOPS-Modi angeben:
  - Automatischer Modus — Amazon FSx skaliert Ihre SSD-IOPS automatisch, um 3 bereitgestellte SSD-IOPS pro GiB SSD-Speicherkapazität aufrechtzuerhalten, bis zu der maximalen SSD-IOPS für Ihre Dateisystemkonfiguration.

    > **Note**
    >
    > Weitere Informationen zur maximalen Anzahl von SSD-IOPS, die Sie für Ihr FSx for ONTAP-Dateisystem bereitstellen können, finden Sie unter. Auswirkungen der Durchsatzkapazität auf die Leistung

  - Benutzerbereitgestellter Modus — Sie geben die Anzahl der SSD-IOPS an, die größer oder gleich 3 IOPS pro GiB SSD-Speicherkapazität sein muss. Wenn Sie sich für die Bereitstellung eines höheren IOPS-Levels entscheiden, zahlen Sie für die durchschnittlich bereitgestellten IOPS-Werte, die über Ihrem inbegriffenen Tarif für den Monat liegen, gemessen in IOPS-Monaten.

Weitere Informationen zur Preisgestaltung finden Sie unter Amazon FSx for NetApp ONTAP Pricing.

Wann sollte die SSD-Speicherkapazität erhöht werden

Wenn Ihnen der verfügbare SSD-Speicher ausgeht, empfehlen wir Ihnen, die Speicherkapazität Ihres Dateisystems zu erhöhen. Wenn der Speicherplatz knapp wird, deutet dies darauf hin, dass Ihre SSD-Stufe für den aktiven Teil Ihres Datensatzes zu klein ist.

Verwenden Sie die Metriken auf Dateisystemebene `StorageCapacity` und `StorageUsed` Amazon CloudWatch , um die Menge an freiem Speicherplatz zu überwachen, der auf dem Dateisystem verfügbar ist. Sie können einen CloudWatch Alarm für eine Metrik erstellen und sich benachrichtigen lassen, wenn sie einen bestimmten Schwellenwert unterschreitet. Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch.

> **Note**
>
> Wir empfehlen, die SSD-Speicherkapazität nicht über 80% zu nutzen, um sicherzustellen, dass Datenklassifizierung, Durchsatzskalierung und andere Wartungsaktivitäten ordnungsgemäß funktionieren und dass Kapazität für zusätzliche Daten verfügbar ist. Bei Dateisystemen mit horizontaler Skalierung gilt diese Empfehlung sowohl für die durchschnittliche Auslastung aller Aggregate Ihres Dateisystems als auch für jedes einzelne Aggregat.

Weitere Informationen darüber, wie der SSD-Speicher eines Dateisystems verwendet wird und wie viel SSD-Speicher für Dateimetadaten und Betriebssoftware reserviert ist, finden Sie unter. Auswahl der richtigen Menge an SSD-Speicher für das Dateisystem

Überwachung der SSD-Speichernutzung

Sie können die SSD-Speicherkapazitätsauslastung Ihres Dateisystems mithilfe einer Vielzahl von AWS NetApp Tools überwachen. Mit Amazon können CloudWatch Sie die Speicherkapazitätsauslastung überwachen und Alarme einrichten, die Sie benachrichtigen, wenn die Speicherkapazitätsauslastung einen anpassbaren Schwellenwert erreicht.

> **Note**
>
> Wir empfehlen, dass Sie die Speicherkapazitätsauslastung Ihrer SSD-Speicherstufe nicht über 80% überschreiten. Dadurch wird sichergestellt, dass das Tiering ordnungsgemäß funktioniert, und es entsteht Mehraufwand für neue Daten. Wenn Ihre SSD-Speicherstufe

konstant über 80% der Speicherkapazität ausgelastet ist, können Sie die Kapazität Ihrer SSD-Speicherstufe erhöhen. Weitere Informationen finden Sie unter Aktualisierung des Dateisystems, des SSD-Speichers und der IOPS.

Sie können den verfügbaren SSD-Speicher eines Dateisystems und die gesamte Speicherverteilung in der Amazon FSx-Konsole einsehen. Das Diagramm Verfügbare SSD-Speicherkapazität zeigt die Menge der verfügbaren SSD-basierten Speicherkapazität in einem Dateisystem im Zeitverlauf. Das Diagramm zur Speicherverteilung zeigt, wie die Gesamtspeicherkapazität eines Dateisystems derzeit auf drei Kategorien verteilt ist:

- Ebene des Kapazitätspools
- SSD-Stufe — verfügbar
- SSD-Stufe — verwendet

Sie können die SSD-Speicherkapazitätsauslastung Ihres Dateisystems in der überwachen AWS Management Console, indem Sie das folgende Verfahren verwenden.

Zur Überwachung der verfügbaren SSD-Speicherkapazität im Dateisystem (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie in der linken Navigationsspalte Dateisysteme und dann das ONTAP Dateisystem aus, für das Sie Informationen zur Speicherkapazität anzeigen möchten. Die Detailseite des Dateisystems wird angezeigt.
3. Wählen Sie im zweiten Bereich die Registerkarte Überwachung und Leistung und dann Speicher. Die Diagramme Verfügbare Primärspeicherkapazität und Speicherkapazitätsauslastung pro Aggregat werden angezeigt.

Einen Alarm für die Speichernutzung einrichten

Wir empfehlen, eine durchschnittliche SSD-Speicherkapazitätsauslastung von 80% kontinuierlich nicht zu überschreiten. Gelegentliche SSD-Speichernutzungsspitzen von über 80% sind akzeptabel. Wenn Sie eine durchschnittliche Auslastung von unter 80% beibehalten, steht Ihnen genügend Kapazität zur Verfügung, um Ihren Speicherplatz ohne Probleme zu erweitern. Das folgende Verfahren zeigt, wie Sie einen CloudWatch Alarm erstellen, der Sie darauf hinweist, wenn sich die SSD-Speicherauslastung Ihres Dateisystems 80% nähert.

Um einen CloudWatch Alarm für die Nutzung des primären Speichers zu erstellen

Verwenden Sie die Metrik, um die durchschnittliche SSD-Speicherkapazitätsauslastung zu berechnen. `StorageUsed` Dividieren Sie durch das Maximum StorageCapacity für denselben Zeitraum, wobei die StorageTier Dimension SSD entspricht.

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich Dateisysteme und dann das Dateisystem aus, für das Sie den Alarm erstellen möchten.
3. Wählen Sie auf der Übersichtsseite die Option Überwachung aus.
4. Wählen Sie „ CloudWatch Alarm erstellen“. Sie werden in der CloudWatch Konsole zur Seite „Alarme“ **>** „Alarm erstellen“ **>** „Metrik und Bedingungen angeben“ weitergeleitet.
5. Wählen Sie Select metric (Metrik auswählen) aus.
6. Wählen Sie im Abschnitt Metrics die Option FSx aus.
7. Wählen Sie die Metrikkategorie „Detaillierte Dateisystem-Metriken“.
8. Um nur die Messwerte anzuzeigen, die für das Dateisystem verfügbar sind, für das Sie den Alarm erstellen, geben Sie die ID des Dateisystems in das Suchfeld ein.
9. Wählen Sie für das Dateisystem, für das Sie den Alarm einstellen möchten, die folgenden Metriken aus:

Metrikname	StorageTier	DataType
StorageUsed	SSD	Alle
StorageCapacity	SSD	Alle

10. Wählen Sie die Registerkarte Graphed metrics (Grafisch dargestellte Metriken) aus. Führen Sie für alle Metriken, die Sie zuvor hinzugefügt haben, die folgenden Aktionen durch:
    - Setzen Sie den Wert in der Statistikspalte für jede Metrik auf Durchschnitt.
    - Stellen Sie den Wert für den Zeitraum auf einen der vordefinierten Bewertungszeiträume ein.
11. Wählen Sie das Dropdown-Menü Add math (Berechnung hinzufügen) und dann in der Liste der vordefinierten Metrikberechnungs-Ausdrücke die Option Start with an empty expression (Mit leerem Ausdruck beginnen) aus.

Nachdem Sie Start with an empty expression (Mit einem leeren Ausdruck beginnen) ausgewählt haben, erscheint ein Feld für mathematische Ausdrücke, in dem Sie mathematische Ausdrücke anwenden oder bearbeiten können.

12. Geben Sie im Feld Mathematischen Ausdruck bearbeiten den Ausdruck für die Division der `StorageUsed` Metrik durch die `StorageCapacity` Metrik wie folgt ein:

    - Geben Sie die Bezeichnung für die `StorageUsed` Metrik ein, zum Beispiel m1.
    - Geben Sie den Schrägstrich/für die Divisionsoperation ein.
    - Geben Sie die Bezeichnung für die `StorageCapacity` Metrik ein.

    Wählen Sie Apply (Anwenden) aus.

13. Deaktivieren Sie die Kontrollkästchen links neben den Metriken auf der Seite. Nur das Kontrollkästchen neben dem Ausdruck, der für den Alarm verwendet werden soll, sollte aktiviert sein. Der Ausdruck, den Sie für den Alarm wählen, muss eine einzige Zeitreihe ergeben und nur eine Zeile im Diagramm anzeigen. Wählen Sie dann Select Metric (Metrik auswählen) aus.

    Die Seite Specify metric and conditions (Metrik und Bedingungen festlegen) wird angezeigt, die ein Diagramm und andere Informationen über den von Ihnen ausgewählten mathematischen Ausdruck anzeigt.

14. Geben Sie für Whenever *`expression`* is an, dass der Ausdruck größer, kleiner oder gleich dem Schwellenwert sein muss. Geben Sie unter than... (dann ...) den Schwellenwert an.

    Um einen Alarm auszulösen, der Sie benachrichtigt, wenn sich die SSD-Speicherkapazität dem Schwellenwert von 80% nähert, legen Sie die Einstellung Immer dann fest, wenn der ***`Ausdruck`*** dem Schwellenwert entspricht, und geben Sie einen Schwellenwert von 80% an.

15. Wählen Sie Additional configuration (Zusätzliche Konfiguration). Geben Sie unter Datapoints to alarm (Datenpunkte für Alarm) an, wie viele Auswertungszeiträume (Datenpunkte) im Status `ALARM` sein müssen, damit der Alarm ausgelöst wird. Wenn die beiden Werte hier übereinstimmen, erstellen Sie einen Alarm, der in den Status `ALARM` wechselt, wenn entsprechend viele aufeinanderfolgende Zeiträume überschritten werden.

    Um einen M aus N Alarm zu erstellen, geben Sie eine niedrigere Zahl für den ersten Wert als für den zweiten Wert an. Weitere Informationen finden Sie unter Auswertung eines Alarms im CloudWatch Amazon-Benutzerhandbuch.

16. Wählen Sie für Missing data treatment (Behandlung von fehlenden Daten) aus, wie sich der Alarm verhalten soll, wenn einige Datenpunkte fehlen. Um unnötige und irreführende Änderungen der Alarmbedingungen zu verhindern und Ihre Alarme so zu konfigurieren, dass sie gegen fehlende Datenpunkte resistent sind, finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Konfiguration der Behandlung fehlender Daten durch CloudWatch Alarme.

    > **Note**
    >
    > Metriken dürfen während der Wartung des Dateisystems nicht veröffentlicht werden.

17. Wählen Sie Weiter aus.
18. Wählen Sie unter Benachrichtigung ein SNS-Thema aus, das benachrichtigt werden soll, wenn sich der Alarm im `ALARM` Status State, `OK` State oder `INSUFFICIENT` _DATA befindet.

    Wenn Sie die Option Create topic (Thema erstellen) 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.

    Um zu erreichen, dass der Alarm mehrere Benachrichtigungen für den gleichen Alarmstatus oder für verschiedene Statuswerte sendet, wählen Sie Benachrichtigung hinzufügen.

    Damit der Alarm keine Benachrichtigungen sendet, wählen Sie Remove (Entfernen).

    Wenn Sie Ihnen eine E-Mail oder eine Amazon SNS SNS-Benachrichtigung senden möchten CloudWatch , wenn der Alarmstatus die Aktion auslöst, wählen Sie einen Alarmstatus für Wann immer dieser Alarmstatus ist.

19. Wenn Sie fertig sind, wählen Sie Weiter.

20. Geben Sie einen Namen und eine Beschreibung für den Alarm ein. Der Name darf nur ASCII-Zeichen enthalten. Wählen Sie anschließend Weiter.
21. Überprüfen Sie auf der Seite Vorschau und Erstellung den Alarm, den Sie gerade erstellen möchten, und wählen Sie dann Alarm erstellen.

Einsparungen bei der Speichereffizienz anzeigen

Wenn diese Option aktiviert ist, können Sie in der Amazon FSx-Konsole, der Amazon-Konsole und der ONTAP CLI sehen, wie viel Speicherkapazität Sie sparen. CloudWatch

Um die Einsparungen bei der Speichereffizienz zu sehen (Konsole)

Die Einsparungen bei der Speichereffizienz, die in der Amazon FSx-Konsole für ein FSx for ONTAP-Dateisystem angezeigt werden, beinhalten die Einsparungen von und. FlexClones SnapShots

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie aus der Liste der Dateisysteme das Dateisystem FSx for ONTAP aus, für das Sie die Speichereffizienz beim Speichern anzeigen möchten.
3. Wählen Sie im zweiten Bereich der Seite mit den Dateisystemdetails auf der Registerkarte Überwachung und Leistung die Option Zusammenfassung aus.
4. Die Tabelle mit den Einsparungen bei der Speichereffizienz zeigt, wie viel Speicherplatz Sie als Prozentsatz Ihrer logischen Datengröße und in physischen Byte sparen.

So zeigen Sie Einsparungen bei der Speichereffizienz (ONTAPCLI) an

Sie können allein durch Komprimierung, Komprimierung und Deduplizierung Einsparungen bei der Speichereffizienz erzielen — ohne die Auswirkungen von Snapshots und FlexClones —, indem Sie den `storage aggregate show-efficiency` Befehl über die CLI ausführen. ONTAP Weitere Informationen finden Sie im Documentation Center unter Storage Aggregate Show-Efficiency. NetApp ONTAP

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Der storage aggregate show-efficiency Befehl zeigt Informationen zur Speichereffizienz aller Aggregate an. Die Speichereffizienz wird auf vier verschiedenen Ebenen angezeigt:

   - Gesamt
   - Aggregate
   - Volume
   - Snapshot und FlexClone Volume

```
::*> aggr show-efficiency

Aggregate: aggr1
     Node: node1

Total Data Reduction Efficiency Ratio:  3.29:1
Total Storage Efficiency Ratio:         4.29:1
Aggregate: aggr2
     Node: node1

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

cluster::*> aggr show-efficiency -details

Aggregate: aggr1
     Node: node1

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

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

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

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

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

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

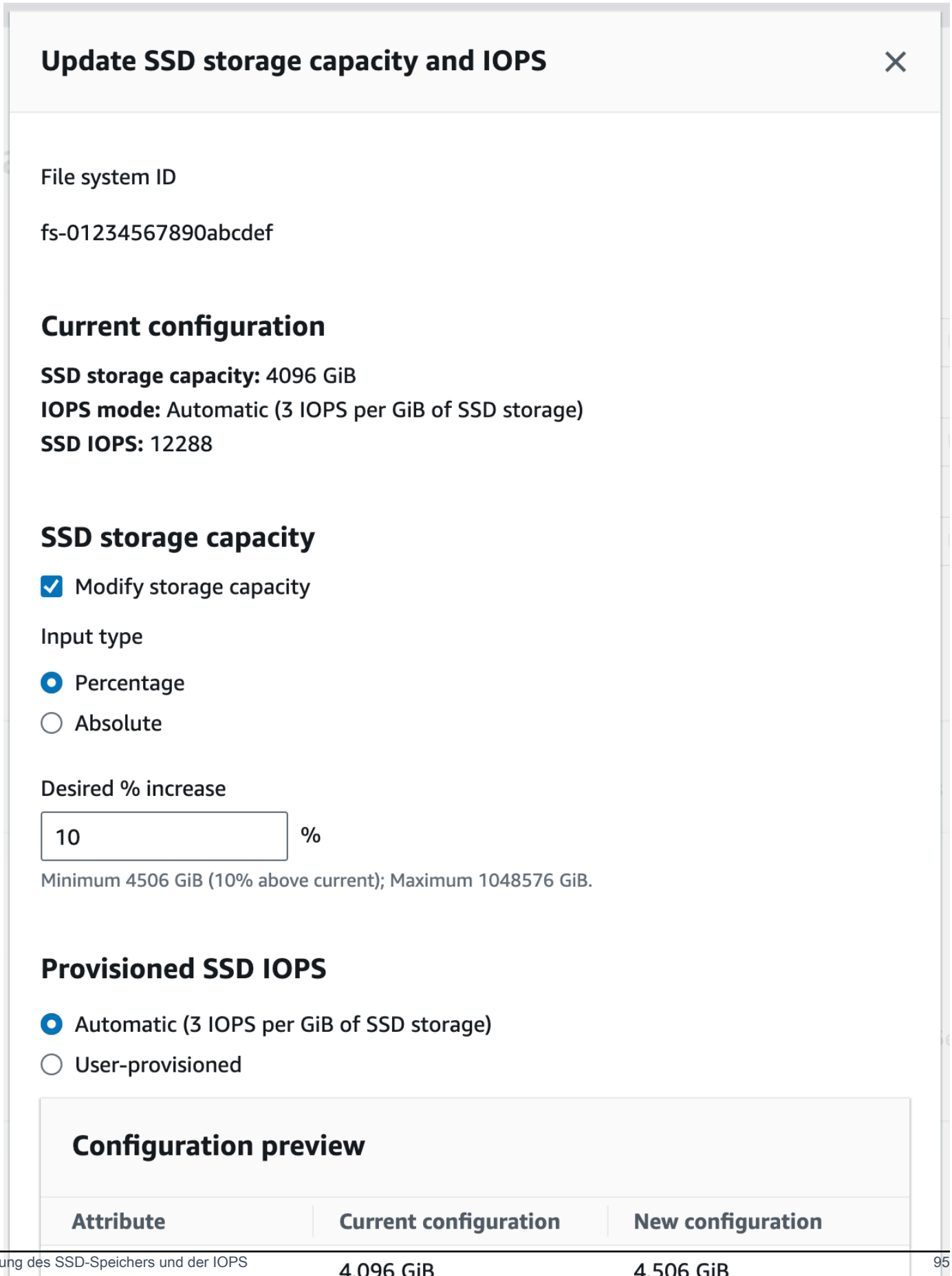
Änderung der SSD-Speicherkapazität und der bereitgestellten IOPS

Sie können den SSD-basierten Speicher eines Dateisystems erhöhen und die Anzahl der bereitgestellten SSD-IOPS erhöhen oder verringern, indem Sie die Amazon FSx-Konsole, die und die AWS CLI API verwenden.

Um die SSD-Speicherkapazität oder die bereitgestellten IOPS für ein Dateisystem (Konsole) zu aktualisieren

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich die Option Dateisysteme aus. Wählen Sie in der Liste Dateisysteme das FSx for ONTAP-Dateisystem aus, für das Sie die SSD-Speicherkapazität und SSD-IOPS aktualisieren möchten.
3. Wählen Sie „Aktionen“ > „Speicherkapazität aktualisieren“. Oder wählen Sie im Abschnitt Zusammenfassung neben dem Wert für die SSD-Speicherkapazität des Dateisystems die Option Aktualisieren aus.

   Das Dialogfeld „SSD-Speicherkapazität und IOPS aktualisieren“ wird angezeigt.


Update SSD storage capacity and IOPS
File system ID
fs-01234567890abcdef
Current configuration
SSD storage capacity: 4096 GiB
IOPS mode: Automatic (3 IOPS per GiB of SSD storage)
SSD IOPS: 12288
SSD storage capacity
Modify storage capacity
Input type
Percentage
Absolute
Desired % increase
10
%
Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.
Provisioned SSD IOPS
Automatic (3 IOPS per GiB of SSD storage)
User-provisioned
Configuration preview
Attribute
Current configuration
New configuration
SSD storage capacity
4,096 GiB
(2,048 GiB per HA pair)
4,506 GiB
(2,253 GiB per HA pair)
Mode: Automatic
Mode: Automatic

4. Um die SSD-Speicherkapazität zu erhöhen, wählen Sie Speicherkapazität ändern aus.
5. Wählen Sie als Eingabetyp eine der folgenden Optionen aus:
   - Um die neue SSD-Speicherkapazität als prozentuale Änderung gegenüber dem aktuellen Wert einzugeben, wählen Sie Prozent aus.
   - Um den neuen Wert in GiB einzugeben, wählen Sie Absolut.
6. Geben Sie je nach Eingabetyp einen Wert für Gewünschte Erhöhung in% ein.
   - Geben Sie unter Prozentsatz den Wert für die prozentuale Erhöhung ein. Dieser Wert muss mindestens 10 Prozent über dem aktuellen Wert liegen.
   - Geben Sie für Absolut den neuen Wert in GiB bis zum zulässigen Höchstwert von 196.608 GiB ein.
7. Für bereitgestellte SSD-IOPS haben Sie zwei Möglichkeiten, die Anzahl der bereitgestellten SSD-IOPS für Ihr Dateisystem zu ändern:
   - Wenn Sie möchten, dass Amazon FSx Ihre SSD-IOPS automatisch skaliert, sodass 3 bereitgestellte SSD-IOPS pro GiB SSD-Speicherkapazität (bis zu einem Maximum von 160.000) beibehalten werden, wählen Sie Automatisch.
   - Wenn Sie die Anzahl der SSD-IOPS angeben möchten, wählen Sie User-provisioned. Geben Sie eine absolute Anzahl von IOPS ein, die mindestens dem Dreifachen der Menge an GiB Ihrer SSD-Speicherebene entspricht und höchstens 160.000 beträgt.

> **Note**
>
> Weitere Informationen zur maximalen Anzahl von SSD-IOPS, die Sie für Ihr FSx for ONTAP-Dateisystem bereitstellen können, finden Sie unter. Auswirkungen der Durchsatzkapazität auf die Leistung

8. Wählen Sie Aktualisieren.

> **Note**
>
> Am Ende der Eingabeaufforderung wird eine Konfigurationsvorschau für Ihre neue SSD-Speicherkapazität und SSD-IOPS angezeigt. Bei Dateisystemen mit horizontaler Skalierung wird auch der Wert pro HA-Paar angezeigt.

So aktualisieren Sie die SSD-Speicherkapazität und die bereitgestellten IOPS für ein Dateisystem (CLI)

Verwenden Sie den AWS CLI Befehl update-file-systemoder die entsprechende API-Aktion, um die SSD-Speicherkapazität und die bereitgestellten IOPS für ein FSx for ONTAP-Dateisystem zu aktualisieren. UpdateFileSystem Stellen Sie die folgenden Parameter mit Ihren Werten ein:

- Stellen `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.
- Um Ihre SSD-Speicherkapazität `--storage-capacity` zu erhöhen, legen Sie den Zielwert für die Speicherkapazität fest, der mindestens 10 Prozent über dem aktuellen Wert liegen muss.
- Verwenden Sie die Eigenschaft, um Ihre bereitgestellten SSD-IOPS zu ändern. `--ontap-configuration DiskIopsConfiguration` Diese Eigenschaft hat zwei Parameter und: `Iops` `Mode`
  - Wenn Sie die Anzahl der bereitgestellten IOPS angeben möchten, verwenden Sie `Iops=`*`number_of_IOPS`* (bis zu einem Maximum von 160.000) und. `Mode=USER_PROVISIONED` Der IOPS-Wert muss größer oder gleich dem Dreifachen der angeforderten SSD-Speicherkapazität sein. Wenn Sie die Speicherkapazität nicht erhöhen, muss der IOps-Wert größer oder gleich dem Dreifachen der aktuellen SSD-Speicherkapazität sein.
  - Wenn Sie möchten, dass Amazon FSx Ihre SSD-IOPS automatisch erhöht, verwenden Sie den `Mode=AUTOMATIC` `Iops` Parameter und verwenden Sie ihn nicht. Amazon FSx verwaltet automatisch 3 SSD-IOPS pro GiB der bereitgestellten SSD-Speicherkapazität (bis zu einem Maximum von 160.000).

> **Note**
>
> Weitere Informationen zur maximalen Anzahl von SSD-IOPS, die Sie für Ihr FSx for ONTAP-Dateisystem bereitstellen können, finden Sie unter. Auswirkungen der Durchsatzkapazität auf die Leistung

Im folgenden Beispiel wird der SSD-Speicher des Dateisystems auf 2000 GiB erhöht und die Anzahl der vom Benutzer bereitgestellten SSD-IOPS auf 7000 festgelegt.

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

Verwenden Sie den Befehl, um den Fortschritt des Updates zu überwachen. describe-file-systems AWS CLI Suchen Sie in der Ausgabe nach dem `AdministrativeActions` Abschnitt.

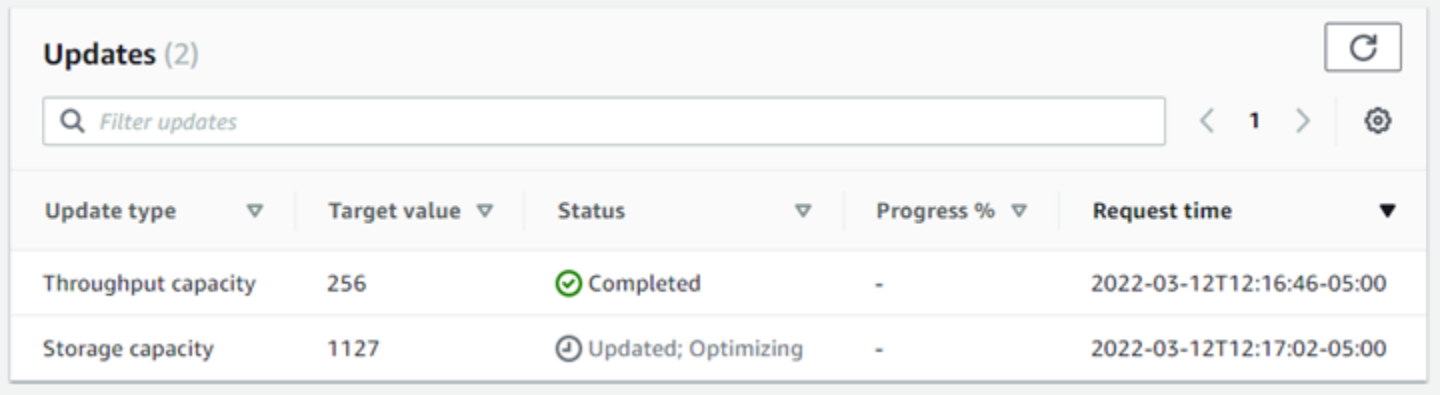
Weitere Informationen finden Sie AdministrativeActionin der Amazon FSx for NetApp ONTAP API-Referenz.

Überwachung der Speicherkapazität und der IOPS-Updates

Sie können den Fortschritt eines SSD-Speicherkapazitäts- und IOPS-Updates mithilfe der Amazon FSx-Konsole, CLI und API überwachen.

Um Speicher- und IOPS-Updates zu überwachen (Konsole)

Auf der Registerkarte Updates auf der Seite mit den Dateisystemdetails für Ihr FSx for ONTAP-Dateisystem können Sie die 10 neuesten Updates für jeden Updatetyp einsehen.



Für SSD-Speicherkapazität und IOPS-Updates können Sie die folgenden Informationen einsehen:

Art des Updates

Unterstützte Typen sind Speicherkapazität, Modus und IOPS. Die Werte für Modus und IOPS werden für alle Anforderungen an Speicherkapazität und IOPS-Skalierung aufgeführt.

Zielwert

Der Wert, auf den Sie angegeben haben, um die SSD-Speicherkapazität oder IOPS des Dateisystems zu aktualisieren.

Status

Der aktuelle Status des Updates. Die möglichen Werte lauten wie folgt:

- Ausstehend — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.

- In Bearbeitung — Amazon FSx verarbeitet die Aktualisierungsanfrage.
- Aktualisiert; Optimierung — Amazon FSx hat die SSD-Speicherkapazität des Dateisystems erhöht. Bei der Speicheroptimierung werden Ihre Daten jetzt im Hintergrund neu verteilt.
- Abgeschlossen — Das Update wurde erfolgreich abgeschlossen.
- Fehlgeschlagen — Die Aktualisierungsanforderung ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Details zu sehen.

Fortschritt%

Zeigt den Fortschritt des Speicheroptimierungsprozesses in Prozent an.

Uhrzeit der Anfrage

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

Zur Überwachung von Speicher- und IOPS-Updates (CLI)

Mithilfe des describe-file-systems AWS CLI Befehls und der DescribeFileSystemsAPI-Operation können Sie Anfragen zur Erhöhung der SSD-Speicherkapazität im Dateisystem anzeigen und überwachen. Das `AdministrativeActions` Array listet die 10 neuesten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die SSD-Speicherkapazität eines Dateisystems erhöhen, werden zwei `AdministrativeActions` Aktionen generiert: eine `FILE_SYSTEM_UPDATE` und eine `STORAGE_OPTIMIZATION` Aktion.

Das folgende Beispiel zeigt einen Auszug der Antwort auf einen `describe-file-systems` CLI-Befehl. Für das Dateisystem steht eine administrative Maßnahme zur Erhöhung der SSD-Speicherkapazität auf 2000 GiB und der bereitgestellten SSD-IOPS auf 7000 aus.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
             }
```

```
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1586797629.095,
        "Status": "PENDING"
    }
]
```

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 auf`UPDATED_OPTIMIZING`. Die Speicherkapazität zeigt den neuen größeren Wert an und Amazon FSx beginnt mit der Verarbeitung der `STORAGE_OPTIMIZATION` administrativen Aktion. Dieses Verhalten wird im folgenden Auszug aus der Antwort eines `describe-file-systems` CLI-Befehls 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 in`COMPLETED`, und die `STORAGE_OPTIMIZATION` Aktion wird nicht mehr angezeigt.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586799169.445,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "ProgressPercent": 41,
        "RequestTime": 1586799169.445,
        "Status": "IN_PROGRESS"
    }
```

```
]
```

Wenn die Speicherkapazität- oder IOPS-Aktualisierungsanforderung fehlschlägt, ändert sich der Status der `FILE_SYSTEM_UPDATE` Aktion auf`FAILED`, wie im folgenden Beispiel gezeigt. Die `FailureDetails` Eigenschaft stellt Informationen über den Fehler bereit.

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

Dynamisches Erhöhen der SSD-Speicherkapazität

Sie können die folgende Lösung verwenden, um die SSD-Speicherkapazität eines FSx for ONTAP-Dateisystems dynamisch zu erhöhen, wenn die Menge der verwendeten SSD-Speicherkapazität einen von Ihnen angegebenen Schwellenwert überschreitet. Diese AWS CloudFormation Vorlage stellt automatisch alle Komponenten bereit, die zur Definition des Schwellenwerts für die Speicherkapazität, des CloudWatch Amazon-Alarms auf der Grundlage dieses Schwellenwerts und der AWS Lambda Funktion zur Erhöhung der Speicherkapazität des Dateisystems erforderlich sind.

Die Lösung stellt automatisch alle benötigten Komponenten bereit und verwendet die folgenden Parameter:

- Ihre FSx for ONTAP Dateisystem-ID.
- Der verwendete SSD-Speicherkapazitätsschwellenwert (numerischer Wert). Dies ist der Prozentsatz, bei dem der CloudWatch Alarm ausgelöst wird.

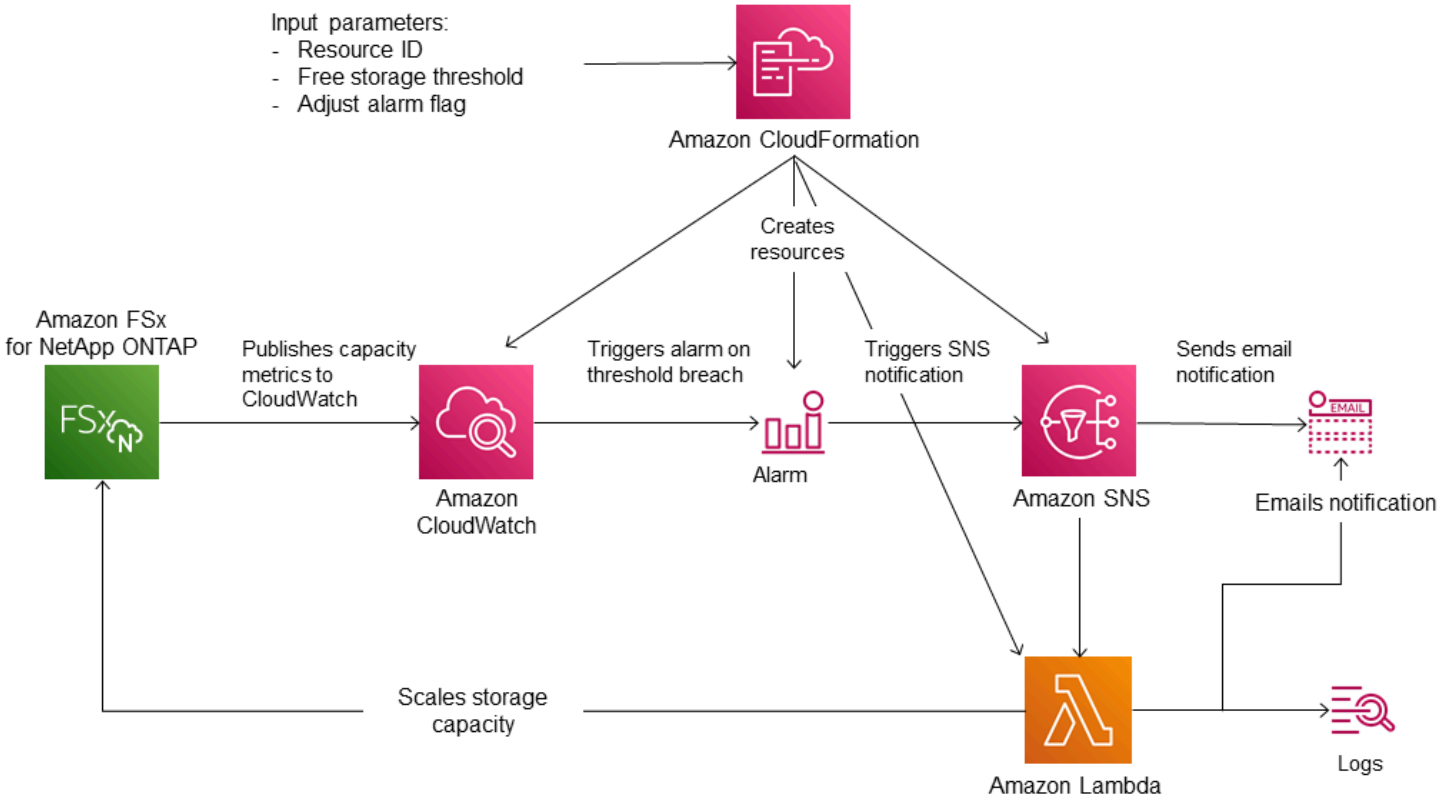
- Der Prozentsatz, um den die Speicherkapazität erhöht werden soll (%).
- Die E-Mail-Adresse, die für den Empfang von Skalierungsbenachrichtigungen verwendet wird.

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 erstellt AWS Cloud.



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 genutzte Speicherkapazität des Dateisystems den angegebenen Schwellenwert überschreitet, und sendet eine Nachricht an die Amazon SNS SNS-Warteschlange. Ein Alarm wird nur ausgelöst, wenn die genutzte Kapazität des Dateisystems den Schwellenwert kontinuierlich für einen Zeitraum von 5 Minuten überschreitet.
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. 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 die Bereitstellung der Komponenten, die zur automatischen Erhöhung der Speicherkapazität eines FSx for ONTAP-Dateisystems verwendet werden. AWS CloudFormation Um diese Lösung zu verwenden, laden Sie die SxOntapDynamicStorageScaling AWS CloudFormation F-Vorlage 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 Schwellenwert für die verwendete Speicherkapazität an, bei dem ein Alarm ausgelöst und die Speicherkapazität des Dateisystems automatisch erhöht werden soll. Dieser Wert wird als Prozentsatz (%) der aktuellen Speicherkapazität des Dateisystems angegeben. Es wird davon ausgegangen, dass das Dateisystem über eine geringe freie Speicherkapazität verfügt, wenn der verwendete Speicher diesen Schwellenwert überschreitet.

EmailAddress

Kein Standardwert. Gibt die E-Mail-Adresse an, die für das SNS-Abonnement verwendet werden soll, und empfängt Warnmeldungen zum Schwellenwert für die Speicherkapazität.

PercentIncrease

Die Standardeinstellung ist 20%. Gibt den Betrag an, um den die Speicherkapazität erhöht werden soll, ausgedrückt als Prozentsatz der aktuellen Speicherkapazität.

> **Note**
>
> Die Speicherskalierung wird jedes Mal versucht, wenn der CloudWatch Alarm in den `ALARM` Status wechselt. Wenn Ihre SSD-Speicherkapazitätsauslastung nach dem Versuch einer Speicherskalierung weiterhin über dem Schwellenwert liegt, wird die Speicherskalierung nicht erneut versucht.

MaxF B SxSizeinGi

Die Standardeinstellung ist 196608. Gibt die maximal unterstützte Speicherkapazität für den SSD-Speicher an.

Automatisierte Bereitstellung mit AWS CloudFormation

Mit dem folgenden Verfahren wird ein AWS CloudFormation Stack konfiguriert und bereitgestellt, um die Speicherkapazität eines FSx for ONTAP-Dateisystems automatisch zu erhöhen. Die Bereitstellung dauert einige Minuten. Weitere Informationen zum Erstellen eines CloudFormation Stacks finden Sie im AWS CloudFormation Benutzerhandbuch unter Erstellen eines Stacks auf der AWS CloudFormation Konsole.

> **Note**
>
> Bei der Implementierung dieser Lösung fallen die zugehörigen AWS Dienste in Rechnung. Weitere Informationen finden Sie auf den Seiten mit den Preisdetails für diese Dienste.

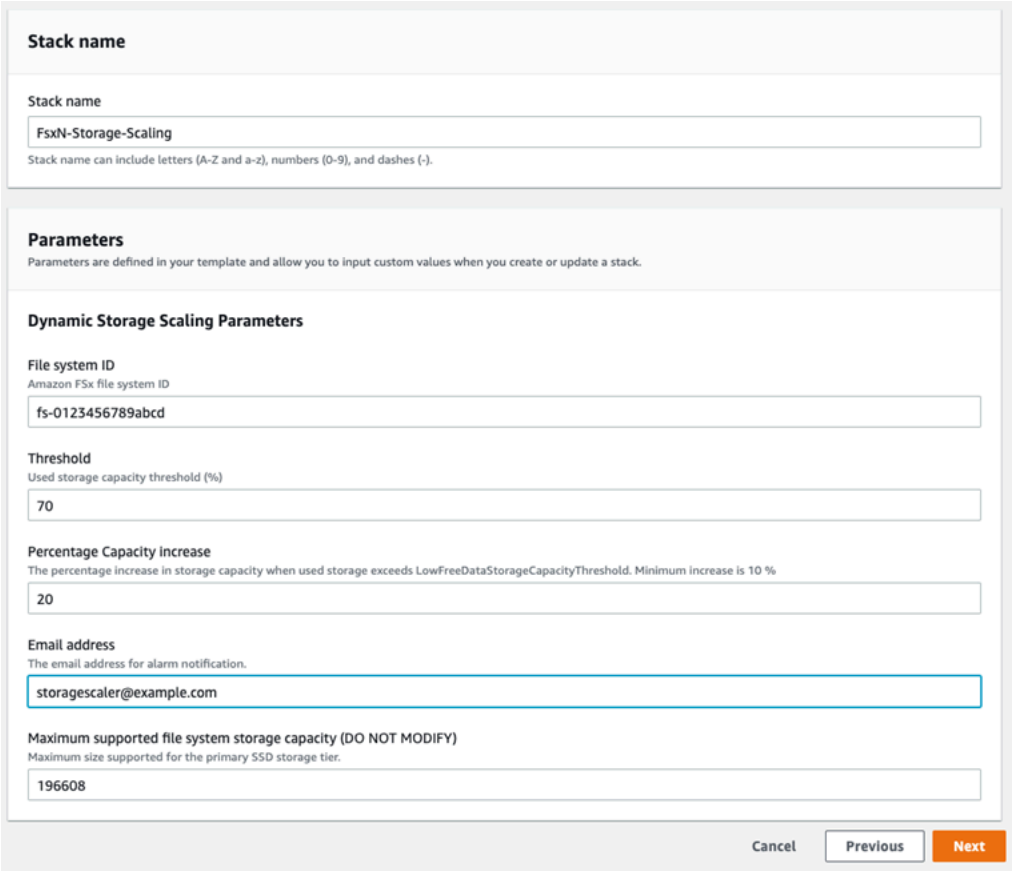
Bevor Sie beginnen, müssen Sie die ID des Amazon FSx-Dateisystems, das in der Amazon Virtual Private Cloud (Amazon VPC) läuft, in Ihrem haben. AWS-Konto Weitere Informationen zum Erstellen von Amazon FSx-Ressourcen finden Sie unterErste Schritte mit Amazon FSx für NetApp ONTAP.

So starten Sie den Lösungsstapel zur automatischen Erhöhung der Speicherkapazität

1. Laden Sie die SxOntapDynamicStorageScaling AWS CloudFormation F-Vorlage herunter.

> **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. Allgemeine AWS-Referenz

2. Wählen Sie in der AWS CloudFormation Konsole Stack erstellen > Mit neuen Ressourcen aus.
3. Wählen Sie „Vorlage ist fertig“. Wählen Sie im Abschnitt Vorlage angeben die Option Vorlagendatei hochladen und laden Sie die Vorlage hoch, die Sie heruntergeladen haben.
4. Geben Sie im Feld Stackdetails angeben die Werte für Ihre Lösung zur automatischen Erhöhung der Speicherkapazität ein.



5. Geben Sie einen Stack-Namen ein.

6. Überprüfen Sie unter Parameter die Parameter für die Vorlage und ändern Sie sie, um sie an die Anforderungen Ihres Dateisystems anzupassen. Wählen Sie anschließend Weiter.

> **Note**
>
> Bestätigen Sie die SNS-Abonnement-E-Mail, die Sie nach der Bereitstellung der CloudFormation Vorlage erhalten, um E-Mail-Benachrichtigungen zu erhalten, wenn versucht wird, mit dieser Vorlage zu skalieren.

7. Geben Sie die gewünschten Optionseinstellungen für Ihre benutzerdefinierte Lösung ein, und wählen Sie dann Weiter aus.
8. Überprüfen und bestätigen Sie unter Überprüfen die Lösungseinstellungen. Sie müssen das Kontrollkästchen aktivieren, das bestätigt, dass die Vorlage IAM-Ressourcen erstellt.
9. 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 ein paar Minuten sollte 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 CloudFormation Benutzerhandbuch.

Speicherkapazität des Volumens

FSx for ONTAP-Volumes sind virtuelle Ressourcen, die Sie verwenden, um Daten zu gruppieren, zu bestimmen, wie Daten gespeichert werden, und um die Art des Zugriffs auf Ihre Daten zu bestimmen. Volumes verbrauchen wie Ordner selbst keine Speicherkapazität des Dateisystems. Nur die auf einem Volume gespeicherten Daten verbrauchen SSD-Speicher und, abhängig von der Tiering-Richtlinie des Volumes, den Kapazitätspool-Speicher. Sie legen die Größe eines Volumes fest, wenn Sie es erstellen, und Sie können seine Größe später ändern. Sie können die Speicherkapazität Ihrer FSx for ONTAP-Volumes mithilfe der API AWS Management Console, AWS CLI und der ONTAP CLI überwachen und verwalten.

Themen

- Tiering von Volumendaten

- Snapshots und Volume-Speicherkapazität
- Kapazität der Volumendatei
- Die Speicherkapazität eines Volumes aktualisieren
- Automatische Volumengrößenanpassung aktivieren
- Überwachung der Speicherkapazität des Volumes
- Festlegung der Tiering-Richtlinie für ein Volume
- Einstellung der Mindestkühltage
- Festlegung der Cloud-Abruf-Richtlinie für ein Volume
- Die Dateikapazität eines Volumes anzeigen
- Erhöhung der maximalen Anzahl von Dateien auf einem Volume
- Den Cloud-Schreibmodus eines Volumes aktivieren

Tiering von Volumendaten

Ein Amazon FSx for NetApp ONTAP-Dateisystem hat zwei Speicherstufen: Primärspeicher und Kapazitätspoolspeicher. Primärspeicher ist ein bereitgestellter, skalierbarer, leistungsstarker SSD-Speicher, der speziell für den aktiven Teil Ihres Datensatzes entwickelt wurde. Beim Kapazitätspoolspeicher handelt es sich um eine vollständig elastische Speicherebene, die auf Petabyte skaliert werden kann und für Daten, auf die selten zugegriffen wird, kostenoptimiert ist.

Die Daten auf den einzelnen Volumes werden automatisch der Speicherebene des Kapazitätspools zugeordnet, basierend auf der Tiering-Richtlinie, der Kühlzeit und den Schwellenwerten des Volumes. In den folgenden Abschnitten werden die ONTAP Volume-Tiering-Richtlinien und die Schwellenwerte beschrieben, anhand derer bestimmt wird, wann Daten dem Kapazitätspool zugeordnet werden.

Richtlinien für das Volumen-Tiering

Sie bestimmen, wie Sie die Speicherstufen Ihres FSx for ONTAP-Dateisystems verwenden, indem Sie die Tiering-Richtlinie für jedes Volume im Dateisystem auswählen. Sie wählen die Tiering-Richtlinie, wenn Sie ein Volume erstellen, und Sie können sie jederzeit mit der Amazon FSx-Konsole AWS CLI, API oder mithilfe von NetApp Verwaltungstools ändern. Sie können aus einer der folgenden Richtlinien wählen, die festlegen, welche Daten, falls vorhanden, dem Kapazitätspool-Speicher zugewiesen werden.

> **Note**
>
> Durch Tiering können Ihre Datei- und Snapshot-Daten auf die Ebene des Kapazitätspools verschoben werden. Dateimetadaten verbleiben jedoch immer auf der SSD-Ebene. Weitere Informationen finden Sie unter Wie wird SSD-Speicher verwendet.

- Automatisch — Diese Richtlinie verschiebt alle kalten Daten — Benutzerdaten und Snapshots — auf die Ebene des Kapazitätspools. Die Kühlrate der Daten wird durch die Kühlzeit der Richtlinie bestimmt, die standardmäßig 31 Tage beträgt und auf Werte zwischen 2 und 183 Tagen konfigurierbar ist. Wenn die zugrundeliegenden kalten Datenblöcke nach dem Zufallsprinzip gelesen werden (wie bei einem typischen Dateizugriff), werden sie heiß gemacht und auf die primäre Speicherebene geschrieben. Wenn kalte Datenblöcke sequentiell gelesen werden (z. B. durch einen Antivirenscan), bleiben sie kalt und verbleiben auf der Speicherebene des Kapazitätspools. Dies ist die Standardrichtlinie beim Erstellen eines Volumes mit der Amazon FSx-Konsole.
- Nur Snapshot — Diese Richtlinie verschiebt nur Snapshot-Daten auf die Speicherstufe des Kapazitätspools. Die Geschwindigkeit, mit der Snapshots dem Kapazitätspool zugeordnet werden, wird durch die Kühlzeit der Richtlinie bestimmt, die standardmäßig auf 2 Tage festgelegt ist und auf Werte zwischen 2 und 183 Tagen konfigurierbar ist. Wenn Cold-Snapshot-Daten gelesen werden, werden sie heiß gemacht und auf die primäre Speicherebene geschrieben. Dies ist die Standardrichtlinie beim Erstellen eines Volumes mithilfe der AWS CLI Amazon FSx-API oder der NetApp ONTAP CLI.
- Alle — Diese Richtlinie markiert alle Benutzerdaten und Snapshot-Daten als kalt und speichert sie auf der Ebene des Kapazitätspools. Wenn Datenblöcke gelesen werden, bleiben sie kalt und werden nicht auf die primäre Speicherebene geschrieben. Wenn Daten mit der All-Tiering-Richtlinie auf ein Volume geschrieben werden, werden sie zunächst immer noch auf die SSD-Speicherebene geschrieben und dann durch einen Hintergrundprozess in den Kapazitätspool aufgeteilt. Beachten Sie, dass Dateimetadaten immer auf der SSD-Ebene verbleiben.
- Keine — Mit dieser Richtlinie werden alle Daten Ihres Volumes auf der primären Speicherebene gespeichert und verhindert, dass sie in den Kapazitätspool-Speicher verschoben werden. Wenn Sie ein Volume auf diese Richtlinie festlegen, nachdem es eine andere Richtlinie verwendet hat, werden die vorhandenen Daten auf dem Volume, das sich im Kapazitätspool-Speicher befand, durch einen Hintergrundprozess in den SSD-Speicher verschoben, solange Ihre SSD-Auslastung unter 90% liegt. Dieser Hintergrundprozess kann beschleunigt werden, indem Sie absichtlich Daten

lesen oder die Cloud-Abruf-Richtlinie Ihres Volumes ändern. Weitere Informationen finden Sie unter Richtlinien für den Cloud-Abruf.

Als bewährte Methode empfehlen wir Ihnen, bei der Migration von Daten, die Sie langfristig im Kapazitätspoolspeicher speichern möchten, die Auto-Tiering-Richtlinie für Ihr Volume zu verwenden. Bei Auto-Tiering werden Daten auf der SSD-Speicherebene für mindestens 2 Tage (basierend auf der Kühlzeit des Volumes) gespeichert, bevor sie in die Kapazitätspoolebene verschoben werden. Durch die Aufbewahrung von Daten auf dem SSD-Speicher für mindestens 2 Tage kann ONTAP die Komprimierung und Deduplizierung Ihrer Daten nach dem Prozess reduzieren. Diese Einsparungen bleiben erhalten, wenn Daten in den Kapazitätspool aufgeteilt werden. ONTAP führt nur die Komprimierung und Deduplizierung nach dem Prozess für Daten auf SSD-Speichern durch. Wenn Sie also diese Richtlinie wählen, können Sie Ihre langfristigen Speichereinsparungen maximieren. Sie können auch die Übertragungsgeschwindigkeiten der ersten Backups, die Sie von Ihren Volumes erstellen, maximieren, da sich die zu sichernden Daten auf SSD-Speichern befinden.

Weitere Informationen zum Einrichten oder Ändern der Tiering-Richtlinie eines Volumes finden Sie unterFestlegung der Tiering-Richtlinie für ein Volume.

Abkühlphase nach Staffelung

Die Stufen-Kühlzeit eines Volumes legt fest, wie lange es dauert, bis Daten auf der SSD-Stufe als kalt markiert werden. Die Kühlzeit gilt für die Richtlinien `Auto` und das `Snapshot-only` Tiering. Sie können die Kühlzeit auf einen Wert im Bereich von 2 bis 183 Tagen festlegen. Weitere Informationen zur Einstellung der Kühlzeit finden Sie unterEinstellung der Mindestkühltage.

Die Daten werden 24 bis 48 Stunden nach Ablauf der Kühlzeit gestaffelt. Tiering ist ein Hintergrundprozess, der Netzwerkressourcen verbraucht und eine niedrigere Priorität als Anfragen an Kunden hat. Tiering-Aktivitäten werden gedrosselt, wenn fortlaufende Anfragen an den Kunden gestellt werden.

Richtlinien für den Cloud-Abruf

Die Cloud-Abruf-Richtlinie eines Volumes legt die Bedingungen fest, die festlegen, wann Daten, die aus der Kapazitätspoolebene gelesen wurden, auf die SSD-Stufe heraufgestuft werden dürfen. Wenn die Cloud-Abruf-Richtlinie auf etwas anderes als festgelegt ist`Default`, hat diese Richtlinie Vorrang vor dem Abrufverhalten der Tiering-Richtlinie Ihres Volumes. Für ein Volume kann eine der folgenden Cloud-Abruf-Richtlinien gelten:

- Standard — Diese Richtlinie ruft gestaffelte Daten auf der Grundlage der dem Volume zugrunde liegenden Tiering-Richtlinie ab. Dies ist die Standardrichtlinie für den Cloud-Abruf für alle Volumes.
- Nie — Mit dieser Richtlinie werden niemals gestaffelte Daten abgerufen, unabhängig davon, ob es sich um sequentielle oder zufällige Lesevorgänge handelt. Dies ist vergleichbar mit der Einstellung der Tiering-Richtlinie für Ihr Volume auf Alle, mit der Ausnahme, dass Sie sie zusammen mit anderen Richtlinien (Automatisch, Nur Snapshot) verwenden können, um Daten anhand der Mindestkühlzeit statt sofort zu klassifizieren.
- Beim Lesen — Mit dieser Richtlinie werden abgestufte Daten für alle clientgesteuerten Datenlesevorgänge abgerufen. Diese Richtlinie hat keine Auswirkung, wenn die Richtlinie „All Tiering“ verwendet wird.
- Heraufstufen — Diese Richtlinie kennzeichnet alle Daten eines Volumes, die sich im Kapazitätspool befinden, für den Abruf auf die SSD-Stufe. Die Daten werden markiert, wenn der tägliche Hintergrund-Tiering-Scanner das nächste Mal ausgeführt wird. Diese Richtlinie ist vorteilhaft für Anwendungen mit zyklischen Workloads, die zwar selten ausgeführt werden, bei deren Ausführung aber Leistung auf SSD-Ebene erforderlich ist. Diese Richtlinie hat keine Auswirkung, wenn die All-Tiering-Richtlinie verwendet wird.

Informationen zum Einrichten der Cloud-Abruf-Richtlinie für ein Volume finden Sie unter. Festlegung der Cloud-Abruf-Richtlinie für ein Volume

Schwellenwerte für die Staffelung

Die SSD-Speicherkapazitätsauslastung eines Dateisystems bestimmt, wie das Tiering-Verhalten für all Ihre Volumes ONTAP verwaltet wird. Basierend auf der SSD-Speicherkapazitätsnutzung eines Dateisystems legen die folgenden Schwellenwerte das Tiering-Verhalten wie beschrieben fest. Informationen zur Überwachung der Kapazitätsauslastung der SSD-Speicherebene eines Volumes finden Sie unter. Überwachung der Speicherkapazität des Volumes

> **Note**
>
> Wir empfehlen, die Speicherkapazitätsauslastung Ihrer SSD-Speicherstufe nicht zu überschreiten. Bei Dateisystemen mit horizontaler Skalierung gilt diese Empfehlung sowohl für die durchschnittliche Gesamtauslastung aller Aggregate Ihres Dateisystems als auch für die Auslastung jedes einzelnen Aggregats. Dadurch wird sichergestellt, dass das Tiering ordnungsgemäß funktioniert, und es entsteht Mehraufwand für neue Daten. Wenn Ihre SSD-Speicherstufe konstant über 80% der Speicherkapazität ausgelastet ist, können Sie

die Kapazität Ihrer SSD-Speicherstufe erhöhen. Weitere Informationen finden Sie unter Aktualisierung des Dateisystems, des SSD-Speichers und der IOPS.

FSx for ONTAP verwendet die folgenden Schwellenwerte für die Speicherkapazität, um das Tiering auf Volumes zu verwalten:

- <= 50% SSD-Speicher-Tier-Auslastung — Bei diesem Schwellenwert gilt die SSD-Speicherebene als nicht ausgelastet, und nur bei Volumes, die die All-Tiering-Policy verwenden, werden Daten auf Kapazitätspoolspeicher aufgeteilt. Bei Volumes mit den Richtlinien „Automatisch“ und „Nur Snapshot“ werden die Daten bei diesem Schwellenwert nicht gestaffelt.
- > 50% SSD-Speicher-Tier-Auslastung — Bei Volumes mit automatischen und reinen Snapshot-Richtlinien werden die Daten auf der Grundlage der Einstellung „Mindestkühltage“ gestaffelt. Die Standardeinstellung ist 31 Tage.
- >= 90% SSD-Speicher-Tier-Auslastung — Bei diesem Schwellenwert priorisiert Amazon FSx die Erhaltung von Speicherplatz auf der SSD-Speicherebene. Kalte Daten aus der Kapazitätspoolstufe werden nicht mehr in die SSD-Speicherstufe verschoben, wenn sie für Volumes mithilfe der Richtlinien „Automatisch“ und „Nur Snapshot“ gelesen werden.
- >= 98% Auslastung der SSD-Speicherebene — Sämtliche Tiering-Funktionen werden beendet, wenn die SSD-Speicherebene mindestens 98% ausgelastet ist. Sie können weiterhin von den Speicherebenen lesen, aber Sie können nicht in die Stufen schreiben.

Snapshots und Volume-Speicherkapazität

Ein Snapshot ist ein schreibgeschütztes Image eines Amazon FSx for NetApp ONTAP-Volumes zu einem bestimmten Zeitpunkt. Snapshots bieten Schutz vor versehentlichem Löschen oder Ändern von Dateien in Ihren Volumes. Mit Snapshots können Ihre Benutzer auf einfache Weise einzelne Dateien oder Ordner aus einem früheren Snapshot anzeigen und wiederherstellen.

Schnappschüsse werden zusammen mit den Daten Ihres Dateisystems gespeichert und verbrauchen die Speicherkapazität des Dateisystems. Snapshots verbrauchen jedoch nur Speicherkapazität für die Teile der Dateien, die sich seit dem letzten Snapshot geändert haben. Snapshots sind nicht in Backups Ihrer Dateisystem-Volumes enthalten.

Snapshots sind standardmäßig auf Ihren Volumes aktiviert, wobei die standardmäßige Snapshot-Richtlinie verwendet wird. Snapshots werden im `.snapshot` Verzeichnis im Stammverzeichnis eines

Volumes gespeichert. Sie können die Volume-Speicherkapazität für Snapshots auf folgende Weise verwalten:

- Snapshot-Richtlinien — Wählen Sie eine integrierte Snapshot-Richtlinie oder eine benutzerdefinierte Richtlinie, die Sie in der ONTAP CLI oder REST API erstellt haben.
- Manuelles Löschen von Snapshots — Gewinnen Sie Speicherkapazität zurück, indem Sie Snapshots manuell löschen.
- Eine Richtlinie zum automatischen Löschen von Snapshots erstellen — Erstellen Sie eine Richtlinie, die mehr Snapshots löscht als die standardmäßige Snapshot-Richtlinie.
- Automatische Snapshots ausschalten — Sparen Sie Speicherkapazität, indem Sie automatische Snapshots deaktivieren.

Weitere Informationen finden Sie unter Arbeiten mit Snapshots.

Kapazität der Volumendatei

Amazon FSx for NetApp ONTAP-Volumes verfügen über Dateizeiger, die zum Speichern von Dateimetadaten wie Dateiname, Uhrzeit des letzten Zugriffs, Berechtigungen und Größe verwendet werden und als Zeiger auf Datenblöcke dienen. Diese Dateizeiger werden Inodes genannt, und jedes Volume hat eine begrenzte Kapazität für die Anzahl der Inodes, die als Volume-Dateikapazität bezeichnet wird. Wenn auf einem Volume die verfügbaren Dateien (Inodes) knapp werden oder die verfügbaren Dateien (Inodes) erschöpft sind, können Sie keine zusätzlichen Daten auf dieses Volume schreiben.

Die Anzahl der Dateisystemobjekte — Dateien, Verzeichnisse, Snapshot-Kopien —, die ein Volume enthalten kann, hängt davon ab, wie viele Inodes es hat. Die Anzahl der Inodes in einem Volume steigt entsprechend der Speicherkapazität des Volumes (und der Anzahl der Volume-Bestandteile bei Volumes). FlexGroup Standardmäßig haben FlexVol Volumes (oder FlexGroup Bestandteile) mit einer Speicherkapazität von 648 GiB oder mehr alle dieselbe Anzahl von Inodes: 21.251.126. Wenn Sie ein Volume erstellen, das größer als 648 GiB ist und es mehr als 21.251.126 Inodes haben soll, müssen Sie die maximale Anzahl von Inodes (Dateien) manuell erhöhen. Weitere Informationen zum Anzeigen der maximalen Anzahl von Dateien für ein Volume finden Sie unter. Die Dateikapazität eines Volumes anzeigen

Die Standardanzahl von Inodes auf einem Volume ist 1 Inode pro 32 KiB Volume-Speicherkapazität, bis zu einer Volume-Größe von 648 GiB. Für ein 1-GiB-Volumen:

Volume_Size_in_Bytes × (1 Datei ÷ inode_size_in_bytes) = maximale_Anzahl_der_Dateien

1.073.741.824 Byte × (1 Datei ÷32.768 Byte) = 32.768 Dateien

Sie können die maximale Anzahl von Inodes, die ein Volume enthalten kann, auf maximal 1 Inode pro 4 KiB Speicherkapazität erhöhen. Bei einem 1-GiB-Volumen erhöht sich dadurch die maximale Anzahl von Inodes oder Dateien von 32.768 auf 262.144:

1.073.741.824 Byte × (1 Datei ÷4096 Byte) = 262.144 Dateien

Ein FSx for ONTAP-Volume kann maximal 2 Milliarden Inodes haben.

Hinweise zum Ändern der maximalen Anzahl von Dateien, die ein Volume speichern kann, finden Sie unter. Erhöhung der maximalen Anzahl von Dateien auf einem Volume

Die Speicherkapazität eines Volumes aktualisieren

Sie können die Volume-Speicherkapazität verwalten, indem Sie die Volume-Größe mithilfe der API AWS Management Console, AWS CLI und der ONTAP CLI manuell erhöhen oder verringern. Sie können auch die automatische Volumenanpassung aktivieren, sodass die Volume-Größe automatisch vergrößert oder verkleinert wird, wenn bestimmte Schwellenwerte für die genutzte Speicherkapazität erreicht werden. Sie verwenden die ONTAP CLI, um die automatische Volumenanpassung zu verwalten.

Um die Speicherkapazität eines Volumes zu ändern (Konsole)

- Sie können die Speicherkapazität eines Volumes mithilfe der Amazon FSx-Konsole und der API erhöhen oder verringern. AWS CLI Weitere Informationen finden Sie unter Ein Volume aktualisieren.

Sie können die ONTAP CLI auch verwenden, um die Speicherkapazität eines Volumes mit dem `volume modify`Befehl zu ändern.

Um die Größe eines Volumes zu ändern (ONTAP CLI)

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Verwenden Sie den Befehl volume modify ONTAP CLI, um die Speicherkapazität eines Volumes zu ändern. Führen Sie den folgenden Befehl aus und verwenden Sie dabei Ihre Daten anstelle der folgenden Werte:

   - *svm_name*Ersetzen Sie es durch den Namen der virtuellen Speichermaschine (SVM), auf der das Volume erstellt wurde.
   - *vol_name*Ersetzen Sie es durch den Namen des Volumes, dessen Größe Sie ändern möchten.
   - *vol_size*Ersetzen Sie es durch die neue Größe des Volumes im Format *integer*[KB|MB|GB|TB|PB], z. B. 100GB um die Volumegröße auf 100 Gigabyte zu erhöhen.

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

Automatische Volumengrößenanpassung aktivieren

Automatische Volumenanpassung, sodass das Volume automatisch auf eine bestimmte Größe anwächst, wenn es einen Schwellenwert für belegten Speicherplatz erreicht. Sie können dies für FlexVol Volumetypen (der Standard-Volumetyp für FSx for ONTAP) mit dem Befehl ONTAP volume autosizeCLI tun.

So aktivieren Sie die automatische Volumengrößenanpassung (ONTAP CLI)

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *management_endpoint_ip*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Verwenden Sie den `volume autosize` Befehl wie abgebildet und ersetzen Sie dabei die folgenden Werte:

   - *svm_name*Ersetzen Sie es durch den Namen der SVM, auf der das Volume erstellt wurde.

- *vol_name*Ersetzen Sie es durch den Namen des Volumes, dessen Größe Sie ändern möchten.
- *grow_threshold*Ersetzen Sie es durch einen Prozentwert für den verwendeten Speicherplatz (z. B.90), bei dem das Volumen automatisch vergrößert wird (bis zum *max_size*Wert).
- *max_size*Ersetzen Sie es durch die maximale Größe, auf die das Volumen anwachsen kann. Verwenden Sie das Format *integer*[KB|MB|GB|TB|PB], 300TB z. B. Die maximale Größe beträgt 300 TB. Die Standardeinstellung ist 120% der Volume-Größe.
- Ersetzen Sie *min_size* durch die Mindestgröße, auf die das Volume geschrumpft wird. *Verwenden Sie dasselbe Format wie für max_size.*
- Ersetzen Sie *shrink_threshold* durch den Prozentsatz des verwendeten Speicherplatzes, bei dem das Volumen automatisch verkleinert wird.

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

Überwachung der Speicherkapazität des Volumes

Sie können den verfügbaren Speicher eines Volumes und seine Speicherverteilung in AWS Management Console AWS CLI, und der NetApp ONTAP CLI anzeigen.

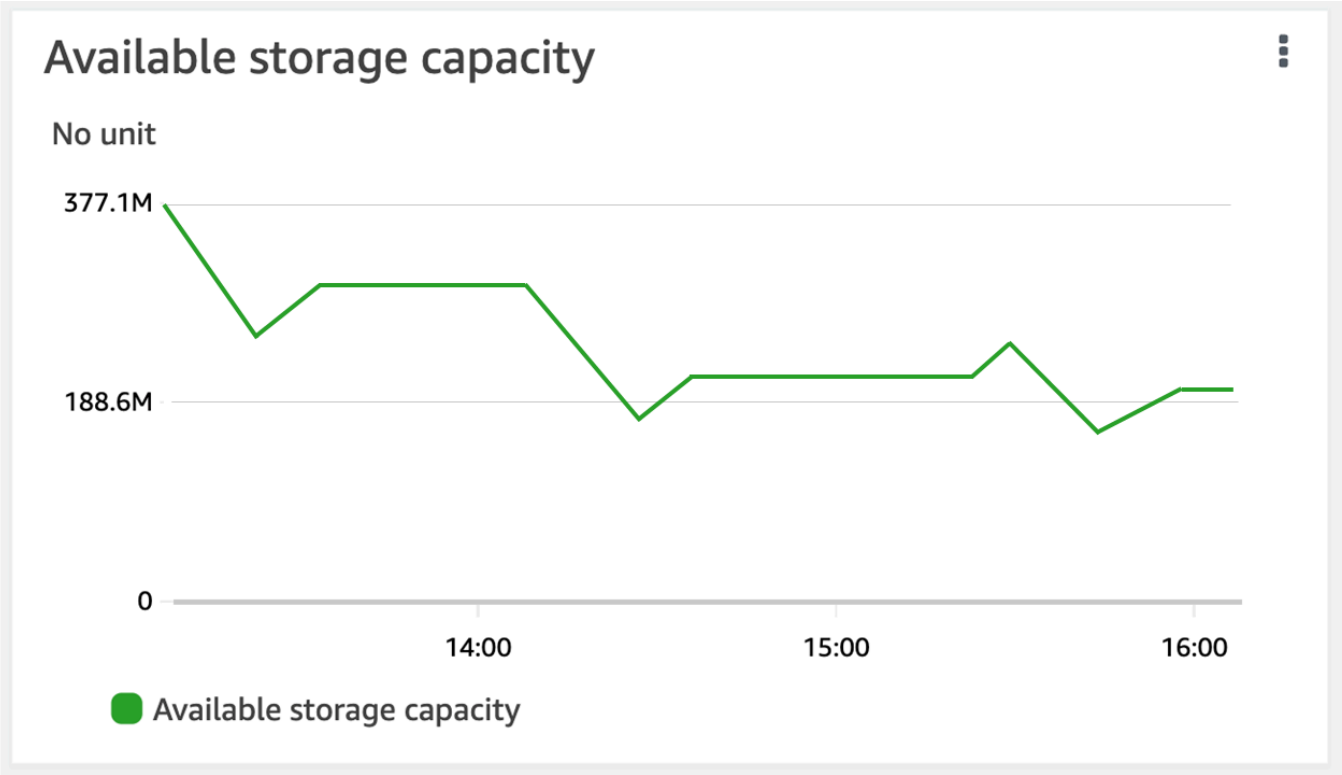
Um die Speicherkapazität eines Volumes zu überwachen (Konsole)

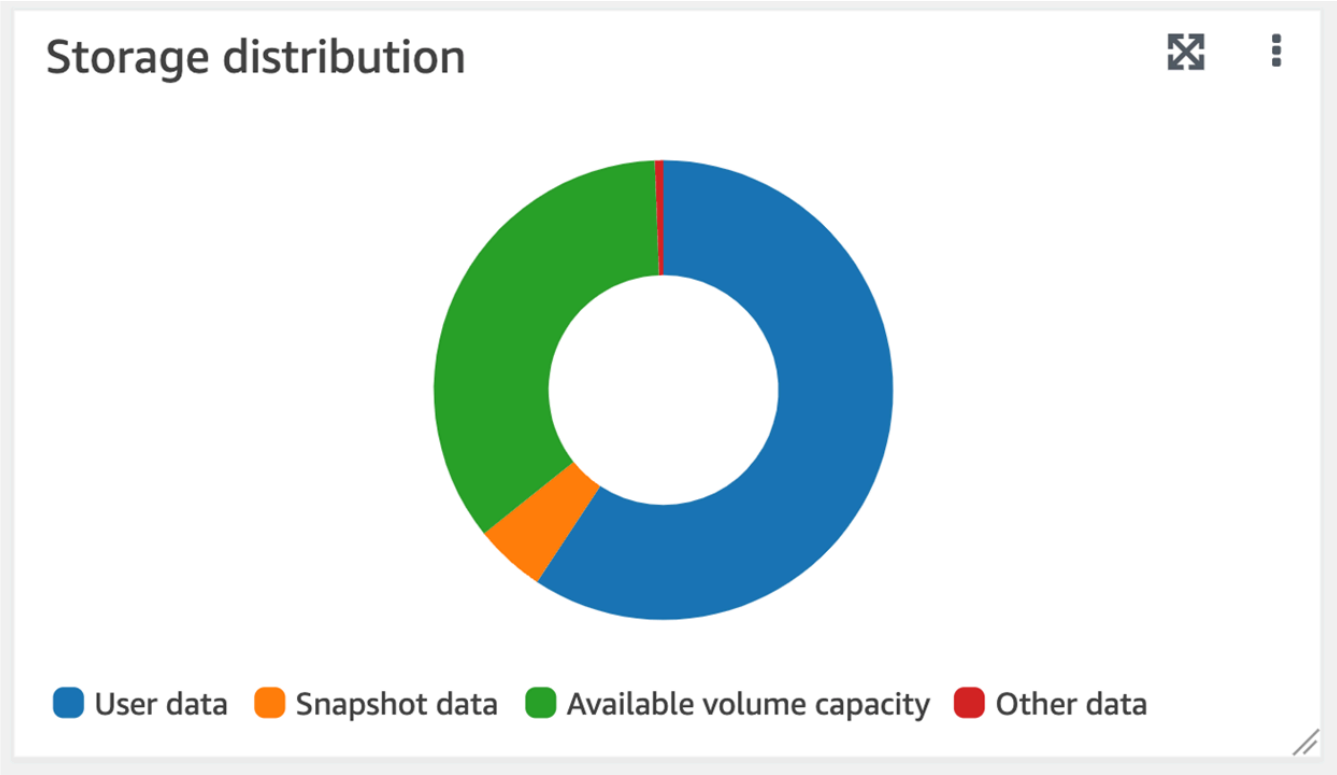
Das Diagramm „Verfügbarer Speicherplatz“ zeigt die Menge an freier Speicherkapazität auf einem Volume im Laufe der Zeit. Das Diagramm zur Speicherverteilung zeigt, wie die Speicherkapazität eines Volumes derzeit auf vier Kategorien verteilt ist:

- Benutzerdaten
- Snapshot-Daten
- Verfügbare Volumenkapazität
- Andere Daten

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.

2. Wählen Sie in der linken Navigationsspalte Volumes und anschließend das ONTAP-Volume aus, für das Sie Informationen zur Speicherkapazität anzeigen möchten. Die Seite mit den Datenträgerdetails wird angezeigt.
3. Wählen Sie im zweiten Bereich die Registerkarte Überwachung aus. Die Diagramme Verfügbarer Speicher und Speicherverteilung werden zusammen mit mehreren anderen Diagrammen angezeigt.





So überwachen Sie die Speicherkapazität eines Volumes (ONTAPCLI)

Mit dem `volume show-space` ONTAP CLI-Befehl können Sie überwachen, wie die Speicherkapazität Ihres Volumes verbraucht wird. Weitere Informationen finden Sie `volume show-space`im NetApp ONTAP Documentation Center.

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Zeigen Sie die Nutzung der Speicherkapazität eines Volumes an, indem Sie den folgenden Befehl eingeben und dabei die folgenden Werte ersetzen:

   - *`svm_name`*Ersetzen Sie es durch den Namen der SVM, auf der das Volume erstellt wurde.

- *vol_name*Ersetzen Sie es durch den Namen des Volumes, für das Sie die Data-Tiering-Richtlinie festlegen.

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

Wenn der Befehl erfolgreich ist, erhalten Sie eine Ausgabe, die der folgenden ähnelt:

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

Total Used                             10.03GB        91%

Total Physical Used                    10.03GB        91%
```

Die Ausgabe dieses Befehls zeigt, wie viel physischen Speicherplatz verschiedene Datentypen auf diesem Volume belegen. Außerdem wird der Prozentsatz der Gesamtkapazität angezeigt, den die einzelnen Datentypen verbrauchen. In diesem Beispiel `Snapshot Spill` `Snapshot Reserve` verbrauchen sie zusammen 90 Prozent der Kapazität des Volumes.

`Snapshot Reserve`zeigt die Menge an Festplattenspeicher, die für das Speichern von Snapshot-Kopien reserviert ist. Wenn der Speicherplatz für Snapshot-Kopien den reservierten Speicherplatz überschreitet, wird er in das Dateisystem übertragen. Dieser Betrag wird unter `Snapshot Spill` angezeigt.

Um den verfügbaren Speicherplatz zu erhöhen, können Sie entweder die Größe des Volumes erhöhen oder Snapshots löschen, die Sie nicht verwenden, wie in den folgenden Verfahren gezeigt.

Für FlexVol Volumetypen (der Standard-Volumetyp für FSx für ONTAP-Volumes) können Sie auch die automatische Volumenanpassung aktivieren. Wenn Sie die automatische Anpassung aktivieren,

erhöht sich die Volumegröße automatisch, wenn bestimmte Schwellenwerte erreicht werden. Sie können automatische Snapshots auch deaktivieren. Beide Funktionen werden in den folgenden Abschnitten erklärt.

Festlegung der Tiering-Richtlinie für ein Volume

Sie können die Tiering-Richtlinie eines Volumes mithilfe der API AWS Management Console, AWS CLI und der ONTAP CLI ändern.

Um die Data-Tiering-Richtlinie eines Volumes zu ändern (Konsole)

Gehen Sie wie folgt vor, um die Data-Tiering-Richtlinie eines Volumes mithilfe von zu ändern. AWS Management Console

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich Volumes und dann das ONTAP-Volume aus, für das Sie die Data-Tiering-Richtlinie ändern möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option Volume aktualisieren aus. Das Fenster „Volume aktualisieren“ wird angezeigt.
4. Wählen Sie unter Capacity Pool Tiering Policy die neue Policy für das Volume aus. Weitere Informationen finden Sie unter Richtlinien für das Volumen-Tiering.
5. Wählen Sie „Aktualisieren“, um die neue Richtlinie auf das Volume anzuwenden.

So legen Sie die Tiering-Richtlinie (CLI) eines Volumes fest

- Ändern Sie die Tiering-Richtlinie eines Volumes mithilfe des CLI-Befehls update-volume (UpdateVolumeentspricht der Amazon FSx-API-Aktion). Im folgenden CLI-Befehlsbeispiel wird die Data-Tiering-Richtlinie eines Volumes auf festgelegt. `SNAPSHOT_ONLY`

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

  Bei einer erfolgreichen Anfrage antwortet das System mit der Beschreibung des Volumes.

  ```
  {
      "Volume": {
          "CreationTime": "2021-10-05T14:27:44.332000-04:00",
  ```

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

So ändern Sie die Tiering-Richtlinie eines Volumes (ONTAP CLI)

Sie verwenden den `volume modify` ONTAP CLI-Befehl, um die Tiering-Richtlinie eines Volumes festzulegen. Weitere Informationen finden Sie `volume modify`im NetApp ONTAP Documentation Center.

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Rufen Sie mit dem folgenden Befehl den erweiterten ONTAP CLI Modus auf.

```
FSx::> set adv

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

3. Verwenden Sie den folgenden Befehl, um die Volume-Data-Tiering-Richtlinie zu ändern und die folgenden Werte zu ersetzen:

   - *svm_name*Ersetzen Sie es durch den Namen der SVM, auf der das Volume erstellt wurde.
   - *vol_name*Ersetzen Sie es durch den Namen des Volumes, für das Sie die Data-Tiering-Richtlinie festlegen.
   - Ersetzen Sie *tiering_policy*durch die gewünschte Richtlinie. Gültige Werte sind `snapshot-only`, `auto`, `all` oder `none`. Weitere Informationen finden Sie unter Richtlinien für das Volumen-Tiering.

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

Einstellung der Mindestkühltage

Die Mindestkühltage für ein Volumen legen den Schwellenwert fest, anhand dessen bestimmt wird, welche Daten warm und welche kalt sind. Sie können die Mindestkühltage eines Volumes mithilfe einer API AWS CLI und der ONTAP CLI festlegen.

So legen Sie die Mindestkühltage eines Volumes fest (CLI)

- Ändern Sie eine Volume-Konfiguration mithilfe des CLI-Befehls update-volume (UpdateVolumeentspricht der Amazon FSx-API-Aktion). Das folgende CLI-Befehlsbeispiel legt die Werte eines Volumes `CoolingPeriod` auf 104 Tage fest.

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

Das System antwortet mit der Beschreibung des Datenträgers für eine erfolgreiche Anfrage.


```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 104,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```


So legen Sie die Mindestkühltage eines Volumes fest (ONTAP CLI)

Verwenden Sie den Befehl `volume modify` ONTAP CLI, um die Mindestanzahl an Kühltagen für ein vorhandenes Volume festzulegen. Weitere Informationen finden Sie `volume modify`im NetApp ONTAP Documentation Center.

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Rufen Sie mit dem folgenden Befehl den erweiterten ONTAP CLI Modus auf.

```
FSx::> set adv

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

3. Verwenden Sie den folgenden Befehl, um die Mindestkühltage Ihres Volumes zu ändern, und ersetzen Sie dabei die folgenden Werte:

   - *svm_name*Ersetzen Sie es durch den Namen der SVM, auf der das Volume erstellt wurde.
   - *vol_name*Ersetzen Sie es durch den Namen des Volumes, für das Sie die Kühltage festlegen.
   - *cooling_days*Ersetzen Sie es durch den gewünschten Wert, eine Ganzzahl zwischen 2 und 183.

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

Das System reagiert auf eine erfolgreiche Anfrage wie folgt.

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

Festlegung der Cloud-Abruf-Richtlinie für ein Volume

Verwenden Sie den `volume modify` ONTAP CLI-Befehl, um die Cloud-Abruf-Richtlinie für ein vorhandenes Volume festzulegen. Weitere Informationen finden Sie `volume modify`im NetApp ONTAP Documentation Center.

So legen Sie die Cloud-Abruf-Richtlinie eines Volumes fest (ONTAP CLI)

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den

folgenden Befehl ausführen. *management_endpoint_ip*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Rufen Sie mit dem folgenden Befehl den erweiterten ONTAP CLI Modus auf.

```
FSx::> set adv

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

3. Verwenden Sie den folgenden Befehl, um die Cloud-Abruf-Richtlinie des Volumes festzulegen, und ersetzen Sie dabei die folgenden Werte:

   - *svm_name*Ersetzen Sie es durch den Namen der SVM, auf der das Volume erstellt wurde.
   - *vol_name*Ersetzen Sie es durch den Namen des Volumes, für das Sie die Cloud-Abruf-Richtlinie festlegen.
   - *retrieval_policy*Ersetzen Sie es durch den gewünschten Wert, entweder`default`, `on-read`never, oder`promote`.

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

Das System reagiert auf eine erfolgreiche Anfrage wie folgt.

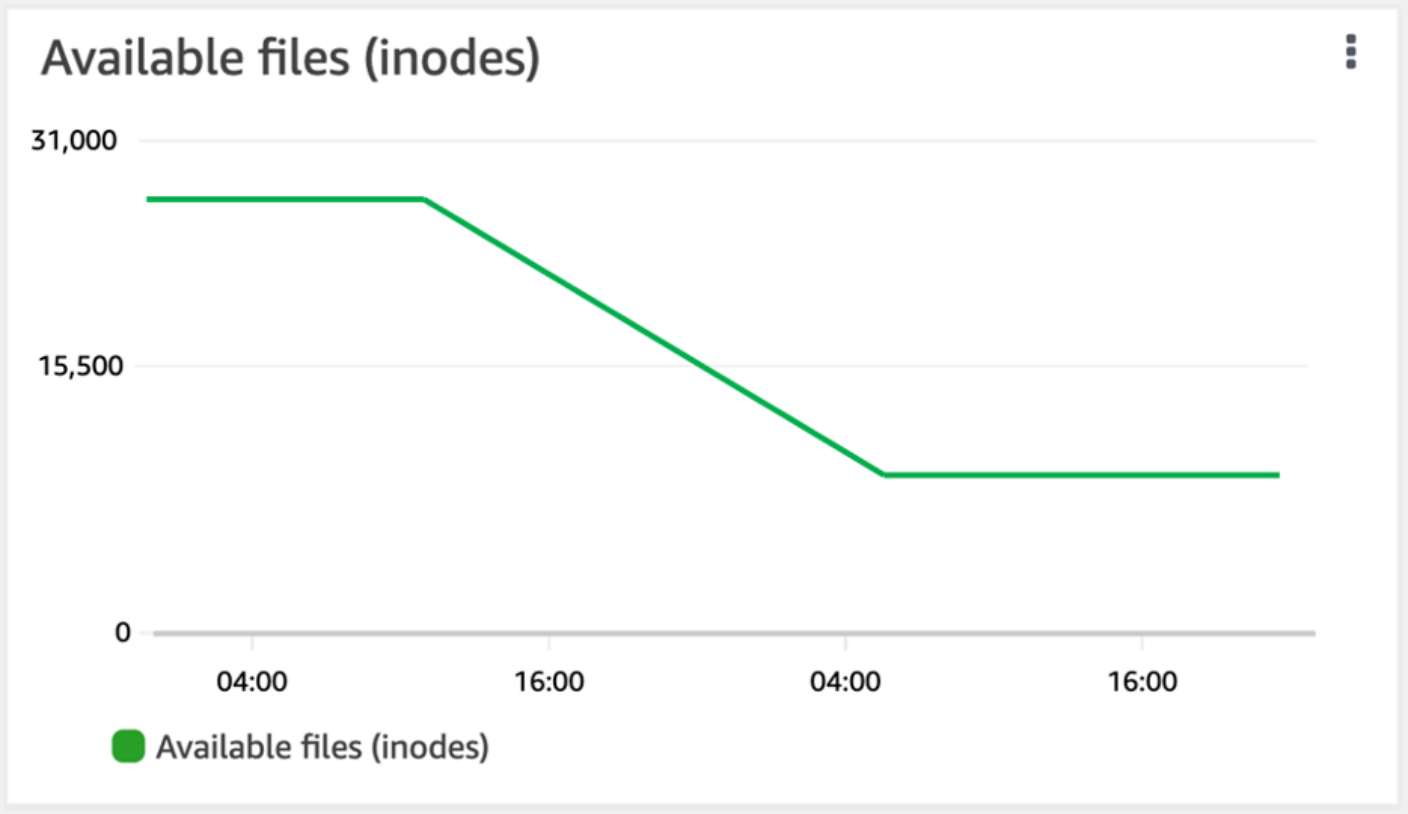
```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Die Dateikapazität eines Volumes anzeigen

Sie können eine der folgenden Methoden verwenden, um die maximal zulässige Anzahl von Dateien und die Anzahl der bereits auf einem Volume verwendeten Dateien anzuzeigen.

- Die CloudWatch Volumenmetriken `FilesCapacity` und`FilesUsed`.

- Navigieren Sie in der Amazon FSx-Konsole auf der Registerkarte Überwachung Ihres Volumes zum Diagramm Verfügbare Dateien (Inodes). Die folgende Abbildung zeigt die verfügbaren Dateien (Inodes) auf einem Volume, die im Laufe der Zeit abnehmen.



Erhöhung der maximalen Anzahl von Dateien auf einem Volume

FSx for ONTAP-Volumes kann die Dateikapazität knapp werden, wenn die Anzahl der verfügbaren Inodes oder Dateizeiger erschöpft ist.

So erhöhen Sie die maximale Anzahl von Dateien auf einem Volume (ONTAPCLI)

Sie verwenden den `volume modify` ONTAP CLI-Befehl, um die maximale Anzahl von Dateien auf einem Volume zu erhöhen. Weitere Informationen finden Sie `volume modify`im NetApp ONTAP Documentation Center.

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Führen Sie je nach Anwendungsfall einen der folgenden Schritte durch. Ersetzen Sie *svm_name*und *vol_name*durch Ihre Werte.

   - Gehen Sie wie folgt vor, um ein Volume so zu konfigurieren, dass immer die maximale Anzahl von Dateien (Inodes) verfügbar ist:

     1. Rufen Sie den erweiterten Modus in der ONTAP CLI mit dem folgenden Befehl auf.

        ```
        ::> set adv
        ```

     2. Nachdem Sie diesen Befehl ausgeführt haben, sehen Sie diese Ausgabe. Geben Sie einy, um fortzufahren.

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

     3. Geben Sie den folgenden Befehl ein, um immer die maximale Anzahl von Dateien auf dem Volume zu verwenden:

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

   - Verwenden Sie den folgenden Befehl, um die Gesamtzahl der auf dem Volume zulässigen Dateien bis zu einem möglichen Höchstwert von 2 Milliarden manuell anzugeben: *max_number_files* = (current_size_of_volume) × (1 file ÷ 4 KiB)

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

Den Cloud-Schreibmodus eines Volumes aktivieren

Verwenden Sie den `volume modify` ONTAP CLI-Befehl, um den Cloud-Schreibmodus für ein vorhandenes Volume zu aktivieren oder zu deaktivieren. Weitere Informationen finden Sie `volume modify`im NetApp ONTAP Documentation Center.

Voraussetzungen für die Einstellung des Cloud-Schreibmodus sind:

- Bei dem Volume muss es sich um ein vorhandenes Volume handeln. Sie können die Funktion nur auf einem vorhandenen Volume aktivieren.
- Bei dem Volume muss es sich um ein RW-Volume (Read-Write-Volume) handeln.
- Für das Volume muss die All-Tiering-Richtlinie gelten. Weitere Informationen zum Ändern der Einstufungsrichtlinie eines Volumes finden Sie unter. Festlegung der Tiering-Richtlinie für ein Volume

Der Cloud-Schreibmodus ist beispielsweise bei Migrationen hilfreich, bei denen große Datenmengen mithilfe des NFS-Protokolls in ein Dateisystem übertragen werden.

So legen Sie den Cloud-Schreibmodus eines Volumes fest (ONTAP CLI)

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *management_endpoint_ip*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.
2. Rufen Sie mit dem folgenden Befehl den erweiterten ONTAP CLI Modus auf.

   ```
   FSx::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```
3. Verwenden Sie den folgenden Befehl, um den Cloud-Schreibmodus des Volumes festzulegen, und ersetzen Sie dabei die folgenden Werte:

   - *svm_name*Ersetzen Sie es durch den Namen der SVM, auf der das Volume erstellt wurde.
   - *vol_name*Ersetzen Sie es durch den Namen des Volumes, für das Sie den Cloud-Schreibmodus einstellen.
   - *vol_cw_mode*Ersetzen Sie entweder durch`true`, um den Cloud-Schreibmodus auf dem Volume `false` zu aktivieren oder zu deaktivieren.

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

Das System reagiert auf eine erfolgreiche Anfrage wie folgt.

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

Schützen Ihrer Daten

Neben der automatischen Replikation der Daten Ihres Dateisystems, um eine hohe Haltbarkeit zu gewährleisten, bietet Ihnen Amazon FSx die folgenden Optionen, um die auf Ihren Dateisystemen gespeicherten Daten weiter zu schützen:

- Native Amazon-FSx-Backups unterstützen Ihre Anforderungen an die Aufbewahrung und Compliance von Backups in Amazon FSx . Sie können auch verwenden, AWS Backup um Ihre Backups in der AWS-Services Cloud zentral zu verwalten, zu automatisieren und zu schützen.
- Snapshots ermöglichen es Ihren Benutzern, Änderungen an Dateien einfach rückgängig zu machen und Dateiversionen zu vergleichen, indem Dateien mit früheren Versionen wiederhergestellt werden.
- Replikation Ihres Amazon-FSx-Dateisystems in ein zweites Dateisystem, um Datenschutz und Wiederherstellung bereitzustellen. Wenn die Replikation aktiviert ist, erfolgt sie automatisch und nach Plan.
- SnapLock kann Ihre Dateien schützen, indem sie in einen Write Once Read Many (WORM)-Status übergehen, wodurch Änderungen oder Löschungen für einen bestimmten Aufbewahrungszeitraum verhindert werden.

Themen

- Arbeiten mit Backups
- Arbeiten mit Snapshots
- Geplante Replikation mit NetApp SnapMirror
- Schützen Ihrer Daten mit SnapLock

Arbeiten mit Backups

Mit FSx for ONTAP können Sie automatische tägliche Backups und vom Benutzer initiierte Backups der Volumes in Ihrem Dateisystem erstellen. FSx for ONTAP Backups erfolgen pro Volume, sodass jedes Backup nur die Daten auf einem bestimmten Volume enthält. Amazon FSx-Backups sind äußerst robust und inkrementell.

Alle Amazon FSx-Backups (automatische tägliche Backups und vom Benutzer initiierte Backups) sind inkrementell. Das bedeutet, dass nur die Daten auf dem Volume gespeichert werden, die sich

nach Ihrer letzten Sicherung geändert haben. Dadurch werden der Zeitaufwand für die Erstellung des Backups und der für das Backup benötigte Speicherplatz minimiert, wodurch Speicherkosten eingespart werden, da keine Daten dupliziert werden. Wenn Sie ein Backup löschen, werden nur die Daten entfernt, die für dieses Backup eindeutig sind. Jedes Amazon FSx-Backup enthält alle Informationen, die benötigt werden, um aus dem Backup ein neues Volume zu erstellen, wodurch effektiv ein point-in-time Snapshot des Dateisystem-Volumes wiederhergestellt wird.

Das Erstellen regelmäßiger Backups für Ihre Volumes ist eine bewährte Methode, mit der Sie Ihre Anforderungen an Datenaufbewahrung und Compliance erfüllen können. Die Arbeit mit Amazon FSx-Backups ist einfach, egal ob es um das Erstellen von Backups, das Wiederherstellen aus einem Backup oder das Löschen eines Backups geht.

Amazon FSx unterstützt das Sichern von ONTAP FlexVol Volumes (auf allen Dateisystemen) und FlexGroup Volumes mit einem `OntapVolumeType` of `RW` (Lese-/Schreibzugriff).

> **Note**
>
> Amazon FSx unterstützt keine Sicherung von Data Protection- (DP) -Volumes, Load-Sharing- (LS) -Volumes oder FlexCache Ziel-Volumes.

Die Anzahl der Backups, die Sie pro Dateisystem und pro Volume speichern können, ist begrenzt. Weitere Informationen finden Sie unter Kontingente, die Sie erhöhen können und Ressourcenkontingente für jedes Dateisystem.

Themen

- Wie funktionieren Backups
- Speicheranforderungen
- Arbeiten Sie mit automatischen täglichen Backups
- Arbeiten mit vom Benutzer initiierten Backups
- Tags in Backups kopieren
- Leistung Backup und wiederherstellen
- Verwendung AWS Backup mit Amazon FSx
- Backups auf einem neuen Volume wiederherstellen
- Löschen eines Backups
- Backups und Offline-Volumes

- Erstellen eines vom Benutzer initiierten Backups
- Eine Sicherung auf einem neuen Volume wiederherstellen
- Löschen einer Sicherung

Wie funktionieren Backups

Amazon FSx-Backups verwenden Snapshots — also schreibgeschützte Images Ihrer Volumes — point-in-time, um die Inkrementalität zwischen den Backups aufrechtzuerhalten. Jedes Mal, wenn ein Backup erstellt wird, erstellt Amazon FSx zunächst einen Snapshot Ihres Volumes. Der Backup-Snapshot wird auf Ihrem Volume gespeichert und belegt Speicherplatz auf Ihrer SSD-Speicherebene. Amazon FSx vergleicht dann diesen Snapshot mit dem vorherigen Backup-Snapshot (falls vorhanden) und kopiert nur die geänderten Daten in Ihr Backup.

Wenn kein vorheriger Backup-Snapshot existiert, wird der gesamte Inhalt des letzten Backup-Snapshots in Ihr Backup kopiert. Nachdem der letzte Backup-Snapshot erfolgreich erstellt wurde, löscht Amazon FSx den vorherigen Backup-Snapshot. Der für das letzte Backup verwendete Snapshot verbleibt in Ihrem Volume, bis das nächste Backup erstellt wird. Dann wiederholt sich der Vorgang. Um die Speicherkosten für Backups zu optimieren, ONTAP bleiben die Einsparungen bei der Speichereffizienz eines Volumes bei seinen Backups erhalten.

Amazon FSx kann keine Volumes sichern, die offline sind.

Speicheranforderungen

Um Backups Ihrer Volumes erstellen zu können, müssen sowohl Ihr Volume als auch Ihr Dateisystem über genügend SSD-Speicherkapazität verfügen, um einen Backup-Snapshot zu speichern. Wenn Sie einen Backup-Snapshot erstellen, darf die zusätzliche Speicherkapazität, die durch den Snapshot verbraucht wird, nicht dazu führen, dass das Volume 98% des SSD-Speichers ausnutzt. In diesem Fall schlägt das Backup fehl. Sie können den SSD-Speicher eines Volumes oder Dateisystems jederzeit erhöhen, um sicherzustellen, dass Ihre Backups nicht unterbrochen werden.

Arbeiten Sie mit automatischen täglichen Backups

Automatische tägliche Backups der Volumes Ihres Dateisystems sind standardmäßig aktiviert, wenn Sie ein Dateisystem erstellen. Sie können automatische tägliche Backups für ein Dateisystem jederzeit aktivieren oder deaktivieren. Automatische tägliche Backups erfolgen während des täglichen Backup-Fensters, das automatisch festgelegt wird, wenn Sie ein Dateisystem erstellen. Sie können das tägliche Backup-Fenster jederzeit ändern. Wir empfehlen Ihnen, für Ihr tägliches Backup eine

Tageszeit zu wählen, die außerhalb der normalen Betriebszeiten der Anwendungen liegt, die Ihre Volumes verwenden, um eine bessere Backup-Leistung zu erzielen. Weitere Informationen finden Sie unter Leistung Backup und wiederherstellen.

Sie können den Aufbewahrungszeitraum für automatische tägliche Backups in der Konsole bei der Erstellung eines Dateisystems oder zu einem beliebigen Zeitpunkt auf 1 bis 90 Tage festlegen. Die standardmäßige Aufbewahrungsfrist für automatische tägliche Backups beträgt 30 Tage. Der Dienst löscht ein automatisches tägliches Backup, sobald die Aufbewahrungsfrist abgelaufen ist. Mithilfe der CLI oder API können Sie den Aufbewahrungszeitraum auf 0 bis 90 Tage festlegen. Wenn Sie ihn auf 0 setzen, werden automatische tägliche Backups deaktiviert.

Das tägliche Backup-Fenster und die Aufbewahrungsfrist für Backups sind Einstellungen auf Dateisystemebene, die für alle Volumes in Ihrem Dateisystem gelten. Sie können die Amazon FSx-Konsole, die oder die API verwenden AWS CLI, um das Backup-Fenster und die Aufbewahrungsdauer für Backups für Ihre Dateisysteme zu ändern und automatische tägliche Backups ein- oder auszuschalten. Weitere Informationen finden Sie unter Aktualisierung eines Dateisystems.

Sie können kein Volume-Backup erstellen, wenn das Volume offline ist. Weitere Informationen finden Sie unter Backups und Offline-Volumes.

> **Note**
>
> Automatische tägliche Backups haben eine maximale Aufbewahrungsdauer von 90 Tagen, aber vom Benutzer initiierte Backups, die Sie erstellen, einschließlich Backups, die mit erstellt wurden AWS Backup, werden für immer aufbewahrt, sofern Sie oder der AWS Backup Dienst sie nicht löschen.

Sie können ein automatisches tägliches Backup mithilfe der Konsole, CLI und API manuell löschen. Wenn Sie ein Volume löschen, löschen Sie auch die automatischen täglichen Backups für dieses Volume. Amazon FSx bietet die Möglichkeit, eine endgültige Sicherung eines Volumes zu erstellen, bevor Sie es löschen. Das endgültige Backup wird für immer aufbewahrt, sofern Sie es nicht löschen. Weitere Informationen finden Sie unter. Löschen eines Backups

Arbeiten mit vom Benutzer initiierten Backups

Mit Amazon FSx können Sie mithilfe der API, und jederzeit manuell Backups der AWS Management Console Volumes Ihres Dateisystems erstellen. AWS CLI Ihre vom Benutzer initiierten Backups sind

im Vergleich zu anderen Backups, die möglicherweise für ein Volume erstellt wurden, inkrementell und werden für immer aufbewahrt, sofern Sie sie nicht löschen. Benutzerinitiierte Backups werden auch nach dem Löschen des Volumes oder des Dateisystems, auf dem die Backups erstellt wurden, beibehalten. Sie können vom Benutzer initiierte Backups nur mithilfe der Amazon FSx-Konsole, API oder CLI löschen. Sie werden niemals automatisch von Amazon FSx gelöscht. Weitere Informationen finden Sie unter Löschen eines Backups.

Sie können kein Volume-Backup erstellen, wenn das Volume offline ist. Weitere Informationen finden Sie unter Backups und Offline-Volumes.

Tags in Backups kopieren

Wenn Sie ein Volume mithilfe der CLI oder API erstellen oder aktualisieren, können Sie aktivieren, `CopyTagsToBackups` dass alle Tags auf Ihrem Volume automatisch in dessen Backups kopiert werden. Wenn Sie jedoch bei der Erstellung eines vom Benutzer initiierten Backups Tags hinzufügen, einschließlich der Benennung eines Backups, wenn Sie die Konsole verwenden, kopiert der Service keine Tags vom Volume, auch wenn `CopyTagsToBackups` es aktiviert ist.

Leistung Backup und wiederherstellen

Eine Vielzahl von Faktoren kann die Leistung von Sicherungs- und Wiederherstellungsvorgängen beeinflussen. Backup- und Wiederherstellungsvorgänge sind Hintergrundprozesse, was bedeutet, dass sie im Vergleich zu Client-I/O-Vorgängen eine niedrigere Priorität haben. Client-I/O-Operationen umfassen das Lesen und Schreiben von NFS-, CIFS- und iSCSI-Daten. Alle Hintergrundprozesse, einschließlich Sicherungs- und Wiederherstellungsvorgänge, nutzen nur den ungenutzten Teil der Durchsatzkapazität Ihres Dateisystems. Die Fertigstellung kann je nach Größe Ihres Backups und der Menge der ungenutzten Durchsatzkapazität in Ihrem Dateisystem zwischen einigen Minuten und einigen Stunden dauern.

Zu den weiteren Faktoren, die sich auf die Sicherungs- und Wiederherstellungsleistung auswirken, gehören die Speicherebene, in der Ihre Daten gespeichert sind, und das Datensatzprofil. Wir empfehlen, dass Sie die ersten Backups Ihrer Volumes erstellen, wenn sich die meisten Daten auf SSD-Speichern befinden. Datensätze, die hauptsächlich kleine Dateien enthalten, weisen in der Regel eine geringere Leistung auf als Datensätze ähnlicher Größe, die hauptsächlich große Dateien enthalten. Das liegt daran, dass die Verarbeitung einer großen Anzahl kleiner Dateien mehr CPU-Zyklen und Netzwerk-Overhead verbraucht als die Verarbeitung weniger großer Dateien.

Im Allgemeinen können Sie bei der Sicherung von Daten, die auf der SSD-Speicherebene gespeichert sind, mit den folgenden Sicherungsraten rechnen:

- 750 MBps bei mehreren gleichzeitigen Backups, die hauptsächlich große Dateien enthalten.
- 100 MBps über mehrere gleichzeitige Backups, die hauptsächlich kleine Dateien enthalten.

Im Allgemeinen können Sie mit den folgenden Wiederherstellungsraten rechnen:

- 250 MBps bei mehreren gleichzeitigen Wiederherstellungen, die hauptsächlich große Dateien enthalten.
- 100 MBps bei mehreren gleichzeitigen Wiederherstellungen, die hauptsächlich kleine Dateien enthalten.

Verwendung AWS Backup mit Amazon FSx

AWS Backup ist eine einfache und kostengünstige Möglichkeit, Ihre Daten zu schützen, indem Sie Ihre Amazon FSx for NetApp ONTAP-Volumes sichern. AWS Backup ist ein einheitlicher Backup-Service, der die Erstellung, Wiederherstellung und Löschung von Backups vereinfacht und gleichzeitig eine verbesserte Berichterstattung und Prüfung bietet. AWS Backup erleichtert die Entwicklung einer zentralen Backup-Strategie zur Einhaltung gesetzlicher, regulatorischer und beruflicher Vorschriften. AWS Backup erleichtert außerdem den Schutz Ihrer AWS Speichervolumes, Datenbanken und Dateisysteme, indem es einen zentralen Ort bereitstellt, an dem Sie Folgendes tun können:

- Konfigurieren und prüfen Sie die AWS Ressourcen, die Sie sichern möchten.
- Automatisieren geplanter Sicherungen
- Festlegen von Aufbewahrungsrichtlinien
- Überwachen Sie alle aktuellen Sicherungs-, Kopier- und Wiederherstellungsaktivitäten.

AWS Backup verwendet die integrierte Backup-Funktionalität von Amazon FSx. Backups, die mit der AWS Backup Konsole erstellt wurden, haben dieselbe Konsistenz und Leistung des Dateisystems, sind inkrementell im Vergleich zu allen anderen Amazon FSx-Backups, die Sie von Ihrem Volume erstellen (vom Benutzer initiiert oder automatisch), und bieten dieselben Wiederherstellungsoptionen wie Backups, die über die Amazon FSx-Konsole erstellt wurden. Wenn Sie AWS Backup diese Backups verwalten, erhalten Sie zusätzliche Funktionen, wie z. B. die Möglichkeit, geplante Backups so oft wie jede Stunde zu erstellen. Sie können eine zusätzliche Schutzebene hinzufügen, um Backups vor unbeabsichtigten oder böswilligen Löschungen zu schützen, indem Sie sie in einem Tresor speichern. AWS Backup

Backups, AWS Backup die von erstellt wurden, gelten als vom Benutzer initiierte Backups und werden auf das vom Benutzer initiierte Backup-Kontingent für Amazon FSx angerechnet. Weitere Informationen finden Sie unter Kontingente, die Sie erhöhen können. Sie können Backups, die AWS Backup in der Amazon FSx-Konsole, CLI und API erstellt wurden, anzeigen und wiederherstellen. Sie können jedoch keine Backups löschen, die AWS Backup in der Amazon FSx-Konsole, CLI oder API erstellt wurden. Weitere Informationen finden Sie unter Erste Schritte mit AWS Backup im AWS Backup Entwicklerhandbuch.

AWS Backup kann keine Volumes sichern, die offline sind.

Backups auf einem neuen Volume wiederherstellen

Sie können ein Volume-Backup auf einem neuen Volume wiederherstellen und so einen point-in-time Snapshot eines Volumes mithilfe der Konsole, CLI oder API effektiv wiederherstellen.

Bei der Wiederherstellung eines Backups werden zunächst alle Daten auf die SSD-Speicherebene geschrieben, bevor der Service beginnt, Daten gemäß der Tiering-Richtlinie, die Sie für das wiederhergestellte Volume festgelegt haben, dem Kapazitätspool-Speicher zuzuordnen. Bei der Wiederherstellung eines Backups auf einem Volume mit einer Tiering-Richtlinie von `All` werden die Daten in regelmäßigen Abständen im Hintergrund dem Kapazitätspool zugewiesen. Bei der Wiederherstellung eines Backups auf einem Volume mit einer Tiering-Richtlinie von `Snapshot Only` oder werden die Daten dem Kapazitätspool zugeordnet`Auto`, wenn die SSD-Auslastung für das Dateisystem mehr als 50% beträgt, und die Kühlrate wird durch die Kühlperiode der Tiering-Richtlinie bestimmt.

Wenn Sie ein FlexGroup Volume-Backup auf einem Dateisystem wiederherstellen, das über eine andere Anzahl von Hochverfügbarkeitspaaren (HA) verfügt als das ursprüngliche Dateisystem, fügt Amazon FSx möglicherweise zusätzliche konstituierende Volumes hinzu, um sicherzustellen, dass die Komponenten gleichmäßig verteilt sind.

step-by-step Anweisungen zum Wiederherstellen eines Backups auf einem neuen Volume finden Sie unter. Eine Sicherung auf einem neuen Volume wiederherstellen

> **Note**
>
> Ein wiederhergestelltes Volume hat immer denselben Volumestil wie das ursprüngliche Volume. Sie können den Lautstärkestil bei der Wiederherstellung nicht ändern.

Löschen eines Backups

Sie können automatische tägliche Backups und vom Benutzer initiierte Backups Ihrer Volumes löschen. Das Löschen eines Backups ist eine permanente, nicht wiederherstellbare Aktion. Alle Daten in einem gelöschten Backup werden ebenfalls gelöscht. Löschen Sie kein Backup, es sei denn, Sie sind sich sicher, dass Sie dieses Backup in future nicht mehr benötigen werden. Anweisungen zum Löschen von Backups finden Sie unterLöschen einer Sicherung.

Sie können keine Backups löschen AWS Backup, die mit der Amazon FSx-Konsole AWS Backup, CLI oder API erstellt wurden oder einen Typ haben. Informationen zum Löschen von Backups, die von erstellt wurden AWS Backup, finden Sie unter Löschen von Backups im AWS Backup Developer Guide.

Sie können die Sicherung eines Volumes nicht löschen, wenn das Volume offline ist. Weitere Informationen finden Sie unter Backups und Offline-Volumes.

> **Important**
>
> Löschen Sie nicht den allgemeinen Snapshot auf dem Volume, da er dazu dient, die Inkrementalität zwischen Ihren Backups aufrechtzuerhalten. Wenn Sie den gemeinsamen Snapshot auf dem Volume löschen, wird beim nächsten Backup das gesamte Volume gesichert und nicht nur ein inkrementelles Backup.

Backups und Offline-Volumes

Sie können keine Volume-Backups erstellen oder löschen, wenn das Volume offline ist. Verwenden Sie den `volume show`ONTAPCLI-Befehl, um den aktuellen Status und Status eines Volumes zu ermitteln.

Um ein Offline-Volume wieder online zu schalten, verwenden Sie den `volume online`ONTAPCLI-Befehl wie im folgenden Beispiel:

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

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

Erstellen eines vom Benutzer initiierten Backups

Das folgende Verfahren beschreibt, wie Sie mit der Amazon FSx-Konsole ein vom Benutzer initiiertes Backup eines Volumes erstellen.

Sie können kein Volume-Backup erstellen, wenn das Volume offline ist. Weitere Informationen finden Sie unter Backups und Offline-Volumes.

Um ein vom Benutzer initiiertes Backup eines Volumes (Konsole) zu erstellen

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Navigieren Sie zu Dateisysteme und wählen Sie das ONTAP Dateisystem aus, für das Sie ein Volume sichern möchten.
3. Wählen Sie die Registerkarte Volumes.
4. Wählen Sie das Volume aus, das Sie sichern möchten.
5. Wählen Sie unter Aktionen die Option Backup erstellen aus.
6. Geben Sie im sich öffnenden Dialogfeld „Backup erstellen“ einen Namen für Ihr Backup ein. Backup-Namen können maximal 256 Unicode-Zeichen enthalten, einschließlich Buchstaben, Leerzeichen, Zahlen und Sonderzeichen. + - = _:/
7. Wählen Sie Create backup (Backup erstellen).

Sie haben jetzt eine Sicherungskopie eines Volumes Ihres Dateisystems erstellt. Sie finden eine Tabelle mit all Ihren Backups in der Amazon FSx-Konsole, indem Sie in der linken Navigationsleiste Backups wählen. Sie können nach dem Namen suchen, den Sie Ihrem Backup gegeben haben, und die Tabelle filtern, um nur passende Ergebnisse anzuzeigen.

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.

Eine Sicherung auf einem neuen Volume wiederherstellen

Die folgenden Verfahren beschreiben, wie Sie ein FSx for ONTAP-Backup mit dem und auf einem neuen Volume wiederherstellen. AWS Management Console AWS CLI

So stellen Sie ein Volume-Backup auf einem neuen Volume wieder her (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.

2. Wählen Sie im Navigationsbereich Backups und dann das FSx for ONTAP-Volume-Backup aus, das Sie wiederherstellen möchten.
3. Wählen Sie im Aktionsmenü oben rechts die Option Backup wiederherstellen aus. Die Seite „Volume aus Backup erstellen“ wird angezeigt.
4. Wählen Sie aus den Dropdownmenüs das Dateisystem FSx for ONTAP und die virtuelle Storage-Maschine aus, auf der Sie das Backup wiederherstellen möchten.
5. Unter Volumendetails gibt es mehrere Auswahlmöglichkeiten. Geben Sie zunächst den Namen des Volumes ein. Sie können bis zu 203 alphanumerische Zeichen oder Unterstriche (_) verwenden.
6. Geben Sie für Volumengröße eine beliebige ganze Zahl im Bereich von 20—314572800 ein, um die Größe in Mebibyte (MiB) anzugeben.
7. Wählen Sie für Volumetyp die Option Lesen-Schreiben (RW), um ein Volumen zu erstellen, das lesbar und beschreibbar ist, oder Data Protection (DP), um ein Volume zu erstellen, das schreibgeschützt ist und als Ziel einer Oder-Beziehung verwendet werden kann. NetApp SnapMirror SnapVault Weitere Informationen finden Sie unter Volume-Typen.
8. Geben Sie für Junction Path einen Speicherort im Dateisystem ein, an dem das Volume bereitgestellt werden soll. Dem Namen muss beispielsweise `/vol3` ein Schrägstrich vorangestellt werden.
9. Wählen Sie für Speichereffizienz die Option Aktiviert, um die ONTAP Speichereffizienzfunktionen (Deduplizierung, Komprimierung und Komprimierung) zu aktivieren. Weitere Informationen finden Sie unter FSx für ONTAP-Speichereffizienz.
10. Wählen Sie für den Sicherheitsstil Volume entweder Unix (Linux), NTFS oder Mixed. Der Sicherheitsstil eines Volumes bestimmt, ob NTFS- oder UNIX-ACLs für den Zugriff über mehrere Protokolle bevorzugt werden. Der MIXED-Modus ist für den Zugriff über mehrere Protokolle nicht erforderlich und wird nur erfahrenen Benutzern empfohlen.
11. Wählen Sie unter Snapshot-Richtlinie eine Snapshot-Richtlinie für das Volume aus. Weitere Informationen zu Snapshot-Richtlinien finden Sie unterSnapshot-Richtlinien.

    Wenn Sie „Benutzerdefinierte Richtlinie“ wählen, müssen Sie den Namen der Richtlinie im Feld „Benutzerdefinierte Richtlinie“ angeben. Die benutzerdefinierte Richtlinie muss bereits auf der SVM oder im Dateisystem vorhanden sein. Sie können eine benutzerdefinierte Snapshot-Richtlinie mit der ONTAP CLI oder der REST-API erstellen. Weitere Informationen finden Sie in der NetApp ONTAP Produktdokumentation unter Erstellen einer Snapshot-Richtlinie.
12. Die gültigen Werte für die Kühlperiode der Tiering-Richtlinie liegen zwischen 2 und 183 Tagen. Die Abkühlperiode eines Volumes definiert die Anzahl der Tage, bevor Daten, auf die nicht

zugegriffen wurde, als kalt markiert und in den Capacity-Pool-Speicher verschoben werden. Diese Einstellung wirkt sich nur auf die `Snapshot-only` Richtlinien `Auto` und aus.

13. Im Bereich Erweitert können Sie unter SnapLockKonfiguration die Standardeinstellung Deaktiviert beibehalten oder Aktiviert wählen, um ein SnapLock Volume zu konfigurieren. Weitere Informationen zur Konfiguration eines SnapLock Compliance Volumes oder eines SnapLock Enterprise Volumes finden Sie unter Erstellen eines SnapLock Compliance-Volumes undErstellen eines SnapLock Enterprise-Volumes. Mehr über SnapLock erfahren Sie unter Schützen Ihrer Daten mit SnapLock.
14. Wählen Sie Bestätigen, um das Volume zu erstellen.

So stellen Sie ein Volume-Backup auf einem neuen Volume wieder her (CLI)

Verwenden Sie den create-volume-from-backupCLI-Befehl oder den entsprechenden CreateVolumeFromBackupAPI-Befehl, um ein Volume-Backup auf einem neuen Volume wiederherzustellen.

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

  Die Systemantwort für eine erfolgreiche Anfrage:

  ```
  {
        "Volume": {
            "CreationTime": 1692721488.428,
            "FileSystemId": "fs-07ab735385276ed60",
            "Lifecycle": "CREATING",
            "Name": "demo",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
                "JunctionPath": "/demo",
                "SizeInMegabytes": 100000,
                "StorageEfficiencyEnabled": true,
                "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
                "StorageVirtualMachineRoot": false,
                "TieringPolicy": {
                    "Name": "ALL"
                },
  ```
  ```

```
                "OntapVolumeType": "DP",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
            },
            "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
            "VolumeId": "fsvol-0b6ec764c9c5f654a",
            "VolumeType": "ONTAP",

        }
    }
```


Löschen einer Sicherung

Sie können automatische tägliche Backups und vom Benutzer initiierte Backups mithilfe der Amazon FSx-Konsole, CLI und API löschen, wie in den folgenden Verfahren beschrieben.

Informationen zum Löschen von Backups, die mit erstellt wurden AWS Backup, finden Sie unter Löschen von Backups im AWS Backup Entwicklerhandbuch.

So löschen Sie eine Sicherung (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Konsolen-Dashboard in der linken Navigationsleiste Backups aus.
3. Wählen Sie in der Tabelle Backups das Backup aus, das Sie löschen möchten, und wählen Sie dann Backup löschen aus.
4. Vergewissern Sie sich im sich öffnenden Dialogfeld „Backups löschen“, dass es sich bei der angezeigten Backup-ID um das Backup handelt, das Sie löschen möchten.
5. Vergewissern Sie sich, dass das Kontrollkästchen für das Backup, das Sie löschen möchten, aktiviert ist.
6. Wählen Sie Backups löschen.

Ihr Backup und alle enthaltenen Daten sind jetzt dauerhaft und unwiederbringlich gelöscht.

Um ein Backup zu löschen (CLI)

- Verwenden Sie den CLI-Befehl delete-backup oder die entsprechende DeleteBackup API-Aktion, um ein FSx for ONTAP-Volume-Backup zu löschen, wie im folgenden Beispiel gezeigt.

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

Die Systemantwort enthält die ID des Backups, das gelöscht wird, und seinen Lebenszyklusstatus, `DELETED` was darauf hinweist, dass die Anfrage erfolgreich war.

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

Arbeiten mit Snapshots

Ein Snapshot ist ein schreibgeschütztes Image eines Volumes von Amazon FSx für NetApp ONTAP zu einem bestimmten Zeitpunkt. Snapshots bieten Schutz vor versehentlichem Löschen oder Ändern von Dateien auf Ihren Volumes. Mit Snapshots können Ihre Benutzer problemlos einzelne Dateien oder Ordner aus einem früheren Snapshot anzeigen und wiederherstellen. Auf diese Weise können Benutzer Änderungen einfach rückgängig machen und Dateiversionen vergleichen.

Da Snapshots zusammen mit den Daten Ihres Dateisystems gespeichert werden, verbrauchen sie die Speicherkapazität des Dateisystems. Snapshots verbrauchen jedoch nur Speicherkapazität für die geänderten Dateiteile seit dem letzten Snapshot. Beachten Sie, dass Snapshots zum Zeitpunkt der Erstellung keine Kapazität verbrauchen. Snapshots, die in Ihrem Dateisystem gespeichert sind, sind nicht in Backups Ihrer Dateisystem-Volumes enthalten.

Snapshots sind standardmäßig auf Ihren Volumes mithilfe der Standard-Snapshot-Richtlinie aktiviert. Ihr FSx-für-ONTAP-Dateisystem verfügt über drei integrierte Snapshot-Richtlinien, aus denen Sie beim Erstellen oder Aktualisieren eines Volumes in der Amazon-FSx-Konsole AWS CLI, der oder der Amazon-FSx-API wählen können. Sie können auch eine benutzerdefinierte Snapshot-Richtlinie oder Snapshots auf Abruf mit der ONTAP-CLI oder REST-API erstellen. Snapshots werden im `.snapshot` Verzeichnis im Stammverzeichnis eines Volumes gespeichert. Sie können jederzeit bis zu 1 023 Snapshots pro Volume speichern. Sobald Sie dieses Limit erreicht haben, müssen Sie einen vorhandenen Snapshot löschen, bevor ein neuer Snapshot Ihres Volumes erstellt werden kann.

Themen

- Snapshot-Richtlinien
- Wiederherstellen einzelner Dateien und Ordner

- Wiederherstellen von Dateien aus Snapshots
- Löschen von Snapshots
- Erstellen einer Richtlinie zum automatischen Löschen von Snapshots
- Snapshot löschen
- Deaktivieren automatischer Snapshots
- Snapshot-Reservierung
- Aktualisieren der Snapshot-Reservierung des Volumes

Snapshot-Richtlinien

Die Snapshot-Richtlinie definiert, wie das System Snapshots für ein Volume erstellt. Die Richtlinie gibt an, wann Snapshots erstellt werden sollen, wie viele Kopien aufbewahrt werden sollen und wie sie benannt werden sollen. Es gibt drei integrierte Snapshot-Richtlinien für FSx für ONTAP:

- `default`
- `default-1weekly`
- `none`

Standardmäßig ist jedes Volume der `default` Snapshot-Richtlinie des Dateisystems zugeordnet. Wir empfehlen, diese Richtlinie für die meisten Workloads zu verwenden.

Die `default` Richtlinie erstellt automatisch Snapshots nach dem folgenden Zeitplan, wobei die ältesten Snapshot-Kopien gelöscht wurden, um Platz für neuere Kopien zu schaffen:

- Maximal sechs stündliche Snapshots, die fünf Minuten nach der Stunde aufgenommen wurden.
- Maximal zwei tägliche Snapshots, aufgenommen von Montag bis Samstag um 10 Minuten nach Mitternacht.
- Maximal zwei wöchentliche Snapshots, die jeden Sonntag um 15 Minuten nach Mitternacht aufgenommen werden.

> **Note**
>
> Snapshot-Zeiten basieren auf der Zeitzone des Dateisystems, die standardmäßig auf Coordinated Universal Time (UTC) festgelegt ist. Informationen zum Ändern der Zeitzone

finden Sie unter Anzeigen und Festlegen der Systemzeitzone in der NetApp Support-Dokumentation.

Die `default-1weekly` Richtlinie funktioniert auf die gleiche Weise wie die `default` Richtlinie, mit der Ausnahme, dass sie nur einen Snapshot aus dem wöchentlichen Zeitplan beibehält.

Die `none` Richtlinie erstellt keine Snapshots. Sie können diese Richtlinie Volumes zuweisen, um zu verhindern, dass automatische Snapshots erstellt werden.

Sie können eine benutzerdefinierte Snapshot-Richtlinie auch mit der ONTAP-CLI oder REST-API erstellen. Weitere Informationen finden Sie unter Erstellen einer Snapshot-Richtlinie in der NetApp ONTAP-Produktdokumentation. Sie können eine Snapshot-Richtlinie auswählen AWS CLI, während Sie ein Volume in der Amazon-FSx-Konsole, der oder der Amazon-FSx-API erstellen oder aktualisieren. Weitere Informationen finden Sie unter Volumen erstellen und Ein Volume aktualisieren.

Wiederherstellen einzelner Dateien und Ordner

Mithilfe der Snapshots auf Ihrem Amazon-FSx-Dateisystem können Ihre Benutzer schnell frühere Versionen einzelner Dateien oder Ordner wiederherstellen. Auf diese Weise können sie gelöschte oder geänderte Dateien wiederherstellen, die auf dem freigegebenen Dateisystem gespeichert sind. Sie tun dies auf Self-Service- Weise direkt auf ihrem Desktop ohne Administratorunterstützung. Dieser Self-Service-Ansatz erhöht die Produktivität und reduziert den administrativen Workload.

Linux- und macOS-Clients können Snapshots im `.snapshot` Verzeichnis im Stammverzeichnis eines Volumes anzeigen. Windows-Clients können Snapshots auf der `Previous Versions` Registerkarte von Windows Explorer anzeigen (wenn Sie mit der rechten Maustaste auf eine Datei oder einen Ordner klicken).

Wiederherstellen von Dateien aus Snapshots

So stellen Sie eine Datei aus einem Snapshot wieder her (Linux- und macOS-Clients)

1. Wenn die ursprüngliche Datei noch vorhanden ist und Sie nicht möchten, dass sie von der Datei in einem Snapshot überschrieben wird, verwenden Sie Ihren Linux- oder macOS-Client, um die ursprüngliche Datei umzubenennen oder in ein anderes Verzeichnis zu verschieben.
2. Suchen Sie im `.snapshot` Verzeichnis den Snapshot, der die Version der Datei enthält, die Sie wiederherstellen möchten.

3. Kopieren Sie die Datei aus dem `.snapshot` Verzeichnis in das Verzeichnis, in dem die Datei ursprünglich vorhanden war.

So stellen Sie eine Datei aus einem Snapshot wieder her (Windows-Clients)

Benutzer auf Windows-Clients können Dateien mithilfe der vertrauten Windows File Explorer-Oberfläche in früheren Versionen wiederherstellen.

1. Um eine Datei wiederherzustellen, wählen Benutzer die wiederherzustellende Datei und dann im Kontextmenü (rechte Maustaste) die Option Vorherige Versionen wiederherstellen aus.
2. Benutzer können dann eine frühere Version aus der Liste Frühere Versionen anzeigen und wiederherstellen.

Daten in Snapshots sind schreibgeschützt. Wenn Sie Änderungen an Dateien und Ordnern vornehmen möchten, die auf der Registerkarte Frühere Versionen aufgeführt sind, müssen Sie eine Kopie der Dateien und Ordner, die Sie ändern möchten, an einem beschreibbaren Speicherort speichern und Änderungen an den Kopien vornehmen.

Löschen von Snapshots

Snapshots sind schreibgeschützte Images eines früheren Status Ihres Volumes und sind standardmäßig auf allen FSx-für point-in-time -ONTAP-Volumes aktiviert, um Ihre Daten zu schützen. Snapshots verbrauchen Speicherkapazität nur für die Teile von Dateien, die sich seit dem letzten Snapshot geändert haben. Aus diesem Grund können Snapshots aus alten Daten einen erheblichen Teil der Kapazität Ihres Volumes in Anspruch nehmen, wenn Ihr Workload Daten schnell ändert.

Die zuvor bereitgestellte `volume show-space` Befehlsausgabe zeigt beispielsweise 140 KB von `User Data`. Das Volume hatte jedoch 9,8 GB, `User Data` bevor die Benutzerdaten gelöscht wurden. Auch wenn Sie die Dateien aus Ihrem Volume gelöscht haben, verweist ein Snapshot möglicherweise immer noch auf alte Benutzerdaten. Aus diesem Grund belegen `Snapshot Reserve` und `Snapshot Spill` im vorherigen Beispiel insgesamt 9,8 GB Speicherplatz, obwohl praktisch keine Benutzerdaten auf dem Volume vorhanden sind.

Um Speicherplatz auf Volumes freizugeben, können Sie ältere Snapshots löschen, die Sie nicht mehr benötigen. Erstellen Sie dazu eine Richtlinie zum automatischen Löschen von Snapshots oder löschen Sie Snapshots manuell. Durch das Löschen eines Snapshots werden die geänderten Daten gelöscht, die auf dem Snapshot gespeichert sind.

Erstellen einer Richtlinie zum automatischen Löschen von Snapshots

Sie können eine Richtlinie erstellen, um Snapshots automatisch zu löschen, wenn der verfügbare Speicherplatz in Ihrem Volume knapp wird. Verwenden Sie den folgenden Befehl, um eine Richtlinie zum automatischen Löschen für ein Volume einzurichten.

Bevor Sie diesen Befehl ausführen, ersetzen Sie die folgenden Werte:

- Ersetzen Sie durch *`svm_name`* den Namen der SVM, auf der das Volume erstellt wird.
- Ersetzen Sie *`vol_name`* durch den Namen des Volumes.

`-trigger`Weisen Sie für einen der folgenden Werte zu:

- `volume` – Wird verwendet, `volume` wenn der Schwellenwert, bei dem Snapshots gelöscht werden sollen, einem Kapazitätsschwellenwert für das gesamte verwendete Volumen entspricht. Die Schwellenwerte für die Kapazität des verwendeten Volumes, die das Löschen von Snapshots auslösen, werden durch die Größe Ihres Volumes bestimmt, wobei die Schwellenwertskalierung zwischen 85 und 98 Prozent der genutzten Kapazität liegt. Kleinere Volumes haben einen kleineren Schwellenwert und größere Volumes haben einen größeren.
- `snap_reserve` – Wird verwendet`snap_reserve`, wenn Sie möchten, dass Snapshots gelöscht werden, je nachdem, was in Ihrer Snapshot-Reservierung gespeichert werden kann.

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true
 -trigger [volume|snap_reserve]
```

Weitere Informationen finden Sie im NetApp ONTAP-Dokumentationscenter unter dem Befehl zum automatischen Löschen von Volume-Snapshots.

Snapshot löschen

Verwenden Sie den folgenden Befehl, um Snapshots manuell zu löschen. Bevor Sie diesen Befehl ausführen, ersetzen Sie die folgenden Werte:

- Ersetzen Sie durch *`svm_name`* den Namen der SVM, auf der das Volume erstellt wird.
- Ersetzen Sie *`vol_name`* durch den Namen des Volumes.

- Ersetzen Sie *snapshot_name* durch den Namen des Snapshots. Dieser Befehl unterstützt Platzhalterzeichen (*) für *snapshot_name*. Daher können Sie alle stündlichen Snapshots löschen, z. B. mithilfe von `hourly*`.

> **Important**
>
> Wenn Sie Amazon-FSx-Backups aktiviert haben, behält Amazon FSx einen Snapshot für die neueste Amazon-FSx-Backup jedes Volumes bei. Diese Snapshots werden verwendet, um die Inkrementalität zwischen Sicherungen aufrechtzuerhalten, und dürfen nicht mit dieser Methode gelöscht werden.

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

Weitere Informationen zum manuellen Löschen von Snapshots finden Sie unter dem volume snapshot delete Befehl im NetApp ONTAP Documentation Center .

Deaktivieren automatischer Snapshots

Automatische Snapshots werden durch die Standard-Snapshot-Richtlinie für Volumes in Ihrem FSx-für-ONTAP-Dateisystem aktiviert. Wenn Sie keine Snapshots Ihrer Daten benötigen (z. B. wenn Sie Testdaten verwenden), können Sie Snapshots deaktivieren, indem Sie die Snapshot-Richtlinie des Volumes none mithilfe der AWS Management Console, AWS CLI der - und -API und der -ONTAPCLI auf setzen, wie in den folgenden Verfahren beschrieben.

So deaktivieren Sie automatische Snapshots (AWS Management Console)

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Navigieren Sie zu Dateisysteme und wählen Sie das ONTAP-Dateisystem aus, für das Sie ein Volume aktualisieren möchten.
3. Wählen Sie die Registerkarte Volumes aus.
4. Wählen Sie das Volume aus, das Sie aktualisieren möchten.
5. Wählen Sie für Aktionen die Option Volume aktualisieren aus.

   Das Dialogfeld Volume aktualisieren wird mit den aktuellen Einstellungen des Volumes angezeigt.

6. Wählen Sie für Snapshot-Richtlinie die Option Keine aus.
7. Wählen Sie Aktualisieren, um das Volume zu aktualisieren.

So deaktivieren Sie automatische Snapshots (AWS CLI)

- Verwenden Sie den CLI-Befehl update-volume (oder die entsprechende UpdateVolume API-Operation), um `SnapshotPolicy` auf zu setzen`none`, wie im folgenden Beispiel gezeigt.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=none, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

So deaktivieren Sie automatische Snapshots (ONTAP CLI)

1. Verwenden Sie den folgenden Befehl, um die `none` Richtlinie anzuzeigen.

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                         Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ---------------------------------
none                             0 false   Policy for no automatic snapshots.
    Schedule               Count     Prefix                SnapMirror Label
    ---------------------- -----     --------------------- ------------------
    -                          -     -                     -
```

2. Um automatische Snapshots zu deaktivieren, fügen Sie die `none` Richtlinie mit dem folgenden Befehl zu Ihrem Volume hinzu.

   - Ersetzen Sie durch den Namen *`svm_name`* Ihrer SVM.
   - Ersetzen Sie *`vol_name`* durch den Namen Ihres Volumes.

   Wenn Sie aufgefordert werden, fortzufahren, geben Sie ein**y**.

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none

Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
 Snapshot copies on this volume
        that do not match any of the prefixes of the new Snapshot policy will not
 be deleted. However, when
        the new Snapshot policy takes effect, depending on the new retention
 count, any existing Snapshot copies
        that continue to use the same prefixes might be deleted. See the 'volume
 modify' man page for more information.
Do you want to continue? {y|n}: y
Volume modify successful on volume vol_name of Vserver svm_name.
```

Snapshot-Reservierung

Die Snapshot-Kopierreservierung legt einen bestimmten Prozentsatz des Speicherplatzes für das Speichern von Snapshot-Kopien fest. Die Standard-Snapshot-Kopierreservierung ist auf 5 Prozent des Speicherplatzes festgelegt. Wenn die Snapshot-Kopien den Reservierungsbereich überschreiten, werden sie in das aktive Dateisystem übertragen und dieser Prozess wird als Snapshot-Spill bezeichnet.

Der Snapshot-Kopierreservierung muss genügend Speicherplatz für die Snapshot-Kopien zugewiesen sein, einschließlich Volume-Backups. Wenn die Snapshot-Kopien den Reserveplatz überschreiten, müssen Sie die vorhandenen Snapshot-Kopien aus dem aktiven Dateisystem löschen, um den Speicherplatz für die Verwendung des Dateisystems wiederherzustellen. Sie können auch den Prozentsatz des Festplattenspeichers ändern, der Snapshot-Kopien zugewiesen ist.

Immer wenn Snapshots mehr als 100 % der Snapshot-Reserve verbrauchen, beginnen sie, primären SSD-Speicherplatz zu belegen. Dieser Prozess wird als Snapshot-Spill bezeichnet. Wenn die Snapshots weiterhin den aktiven Dateisystemspeicher belegen, besteht die Gefahr, dass das System voll wird. Wenn das System aufgrund von Snapshot-Spill voll wird, können Sie Dateien erst erstellen, nachdem Sie genügend Snapshots gelöscht haben.

Wenn genügend Speicherplatz für Snapshots in der Snapshot-Reserve verfügbar ist, gibt das Löschen von Dateien aus der primären SSD-Stufe Speicherplatz für neue Dateien frei, während die Snapshot-Kopien, die auf diese Dateien verweisen, nur den Speicherplatz in der Snapshot-Kopierreservierung beanspruchen.

Da es keine Möglichkeit gibt, zu verhindern, dass Snapshots Festplattenspeicher belegen, der größer ist als der für sie reservierte Speicherplatz (die Snapshot-Reservation), ist es wichtig, genügend Festplattenspeicher für Snapshots zu reservieren, damit die primäre SSD-Ebene immer Speicherplatz zur Verfügung hat, um neue Dateien zu erstellen oder vorhandene zu ändern.

Wenn ein Snapshot erstellt wird, wenn die Datenträger voll sind, erzeugt das Löschen von Dateien aus dem primären SSD-Kontingent keinen freien Speicherplatz, da auf alle diese Daten auch der neu erstellte Snapshot verwiesen wird. Sie müssen den Snapshot zuvor löschen, um Speicherplatz freizugeben, um Dateien erstellen oder aktualisieren zu können.

Sie können die Menge der Snapshot-Reservierung für ein Volume mithilfe der NetApp ONTAP CLI ändern. Weitere Informationen finden Sie unter Aktualisieren der Snapshot-Reservierung des Volumes.

Aktualisieren der Snapshot-Reservierung des Volumes

Sie können die Menge der Snapshot-Reservierung für ein Volume mithilfe der NetApp ONTAP CLI oder API ändern, wie im folgenden Verfahren beschrieben.

1. Um auf die NetApp ONTAP-CLI zuzugreifen, richten Sie eine SSH-Sitzung am Verwaltungsport des Dateisystems von Amazon FSx für NetApp ONTAP ein, indem Sie den folgenden Befehl ausführen. Ersetzen Sie durch *management_endpoint_ip* die IP-Adresse des Verwaltungsports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Verwenden Sie den `snap reserve` ONTAP-CLI-Befehl, um den Prozentsatz des Festplattenspeichers zu ändern, der für die Snapshot-Kopierreservierung verwendet wird. Ersetzen Sie *vol_name* durch den Namen des Volumes und *percent* `with the percent of disk space you want to reserve for Snapshot copies.`

   ```
   ::> snap reserve vol_name percent
   ```

   Im folgenden Beispiel wird die Snapshot-Reservation für vol1 auf 25 % der Volume-Speicherkapazität geändert.

   ```
   ::> snap reserve vol1 25
   ```

Geplante Replikation mit NetApp SnapMirror

Sie können verwenden NetApp SnapMirror , um die regelmäßige Replikation Ihres FSx-für-ONTAP-Dateisystems zu oder von einem zweiten Dateisystem zu planen. Diese Funktion ist sowohl für regionsinterne als auch für regionsübergreifende Bereitstellungen verfügbar.

NetApp SnapMirror repliziert Daten mit hohen Geschwindigkeiten, sodass Sie eine hohe Datenverfügbarkeit und eine schnelle Datenreplikation über ONTAP-Systeme hinweg erhalten, unabhängig davon AWS, ob Sie zwischen zwei Amazon-FSx-Dateisystemen in oder von On-Premises zu replizieren AWS. Die Replikation kann bis zu alle 5 Minuten geplant werden, obwohl Intervalle sorgfältig auf der Grundlage von RPOs (Recovery Point Objectives), RTOs (Recovery Time Objectives) und Leistungsüberlegungen ausgewählt werden sollten.

Wenn Sie Daten in NetApp Speichersysteme replizieren und die sekundären Daten kontinuierlich aktualisieren, werden Ihre Daten auf dem neuesten Stand gehalten und bleiben bei Bedarf verfügbar. Es sind keine externen Replikationsserver erforderlich. Weitere Informationen zur Verwendung von NetApp SnapMirror zum Replizieren Ihrer Daten finden Sie unter Erfahren Sie mehr über den Replikationsservice in der NetApp BlueXP-Dokumentation.

Sie können zusätzlich zur NetApp ONTAP-CLI und REST-API ein Ziel-Volume für NetApp SnapMirror den Datenschutz (DP) für mithilfe der Amazon-FSx-Konsole AWS CLI, der und der Amazon-FSx-API erstellen. Informationen zum Erstellen eines Ziel-Volumes mit der Amazon-FSx-Konsole und finden Sie AWS CLI unter Volumen erstellen.

Sie können NetApp BlueXP oder die NetApp ONTAP-CLI verwenden, um die Replikation für Ihr Dateisystem zu planen.

> **Note**
>
> Es gibt zwei Arten der SnapMirror Replikation: Volume-Ebene SnapMirror und SVM Disaster Recovery (SVMDR). Nur SnapMirror die Replikation auf Volume-Ebene wird von FSx für ONTAP unterstützt.

Verwenden von NetApp BlueXP zum Planen der Replikation

Sie können NetApp BlueXP verwenden, um die Replikation mit SnapMirror auf Ihrem FSx-für-ONTAP-Dateisystem einzurichten. Weitere Informationen finden Sie unter Replizieren von Daten zwischen Systemen in der NetApp BlueXP-Dokumentation.

Verwenden der NetApp ONTAP-CLI zum Planen der Replikation

Sie können die NetApp ONTAP-CLI verwenden, um die geplante Volume-Replikation zu konfigurieren. Weitere Informationen finden Sie unter Verwalten der SnapMirror Volume-Replikation im NetApp ONTAP-Dokumentationscenter.

Schützen Ihrer Daten mit SnapLock

SnapLock ist eine Funktion, mit der Sie Ihre Dateien schützen können, indem Sie sie in den Status „Write Once Read Many“ (WORM) überführen, wodurch Änderungen oder Löschungen für einen bestimmten Aufbewahrungszeitraum verhindert werden. Sie können verwendenSnapLock, um die Einhaltung gesetzlicher Vorschriften einzuhalten, geschäftskritische Daten vor Ransomware-Angriffen zu schützen und eine zusätzliche Schutzebene für Ihre Daten vor Änderung oder Löschung bereitzustellen.

Amazon FSx für NetApp ONTAP unterstützt die Aufbewahrungsmodi Compliance und Enterprise mit SnapLock. Weitere Informationen finden Sie unter SnapLock-Compliance und SnapLock Unternehmen.

Sie können SnapLock Volumes auf FSx-für-ONTAP-Dateisystemen erstellen, die am oder nach dem 13. Juli 2023 erstellt wurden. Bestehende Dateisysteme erhalten SnapLock Unterstützung während eines bevorstehenden wöchentlichen Wartungsfensters.

Themen

- Funktionsweise von SnapLock
- SnapLock-Compliance
- SnapLock Unternehmen
- Arbeiten mit dem Aufbewahrungszeitraum in SnapLock
- Übergeben von Dateien in den WORM-Status
- Sichern von SnapLock Volumes
- Löschen von SnapLock Volumes

Funktionsweise von SnapLock

SnapLock kann Ihnen helfen, regulatorische und Governance-Zwecke zu erfüllen, indem verhindert wird, dass Ihre Dateien gelöscht, geändert oder umbenannt werden. Wenn Sie ein SnapLock Volume

erstellen, führen Sie ein Commit für Ihre Dateien durch, um einmal zu schreiben, viele (WORM)-Speicher zu lesen und Aufbewahrungszeiträume für die Daten festzulegen. Ihre Dateien können für einen bestimmten Zeitraum oder auf unbestimmte Zeit in einem nicht beschreibbaren, nicht beschreibbaren Status gespeichert werden.

> **Important**
>
> Sie müssen angeben, ob ein Volume zum Zeitpunkt der Erstellung SnapLock Einstellungen verwendet. Ein Nicht-SnapLock--Volume kann nach der Erstellung nicht in ein SnapLock Volume konvertiert werden.

Aufbewahrungsmodi

SnapLock hat zwei Aufbewahrungsmodi: Compliance und Enterprise. Amazon FSx für NetApp ONTAP unterstützt beide. Sie haben unterschiedliche Anwendungsfälle und einige der Funktionen unterscheiden sich, aber beide schützen Ihre Daten mithilfe des WORM-Modells vor Änderung oder Löschung. In der folgenden Tabelle werden einige der Ähnlichkeiten und Unterschiede zwischen diesen Aufbewahrungsmodi erläutert.

SnapLock-Funktion	SnapLock-Compliance	SnapLock Unternehmen
Beschreibung	Dateien, die auf einem Compliance-Volume in WORM übertragen werden, können erst gelöscht werden, wenn ihre Aufbewahrungszeiträume abgelaufen sind.	Dateien, die auf einem Enterprise-Volume in WORM übertragen werden, können von autorisierten Benutzern gelöscht werden, bevor ihre Aufbewahrungszeiträume ablaufen, indem sie privilegi erte Löschungen verwenden.
Anwendungsfälle	• Um regierungs- oder branchenspezifische Vorgaben wie SEC Rule 17a-4(f), FINRA Rule 4511 und CFTC Rule 1.31 zu erfüllen.	• Um die Datenintegrität und interne Compliance einer Organisation zu fördern. • So testen Sie die Aufbewahr ungseinstellungen, bevor Sie SnapLock Compliance verwenden.

SnapLock-Funktion	SnapLock-Compliance	SnapLock Unternehmen
	• Zum Schutz vor Ransomware-Angriffen.	
Autocommit	Ja	Ja
Ereignisbasierte Aufbewahrung (EBR)*	Ja	Ja
Rechtliche Aufbewahrungsfrist*	Ja	Nein
Privilegiertes Löschen	Nein	Ja
Volume-Append-Modus	Ja	Ja
SnapLock -Auditprotokoll-Volumes	Ja	Ja

*EBR- und rechtliche Aufbewahrungsfristen werden in der ONTAP CLI und REST API unterstützt.

SnapLock-Administrator

Sie müssen über SnapLock Administratorrechte verfügen, um bestimmte Aktionen auf SnapLock Volumes ausführen zu können. -SnapLockAdministratorrechte sind in der `vsadmin-snaplock` Rolle in der ONTAP CLI definiert. Sie müssen ein Cluster-Administrator sein, um ein SVM-Administratorkonto (Storage Virtual Machine) mit der SnapLock Administratorrolle zu erstellen.

Sie können die folgenden Aktionen mit der `vsadmin-snaplock` Rolle in der ONTAP CLI ausführen:

- Verwalten Ihres eigenen Benutzerkontos, Ihres lokalen Passworts und Ihrer Schlüsselinformationen
- Verwalten von Volumes, außer Verschieben von Volumes
- Verwalten von Kontingenten, Qtrees, Snapshot-Kopien und Dateien
- Ausführen von SnapLock Aktionen, einschließlich privilegierter Löschung und gesetzlicher Aufbewahrungsfristen
- Konfigurieren der Protokolle Network File System (NFS) und Server Message Block (SMB)

- Konfigurieren von Domain Name System (DNS), Lightweight Directory Access Protocol (LDAP) und Network Information Service (NIS)-Services
- Aufträge überwachen

Im folgenden Verfahren wird beschrieben, wie Sie einen SnapLock Administrator in der ONTAP CLI erstellen. Sie müssen als Cluster-Administrator bei einer sicheren Verbindung angemeldet sein, z. B. Secure Shell Protocol (SSH), um diese Aufgabe ausführen zu können.

So erstellen Sie ein SVM-Administratorkonto mit der Rolle vsadmin-snaplock in der ONTAP CLI

- Führen Sie den folgenden Befehl aus. Ersetzen Sie *SVM_name* und *SnapLockAdmin* durch Ihre eigenen Informationen.

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

SnapLock -Auditprotokoll-Volumes

Ein SnapLock Audit-Protokoll-Volume enthält SnapLock Audit-Protokolle, die Zeitstempel von Ereignissen enthalten, z. B. wann ein SnapLock Administrator erstellt wurde, wann privilegierte Löschvorgänge ausgeführt wurden oder wann eine gesetzliche Aufbewahrungsfrist für Dateien festgelegt wurde. Das SnapLock Prüfprotokoll-Volume ist eine nicht löschbare Aufzeichnung von Ereignissen.

Sie müssen ein SnapLock Audit-Protokoll-Volume in derselben SVM wie das SnapLock Volume für die folgenden Aktionen erstellen:

- So aktivieren oder deaktivieren Sie das Löschen von Rechten auf einem SnapLock Enterprise-Volume.
- So wenden Sie die gesetzliche Aufbewahrungsfrist für eine Datei in einem SnapLock Compliance-Volume an.

Warning

- Der Mindestaufbewahrungszeitraum für ein SnapLock Prüfprotokoll-Volume beträgt sechs Monate. Bis zum Ablauf dieses Aufbewahrungszeitraums können das SnapLock Audit-Protokoll-Volume sowie die damit verknüpfte SVM und das Dateisystem nicht gelöscht werden, selbst wenn das Volume im SnapLock Enterprise-Modus erstellt wurde.
- Wenn eine Datei mit privilegiertem Löschen gelöscht wird und ihr Aufbewahrungszeitraum länger als der Aufbewahrungszeitraum des Volumes ist, erbt das Audit-Protokoll-Volume den Aufbewahrungszeitraum der Datei. Wenn beispielsweise eine Datei mit einem Aufbewahrungszeitraum von 10 Monaten mit privilegiertem Löschen gelöscht wird und der Aufbewahrungszeitraum des Audit-Protokoll-Volumes sechs Monate beträgt, wird der Aufbewahrungszeitraum des Audit-Protokoll-Volumes auf 10 Monate verlängert.

Sie können nur ein aktives SnapLock Audit-Protokoll-Volume in einer SVM haben, aber es kann von mehreren SnapLock Volumes in der SVM gemeinsam genutzt werden. Um ein SnapLock Audit-Protokoll-Volume erfolgreich zu mounten, legen Sie den Verbindungspfad auf fest/`snaplock_audit_log`. Es können keine anderen Volumes diesen Verbindungspfad verwenden, auch keine Volumes, bei denen es sich nicht um Audit-Protokoll-Volumes handelt.

Sie finden SnapLock Prüfungsprotokolle im -/`snaplock_log`Verzeichnis unter dem Stammverzeichnis des Prüfungsprotokoll-Volumes. Operationen zum privilegierten Löschen werden im `privdel_log` Unterverzeichnis protokolliert. Die Start- und Endvorgänge für rechtliche Aufbewahrungsfristen werden in protokolliert/`snaplock_log/legal_hold_logs/`. Alle anderen Protokolle werden im `system_log` Unterverzeichnis gespeichert.

Sie können ein SnapLock Audit-Protokoll-Volume mit der Amazon-FSx-Konsole, der AWS CLI, der Amazon-FSx-API sowie der ONTAP CLI und REST-API erstellen.

Note

Ein Data Protection (DP)-Volume kann nicht als SnapLock Audit-Protokoll-Volume verwendet werden.

Im folgenden Verfahren wird erläutert, wie Sie ein SnapLock Audit-Protokoll-Volume in der Amazon-FSx-Konsole erstellen.

So erstellen Sie ein SnapLock Audit-Protokoll-Volume in der Amazon-FSx-Konsole

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie den Anweisungen zum Erstellen eines neuen Volumes in Volumen erstellen.
3. Wählen Sie im Abschnitt Erweitert für SnapLock Konfiguration die Option Aktiviert aus.

   Aktivieren Sie das Kontrollkästchen, um die Warnung zum Aktivieren von SnapLock auf dem Volume zu bestätigen.
4. Wählen Sie für Audit-Protokoll-Volume die Option Aktiviert aus.

   Stellen Sie sicher, dass der Verbindungspfad auf festgelegt ist`/snaplock_audit_log`.
5. Folgen Sie den restlichen Schritten zum Erstellen eines neuen Volumes in Volumen erstellen.
6. Wählen Sie Bestätigen, um das Volume zu erstellen.

Um das SnapLock Audit-Protokoll-Volume mit der Amazon-FSx-API zu aktivieren, verwenden Sie `AuditLogVolume` in der `CreateSnaplockConfiguration`.

Zugreifen auf Ihre Daten in einem SnapLock Volume

Sie können offene Dateiprotokolle wie NFS und SMB verwenden, um auf Ihre Daten in einem SnapLock Volume zuzugreifen. Es gibt keine Auswirkungen auf die Leistung, wenn Daten auf ein SnapLock Volume geschrieben oder Daten gelesen werden, die durch WORM geschützt sind.

Sie können Dateien mit NFS und SMB über SnapLock Volumes hinweg kopieren, aber sie behalten ihre WORM-Eigenschaften nicht auf dem Ziel-SnapLockVolume bei. Sie müssen die kopierten Dateien erneut in WORM festschreiben, um zu verhindern, dass sie geändert oder gelöscht werden. Weitere Informationen finden Sie unter Übergeben von Dateien in den WORM-Status.

Sie können SnapLock Daten auch mit replizierenSnapMirror, aber die Quell- und Ziel-Volumes müssen SnapLock Volumes mit demselben Aufbewahrungsmodus sein (beide müssen beispielsweise Compliance oder Enterprise sein).

SnapLock-Compliance

Amazon FSx für NetApp ONTAP unterstützt SnapLock Compliance-Volumes.

Verwenden von SnapLock Compliance

In diesem Abschnitt werden Anwendungsfälle und Überlegungen für den Compliance-Aufbewahrungsmodus beschrieben.

Anwendungsfälle für SnapLock Compliance

Sie können den Compliance-Aufbewahrungsmodus für die folgenden Anwendungsfälle auswählen.

- Sie können SnapLock Compliance verwenden, um regierungs- oder branchenspezifische Vorgaben wie SEC Rule 17a-4(f), FINRA Rule 4511 und CFTC Rule 1.31 zu erfüllen. SnapLock Die Compliance mit Amazon FSx für NetApp ONTAP wurde anhand dieser Vorgaben und Vorschriften von bewertetCohasset Associates. Weitere Informationen finden Sie im Compliance-Bewertungsbericht für Amazon FSx für NetApp ONTAP.
- Sie können SnapLock Compliance verwenden, um eine umfassende Datenschutzstrategie zu ergänzen oder zu verbessern, um Ransomware-Angriffe zu verfälschen.

Überlegungen zur SnapLock Compliance

Hier sind einige wichtige Punkte, die Sie im Compliance-Aufbewahrungsmodus berücksichtigen sollten.

- Nachdem eine Datei einmal in den Status Schreiben, Lesen vieler (WORM) auf einem SnapLock Compliance-Volume übergegangen ist, kann sie nicht gelöscht werden, bevor ihr Aufbewahrungszeitraum von einem Benutzer abläuft.
- Ein SnapLock Compliance-Volume kann nur gelöscht werden, wenn die Aufbewahrungszeiträume aller WORM-Dateien auf dem Volume abgelaufen sind und die WORM-Dateien aus dem Volume gelöscht wurden.
- Sie können ein SnapLock Compliance-Volume nach der Erstellung nicht umbenennen.
- Sie können verwenden, SnapMirror um WORM-Dateien zu replizieren, aber das Quell- und das Ziel-Volume müssen denselben Aufbewahrungsmodus haben (z. B. müssen beide Compliance sein).
- Ein SnapLock Compliance-Volume kann nicht in ein SnapLock Enterprise-Volume konvertiert werden und umgekehrt.

Erstellen eines SnapLock Compliance-Volumes

Sie können ein SnapLock Compliance-Volume mit der Amazon-FSx-Konsole, der AWS CLI, der Amazon-FSx-API sowie der ONTAP CLI und REST-API erstellen.

Um ein SnapLock Compliance-Volume mit der Amazon-FSx-API zu erstellen, verwenden Sie `SnaplockType` in der `CreateSnaplockConfiguration`.

Im folgenden Verfahren wird erläutert, wie Sie ein SnapLock Compliance-Volume in der Amazon-FSx-Konsole erstellen.

So erstellen Sie ein SnapLock Compliance-Volume in der Amazon-FSx-Konsole

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie den Anweisungen zum Erstellen eines neuen Volumes in Volumen erstellen.
3. Wählen Sie im Abschnitt Erweitert für SnapLock Konfiguration die Option Aktiviert aus.

   Aktivieren Sie das Kontrollkästchen, um die Warnung zum Aktivieren von SnapLock auf dem Volume zu bestätigen.
4. Wählen Sie für Aufbewahrungsmodus Compliance aus.
5. Wählen Sie für Audit-Protokollvolumen zwischen Aktiviert und Deaktiviert aus.

   Wenn Sie Aktiviert wählen, stellen Sie sicher, dass der Verbindungspfad auf festgelegt ist/`snaplock_audit_log`.

   Weitere Informationen finden Sie unter SnapLock -Auditprotokoll-Volumes.
6. Geben Sie für Aufbewahrungszeitraum Werte für Standardaufbewahrung , Minimale Aufbewahrung und Maximale Aufbewahrung ein. Wählen Sie dann für jede Einheit eine entsprechende Einheit aus.

   Weitere Informationen finden Sie unter Arbeiten mit dem Aufbewahrungszeitraum in SnapLock.
7. Wählen Sie für Autocommit zwischen Aktiviert und Deaktiviert aus.

   Wenn Sie Aktiviert auswählen, geben Sie für Autocommit-Zeitraum einen Wert ein und wählen Sie eine entsprechende Autocommit-Einheit aus.

   Sie können einen Wert zwischen 5 Minuten und 10 Jahren angeben.

   Weitere Informationen finden Sie unter Autocommit.

8. Wählen Sie für Volume-Append-Modus zwischen Aktiviert und Deaktiviert aus.

   Weitere Informationen finden Sie unter Volume-Append-Modus.
9. Folgen Sie den restlichen Schritten zum Erstellen eines neuen Volumes in Volumen erstellen.
10. Wählen Sie Bestätigen, um das Volume zu erstellen.

SnapLock Unternehmen

Amazon FSx für NetApp ONTAP unterstützt SnapLock Enterprise-Volumes.

Verwenden von SnapLock Enterprise

In diesem Abschnitt werden Anwendungsfälle und Überlegungen für den Enterprise-Aufbewahrungsmodus beschrieben.

Anwendungsfälle für SnapLock Enterprise

Sie können den Enterprise-Aufbewahrungsmodus für die folgenden Anwendungsfälle wählen.

- Sie können SnapLock Enterprise verwenden, um nur bestimmte Benutzer zum Löschen von Dateien zu autorisieren.
- Sie können SnapLock Enterprise verwenden, um die Datenintegrität und interne Compliance Ihrer Organisation zu fördern.
- Sie können SnapLock Enterprise verwenden, um Aufbewahrungseinstellungen zu testen, bevor Sie SnapLock Compliance verwenden.

Überlegungen zur Verwendung von SnapLock Enterprise

Im Folgenden finden Sie einige wichtige Punkte, die Sie im Aufbewahrungsmodus für Unternehmen berücksichtigen sollten.

- Sie können verwenden, SnapMirror um WORM-Dateien zu replizieren, aber das Quell- und das Ziel-Volume müssen denselben Aufbewahrungsmodus haben (z. B. müssen beide Enterprise sein).
- Ein SnapLock Volume kann nicht von Enterprise in Compliance oder von Compliance in Enterprise konvertiert werden.
- SnapLock Enterprise unterstützt keine rechtliche Aufbewahrungsfrist.

Privilegiertes Löschen

Einer der wichtigsten Unterschiede zwischen SnapLock Enterprise und SnapLock Compliance besteht darin, dass ein SnapLock Administrator das privilegierte Löschen auf einem SnapLock Enterprise-Volume aktivieren kann, damit eine Datei gelöscht werden kann, bevor der Aufbewahrungszeitraum der Datei abläuft. Der SnapLock Administrator ist der einzige Benutzer, der Dateien aus einem SnapLock Enterprise-Volume löschen kann, auf dem aktive Aufbewahrungsrichtlinien festgelegt sind. Weitere Informationen finden Sie unter SnapLock-Administrator.

Sie können das Löschen von Rechten über die Amazon-FSx-Konsole, die AWS CLI, die Amazon-FSx-API sowie die ONTAP CLI und REST-API aktivieren oder deaktivieren. Um das Löschen von Rechten zu aktivieren, müssen Sie zunächst ein SnapLock Prüfprotokoll-Volume in derselben SVM wie das SnapLock Volume erstellen. Weitere Informationen finden Sie unter SnapLock - Auditprotokoll-Volumes.

Um das privilegierte Löschen mit der Amazon-FSx-API zu aktivieren, verwenden Sie `PrivilegedDelete` in der `CreateSnaplockConfiguration`.

Im folgenden Verfahren wird erläutert, wie Sie das Löschen von Rechten in der Amazon-FSx-Konsole aktivieren.

So aktivieren Sie das Löschen von Rechten auf einem SnapLock Enterprise-Volume in der Amazon-FSx-Konsole

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie den Anweisungen zum Erstellen eines neuen Volumes in Volumen erstellen.
3. Wählen Sie im Abschnitt Erweitert für SnapLock Konfiguration die Option Aktiviert aus.

   Aktivieren Sie das Kontrollkästchen, um die Warnung zum Aktivieren von SnapLock auf dem Volume zu bestätigen.
4. Wählen Sie für Aufbewahrungsmodus die Option Enterprise aus.
5. Wählen Sie für Privileged Delete die Option Aktiviert aus.
6. Folgen Sie den restlichen Schritten zum Erstellen eines neuen Volumes in Volumen erstellen.
7. Wählen Sie Bestätigen, um das Volume zu erstellen.

> **Note**
>
> Sie können keinen privilegierten Löschbefehl ausgeben, um eine Write Once Read Many (WORM)-Datei mit abgelaufenem Aufbewahrungszeitraum zu löschen. Sie können nach Ablauf des Aufbewahrungszeitraums einen normalen Löschvorgang ausführen.

Sie können privilegierte Löschungen dauerhaft deaktivieren, aber diese Aktion kann nicht rückgängig gemacht werden. Wenn das privilegierte Löschen dauerhaft deaktiviert ist, müssen Sie dem SnapLock Enterprise-Volume kein SnapLock Audit-Protokoll-Volume zugeordnet haben.

Um das Löschen von Rechten mit der Amazon-FSx-API dauerhaft zu deaktivieren, verwenden Sie `PrivilegedDelete` in der `CreateSnaplockConfiguration`.

So deaktivieren Sie das Löschen von Berechtigungen auf einem SnapLock Enterprise-Volume in der Amazon-FSx-Konsole dauerhaft

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie den Anweisungen zum Erstellen eines neuen Volumes in Volumen erstellen.
3. Wählen Sie im Abschnitt Erweitert für SnapLock Konfiguration die Option Aktiviert aus.

   Aktivieren Sie das Kontrollkästchen, um die Warnung zum Aktivieren von SnapLock auf dem Volume zu bestätigen.
4. Wählen Sie für Aufbewahrungsmodus die Option Enterprise aus.
5. Wählen Sie für Privilegiertes Löschen die Option Dauerhaft deaktiviert aus.
6. Folgen Sie den restlichen Schritten zum Erstellen eines neuen Volumes in Volumen erstellen.
7. Wählen Sie Bestätigen, um das Volume zu erstellen.

Erstellen eines SnapLock Enterprise-Volumes

Sie können ein SnapLock Enterprise-Volume mit der Amazon-FSx-Konsole, der AWS CLI, der Amazon-FSx-API sowie der ONTAP -CLI und REST-API erstellen.

Um ein SnapLock Unternehmens-Volume mit der Amazon-FSx-API zu erstellen, verwenden Sie `SnaplockType` in der `CreateSnaplockConfiguration`.

So erstellen Sie ein SnapLock Enterprise-Volume in der Amazon-FSx-Konsole

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie den Anweisungen zum Erstellen eines neuen Volumes in Volumen erstellen.
3. Wählen Sie im Abschnitt Erweitert für SnapLock Konfiguration die Option Aktiviert aus.

   Aktivieren Sie das Kontrollkästchen, um die Warnung zum Aktivieren von SnapLock auf dem Volume zu bestätigen.
4. Wählen Sie für Aufbewahrungsmodus die Option Enterprise aus.
5. Wählen Sie für Audit-Protokollvolumen zwischen Aktiviert und Deaktiviert aus.

   Wenn Sie Aktiviert wählen, stellen Sie sicher, dass der Verbindungspfad auf festgelegt ist`/snaplock_audit_log`.

   Weitere Informationen finden Sie unter SnapLock -Auditprotokoll-Volumes.
6. Geben Sie für Aufbewahrungszeitraum Werte für Standardaufbewahrung , Minimale Aufbewahrung und Maximale Aufbewahrung ein. Wählen Sie dann für jede Einheit eine entsprechende Einheit aus.

   Weitere Informationen finden Sie unter Arbeiten mit dem Aufbewahrungszeitraum in SnapLock.
7. Wählen Sie für Autocommit zwischen Aktiviert und Deaktiviert aus.

   Wenn Sie Aktiviert auswählen, geben Sie für Autocommit-Zeitraum einen Wert ein und wählen Sie eine entsprechende Autocommit-Einheit aus.

   Sie können einen Wert zwischen 5 Minuten und 10 Jahren angeben.

   Weitere Informationen finden Sie unter Autocommit.
8. Wählen Sie für Privileged Delete zwischen Aktiviert, Deaktiviert und Dauerhaft deaktiviert aus.

   Weitere Informationen finden Sie unter Privilegiertes Löschen.
9. Wählen Sie für Volume-Append-Modus zwischen Aktiviert und Deaktiviert aus.

   Weitere Informationen finden Sie unter Volume-Append-Modus.
10. Folgen Sie den restlichen Schritten zum Erstellen eines neuen Volumes in Volumen erstellen.
11. Wählen Sie Bestätigen, um das Volume zu erstellen.

Umgehen des Enterprise-Modus

Wenn Sie die Amazon-FSx-Konsole oder Amazon-FSx-API verwenden, müssen Sie über die IAM-`fsx:BypassSnapLockEnterpriseRetention`Berechtigung verfügen, ein SnapLock Enterprise-Volume zu löschen, das WORM-Dateien mit aktiven Aufbewahrungsrichtlinien enthält.

Weitere Informationen finden Sie unter Löschen von SnapLock Volumes.

Arbeiten mit dem Aufbewahrungszeitraum in SnapLock

Wenn Sie ein SnapLock Volume erstellen, können Sie einen Standardaufbewahrungszeitraum für das Volume festlegen, oder Sie können den Aufbewahrungszeitraum für Schreibvorgänge einmal festlegen und viele Dateien (WORM) explizit lesen. Während des Aufbewahrungszeitraums können Sie WORM-geschützte Dateien nicht löschen oder ändern. Der Aufbewahrungszeitraum wird verwendet, um die Aufbewahrungszeit zu berechnen. Wenn Sie beispielsweise eine Datei am 14. Juli 2023 in WORM übertragen und den Aufbewahrungszeitraum auf fünf Jahre festlegen, beträgt die Aufbewahrungszeit bis zum 14. Juli 2028 um Mitternacht.

Weitere Informationen zu WORM finden Sie unter Übergeben von Dateien in den WORM-Status.

Richtlinien für den Aufbewahrungszeitraum

Der Aufbewahrungszeitraum wird durch Werte bestimmt, die Sie den folgenden Parametern zuweisen:

- Standardaufbewahrung – Der Standardaufbewahrungszeitraum, der einer WORM-Datei zugewiesen wird, wenn Sie dafür keinen expliziten Aufbewahrungszeitraum angeben.
- Minimale Aufbewahrung – Der kürzeste Aufbewahrungszeitraum, der einer WORM-Datei zugewiesen werden kann.
- Maximale Aufbewahrung – Der längste Aufbewahrungszeitraum, der einer WORM-Datei zugewiesen werden kann.

> **Note**
>
> Selbst nach Ablauf des Aufbewahrungszeitraums können Sie eine WORM-Datei nicht mehr ändern. Sie können sie nur löschen oder einen neuen Aufbewahrungszeitraum festlegen, um den WORM-Schutz erneut zu aktivieren.

Sie können den Aufbewahrungszeitraum mit mehreren verschiedenen Zeiteinheiten angeben. In der folgenden Tabelle sind die spezifischen unterstützten Bereiche aufgeführt.

Typ	Wert	Hinweise
Sekunden	0 – 65 535	
Minuten	0 – 65 535	
Stunden	0–24	
Tage	0 – 365	
Monate	0 - 12	
Jahre	0–100	
Unendlich	-	Behält die Dateien für immer bei. Verfügbar für Standarda ufbewahrung , Maximale Aufbewahrung und Minimale Aufbewahrung .
Nicht angegeben*	-	Hält die Dateien, bis Sie einen Aufbewahrungszeitraum festlegen. Nur für die Standarda ufbewahrung verfügbar.

* Wenn Sie Dateien mit einem nicht angegebenen Aufbewahrungszeitraum in WORM übertragen, erhalten sie den minimalen Aufbewahrungszeitraum, der für das SnapLock Volume konfiguriert ist. Wenn Sie die WORM-geschützten Dateien auf einen absoluten Aufbewahrungszeitraum umstellen, muss der neue Aufbewahrungszeitraum größer sein als der Mindestzeitraum, den Sie zuvor für die Dateien festgelegt haben.

Abgelaufener Aufbewahrungszeitraum

Nachdem der Aufbewahrungszeitraum einer WORM-Datei abgelaufen ist, können Sie die Datei löschen oder einen neuen Aufbewahrungszeitraum festlegen, um den WORM-Schutz wieder zu aktivieren. WORM-Dateien werden nicht automatisch gelöscht, nachdem ihr Aufbewahrungszeitraum abgelaufen ist. Sie können den Inhalt einer WORM-Datei auch nach Ablauf des Aufbewahrungszeitraums nicht mehr ändern.

Festlegen des Aufbewahrungszeitraums eines SnapLock Volumes

Sie können den Aufbewahrungszeitraum eines SnapLock Volumes über die Amazon-FSx-Konsole, die AWS CLI, die Amazon-FSx-API sowie die ONTAP CLI und REST-API festlegen.

Verwenden Sie die `SnaplockRetentionPeriod` Konfiguration , um den Aufbewahrungszeitraum mit der Amazon-FSx-API festzulegen.

Im folgenden Verfahren wird erläutert, wie Sie den Aufbewahrungszeitraum in der Amazon-FSx-Konsole festlegen.

So legen Sie den Aufbewahrungszeitraum eines SnapLock Volumes in der Amazon-FSx-Konsole fest

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie den Anweisungen zum Erstellen eines neuen Volumes in Volumen erstellen.
3. Wählen Sie im Abschnitt Erweitert für SnapLock Konfiguration die Option Aktiviert aus.

   Aktivieren Sie das Kontrollkästchen, um die Warnung zum Aktivieren von SnapLock auf dem Volume zu bestätigen.
4. Geben Sie für Aufbewahrungszeitraum Werte für Standardaufbewahrung , Minimale Aufbewahrung und Maximale Aufbewahrung ein. Wählen Sie dann für jede Einheit eine entsprechende Einheit aus.
5. Folgen Sie den restlichen Schritten zum Erstellen eines neuen Volumes in Volumen erstellen.
6. Wählen Sie Bestätigen, um das Volume zu erstellen.

Übergeben von Dateien in den WORM-Status

In diesem Abschnitt wird erläutert, wie Sie Ihre Dateien in den Status Schreiben einmal lesen, viele lesen (WORM) überführen können. Außerdem wird der Volume-Append-Modus erörtert, bei dem Daten inkrementell in WORM-geschützte Dateien geschrieben werden.

Autocommit

Sie können Autocommit verwenden, um Dateien in WORM zu übertragen, wenn sie für einen von Ihnen angegebenen Zeitraum nicht geändert wurden. Sie können Autocommit über die Amazon-FSx-Konsole, die AWS CLI, die Amazon-FSx-API sowie die ONTAP CLI und REST-API aktivieren.

Sie können einen Autocommit-Zeitraum zwischen fünf Minuten und 10 Jahren angeben. In der folgenden Tabelle sind die spezifischen unterstützten Bereiche aufgeführt.

Einheit	Wert
Minuten	5–65 535
Stunden	1 – 65 535
Tage	1 – 3 650
Monate	1 – 120
Jahre	1 – 10

Um Autocommit mit der Amazon-FSx-API zu aktivieren, verwenden Sie `AutocommitPeriod` in der `CreateSnaplockConfiguration`.

Im folgenden Verfahren wird erläutert, wie Sie Autocommit auf der Amazon-FSx-Konsole aktivieren.

So aktivieren Sie Autocommit in der Amazon-FSx-Konsole

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie den Anweisungen zum Erstellen eines neuen Volumes in Volumen erstellen.
3. Wählen Sie im Abschnitt Erweitert für SnapLock Konfiguration die Option Aktiviert aus.

   Aktivieren Sie das Kontrollkästchen, um die Warnung zum Aktivieren von SnapLock auf dem Volume zu bestätigen.
4. Wählen Sie für Autocommit die Option Aktiviert aus.
5. Geben Sie für Autocommit-Zeitraum einen Wert ein und wählen Sie eine entsprechende Autocommit-Einheit aus.

   Sie können einen Wert zwischen 5 Minuten und 10 Jahren angeben.

6. Folgen Sie den restlichen Schritten zum Erstellen eines neuen Volumes in Volumen erstellen.
7. Wählen Sie Bestätigen, um das Volume zu erstellen.

Volume-Append-Modus

Sie können vorhandene Daten in einer WORM-geschützten Datei nicht ändern. SnapLock Mit können Sie jedoch den Schutz für vorhandene Daten mithilfe von WORM-anfügbaren Dateien aufrechterhalten. Sie können beispielsweise Protokolldateien generieren oder Audio- oder Video-Streaming-Daten beibehalten, während Sie Daten inkrementell in sie schreiben. Sie können den Volume-Append-Modus mit der Amazon-FSx-Konsole, der AWS CLI, der Amazon-FSx-API sowie der ONTAP CLI und REST-API aktivieren oder deaktivieren.

Anforderungen für die Aktualisierung des Volume-Append-Modus

- Das SnapLock Volume muss nicht gemountet werden.
- Das SnapLock Volume muss keine Snapshot-Kopien und Benutzerdaten enthalten.

Um den Volume-Append-Modus mit der Amazon-FSx-API zu aktivieren, verwenden Sie `VolumeAppendModeEnabled` in der `CreateSnaplockConfiguration`.

Im folgenden Verfahren wird erläutert, wie Sie den Volume-Append-Modus auf der Amazon-FSx-Konsole aktivieren.

So aktivieren Sie den Volume-Append-Modus in der Amazon-FSx-Konsole

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie den Anweisungen zum Erstellen eines neuen Volumes in Volumen erstellen.
3. Wählen Sie im Abschnitt Erweitert für SnapLock Konfiguration die Option Aktiviert aus.

   Aktivieren Sie das Kontrollkästchen, um die Warnung zum Aktivieren von SnapLock auf dem Volume zu bestätigen.
4. Wählen Sie für Volume-Append-Modus die Option Aktiviert aus.
5. Folgen Sie den restlichen Schritten zum Erstellen eines neuen Volumes in Volumen erstellen.
6. Wählen Sie Bestätigen, um das Volume zu erstellen.

Ereignisbasierte Aufbewahrung (EBR)

Sie können die ereignisbasierte Aufbewahrung (EBR) verwenden, um benutzerdefinierte Richtlinien mit zugehörigen Aufbewahrungszeiträumen zu erstellen. Sie können beispielsweise alle Dateien in einem angegebenen Pfad in WORM übertragen und den Aufbewahrungszeitraum für ein Jahr mit den `snaplock event-retention apply` Befehlen `snaplock event-retention policy create` und festlegen. Wenn Sie EBR verwenden, müssen Sie ein Volume, ein Verzeichnis oder eine Datei angeben. Der Aufbewahrungszeitraum, den Sie beim Erstellen der EBR-Richtlinie auswählen, wird auf alle Dateien im angegebenen Pfad angewendet.

EBR wird von der ONTAP CLI und der REST-API unterstützt.

> **Note**
>
> ONTAP unterstützt EBR mit - FlexGroup Volumes nicht.

In den folgenden Verfahren wird erläutert, wie Sie eine EBR-Richtlinie erstellen, anwenden, ändern und löschen. Sie müssen SnapLock Administrator sein (die `vsadmin-snaplock` Rolle haben), um diese Aufgaben in der ONTAP CLI ausführen zu können. Weitere Informationen finden Sie unter SnapLock-Administrator.

So erstellen Sie eine EBR-Richtlinie in der ONTAP CLI

Führen Sie den folgenden Befehl aus. Ersetzen Sie *p1* und *„10 Jahre“* durch Ihre eigenen Informationen.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

So wenden Sie eine EBR-Richtlinie in der ONTAP CLI an

Führen Sie den folgenden Befehl aus. Ersetzen Sie *p1* und *slc* durch Ihre eigenen Informationen. Sie können einen Pfad nach dem Schrägstrich (/) hinzufügen, wenn Sie einen bestimmten Pfad für die EBR-Richtlinie angeben möchten. Andernfalls wendet dieser Befehl die EBR-Richtlinie auf alle Dateien auf dem Volume an.

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

So ändern Sie eine EBR-Richtlinie in der ONTAP CLI

Führen Sie den folgenden Befehl aus. Ersetzen Sie *p1* und *„5 Jahre“* durch Ihre eigenen Informationen.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

So löschen Sie eine EBR-Richtlinie in der ONTAP CLI

Führen Sie den folgenden Befehl aus. Ersetzen Sie *p1* durch Ihre eigenen Informationen.

```
vs1::> snaplock event-retention policy delete -name p1
```

Verwandte Befehle im NetApp Documentation Center :

- Abbruch der Snaplock-Ereignisaufbewahrung
- Snaplock-Ereignisaufbewahrung: show-vservers
- Anzeige der Snaplock-Ereignisaufbewahrung
- Snaplock-Ereignisaufbewahrungsrichtlinie anzeigen

Rechtliche Aufbewahrungsfrist

Sie können WORM-Dateien für einen unbestimmten Zeitraum aufbewahren, indem Sie die gesetzliche Aufbewahrungsfrist verwenden. Die gesetzliche Aufbewahrungsfrist wird in der Regel zu Zwecken der Telefonie verwendet. Eine WORM-Datei, die einer gesetzlichen Aufbewahrungsfrist unterliegt, kann erst gelöscht werden, wenn die gesetzliche Aufbewahrungsfrist aufgehoben wurde.

Die gesetzliche Aufbewahrungsfrist wird von der ONTAP CLI und der REST-API unterstützt.

> **Note**
>
> ONTAP unterstützt keine gesetzliche Aufbewahrungsfrist bei - FlexGroup Volumes.

In den folgenden Verfahren wird erläutert, wie Sie eine gesetzliche Aufbewahrungsfrist starten und beenden. Sie müssen SnapLock Administrator sein (die `vsadmin-snaplock` Rolle haben), um diese Aufgaben in der ONTAP CLI ausführen zu können. Weitere Informationen finden Sie unter SnapLock-Administrator.

So starten Sie eine rechtliche Aufbewahrungsfrist für eine Datei in einem SnapLock Compliance-Volume mit der ONTAP CLI

Führen Sie den folgenden Befehl aus. Ersetzen Sie *microSD1*, *slc_vol1* und *file1* durch Ihre eigenen Informationen.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

So starten Sie eine rechtliche Aufbewahrungsfrist für alle Dateien in einem SnapLock Compliance-Volume mit der ONTAP CLI

Führen Sie den folgenden Befehl aus. Ersetzen Sie *microSD1* und *slc_vol1* durch Ihre eigenen Informationen.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -path /
```

So beenden Sie eine rechtliche Aufbewahrungsfrist für eine Datei in einem SnapLock Compliance-Volume mit der ONTAP CLI

Führen Sie den folgenden Befehl aus. Ersetzen Sie *microSD1*, *slc_vol1* und *file1* durch Ihre eigenen Informationen.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

So beenden Sie eine rechtliche Aufbewahrungsfrist für alle Dateien in einem SnapLock Compliance-Volume mit der ONTAP CLI

Führen Sie den folgenden Befehl aus. Ersetzen Sie *microSD1* und *slc_vol1* durch Ihre eigenen Informationen.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -path /
```

> **Note**
>
> Wir empfehlen Ihnen, die `-operation-status` mit dem `snaplock legal-hold show` Befehl zu überwachen, wenn Sie eine gesetzliche Aufbewahrungsfrist ausgeben, um sicherzustellen, dass sie nicht fehlschlägt.

Verwandte Befehle im NetApp Documentation Center :

- Snaplock-Abbruch aufgrund gesetzlicher Aufbewahrungsfristen
- Snaplock-Dump-Dateien für rechtliche Aufbewahrungsfristen
- Snaplock-Dump-Litigationen für rechtliche Aufbewahrungsfristen
- Snaplock-Anzeige für rechtliche Aufbewahrungsfristen

Sichern von SnapLock Volumes

Sie können SnapLock Volumes für zusätzlichen Datenschutz sichern. Wenn Sie ein SnapLock Volume wiederherstellen, bleiben die ursprünglichen Einstellungen des Volumes, wie z. B. die Standardaufbewahrung, die Mindestaufbewahrung und die maximale Aufbewahrung, erhalten. Einmal schreiben, viele lesen (WORM)-Einstellungen und gesetzliche Aufbewahrungsfristen werden ebenfalls beibehalten.

> **Note**
>
> Sie können ein SnapLock FlexGroup Volume nicht sichern.

Sie können die Sicherung eines SnapLock Volumes als - SnapLock oder Nicht--SnapLockVolume wiederherstellen. Sie können die Sicherung eines Nicht--SnapLock-Volumes jedoch nicht als SnapLock Volume wiederherstellen.

Weitere Informationen über Sicherungen finden Sie unter Arbeiten mit Backups.

Löschen von SnapLock Volumes

Sie können ein SnapLock Compliance-Volume löschen, wenn die Aufbewahrungszeiträume aller Schreibvorgänge einmal ablaufen und viele Dateien (WORM) darauf lesen.

> **Note**
>
> Wenn Sie ein schließen, AWS-Konto das - SnapLock Enterprise oder -ComplianceVolumes enthält, AWS und FSx für ONTAP Ihr Konto 90 Tage lang aussetzen, während Ihre Daten intakt bleiben. Wenn Sie Ihr Konto während dieser 90 Tage nicht wieder eröffnen, AWSlöscht Ihre Daten einschließlich Daten in SnapLock Volumes, unabhängig von Ihren Aufbewahrungseinstellungen.

Sie können ein SnapLock Enterprise-Volume jederzeit löschen, wenn Sie über die entsprechenden Berechtigungen verfügen. Sie müssen ein Amazon-FSx-Administrator sein. Unabhängig davon, ob Sie die Amazon-FSx-Konsole oder die Amazon-FSx-API verwenden, benötigen Sie außerdem die IAM`fsx:BypassSnapLockEnterpriseRetention`-IAM-Berechtigung zum Löschen eines SnapLock Enterprise-Volumes, das WORM-Daten mit einer aktiven Aufbewahrungsrichtlinie enthält.

> **Warning**
>
> Der Mindestaufbewahrungszeitraum für ein SnapLock Prüfprotokoll-Volume beträgt sechs Monate. Bis zum Ablauf dieses Aufbewahrungszeitraums können Sie das SnapLock Audit-Protokoll-Volume, die virtuelle Speichermaschine (SVM) oder das Dateisystem, das der SVM zugeordnet ist, nicht löschen – auch wenn das Volume im SnapLock Enterprise-Modus erstellt wurde. Weitere Informationen finden Sie unter SnapLock -Auditprotokoll-Volumes.

So löschen Sie ein SnapLock Enterprise-Volume in der Amazon-FSx-Konsole

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich Volumes aus.
3. Wählen Sie das Volume aus, das Sie löschen möchten.
4. Wählen Sie unter Aktionen die Option Volume löschen aus.
5. Wählen Sie für SnapLock Unternehmensaufbewahrung umgehen die Option Ja aus.
6. Wählen Sie im Bestätigungsdialogfeld eine der folgenden Optionen für Abschließende Sicherung erstellen aus:
   - Wählen Sie Ja, um ein endgültiges Backup des Volumes zu erstellen. Der Name des endgültigen Backups wird angezeigt.
   - Wählen Sie Nein, wenn Sie keine endgültige Sicherung des Volumes wünschen. Sie werden aufgefordert, zu bestätigen, dass nach dem Löschen des Volumes keine automatischen Backups mehr verfügbar sind.
7. Bestätigen Sie das Löschen des Volumes, indem Sie **`delete`** in das Feld Löschen bestätigen eingeben.
8. Wählen Sie Volume(s) löschen aus.

Arbeiten mit Microsoft Active Directory in FSx für ONTAP

Amazon FSx arbeitet mit Microsoft Active Directory zusammen, um in Ihre vorhandenen Umgebungen zu integrieren. Active Directory ist der Microsoft-Verzeichnisservice, der verwendet wird, um Informationen über Objekte im Netzwerk zu speichern und Administratoren und Benutzern zu helfen, diese Informationen zu finden und zu verwenden. Zu diesen Objekten gehören in der Regel gemeinsam genutzte Ressourcen wie Dateiserver und Netzwerkbenutzer- und Computerkonten.

Sie können optional Ihre virtuellen Speichermaschinen (SVMs) von FSx für ONTAP mit Ihrer Active-Directory-Domain verbinden, um Benutzerauthentifizierung und Zugriffskontrolle auf Datei- und Ordnerebene bereitzustellen. Server Message Block (SMB)-Clients können sich dann mit ihren vorhandenen Benutzeridentitäten in Active Directory authentifizieren und auf SVM-Volumes zugreifen. Ihre Benutzer können ihre vorhandenen Identitäten verwenden, um den Zugriff auf einzelne Dateien und Ordner zu steuern. Darüber hinaus können Sie Ihre vorhandenen Dateien und Ordner und ihre Konfigurationen für die Sicherheitszugriffssteuerungsliste (ACL) ohne Änderungen zu Amazon FSx migrieren.

Wenn Sie Amazon FSx für NetApp ONTAP mit einem Active Directory verbinden, verbinden Sie die SVMs des Dateisystems unabhängig mit dem Active Directory. Das bedeutet, dass Sie ein Dateisystem mit einigen SVMs haben können, die mit einem Active Directory verbunden sind, und anderen SVMs, die dies nicht tun.

Nachdem eine SVM mit einem Active Directory verbunden wurde, können Sie die folgenden Active-Directory-Konfigurationseigenschaften aktualisieren:

- IP-Adressen des DNS-Servers
- Benutzername und Passwort des selbstverwalteten Active-Directory-Servicekontos

Themen

- Voraussetzungen für das Verbinden einer SVM mit einem selbstverwalteten Microsoft AD
- Bewährte Methoden für die Arbeit mit Active Directory
- Verbinden von SVMs mit einem Microsoft Active Directory
- Verwalten von SVM-Active-Directory-Konfigurationen

Voraussetzungen für das Verbinden einer SVM mit einem selbstverwalteten Microsoft AD

Bevor Sie eine FSx for ONTAP SVM mit einer selbstverwalteten Microsoft AD-Domain verbinden, stellen Sie sicher, dass Ihr Active Directory und Netzwerk die in den folgenden Abschnitten beschriebenen Anforderungen erfüllen.

Themen

- On-Premises-Active-Directory-Anforderungen
- Anforderungen an die Netzwerkkonfiguration
- Anforderungen an Active-Directory-Servicekonten

On-Premises-Active-Directory-Anforderungen

Stellen Sie sicher, dass Sie bereits über ein On-Premises- oder ein anderes selbstverwaltetes Microsoft AD verfügen, mit dem Sie die SVM verbinden können. Dieses Active Directory sollte die folgende Konfiguration haben:

- Die Funktionsebene der Active-Directory-Domain-Controller-Domain befindet sich auf Windows Server 2000 oder höher.
- Das Active Directory verwendet einen Domänennamen, der nicht im SLD-Format (Single Label Domain) vorliegt. Amazon FSx unterstützt keine SLD-Domänen.
- Wenn Sie Active-Directory-Standorte definiert haben, stellen Sie sicher, dass die Subnetze in der VPC, die Ihrem FSx-für-ONTAP-Dateisystem zugeordnet sind, an denselben Active-Directory-Standorten definiert sind und dass keine Konflikte zwischen Ihren VPC-Subnetzen und den Subnetzen an Ihren Active-Directory-Standorten bestehen.

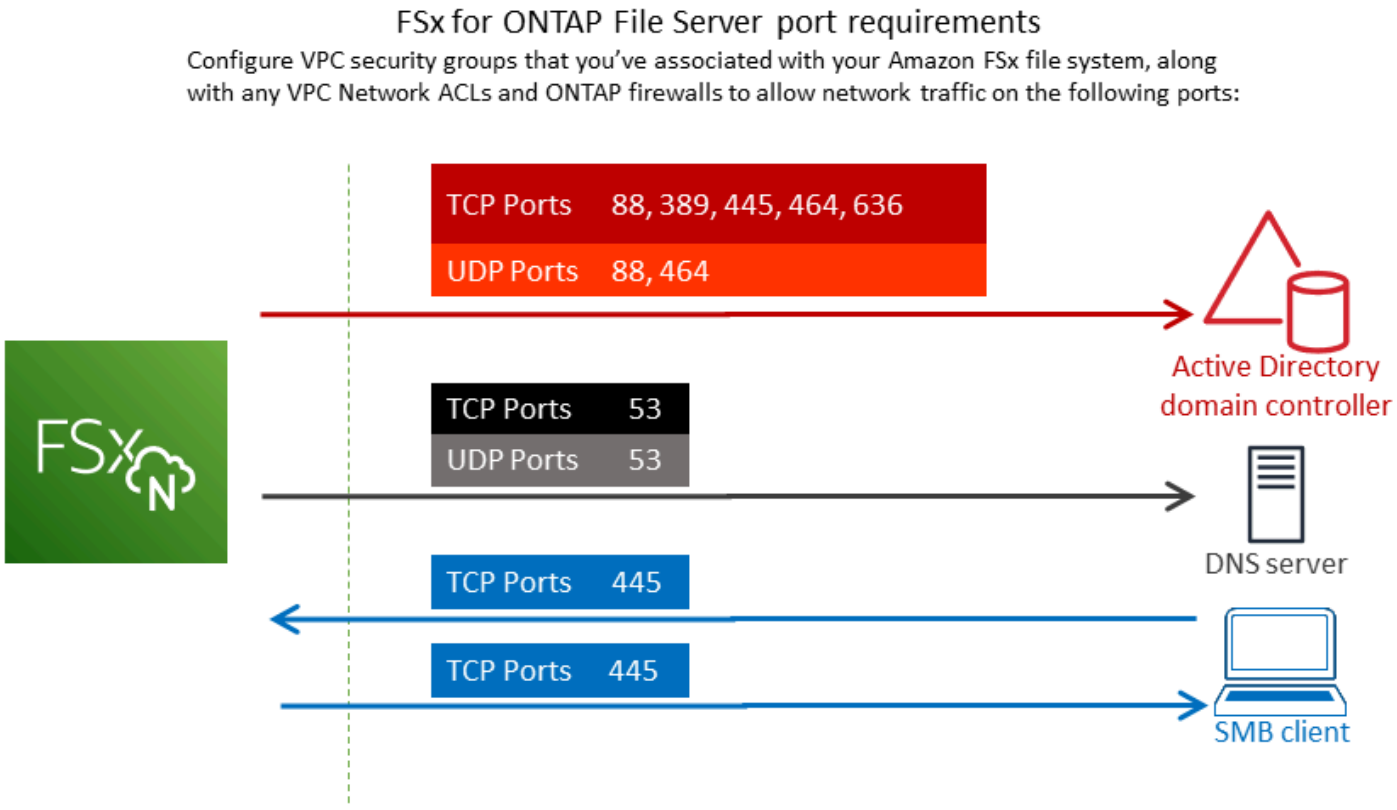
> **Note**
>
> Wenn Sie verwenden AWS Directory Service, unterstützt FSx für ONTAP das Verbinden von SVMs mit dem Simple Active Directory nicht.

Anforderungen an die Netzwerkkonfiguration

Stellen Sie sicher, dass Sie über die folgenden Netzwerkkonfigurationen und die zugehörigen Informationen verfügen.

> **Important**
>
> Damit eine SVM Active Directory beitreten kann, müssen Sie sicherstellen, dass die in diesem Thema dokumentierten Ports Datenverkehr zwischen allen Active Directory Domain Controllern und sowohl iSCSI-IP-Adressen (iscsi_1 und iscsi_2 logical interfaces (LIFs)) auf der SVM zulassen.

- Die IP-Adressen des DNS-Servers und des Active-Directory-Domain-Controllers.
- Konnektivität zwischen der Amazon VPC, in der Sie das Dateisystem erstellenAWS Direct Connect, und Ihrem selbstverwalteten Active Directory mit AWS VPN, oder AWS Transit Gateway.
- Die Sicherheitsgruppe und die VPC-Netzwerk-ACLs für die Subnetze, in denen Sie das Dateisystem erstellen, müssen Datenverkehr an den Ports und in den im folgenden Diagramm gezeigten Richtungen zulassen.



Die Rolle der einzelnen Ports wird in der folgenden Tabelle beschrieben.

Protokoll	Ports	Rolle
TCP/UDP	53	Domain Name System (DNS)
TCP/UDP	88	Kerberos-Authentifizierung
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)
TCP	445	Directory-Services-SMB-Dateifreigabe
TCP/UDP	464	Passwort ändern/festlegen
TCP	636	Lightweight Directory Access Protocol über TLS/SSL (LDAPS)

- Diese Datenverkehrsregeln sollten auch in den Firewalls gespiegelt werden, die für jeden der Active-Directory-Domain-Controller, 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.

Anforderungen an Active-Directory-Servicekonten

Stellen Sie sicher, dass Sie in Ihrem selbstverwalteten Microsoft AD über ein Servicekonto verfügen, das über delegierte Berechtigungen zum Verbinden von Computern mit der Domain verfügt. Ein Servicekonto ist ein Benutzerkonto in Ihrem selbstverwalteten Active Directory, dem bestimmte Aufgaben delegiert wurden.

Dem Servicekonto müssen mindestens die folgenden Berechtigungen in der Organisationseinheit delegiert werden, an die Sie der SVM beitreten:

- Möglichkeit zum Zurücksetzen von Passwörtern
- Möglichkeit, Konten am Lesen und Schreiben von Daten zu hindern

- Möglichkeit zum Festlegen der `-msDS-SupportedEncryptionTypes`Eigenschaft für Computerobjekte
- Überprüfte Fähigkeit zum Schreiben in den DNS-Hostnamen
- Überprüfte Fähigkeit zum Schreiben in den Prinzipalnamen des Service
- Möglichkeit zum Erstellen und Löschen von Computerobjekten
- Überprüfte Fähigkeit zum Lesen und Schreiben von Kontobeschränkungen

Diese stellen den Mindestsatz von Berechtigungen dar, die erforderlich sind, um Computerobjekte mit Ihrem Active Directory zu verbinden. Weitere Informationen finden Sie im Windows Server-Dokumentationsthema Fehler: Zugriff wird verweigert, wenn Nicht-Administratorbenutzer, denen die Kontrolle delegiert wurde, versuchen, Computer mit einem Domain-Controller zu verbinden.

Weitere Informationen zum Erstellen eines Servicekontos mit den richtigen Berechtigungen finden Sie unter Delegieren von Berechtigungen an Ihr Amazon FSx-Servicekonto.

> **Important**
>
> 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 erfordern, dass es Ressourcen zu Ihrer Active-Directory-Domain aufhebt und wieder hinzufügt. Zu diesen Aufgaben gehören das Ersetzen eines ausgefallenen Dateisystems oder einer ausgefallenen SVM oder das Patchen von NetApp ONTAP-Software. Halten Sie Ihre Active-Directory-Konfigurationsinformationen mit Amazon FSx auf dem neuesten Stand, einschließlich der Anmeldeinformationen für das Servicekonto. Weitere Informationen hierzu finden Sie unter Halten Sie Ihre Active Directory-Konfiguration mit Amazon FSx auf dem neuesten Stand.

Wenn Sie AWS und FSx für ONTAP zum ersten Mal verwenden, stellen Sie sicher, dass Sie die ersten Einrichtungsschritte ausführen, bevor Sie Ihre Active-Directory-Integration starten. Weitere Informationen finden Sie unter Einrichten von FSx für ONTAP.

> **Important**
>
> Verschieben Sie keine Computerobjekte, die Amazon FSx in der Organisationseinheit erstellt, nachdem Ihre SVMs erstellt wurden, oder löschen Sie Ihr Active Directory, während Ihre SVM mit ihr verbunden ist. Dies führt dazu, dass Ihre SVMs falsch konfiguriert werden.

Bewährte Methoden für die Arbeit mit Active Directory

Im Folgenden finden Sie einige Vorschläge und Richtlinien, die Sie berücksichtigen sollten, wenn Sie Amazon FSx for NetApp ONTAP SVMs zu Ihrem selbstverwalteten Microsoft Active Directory hinzufügen. Beachten Sie, dass diese als bewährte Methoden empfohlen werden, aber nicht erforderlich sind.

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-Controllern.

Um Amazon FSx-SVMs Ihrer Domain hinzuzufügen, stellen Sie sicher, dass das Dienstkonto über delegierte Berechtigungen verfügt. Mitglieder der Gruppe Domain-Admins verfügen über ausreichende Rechte, um diese Aufgabe auszuführen. Es hat sich jedoch bewährt, ein Dienstkonto zu verwenden, das nur über die dafür erforderlichen Mindestberechtigungen verfügt. Das folgende Verfahren zeigt, wie Sie nur die Berechtigungen delegieren, die für den Beitritt zu FSx for ONTAP SVMs an Ihre Domain erforderlich sind.

Führen Sie dieses Verfahren auf einem Computer aus, der zu Ihrem Verzeichnis hinzugefügt wurde und auf dem das MMC-Snap-In Active Directory-Benutzer und -Computer installiert ist.

So erstellen Sie ein Dienstkonto für Ihre Microsoft Active Directory-Domäne

1. Stellen Sie sicher, dass Sie als Domänenadministrator für Ihre Microsoft Active Directory-Domäne angemeldet sind.
2. Öffnen Sie das MMC-Snap-In „Active Directory-Benutzer und -Computer“.
3. Erweitern Sie im Aufgabenbereich den Domänenknoten.
4. Suchen und öffnen Sie das Kontextmenü (mit der rechten Maustaste) für die Organisationseinheit, die Sie ändern möchten, und wählen Sie dann Delegate Control aus.

5. Wählen Sie auf der Seite des Assistenten zum Delegieren der Steuerung die Option Weiter aus.
6. Wählen Sie Hinzufügen, um einen bestimmten Benutzer oder eine bestimmte Gruppe für Ausgewählte Benutzer und Gruppen hinzuzufügen, und klicken Sie dann auf Weiter.
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 Nur die folgenden Objekte im Ordner und anschließend Computerobjekte aus.
9. Wählen Sie Ausgewählte Objekte in diesem Ordner erstellen und Ausgewählte Objekte in diesem Ordner löschen. Wählen Sie anschließend Weiter.
10. Stellen Sie sicher, dass unter Diese Berechtigungen anzeigen die Optionen Allgemein und Eigenschaftsspezifisch ausgewählt sind.
11. Wählen Sie für Berechtigungen Folgendes aus:
    - Passwort zurücksetzen
    - Kontoeinschränkungen beim Lesen und Schreiben
    - Das Schreiben in den DNS-Hostnamen wurde validiert
    - Das Schreiben in den Dienstprinzipalnamen wurde validiert
    - Schreiben Sie MSDs- SupportedEncryptionTypes
12. Wählen Sie Next (Weiter) und danach Finish (Beenden).
13. Schließen Sie das MMC-Snap-In „Active Directory-Benutzer und -Computer“.

> **Important**
>
> Verschieben Sie keine Computerobjekte, die Amazon FSx in der Organisationseinheit erstellt, nachdem Ihre SVMs erstellt wurden. Wenn Sie das tun, werden Ihre SVMs falsch konfiguriert.

Halten Sie Ihre Active Directory-Konfiguration mit Amazon FSx auf dem neuesten Stand

Um eine ununterbrochene Verfügbarkeit Ihrer Amazon FSx-SVMs zu gewährleisten, aktualisieren Sie die selbstverwaltete Active Directory-Konfiguration (AD) einer SVM, wenn Sie Ihr selbstverwaltetes AD-Setup ändern.

Nehmen wir zum Beispiel an, dass Ihr AD eine zeitbasierte Richtlinie zum Zurücksetzen von Passwörtern verwendet. Stellen Sie in diesem Fall sicher, dass Sie das Passwort für das Servicekonto mit Amazon FSx aktualisieren, sobald das Passwort zurückgesetzt wurde. Verwenden Sie dazu die Amazon FSx-Konsole, die Amazon FSx-API oder. AWS CLI Wenn sich die IP-Adressen des DNS-Servers für Ihre Active Directory-Domain ändern, aktualisieren Sie die IP-Adressen der DNS-Server ebenfalls mit Amazon FSx, sobald die Änderung erfolgt.

Wenn es ein Problem mit der aktualisierten selbstverwalteten AD-Konfiguration gibt, wechselt der SVM-Status zu Fehlkonfiguriert. In diesem Status werden neben der SVM-Beschreibung in der Konsole, der API und der CLI eine Fehlermeldung und eine empfohlene Aktion angezeigt. Wenn ein Problem mit der AD-Konfiguration Ihrer SVM auftritt, stellen Sie sicher, dass Sie die empfohlenen Korrekturmaßnahmen für die Konfigurationseigenschaften ergreifen. Wenn das Problem behoben ist, überprüfen Sie, ob sich der Status Ihrer SVM auf Erstellt ändert.

Weitere Informationen finden Sie unter Aktualisieren einer vorhandenen SVM-Active-Directory-Konfiguration mithilfe der AWS Management ConsoleAWS CLI, und API und Ändern einer Active-Directory-Konfiguration mit der ONTAP-CLI.

Verwendung von Sicherheitsgruppen zur Begrenzung des Datenverkehrs innerhalb Ihrer VPC

Um den Netzwerkverkehr in Ihrer Virtual Private Cloud (VPC) zu begrenzen, können Sie das Prinzip der geringsten Rechte in Ihrer VPC implementieren. Mit anderen Worten, Sie können die Berechtigungen auf das erforderliche Minimum beschränken. Verwenden Sie dazu Sicherheitsgruppenregeln. Weitere Informationen hierzu finden Sie unter Amazon VPC-Sicherheitsgruppen.

Sicherheitsgruppenregeln für ausgehende Nachrichten für die Netzwerkschnittstelle Ihres Dateisystems erstellen

Für mehr Sicherheit sollten Sie erwägen, eine Sicherheitsgruppe mit Regeln für ausgehenden Datenverkehr zu konfigurieren. Diese Regeln sollten ausgehenden Datenverkehr nur zu Ihren selbstverwalteten AD-Domänencontrollern oder innerhalb des Subnetzes oder der Sicherheitsgruppe zulassen. Wenden Sie diese Sicherheitsgruppe auf die VPC an, die mit der elastic network interface Ihres Amazon FSx-Dateisystems verknüpft ist. Weitere Informationen hierzu finden Sie unter Dateisystem-Zugriffskontrolle mit Amazon VPC.

Verbinden von SVMs mit einem Microsoft Active Directory

Ihre Organisation kann Identitäten und Geräte mithilfe eines Active Directory verwalten, unabhängig davon, ob es sich um On-Premises oder in der Cloud handelt. Mit FSx für ONTAP können Sie Ihre SVMs auf folgende Weise direkt mit Ihrer vorhandenen Active-Directory-Domain verbinden:

- Hinzufügen neuer SVMs zu einem Active Directory bei der Erstellung:
  - Mit der Option Standarderstellung in der Amazon-FSx-Konsole zum Erstellen eines neuen FSx-für-ONTAP-Dateisystems können Sie die Standard-SVM einem selbstverwalteten Active Directory hinzufügen. Weitere Informationen finden Sie unter Um ein Dateisystem (Konsole) zu erstellen.
  - Verwenden der Amazon-FSx-Konsole AWS CLIoder der Amazon-FSx-API zum Erstellen einer neuen SVM auf einem vorhandenen FSx-für-ONTAP-Dateisystem. Weitere Informationen finden Sie unter Erstellen einer virtuellen Speichermaschine.
- Verknüpfen vorhandener SVMs mit einem Active Directory:
  - Verwenden der AWS Management Console AWS CLI, und API, um eine SVM mit einem Active Directory zu verbinden, und um erneut zu versuchen, eine SVM mit einem Active Directory zu verbinden, wenn der erste Verbindungsversuch fehlschlägt. Sie können auch einige Active-Directory-Konfigurationseigenschaften für SVMs aktualisieren, die bereits mit einem Active Directory verbunden sind. Weitere Informationen finden Sie unter Verwalten von SVM-Active-Directory-Konfigurationen.
  - Verwenden der NetApp ONTAP-CLI oder REST-API, um SVM-Active-Directory-Konfigurationen hinzuzufügen, erneut zu versuchen, eine Verbindung herzustellen und die Verknüpfung aufzuheben. Weitere Informationen finden Sie unter Verwalten Ihrer SVM-Active-Directory-Konfiguration mit der NetApp CLI.

> **Important**
>
> - Amazon FSx registriert DNS-Datensätze für eine SVM nur, wenn Sie Microsoft DNS als Standard-DNS-Service verwenden. Wenn Sie ein DNS eines Drittanbieters verwenden, müssen Sie DNS-Einträge für Ihre Amazon-FSx-SVMs manuell einrichten, nachdem Sie sie erstellt haben.
> - Wenn Sie verwenden AWS Managed Microsoft AD, müssen Sie eine Gruppe wie AWS Delegierte FSx-Administratoren, AWS Delegierte Administratoren oder eine

benutzerdefinierte Gruppe mit delegierten Berechtigungen an die Organisationseinheit angeben.

Wenn Sie eine FSx-für-ONTAP-SVM direkt mit einem selbstverwalteten Active Directory verbinden, befindet sich die SVM in derselben Active-Directory-Gesamtstruktur (dem logischsten 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.

Informationen, die beim Verbinden einer SVM mit einem Active Directory erforderlich sind

Sie müssen die folgenden Informationen zu Ihrem Active Directory angeben, wenn Sie eine SVM mit einem Active Directory verbinden, unabhängig von der ausgewählten API-Operation:

- Der NetBIOS-Name des Active-Directory-Computerobjekts, das für Ihre SVM erstellt werden soll. Dies ist der Name der SVM in Active Directory, die in Ihrem Active Directory eindeutig sein muss. Verwenden Sie nicht den NetBIOS-Namen der Heimatdomäne. Der NetBIOS-Name darf 15 Zeichen nicht überschreiten.
- Der vollqualifizierte Domänenname (FQDN) Ihres Active Directory. Der FQDN darf 255 Zeichen nicht überschreiten.

  > **Note**
  >
  > Der FQDN darf nicht im SLD-Format (Single Label Domain) vorliegen. Amazon FSx unterstützt keine SLD-Domänen.

- Bis zu drei IP-Adressen der DNS-Server oder Domain-Hosts für Ihre Domain.

  Die IP-Adressen des DNS-Servers und der Active-Directory-Domain-Controller können sich in jedem IP-Adressbereich befinden, mit Ausnahme von:

  - IP-Adressen, die mit Amazon Web Services-eigenen IP-Adressen in diesem in Konflikt stehen AWS-Region. Eine Liste der AWS IP-Adressen nach Region finden Sie in den AWS IP-Adressbereichen .
  - IP-Adressen im folgenden CIDR-Blockbereich: 198.19.0.0/16

- Benutzername und Passwort für ein Servicekonto in Ihrer Active-Directory-Domain, die Amazon FSx beim Beitritt der SVM zur Active-Directory-Domain verwenden soll. Weitere Informationen zu den Anforderungen an Servicekonten finden Sie unter Anforderungen an Active-Directory-Servicekonten.
- (Optional) Die Organisationseinheit (OU) in der Domain, der Sie die SVM beitreten.

> **Note**
>
> Wenn Sie Ihre SVM mit einem AWS Directory Service Active Directory verbinden, müssen Sie eine Organisationseinheit angeben, die sich innerhalb der Standard-Organisationseinheit befindet, die für die Verzeichnisobjekte AWS Directory Service erstellt, die sich auf beziehen AWS. Dies liegt daran, dass AWS Directory Service die keinen Zugriff auf die Standard`Computers`-OU Ihres Active Directory bietet. Wenn Ihre Active-Directory-Domain beispielsweise lautete`example.com`, können Sie die folgende Organisationseinheit angeben: `OU=Computers,OU=example,DC=example,DC=com`.

- (Optional) Die Domänengruppe, an die Sie die Autorität für die Durchführung administrativer Aktionen in Ihrem Dateisystem delegieren. Diese Domänengruppe kann beispielsweise Windows-SMB-Dateifreigaben verwalten, den Besitz von Dateien und Ordnern übernehmen usw. Wenn Sie diese Gruppe nicht angeben, delegiert Amazon FSx diese Berechtigung standardmäßig an die Domain-Admins-Gruppe in Ihrer Active-Directory-Domain.

Verwalten von SVM-Active-Directory-Konfigurationen

In diesem Abschnitt wird beschrieben, wie Sie die AWS Management Console, AWS CLIdie FSx-API und die ONTAP-CLI verwenden, um Folgendes zu tun:

- Verbinden einer vorhandenen SVM mit einem Active Directory
- Ändern einer vorhandenen SVM-Active-Directory-Konfiguration
- Entfernen von SVMs aus einem Active Directory

Um eine SVM aus einem Active Directory zu entfernen, müssen Sie die NetApp ONTAP-CLI verwenden.

Themen

- Verbinden einer SVM mit einem Active Directory mithilfe der AWS Management Console, AWS CLI und API
- Aktualisieren einer vorhandenen SVM-Active-Directory-Konfiguration mithilfe der AWS Management ConsoleAWS CLI, und API
- Verwalten Ihrer SVM-Active-Directory-Konfiguration mit der NetApp CLI

Verbinden einer SVM mit einem Active Directory mithilfe der AWS Management Console, AWS CLI und API

Gehen Sie wie folgt vor, um eine vorhandene SVM mit einem Active Directory zu verbinden. In diesem Verfahren ist die SVM noch nicht mit einem Active Directory verbunden.

So verbinden Sie eine SVM mit einem Active Directory (AWS Management Console)

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie die SVM aus, die Sie einem Active Directory hinzufügen möchten:

   - Wählen Sie im linken Navigationsbereich Dateisysteme und dann das ONTAP-Dateisystem mit der SVM aus, die Sie aktualisieren möchten.
   - Wählen Sie die Registerkarte Virtuelle Speichermaschinen aus.

     – Oder –
   - Um eine Liste aller verfügbaren SVMs anzuzeigen, erweitern Sie im linken Navigationsbereich ONTAP und wählen Sie Virtuelle Speichermaschinen aus. Eine Liste aller SVMs in Ihrem Konto in der AWS-Region wird angezeigt.

   Wählen Sie die SVM, die Sie einem Active Directory hinzufügen möchten, aus der Liste aus.
3. Wählen Sie oben rechts im Bereich SVM-Zusammenfassung die Option Aktionen > Active Directory beitreten/aktualisieren aus. Das Fenster SVM mit einem Active Directory verbinden wird angezeigt.
4. Geben Sie die folgenden Informationen für das Active Directory ein, dem Sie die SVM beitreten:

   - Der NetBIOS-Name des Active-Directory-Computerobjekts, das für Ihre SVM erstellt werden soll. Dies ist der Name der SVM in Active Directory, die in Ihrem Active Directory eindeutig sein muss. Verwenden Sie nicht den NetBIOS-Namen der Heimatdomäne. Der NetBIOS-Name darf 15 Zeichen nicht überschreiten.

- Der vollqualifizierte Domänenname (FQDN) Ihres Active Directory. Der Domänenname darf 255 Zeichen nicht überschreiten.
- IP-Adressen des DNS-Servers – Die IPv4-Adressen der DNS-Server für Ihre Domain.
- Benutzername des Servicekontos – Der Benutzername des Servicekontos in Ihrem vorhandenen Active Directory. Geben Sie kein Domänenpräfix oder Suffix an. Verwenden Sie beispielsweise für `EXAMPLE\ADMIN`nur `ADMIN`.
- Passwort des Servicekontos – Das Passwort für das Servicekonto.
- Passwort bestätigen – Das Passwort für das Servicekonto.
- (Optional) Organisationseinheit (OU) – Der eindeutige Pfadname der Organisationseinheit, der Sie Ihre SVM beitreten möchten.
- Delegierte Dateisystem-Administratorgruppe – Der Name der Gruppe in Ihrem Active Directory, die Ihr Dateisystem verwalten kann.

  Wenn Sie verwenden AWS Managed Microsoft AD, müssen Sie eine Gruppe wie AWS Delegierte FSx-Administratoren, AWS Delegierte Administratoren oder eine benutzerdefinierte Gruppe mit delegierten Berechtigungen an die Organisationseinheit angeben.

  Wenn Sie einem selbstverwalteten Active Directory beitreten, verwenden Sie den Namen der Gruppe in Ihrem Active Directory. Die Standardgruppe ist `Domain Admins`.

5. Wählen Sie Active Directory verbinden aus, um die SVM mithilfe der von Ihnen bereitgestellten Konfiguration mit dem Active Directory zu verbinden.

So verbinden Sie eine SVM mit einem Active Directory (AWS CLI)

- Um eine FSx for ONTAP SVM mit einem Active Directory zu verbinden, verwenden Sie den update-storage-virtual-machine CLI-Befehl (oder die entsprechende UpdateStorageVirtualMachine API-Operation), wie im folgenden Beispiel gezeigt.

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
\
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Nach erfolgreicher Erstellung der virtuellen Speichermaschine gibt Amazon FSx seine Beschreibung im JSON-Format zurück, wie im folgenden Beispiel gezeigt.


```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
```

```
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],

  }
}
```

Aktualisieren einer vorhandenen SVM-Active-Directory-Konfiguration mithilfe der AWS Management ConsoleAWS CLI, und API

Gehen Sie wie folgt vor, um die Active-Directory-Konfiguration einer SVM zu aktualisieren, die bereits mit einem Active Directory verbunden ist.

So aktualisieren Sie eine SVM-Active-Directory-Konfiguration (AWS Management Console)

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie die zu aktualisierende SVM wie folgt aus:

   - Wählen Sie im linken Navigationsbereich Dateisysteme und dann das ONTAP-Dateisystem mit der SVM aus, die Sie aktualisieren möchten.
   - Wählen Sie die Registerkarte Virtuelle Speichermaschinen aus.

     – Oder –

   - Um eine Liste aller verfügbaren SVMs anzuzeigen, erweitern Sie im linken Navigationsbereich ONTAP und wählen Sie Virtuelle Speichermaschinen aus.

     Wählen Sie die SVM, die Sie aktualisieren möchten, aus der Liste aus.
3. Wählen Sie im Bereich SVM-Zusammenfassung die Option Aktionen > Active Directory beitreten/aktualisieren aus. Das Konfigurationsfenster SVM Active Directory aktualisieren wird angezeigt.
4. In diesem Fenster können Sie die folgenden Active-Directory-Konfigurationseigenschaften aktualisieren.

- IP-Adressen des DNS-Servers – Die IPv4-Adressen der DNS-Server für Ihre Domain.
- Benutzername des Servicekontos – Der Benutzername des Servicekontos in Ihrem vorhandenen Active Directory. Geben Sie kein Domänenpräfix oder Suffix an. Geben Sie als `EXAMPLE\ADMIN` `ADMIN`ein.
- Passwort für das Servicekonto – Das Passwort für das Active-Directory-Servicekonto.

5. Nachdem Sie Ihre Aktualisierungen eingegeben haben, wählen Sie Active Directory aktualisieren, um die Änderungen vorzunehmen.

Gehen Sie wie folgt vor, um die Active-Directory-Konfiguration einer SVM zu aktualisieren, die bereits mit einem Active Directory verbunden ist.

So aktualisieren Sie eine SVM-Active-Directory-Konfiguration (AWS CLI)

- Um die Active-Directory-Konfiguration einer SVM mit der AWS CLI oder API zu aktualisieren, verwenden Sie den update-storage-virtual-machine CLI-Befehl (oder die entsprechende UpdateStorageVirtualMachine API-Operation), wie im folgenden Beispiel gezeigt.

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-abcdef0123456789a\
    --active-directory-configuration \
    SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}'
```

Verwalten Ihrer SVM-Active-Directory-Konfiguration mit der NetApp CLI

Sie können die NetApp ONTAP-CLI verwenden, um Ihre SVM mit einem Active Directory zu verbinden und rückgängig zu machen und eine vorhandene SVM-Active-Directory-Konfiguration zu ändern.

Verbinden einer SVM mit einem Active Directory mithilfe der ONTAP-CLI

Sie können vorhandene SVMs mit der ONTAP-CLI mit einem Active Directory verbinden, wie im folgenden Verfahren beschrieben. Sie können dies auch tun, wenn Ihre SVM bereits mit einem Active Directory verbunden ist.

1. Um auf die NetApp ONTAP-CLI zuzugreifen, richten Sie eine SSH-Sitzung am Verwaltungsport des Dateisystems von Amazon FSx für NetApp ONTAP ein, indem Sie den folgenden Befehl ausführen. Ersetzen Sie durch *management_endpoint_ip* die IP-Adresse des Verwaltungsports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Erstellen Sie einen DNS-Eintrag für Ihr Active Directory, indem Sie den vollständigen DNS-Namen (`corp.example.com`) des Verzeichnisses und mindestens eine DNS-Server-IP-Adresse angeben.

   ```
   ::>vserver services name-service dns create -vserver svm_name -
   domains corp.example.com -name-servers dns_ip_1, dns_ip_2
   ```

   Führen Sie den folgenden Befehl aus, um die Verbindung zu Ihren DNS-Servern zu überprüfen. Ersetzen Sie *svm_name* durch Ihre eigenen Informationen.

   ```
   FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name

                               Name Server
   Vserver       Name Server     Status       Status Details
   ------------- --------------- ------------ --------------------------
   svm_name      172.31.14.245   up           Response time (msec): 0
   svm_name      172.31.25.207   up           Response time (msec): 1
   2 entries were displayed.
   ```

3. Führen Sie den folgenden Befehl aus, um Ihre SVM mit Ihrem Active Directory zu verbinden. Beachten Sie, dass Sie eine angeben müssen`computer_name`, die noch nicht in Ihrem Active Directory vorhanden ist, und den DNS-Namen des Verzeichnisses für angeben müssen`-domain`. Geben Sie für die OUs `-OU`ein, denen die SVM beitreten soll, sowie den vollständigen DNS-Namen im DC-Format.

   ```
   ::>vserver cifs create -vserver svm_name -cifs-server computer_name -
   domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
   ```

   Führen Sie den folgenden Befehl aus, um den Status Ihrer Active-Directory-Verbindung zu überprüfen:

```
::>vserver cifs check -vserver svm_name

              Vserver : svm_name
                    Cifs NetBIOS Name : svm_netBIOS_name
                          Cifs Status : Running
                                 Site : Default-First-Site-Name
Node Name       DC Server Name  DC Server IP    Status   Status Details
--------------- --------------  --------------- ------   --------------
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245   up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245   up       Response time (msec): 20
2 entries were displayed.
```

4. Wenn Sie nach diesem Join nicht auf Freigaben zugreifen können, stellen Sie fest, ob das Konto, das Sie für den Zugriff auf die Freigabe verwenden, über Berechtigungen verfügt. Wenn Sie beispielsweise das `Admin` Standardkonto (ein delegierter Administrator) mit einem von AWS verwalteten Active Directory verwenden, müssen Sie den folgenden Befehl in ONTAP ausführen. Die `netbios_domain` entspricht dem Domänennamen Ihres Active Directory (für wird hier `corp.example.com` `netbios_domain` verwendet`example`).

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
 svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

Ändern einer Active-Directory-Konfiguration mit der ONTAP-CLI

Sie können die ONTAP-CLI verwenden, um eine vorhandene Active-Directory-Konfiguration zu ändern.

1. Um auf die NetApp ONTAP-CLI zuzugreifen, richten Sie eine SSH-Sitzung am Verwaltungsport des Dateisystems von Amazon FSx für NetApp ONTAP ein, indem Sie den folgenden Befehl ausführen. Ersetzen Sie durch *`management_endpoint_ip`* die IP-Adresse des Verwaltungsports des Dateisystems.

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

Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Führen Sie den folgenden Befehl aus, um den CIFS-Server der SVM vorübergehend herunterzufahren:

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Wenn Sie die DNS-Einträge Ihres Active Directory ändern müssen, führen Sie den folgenden Befehl aus:

```
::>vserver services name-service dns modify -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1,dns_ip_2
```

Sie können den Verbindungsstatus zu den DNS-Servern Ihres Active Directory mit dem `vserver services name-service dns check -vserver svm_name` Befehl überprüfen.

```
::>vserver services name-service dns check -vserver svm_name
                              Name Server
Vserver       Name Server     Status       Status Details
------------- --------------- ------------ --------------------------
svmciad       dns_ip_1        up           Response time (msec): 1
svmciad       dns_ip_2        up           Response time (msec): 1
2 entries were displayed.
```

4. Wenn Sie die Active-Directory-Konfiguration selbst ändern müssen, können Sie vorhandene Felder mit dem folgenden Befehl ändern und ersetzen:

   - *computer_name* , wenn Sie den NetBIOS-Namen (Computerkonto) der SVM ändern möchten.
   - *domain_name* , wenn Sie den Namen der Domain ändern möchten. Dies sollte dem DNS-Domäneneintrag entsprechen, der in Schritt 3 dieses Abschnitts () notiert wurde`corp.example.com`.
   - `organizational_unit`, wenn Sie die Organisationseinheit (`OU=Computers,OU=example,DC=corp,DC=example,DC=com`) ändern möchten.

   Sie müssen die Active-Directory-Anmeldeinformationen erneut eingeben, die Sie verwendet haben, um dieses Gerät mit dem Active Directory zu verbinden.

```
::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
domain domain_name -OU organizational_unit
```

Sie können den Verbindungsstatus Ihrer Active-Directory-Verbindung mit dem `vserver cifs check -vserver svm_name` Befehl überprüfen.

5. Wenn Sie mit dem Ändern Ihres Active Directory und Ihrer DNS-Konfiguration fertig sind, starten Sie den CIFS-Server wieder, indem Sie den folgenden Befehl ausführen:

```
::>vserver cifs modify -vserver svm_name -status-admin up
```

Aufheben der Verbindung eines Active Directory mit Ihrer SVM mithilfe der NetApp ONTAP-CLI

Die NetApp ONTAP-CLI kann auch verwendet werden, um die Verbindung Ihrer SVM zu einem Active Directory aufzuheben, indem Sie die folgenden Schritte ausführen:

1. Um auf die NetApp ONTAP-CLI zuzugreifen, richten Sie eine SSH-Sitzung am Verwaltungsport des Dateisystems von Amazon FSx für NetApp ONTAP ein, indem Sie den folgenden Befehl ausführen. Ersetzen Sie durch *`management_endpoint_ip`* die IP-Adresse des Verwaltungsports des Dateisystems.

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

Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Löschen Sie den CIFS-Server, der Ihrem Gerät beigetreten ist, aus dem Active Directory, indem Sie den folgenden Befehl ausführen. Damit ONTAP das Maschinenkonto für Ihre SVM löscht, geben Sie die Anmeldeinformationen an, die Sie ursprünglich verwendet haben, um die SVM mit dem Active Directory zu verbinden.

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Wenn Sie die DNS-Einträge Ihres Active Directory ändern müssen, führen Sie den folgenden Befehl aus:

```
FsxId0123456789a::vserver cifs delete -vserver svm_name
```

```
In order to delete an Active Directory machine account for the CIFS server, you
 must supply the name and password of a Windows account with
sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

Enter the user name: user_name

Enter the password:

Warning: There are one or more shares associated with this CIFS server
         Do you really want to delete this CIFS server and all its shares? {y|n}: y
```

4. Löschen Sie die DNS-Server für Ihr Active Directory, indem Sie den folgenden Befehl ausführen:

```
::vserver services name-service dns delete -vserver svm_name
```

Wenn eine Warnung wie die folgende angezeigt wird – die angibt, dass als entfernt werden dns soll ns-switch– und Sie nicht vorhaben, dieses Gerät erneut einem Active Directory beizutreten, können Sie die ns-switch Einträge entfernen.

```
Warning: "DNS" is present as one of the sources in one or more ns-switch databases
 but no valid DNS configuration was found for Vserver
         "svm_name". Remove "DNS" from ns-switch using the "vserver services name-
service ns-switch" command. Configuring "DNS" as a source
         in the ns-switch setting when there is no valid configuration can cause
 protocol access issues.
```

5. (Optional) Entfernen Sie die ns-switch Einträge für , dns indem Sie den folgenden Befehl ausführen. Überprüfen Sie die Quellreihenfolge und entfernen Sie dann den dns Eintrag für die hosts Datenbank, indem Sie die sources so ändern, dass sie nur die anderen aufgelisteten Quellen enthalten. In diesem Beispiel ist die einzige andere Quelle files.

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts

                    Vserver: svm_name
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

6. (Optional) Entfernen Sie den dns Eintrag, indem Sie die `sources` für den Datenbank-Host so ändern, dass sie nur enthält`files`.

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

Leistung von Amazon FSx für NetApp ONTAP

Im Folgenden finden Sie eine Übersicht über die Leistung des Dateisystems von Amazon FSx für NetApp ONTAP mit einer Erläuterung der verfügbaren Leistungs- und Durchsatzoptionen sowie nützlicher Leistungstipps.

Themen

- Wie die Leistung für FSx-für-ONTAP-Dateisysteme gemessen wird
- Leistungsdetails
- Auswirkungen des Bereitstellungstyps auf die Leistung
- Auswirkungen der Speicherkapazität auf die Leistung
- Auswirkungen der Durchsatzkapazität auf die Leistung
- Beispiel: Speicherkapazität und Durchsatzkapazität

Wie die Leistung für FSx-für-ONTAP-Dateisysteme gemessen wird

Die Leistung des Dateisystems wird anhand seiner Latenz, seines Durchsatzes und seiner E/A-Operationen pro Sekunde (IOPS) gemessen.

Latency

Amazon FSx für NetApp ONTAP bietet Latenzen für Dateioperationen unter einer Millisekunde mit SSD-Speicher (Solid State Drive) und Zehn Millisekunden Latenz für Kapazitätspool-Speicher. Darüber hinaus verfügt Amazon FSx auf jedem Dateiserver über zwei Ebenen des Lese-Cachings – NVMe-Laufwerke (nicht flüchtiger Speicherausdruck) und In-Memory – um noch niedrigere Latenzen beim Zugriff auf Ihre am häufigsten gelesenen Daten bereitzustellen.

Durchsatz und IOPS

Jedes Amazon FSx-Dateisystem bietet bis zu zehn GB/s Durchsatz und Millionen IOPS. Die spezifische Menge an Durchsatz und IOPS, die Ihr Workload in Ihrem Dateisystem steuern kann, hängt von der Gesamtdurchsatzkapazität und der Speicherkapazitätskonfiguration Ihres Dateisystems sowie von der Art Ihres Workloads ab, einschließlich der Größe des aktiven Arbeitssatzes.

SMB-Multikanal- und NFS-nconnect-Unterstützung

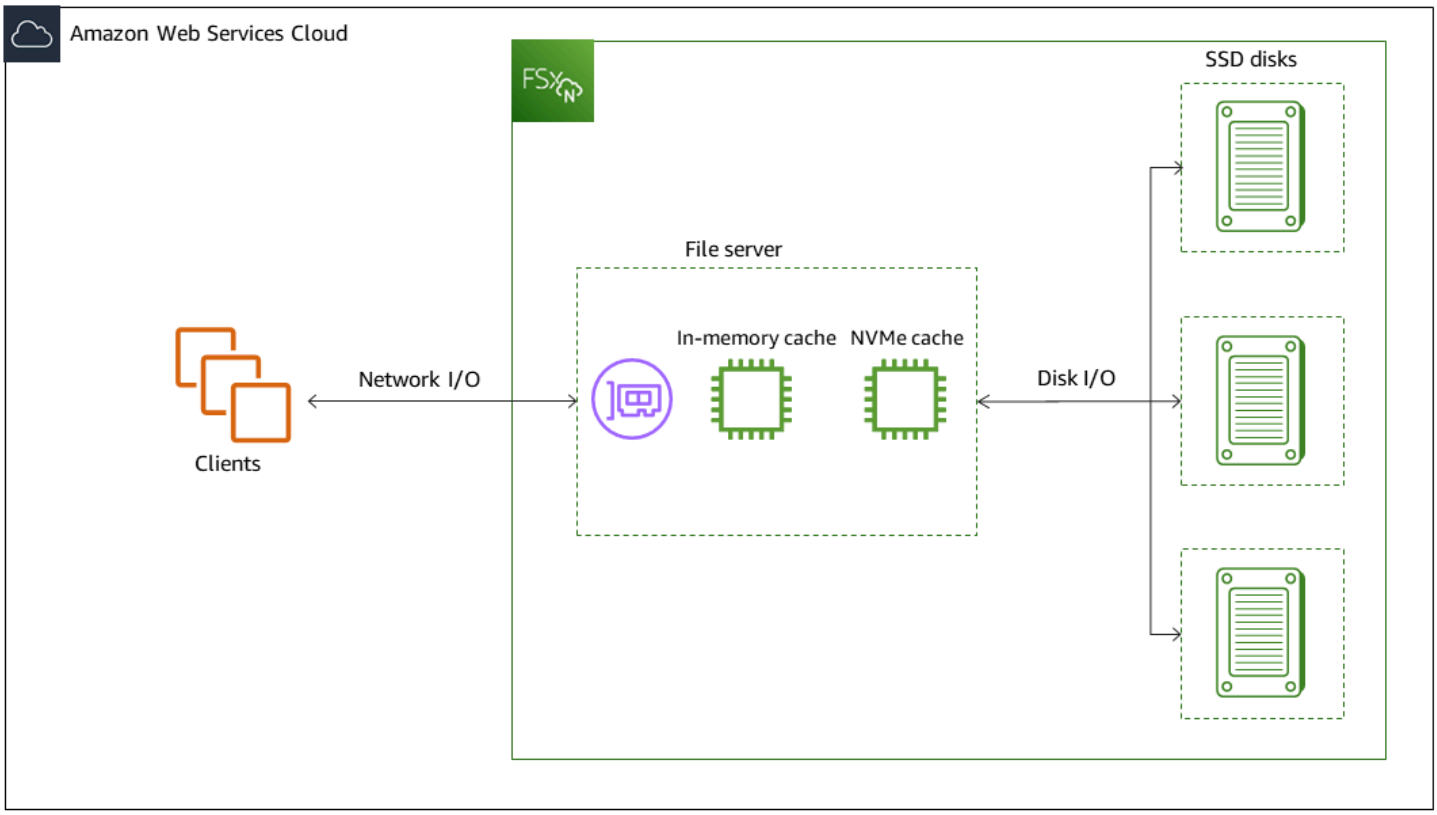
Mit Amazon FSx können Sie SMB Multichannel so konfigurieren, dass mehrere Verbindungen zwischen ONTAP und Clients in einer einzigen SMB-Sitzung bereitgestellt werden. SMB Multichannel verwendet mehrere Netzwerkverbindungen zwischen Client und Server gleichzeitig, um die Netzwerkbandbreite für maximale Auslastung zu aggregieren. Informationen zur Verwendung der NetApp ONTAP-CLI zum Konfigurieren von SMB Multichannel finden Sie unter Konfigurieren von SMB Multichannel für Leistung und Redundanz.

NFS-Clients können die `nconnect` Mounting-Option verwenden, um mehrere TCP-Verbindungen (bis zu 16) einem einzigen NFS-Mount zuzuordnen. Ein solcher NFS-Client Multiplexing-Dateioperationen auf mehrere TCP-Verbindungen auf Round-Robin- Weise und erhält so einen höheren Durchsatz aus der verfügbaren Netzwerkbandbreite. NFSv3 und NFSv4.1+ unterstützen `nconnect`. Die Netzwerkbandbreite der Amazon EC2-Instance beschreibt das Bandbreitenlimit von 5 Gbit/s pro Netzwerkfluss. Sie können dieses Limit umgehen, indem Sie mehrere Netzwerkflüsse mit `nconnect` oder SMB-Multikanal verwenden. Überprüfen Sie in Ihrer NFS-Client-Dokumentation, ob in Ihrer Client-Version unterstützt `nconnect` wird. Weitere Informationen zur NetApp ONTAP-Unterstützung für `nconnect`finden Sie unter ONTAP-Unterstützung für NFSv4.1.

Leistungsdetails

Um das Leistungsmodell von Amazon FSx für NetApp ONTAP im Detail zu verstehen, können Sie die Architekturkomponenten eines Amazon-FSx-Dateisystems untersuchen. Ihre Client-Computing-Instances, unabhängig davon, ob sie sich in AWS oder On-Premises befinden, greifen über eine oder mehrere Elastic Network-Schnittstellen (ENI) auf Ihr Dateisystem zu. Diese Netzwerkschnittstellen befinden sich in der Amazon VPC, die Sie Ihrem Dateisystem zuordnen. Hinter jeder Dateisystem-ENI befindet sich ein NetApp ONTAP-Dateiserver, der Daten über das Netzwerk an die Clients liefert, die auf das Dateisystem zugreifen. Amazon FSx bietet einen schnellen In-Memory-Cache und NVMe-Cache auf jedem Dateiserver, um die Leistung für die am häufigsten aufgerufenen Daten zu verbessern. An jeden Dateiserver sind die SSD-Festplatten angehängt, auf denen Ihre Dateisystemdaten gehostet werden.

Diese Komponenten sind im folgenden Diagramm dargestellt.



Entsprechend diesen Architekturkomponenten – Netzwerkschnittstelle, In-Memory-Cache, NVMe-Cache und Speicher-Volumes – sind die wichtigsten Leistungsmerkmale eines Amazon-FSx-für-NetApp ONTAP-Dateisystems, die den Gesamtdurchsatz und die IOPS-Leistung bestimmen.

- Netzwerk-I/O-Leistung: Durchsatz/IOPS von Anfragen zwischen den Clients und dem Dateiserver (aggregiert)
- Größe des In-Memory- und NVMe-Caches auf dem Dateiserver: Größe des aktiven Arbeitssatzes, der für das Caching geeignet ist
- Festplatten-I/O-Leistung: Durchsatz/IOPS von Anfragen zwischen dem Dateiserver und den Speicherfestplatten

Es gibt zwei Faktoren, die diese Leistungsmerkmale für Ihr Dateisystem bestimmen: die Gesamtmenge der SSD-IOPS und die Durchsatzkapazität, die Sie dafür konfigurieren. Die ersten beiden Leistungsmerkmale – Netzwerk-I/O-Leistung und In-Memory- und NVMe-Cache-Größe – werden ausschließlich durch die Durchsatzkapazität bestimmt, während das dritte – Festplatten-I/O-Leistung – durch eine Kombination aus Durchsatzkapazität und SSD-IOPS bestimmt wird.

Dateibasierte Workloads sind in der Regel hoch, gekennzeichnet durch kurze, intensive Zeiträume hoher E/A mit viel Leerlaufzeit zwischen Spitzen. Um hohe Workloads zu unterstützen, bietet

Amazon FSx zusätzlich zu den Basisgeschwindigkeiten, die ein Dateisystem rund um die Uhr bewältigen kann, die Möglichkeit, sowohl für Netzwerk-I/O- als auch für Festplatten-I/O-Operationen höhere Geschwindigkeiten zu erreichen. Amazon FSx verwendet einen Netzwerk-I/O-Guthabenmechanismus, um Durchsatz und IOPS basierend auf der durchschnittlichen Auslastung zuzuweisen – Dateisysteme sammeln Guthaben an, wenn ihr Durchsatz und ihre IOPS-Nutzung unter ihren Basislimits liegen, und können diese Guthaben verwenden, wenn sie I/O-Operationen ausführen.

Schreibvorgänge verbrauchen doppelt so viel Netzwerkbandbreite wie Lesevorgänge. Eine Schreiboperation muss auf dem sekundären Dateiserver repliziert werden, sodass eine einzelne Schreiboperation zu einem doppelten Netzwerkdurchsatz führt.

Auswirkungen des Bereitstellungstyps auf die Leistung

Sie können zwei Arten von Dateisystemen mit FSx für ONTAP erstellen. Dateisysteme mit einem einzigen Hochverfügbarkeitspaar (HA) von Dateiservern werden als Scale-up-Dateisysteme bezeichnet. Dateisysteme mit mehreren HA-Paaren werden als Scale-Out-Dateisysteme bezeichnet. Weitere Informationen finden Sie unter Paare mit hoher Verfügbarkeit (HA).

Die Dateisysteme FSx für ONTAP Multi-AZ und Single-AZ bieten konsistente Latenzen bei Dateioperationen unter einer Millisekunde mit SSD-Speicher und zehn Millisekunden Latenz mit Kapazitätspool-Speicher. Darüber hinaus bieten Dateisysteme, die die folgenden Anforderungen erfüllen, einen NVMe-Lese-Cache, um Leselatenzen zu reduzieren und IOPS für Daten mit häufigen Lesevorgängen zu erhöhen:

- Multi-AZ-Dateisysteme
- Single-AZ-Skalierungsdateisysteme, die nach dem 28. November 2022 mit mindestens 2 GBpss Durchsatzkapazität erstellt wurden

Die folgenden Tabellen zeigen die Durchsatzkapazität, auf die Dateisysteme je nach Faktoren wie der Anzahl der Hochverfügbarkeitspaare (HA) und der AWS-Regionen Verfügbarkeit hochskaliert werden können.

Scale-up

Diese Leistungsspezifikationen gelten für Scale-up-Dateisysteme.

Maximaler Durchsatz vom SSD-Speicher pro HA-Paar für hochskalierte Dateisysteme

	Region USA Ost (Ohio), Region USA Ost (Nord-Virginia), Region USA West (Oregon) und Europa (Irland)		Alle anderen AWS-Regionen , in denen FSx für ONTAP verfügbar ist	
	Lesedurchsatz (MBps	Schreibdurchsatz (MBps	Lesedurchsatz (MBps	Schreibdurchsatz (MBps
Single-AZ	4,096*	1,000	2,048	750
Multi-AZ	4,096*	1,800	2,048	1,300

> **Note**
>
> * Um 4 GBpss Durchsatzkapazität bereitzustellen, muss Ihr Dateisystem mit mindestens 5 120 GiB SSD-Speicherkapazität und 160 000 SSD-IOPS konfiguriert sein.

Scale-out

Diese Leistungsspezifikationen gelten für Scale-Out-Dateisysteme.

Maximaler Durchsatz vom SSD-Speicher pro HA-Paar für Scale-Out-Dateisysteme

	Lesedurchsatz (MBps	Schreibdurchsatz (MBps
Single-AZ-Skalierung	6,144*	1,100*

> **Note**
>
> * Pro HA-Paar (bis zu 12). Weitere Informationen finden Sie unter Paare mit hoher Verfügbarkeit (HA).

Auswirkungen der Speicherkapazität auf die Leistung

Der maximale Festplattendurchsatz und die IOPS-Werte, die Ihr Dateisystem erreichen kann, sind der niedrigere von:

- die von Ihren Dateiservern bereitgestellte Datenträgerleistung, basierend auf der Durchsatzkapazität, die Sie für Ihr Dateisystem auswählen
- Die Datenträgerleistung, die durch die Anzahl der SSD-IOPS bereitgestellt wird, die Sie für Ihr Dateisystem bereitstellen

Standardmäßig bietet der SSD-Speicher Ihres Dateisystems bis zu den folgenden Datenträgerdurchsatz und IOPS:

- Festplattendurchsatz (MBps TiB Speicher): 768
- Festplatten-IOPS (IOPs pro TiB Speicher): 3 072

Auswirkungen der Durchsatzkapazität auf die Leistung

Jedes Amazon FSx-Dateisystem verfügt über eine Durchsatzkapazität, die Sie beim Erstellen des Dateisystems konfigurieren. Die Durchsatzkapazität Ihres Dateisystems bestimmt die Netzwerk-I/O-Leistung oder die Geschwindigkeit, mit der jeder der Dateiserver, die Ihr Dateisystem hosten, Dateidaten über das Netzwerk für Clients bereitstellen kann, die darauf zugreifen. Eine höhere Durchsatzkapazität verfügt über mehr Arbeitsspeicher und nicht flüchtigen Speicher-Express-Speicher (NVMe) zum Zwischenspeichern von Daten auf jedem Dateiserver und eine höhere Festplatten-I/O-Leistung, die von jedem Dateiserver unterstützt wird.

Sie können optional eine höhere SSD-IOPS-Ebene bereitstellen, wenn Sie Ihr Dateisystem erstellen. Die maximale Menge an SSD-IOPS, die Ihr Dateisystem erreichen kann, hängt auch von der Durchsatzkapazität Ihres Dateisystems ab, auch wenn zusätzliche SSD-IOPS bereitgestellt werden.

Die folgenden Tabellen zeigen den vollständigen Satz von Spezifikationen für die Durchsatzkapazität sowie Basis- und Burst-Level und die Menge des Arbeitsspeichers für die Zwischenspeicherung auf dem Dateiserver in der entsprechenden AWS-Regionen.

Single-AZ (scale-up)

> Diese Leistungsspezifikationen gelten für Single-AZ-Skalierungsdateisysteme, die nach dem 28. November 2022 in der angegebenen erstellt wurden AWS-Regionen.

Leistungsspezifikationen für Dateisysteme in den folgenden AWS-Regionen: USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon) und Europa (Irland)

FSx-Durchsatzkapazität (MBps	Netzwerkdurchsatzkapazität (MBps		Netzwerk-IOPS	In-Memory-Caching (GB)	NVMe-Lese-Caching (GB)	Festplattendurchsatz (MBps		IOPS des SSD-Laufwerks*	
	Baseline	Burst				Baseline	Burst	Baseline	Burst
128	188	1,500	Zehntausende Baseline	16	–	128	1,250	6,000	40 000
256	375	1,500		32	–	256	1,250	12,000	40 000
512	750	1,500	Hunderttausende Baseline	64	–	512	1,250	20,000	40,000
1,024	1,500	–		128	–	1,024	1,250	40,000	–
2 048	3,125	–		256	1,900	2,048	–	80,000	–
4.096	6,250	–		512	5,400	4,096	–	160,000	–

> **Note**
>
> * Ihre SSD-IOPS werden nur verwendet, wenn Sie auf Daten zugreifen, die nicht im In-Memory-Cache oder NVMe-Cache Ihres Dateiservers zwischengespeichert sind.

Diese Leistungsspezifikationen gelten für Single-AZ-Skalierungsdateisysteme in allen anderen , in AWS-Regionen denen FSx für ONTAP verfügbar ist.

Leistungsspezifikationen für Dateisysteme in allen anderen , in AWS-Regionen denen FSx für ONTAP verfügbar ist

FSx-Durchsatzkapazität (MBps	Netzwerkdurchsatzkapazität (MBps		Netzwerk-IOPS	In-Memory-Caching (GB)	Festplattendurchsatz (MBps		IOPS des SSD-Laufwerks*	
	Baseline	Burst			Baseline	Burst	Baseline	Burst
128	150	1,250	Zehntausende Baseline	16	128	600	6,000	18 750
256	300	1,250		32	256	600	12,000	18 750
512	625	1,250	Hunderttausende Baseline	64	512	600	18,750	–
1,024	1,500	–		128	1,024	–	40,000	–
2 048	3,125	–		256	2,048	–	80,000	–

> **Note**
>
> * Ihre SSD-IOPS werden nur verwendet, wenn Sie auf Daten zugreifen, die nicht im In-Memory-Cache oder NVMe-Cache Ihres Dateiservers zwischengespeichert sind.

Single-AZ (scale-out)

Diese Leistungsspezifikationen gelten für Scale-Out-Dateisysteme.

Leistungsspezifikationen für Scale-Out-Dateisysteme

FSx-Durchsatzkapazität (MBps	Netzwerkdurchsatzkapazität (MBps		Netzwerk-IOPS	In-Memory-Caching (GB)	Festplattendurchsatz (MBps		IOPS des SSD-Laufwerks*	
	Baseline	Burst			Baseline	Burst	Baseline	Burst
3 072**	6,250	–	Hunderttausende Baseline	128	3,072	–	100,000	–
6 144**	12,500	–		256	6,144	–	200,000	–

> **Note**
>
> * Ihre SSD-IOPS werden nur verwendet, wenn Sie auf Daten zugreifen, die nicht im In-Memory-Cache oder NVMe-Cache Ihres Dateiservers zwischengespeichert sind.
> ** Pro HA-Paar (bis zu 12). Weitere Informationen finden Sie unter Paare mit hoher Verfügbarkeit (HA).

Multi-AZ (scale-up)

Diese Leistungsspezifikationen gelten für Multi-AZ-Skalierungsdateisysteme, die nach dem 28. November 2022 in der angegebenen erstellt wurden AWS-Regionen.

Leistungsspezifikationen für Dateisysteme in den folgenden AWS-Regionen: USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon) und Europa (Irland)

FSx-Durchsatzkapazität (MBps	Netzwerkdurchsatzkapazität (MBps		Netzwerk-IOPS	In-Memory-Caching (GB)	NVMe-Caching (GB)	Festplattendurchsatz (MBps		IOPS des SSD-Laufwerks*	
	Baseline	Burst				Baseline	Burst	Baseline	Burst

FSx-Durchsatzkapazität (MBps	Netzwerkdurchsatzkapazität (MBps		Netzwerk-IOPS	In-Memory-Caching (GB)	NVMe-Caching (GB)	Festplattendurchsatz (MBps		IOPS des SSD-Laufwerks*	
128	188	1,500	Zehntausende Baseline	16	238	128	1,250	6,000	40 000
256	375	1,500		32	475	256	1,250	12,000	40 000
512	750	1,500	Hunderttausende Baseline	64	950	512	1,250	20,000	40,000
1,024	1,500	–		128	1,900	1,024	1 250	40,000	–
2 048	3,125	–		256	3,800	2,048	–	80,000	–
4.096	6,250	–		512	7,600	4,096	–	160,000	–

> **Note**
>
> * Ihre SSD-IOPS werden nur verwendet, wenn Sie auf Daten zugreifen, die nicht im In-Memory-Cache oder NVMe-Cache Ihres Dateiservers zwischengespeichert sind.

Diese Leistungsspezifikationen gelten für Multi-AZ-Skalierungsdateisysteme in allen anderen , in AWS-Regionen denen FSx für ONTAP verfügbar ist.

Leistungsspezifikationen für Dateisysteme in allen anderen , in AWS-Regionen denen FSx für ONTAP verfügbar ist

FSx-Durchsatzkapazität (MBps	Netzwerkdurchsatzkapazität (MBps		Netzwerk-IOPS	In-Memory-Caching (GB)	NVMe-Caching (GB)	Festplattendurchsatz (MBps		IOPS des SSD-Laufwerks*	
	Baseline	Burst				Baseline	Burst	Baseline	Burst

FSx-Durchsatzkapazität (MBps	Netzwerkdurchsatzkapazität (MBps		Netzwerk-IOPS	In-Memory-Caching (GB)	NVMe-Caching (GB)	Festplattendurchsatz (MBps		IOPS des SSD-Laufwerks*	
128	150	1,250	Zehntausende Baseline	16	150	128	600	6,000	18 750
256	300	1,250		32	300	256	600	12,000	18 750
512	625	1,250	Hunderttausende Baseline	64	600	512	600	18,750	–
1,024	1,500	–		128	1,200	1,024	–	40,000	–
2 048	3,125	–		256	2,400	2,048	–	80,000	–

> **Note**
>
> * Ihre SSD-IOPS werden nur verwendet, wenn Sie auf Daten zugreifen, die nicht im In-Memory-Cache oder NVMe-Cache Ihres Dateiservers zwischengespeichert sind.

Beispiel: Speicherkapazität und Durchsatzkapazität

Das folgende Beispiel zeigt, wie sich Speicherkapazität und Durchsatzkapazität auf die Leistung des Dateisystems auswirken.

Ein Scale-up-Dateisystem, das mit 2 TiB SSD-Speicherkapazität und 512 MBpss Durchsatzkapazität konfiguriert ist, hat die folgenden Durchsatzstufen:

- Netzwerkdurchsatz – Baseline von 625 MBpss und Burst von 1 250 MBpss (siehe Tabelle der Durchsatzkapazität)
- Festplattendurchsatz – 512 MBps Baseline und 600 MBpss Burst.

Ihr Workload, der auf das Dateisystem zugreift, kann daher einen MBps Burst-Durchsatz von bis zu 625 MBpss für Dateioperationen erreichen, die mit aktiv aufgerufenen Daten ausgeführt werden, die im In-Memory-Cache und im NVMe-Cache des Dateiservers zwischengespeichert sind.

Verwaltung von FSx for ONTAP-Ressourcen

Mithilfe der CLI und API von AWS Management Console AWS CLI, und ONTAP können Sie die folgenden Verwaltungsaktionen für FSx for ONTAP-Ressourcen ausführen:

- Dateisysteme, virtuelle Speichermaschinen (SVMs), Volumes, Backups und Tags erstellen, auflisten, aktualisieren und löschen.
- Verwaltung des Zugriffs, Administratorkonten und Passwörter, Kennwortanforderungen, SMB- und iSCSI-Protokolle, Netzwerkzugriff für die Mount-Ziele vorhandener Dateisysteme

Themen

- Verwaltung von FSx für ONTAP-Dateisysteme
- FSx für ONTAP-Dateisysteme erstellen
- Aktualisierung eines Dateisystems
- Löschen eines Dateisystems
- Dateisystemdetails anzeigen
- Verwalten virtueller FSx-für-ONTAP-Speichermaschinen
- Verwaltung von FSx für ONTAP-Volumes
- Eine iSCSI-LUN erstellen
- Verwaltung von SMB-Aktien
- Überwachen des Dateizugriffs
- Skalierung der SSD-Speicherkapazität und der bereitgestellten IOPS
- Verwaltung der Durchsatzkapazität
- Leistungsoptimierung mit Amazon FSx-Wartungsfenstern
- Markieren Sie Ihre Amazon FSx-Ressourcen mit Tags
- Verwaltung von FSx for ONTAP-Ressourcen mithilfe von Anwendungen NetApp

Verwaltung von FSx für ONTAP-Dateisysteme

Ein Dateisystem ist die primäre Amazon FSx-Ressource, analog zu einem lokalen ONTAP-Cluster. Sie geben die Solid-State-Drive-Speicherkapazität (SSD) und die Durchsatzkapazität für Ihr Dateisystem an und wählen eine Virtual Private Cloud (VPC), in der das Dateisystem erstellt werden

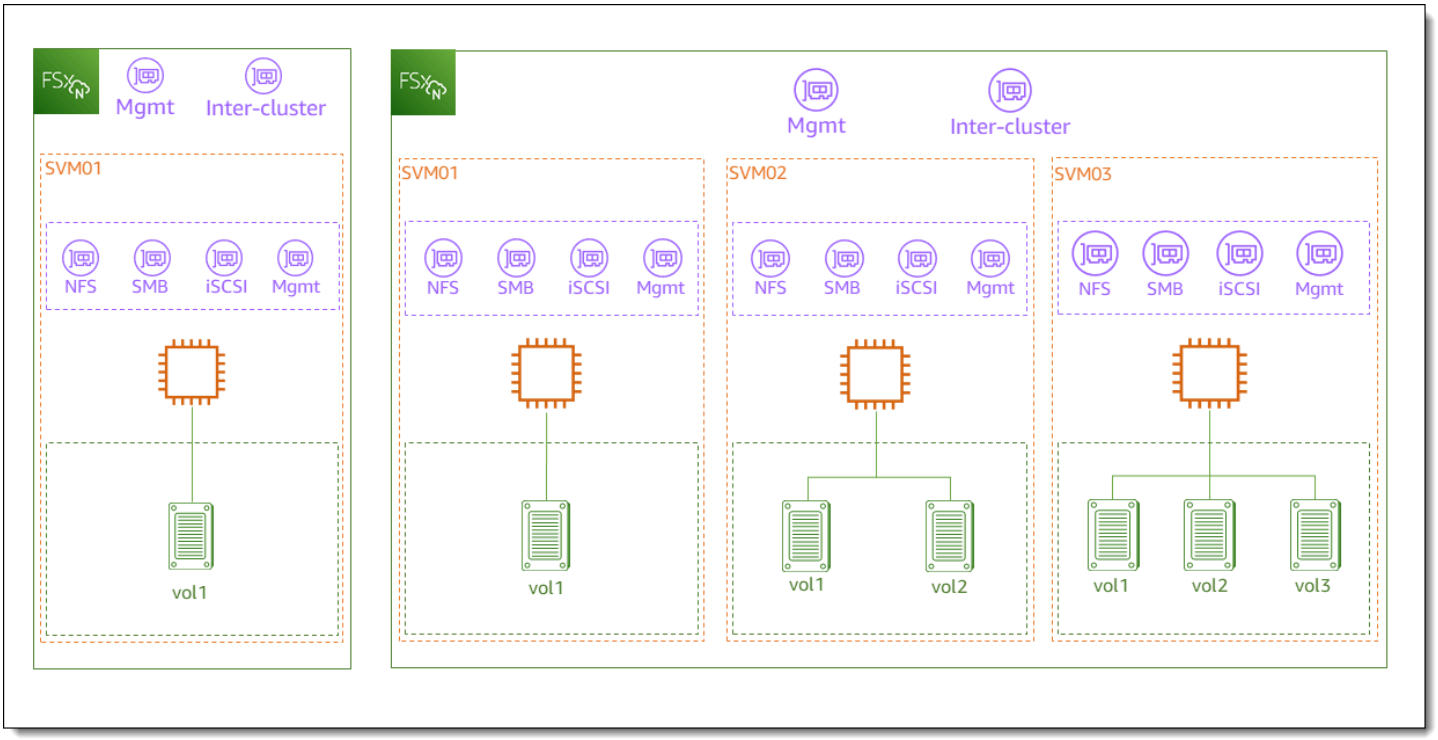
soll. Jedes Dateisystem hat einen Management-Endpunkt, mit dem Sie Ressourcen und Daten mit der ONTAP CLI oder REST API verwalten können.

Ressourcen des Dateisystems

Ein Amazon FSx for NetApp ONTAP-Dateisystem besteht aus den folgenden primären Ressourcen:

- Die physische Hardware des Dateisystems selbst, zu der auch die Dateiserver und Speichermedien gehören.
- Ein oder mehrere Dateiserverpaare mit hoher Verfügbarkeit (HA), die Ihre virtuellen Speichermaschinen (SVMs) hosten. Scale-up-Dateisysteme haben ein HA-Paar und Scale-Out-Dateisysteme haben zwei oder mehr HA-Paare. Jedes HA-Paar hat einen Speicherpool, der als Aggregat bezeichnet wird. Die Sammlung von Aggregaten für alle HA-Paare bildet Ihre SSD-Speicherebene.
- Eine oder mehrere virtuelle Speichermaschinen (SVMs), die die Dateisystem-Volumes hosten und über eigene Anmeldeinformationen und Zugriffsverwaltung verfügen.
- Ein oder mehrere Volumes, die Ihre Daten virtuell organisieren und von Ihren Kunden bereitgestellt werden.

Die folgende Abbildung zeigt die Architektur eines Scale-up-Dateisystems FSx für ONTAP mit einem HA-Paar und die Beziehung zwischen seinen primären Ressourcen. Das Dateisystem FSx for ONTAP auf der linken Seite ist das einfachste Dateisystem mit einer SVM und einem Volume. Das Dateisystem auf der rechten Seite hat mehrere SVMs, wobei einige SVMs mehrere Volumes haben. Dateisysteme und SVMs haben jeweils mehrere Verwaltungsendpunkte, und SVMs haben auch Datenzugriffsendpunkte.



Wenn Sie ein FSx for ONTAP-Dateisystem erstellen, definieren Sie die folgenden Eigenschaften:

- Bereitstellungstyp — Der Bereitstellungstyp Ihres Dateisystems (Multi-AZ oder Single-AZ). Single-AZ-Dateisysteme replizieren Ihre Daten und bieten automatischen Failover innerhalb einer einzigen Availability Zone sowie Scale-Out-Dateisysteme. Multi-AZ-Dateisysteme bieten zusätzliche Stabilität, indem sie auch Ihre Daten replizieren und Failover über mehrere Availability Zones innerhalb derselben unterstützen. AWS-Region
- Speicherkapazität — Dies ist die Menge an SSD-Speicher, bis zu 192 Tebibyte (TiB) für Scale-up-Dateisysteme und 1 Pebibyte (PiB) für Scale-Out-Dateisysteme.
- SSD-IOPS — Standardmäßig umfasst jedes Gigabyte SSD-Speicher drei SSD-IOPS (bis zu dem von Ihrer Dateisystemkonfiguration unterstützten Höchstwert). Sie können optional bei Bedarf zusätzliche SSD-IOPS bereitstellen.
- Durchsatzkapazität — Die konstante Geschwindigkeit, mit der der Dateiserver Daten bereitstellen kann.
- Netzwerke — Die VPC und die Subnetze für die Verwaltungs- und Datenzugriffsendpunkte, die Ihr Dateisystem erstellt. Für ein Multi-AZ-Dateisystem definieren Sie auch einen IP-Adressbereich und Routing-Tabellen.
- Verschlüsselung — Der Schlüssel AWS Key Management Service (AWS KMS), der verwendet wird, um die Dateisystemdaten im Ruhezustand zu verschlüsseln.

- Administratorzugriff — Sie können das Passwort für den `fsxadmin` Benutzer angeben. Sie können diesen Benutzer verwenden, um das Dateisystem mithilfe der NetApp ONTAP CLI und der REST-API zu verwalten.

Sie können FSx for ONTAP-Dateisysteme mithilfe der NetApp ONTAP CLI oder der REST-API verwalten. Sie können auch SnapVault Beziehungen zwischen einem Amazon FSx-Dateisystem und einer anderen ONTAP-Bereitstellung (einschließlich eines anderen Amazon FSx-Dateisystems) einrichten. SnapMirror Jedes FSx for ONTAP-Dateisystem hat die folgenden Dateisystemendpunkte, die den Zugriff auf Anwendungen ermöglichen: NetApp

- Verwaltung — Verwenden Sie diesen Endpunkt, um über Secure Shell (SSH) auf die NetApp ONTAP CLI zuzugreifen oder um die NetApp ONTAP REST API mit Ihrem Dateisystem zu verwenden.
- Intercluster — Verwenden Sie diesen Endpunkt, wenn Sie die Replikation mithilfe NetApp SnapMirror von oder das Caching einrichten. NetApp FlexCache

Weitere Informationen finden Sie unter Verwaltung von FSx for ONTAP-Ressourcen mithilfe von Anwendungen NetApp und Geplante Replikation mit NetApp SnapMirror.

Paare mit hoher Verfügbarkeit (HA)

Jedes Dateisystem FSx for ONTAP wird von einem oder mehreren Dateiserverpaaren mit hoher Verfügbarkeit (HA) in einer Active-Standby-Konfiguration betrieben. In dieser Konfiguration gibt es einen bevorzugten Dateiserver, der aktiv den Datenverkehr abwickelt, und einen sekundären Dateiserver, der übernimmt, wenn der aktive Server nicht verfügbar ist. FSx for ONTAP Scale-up-Dateisysteme werden von einem HA-Paar unterstützt, das eine Durchsatzkapazität von bis zu 4 Gbit/s und 160.000 SSD-IOPs bietet. FSx for ONTAP Scale-out-Dateisysteme werden von bis zu 12 HA-Paaren betrieben, die eine Durchsatzkapazität von bis zu 72 Gbit/s und 2.400.000 SSD-IOPS (6 Gbit/s Durchsatzkapazität und 200.000 SSD-IOPS pro HA-Paar) bieten können.

Wenn Sie Ihr Dateisystem von der Amazon FSx-Konsole aus erstellen, empfiehlt Amazon FSx die Anzahl der HA-Paare, die Sie verwenden sollten, basierend auf Ihrem gewünschten SSD-Speicher. Sie können die Anzahl der HA-Paare auch manuell auf der Grundlage Ihrer Arbeitslast- und Leistungsanforderungen auswählen. Wir empfehlen, dass Sie ein einzelnes HA-Paar verwenden, wenn Ihre Dateisystemanforderungen durch eine Durchsatzkapazität von bis zu 4 Gbit/s und 160.000 SSD-IOPs erfüllt werden, sowie mehrere HA-Paare, wenn Ihre Workloads ein höheres Maß an Leistungsskalierbarkeit erfordern.

Jedes HA-Paar hat ein Aggregat, bei dem es sich um einen logischen Satz physischer Festplatten handelt.

> **Note**
>
> Sie können vorhandenen Dateisystemen keine HA-Paare hinzufügen. Stattdessen können Sie Daten zwischen Dateisystemen (mit unterschiedlichen HA-Paaren) mithilfe von SnapMirror AWS DataSync, oder durch Wiederherstellen Ihrer Daten aus einer Sicherung in einem neuen Dateisystem migrieren.

FSx für ONTAP-Dateisysteme erstellen

In diesem Abschnitt wird beschrieben, wie Sie mithilfe der Amazon FSx-Konsole oder der Amazon FSx-API ein FSx for ONTAP-Dateisystem erstellen. AWS CLI Sie können ein Dateisystem in einer Virtual Private Cloud (VPC) erstellen, die Sie besitzen, oder in einer VPC, die ein anderer mit Ihnen geteilt AWS-Konto hat. Bei der Erstellung eines Multi-AZ-Dateisystems in einer VPC, an der Sie teilnehmen, gibt es einige Überlegungen. Diese Überlegungen werden in diesem Thema erläutert.

Wenn Sie ein neues Dateisystem von der Amazon FSx-Konsole aus erstellen, erstellt Amazon FSx standardmäßig automatisch ein Dateisystem mit einer einzigen virtuellen Speichermaschine (SVM) und einem Volume, sodass Sie über das Network File System (NFS) -Protokoll schnell auf Daten von Linux-Instances zugreifen können. Bei der Erstellung des Dateisystems können Sie die SVM optional einem Active Directory hinzufügen, um den Zugriff von Windows- und macOS-Clients über das SMB-Protokoll (Server Message Block) zu ermöglichen. Nachdem Ihr Dateisystem erstellt wurde, können Sie bei Bedarf weitere SVMs und Volumes erstellen.

Um ein Dateisystem (Konsole) zu erstellen

Bei diesem Verfahren wird die Option Standard create creation verwendet, um ein FSx for ONTAP-Dateisystem mit einer Konfiguration zu erstellen, die Sie an Ihre Bedürfnisse anpassen. Informationen zur Verwendung der Option Schnellerstellung, um schnell ein Dateisystem mit einem Standardsatz von Konfigurationsparametern zu erstellen, finden Sie unter. Schritt 1: Erstellen eines Dateisystems von Amazon FSx für NetApp ONTAP

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Dashboard Create file system aus.

3. Wählen Sie auf der Seite Dateisystemtyp auswählen unter Dateisystemoptionen die Option Amazon FSx for NetApp ONTAP und dann Weiter.
4. Wählen Sie im Abschnitt Erstellungsmethode die Option Standard erstellen aus.
5. Geben Sie im Abschnitt Dateisystemdetails die folgenden Informationen ein:

   - Geben Sie unter Dateisystemname — optional einen Namen für Ihr Dateisystem ein. 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 folgenden Sonderzeichen verwenden: + - =. _:/
   - Wählen Sie als Bereitstellungstyp Multi-AZ oder Single-AZ.
     - Multi-AZ-Dateisysteme replizieren Ihre Daten und unterstützen Failover über mehrere Availability Zones hinweg in derselben. AWS-Region
     - Single-AZ-Dateisysteme replizieren Ihre Daten und bieten automatischen Failover innerhalb einer einzigen Availability Zone.

     > **Note**
     >
     > Wählen Sie Single-AZ, wenn Sie die Option haben möchten, ein Dateisystem mit zwei oder mehr Hochverfügbarkeitspaaren (HA) (bis zu 12) zu erstellen. Weitere Informationen finden Sie unter Paare mit hoher Verfügbarkeit (HA).

     Weitere Informationen finden Sie unter Verfügbarkeit und Beständigkeit.
   - Geben Sie für SSD-Speicherkapazität die Speicherkapazität Ihres Dateisystems in Gibibyte (GiB) ein. Geben Sie eine ganze Zahl im Bereich von 1.024—1.048.576 GiB (bis zu 1 Pebibyte [PiB]) ein.

     Sie können die Speicherkapazität jederzeit nach der Erstellung des Dateisystems nach Bedarf erhöhen. Weitere Informationen finden Sie unter Verwaltung der Speicherkapazität.
   - Für bereitgestellte SSD-IOPS haben Sie zwei Möglichkeiten, die Anzahl der IOPS für Ihr Dateisystem bereitzustellen:
     - Wählen Sie Automatisch (Standardeinstellung), wenn Amazon FSx automatisch 3 IOPS pro GiB SSD-Speicher bereitstellen soll.
     - Wählen Sie Vom Benutzer bereitgestellt, wenn Sie die Anzahl der IOPS angeben möchten. Sie können maximal 200.000 SSD-IOPS pro Dateisystem bereitstellen.

> **Note**
>
> Sie können Ihre bereitgestellten SSD-IOPS erhöhen, nachdem Sie das Dateisystem erstellt haben. Beachten Sie, dass der maximale SSD-IOPS-Wert, den Ihr Dateisystem erreichen kann, auch von der Durchsatzkapazität Ihres Dateisystems abhängt, selbst wenn Sie zusätzliche SSD-IOPS bereitstellen. Weitere Informationen finden Sie unter Auswirkungen der Durchsatzkapazität auf die Leistung und Verwaltung der Speicherkapazität.

- Für die Durchsatzkapazität haben Sie zwei Möglichkeiten, Ihre Durchsatzkapazität in Megabyte pro Sekunde (MBps) zu bestimmen:
  - Wählen Sie Empfohlene Durchsatzkapazität, wenn Amazon FSx die Durchsatzkapazität automatisch auf der Grundlage der von Ihnen ausgewählten Speicherkapazität auswählen soll.
  - Wählen Sie Durchsatzkapazität angeben, wenn Sie die Höhe der Durchsatzkapazität angeben möchten. Wenn Sie diese Option wählen, wird eine Dropdownliste für die Durchsatzkapazität angezeigt, die auf dem von Ihnen ausgewählten Bereitstellungstyp basiert. Sie können auch die Anzahl der HA-Paare (bis zu 12) wählen. Weitere Informationen finden Sie unter Paare mit hoher Verfügbarkeit (HA).

  Die Durchsatzkapazität ist die konstante Geschwindigkeit, mit der der Dateiserver, der Ihr Dateisystem hostet, Daten bereitstellen kann. Weitere Informationen finden Sie unter Leistung von Amazon FSx für NetApp ONTAP.

6. Geben Sie im Abschnitt Netzwerk die folgenden Informationen an:

   - Wählen Sie für Virtual Private Cloud (VPC) die VPC aus, die Sie Ihrem Dateisystem zuordnen möchten.
   - Für VPC-Sicherheitsgruppen können Sie eine Sicherheitsgruppe auswählen, die der Netzwerkschnittstelle Ihres Dateisystems zugeordnet werden soll. Wenn Sie keine angeben, ordnet Amazon FSx die Standardsicherheitsgruppe der VPC Ihrem Dateisystem zu.
   - Geben Sie ein Subnetz für Ihren Dateiserver an. Wenn Sie ein Multi-AZ-Dateisystem erstellen, wählen Sie auch ein Standby-Subnetz für den Standby-Dateiserver.
   - (Nur Multi-AZ) Geben Sie für VPC-Routing-Tabellen die VPC-Routing-Tabellen an, um die Endpunkte Ihres Dateisystems zu erstellen. Wählen Sie alle VPC-Routing-Tabellen aus, die den Subnetzen zugeordnet sind, in denen sich Ihre Clients befinden. Standardmäßig wählt

Amazon FSx die Standard-Routing-Tabelle Ihrer VPC aus. Weitere Informationen finden Sie unter Zugriff auf Daten von außerhalb der Bereitstellungs-VPC.

> **Note**
>
> Amazon FSx verwaltet diese Routing-Tabellen für Multi-AZ-Dateisysteme mithilfe von Tag-basierter Authentifizierung. Diese Routing-Tabellen sind mit gekennzeichnet. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Wenn Sie FSx für ONTAP Multi-AZ-Dateisysteme mit verwenden, empfehlen AWS CloudFormation wir, das Tag manuell hinzuzufügen. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

- (Nur Multi-AZ) Der Endpunkt-IP-Adressbereich gibt den IP-Adressbereich an, in dem die Endpoints für den Zugriff auf Ihr Dateisystem erstellt werden.

  Sie haben drei Optionen für den Endpunkt-IP-Adressbereich:

  - Nicht zugewiesener IP-Adressbereich aus Ihrer VPC — Amazon FSx wählt die letzten 64 IP-Adressen aus dem primären CIDR-Bereich der VPC aus, um sie als Endpunkt-IP-Adressbereich für das Dateisystem zu verwenden. Dieser Bereich wird von mehreren Dateisystemen gemeinsam genutzt, wenn Sie diese Option mehrmals wählen.

    > **Note**
    >
    > Diese Option ist ausgegraut, wenn eine der letzten 64 IP-Adressen im primären CIDR-Bereich einer VPC von einem Subnetz verwendet wird. In diesem Fall können Sie immer noch einen In-VPC-Adressbereich auswählen (d. h. einen Bereich, der nicht am Ende Ihres primären CIDR-Bereichs liegt, oder einen Bereich, der sich in einem sekundären CIDR Ihrer VPC befindet), indem Sie die Option Einen IP-Adressbereich eingeben auswählen.

  - Geben Sie unter Bevorzugtes Subnetz ein Subnetz für Ihren Dateiserver an. Wenn Sie ein Multi-AZ-Dateisystem erstellen, wählen Sie auch ein Standby-Subnetz für den Standby-Dateiserver.
  - (Nur Multi-AZ) Geben Sie für VPC-Routing-Tabellen die VPC-Routing-Tabellen an, um die Endpunkte Ihres Dateisystems zu erstellen. Wählen Sie alle VPC-Routing-Tabellen aus, die den Subnetzen zugeordnet sind, in denen sich Ihre Clients befinden. Standardmäßig wählt Amazon FSx die Standard-Routing-Tabelle Ihrer VPC aus.

- (Nur Multi-AZ) Der Endpunkt-IP-Adressbereich gibt den IP-Adressbereich an, in dem die Endpunkte für den Zugriff auf Ihr Dateisystem erstellt werden.

  Sie haben drei Optionen für den Endpunkt-IP-Adressbereich:

  - Nicht zugewiesener IP-Adressbereich aus Ihrer VPC — Amazon FSx wählt die letzten 64 IP-Adressen aus dem primären CIDR-Bereich der VPC aus, um sie als Endpunkt-IP-Adressbereich für das Dateisystem zu verwenden. Dieser Bereich wird von mehreren Dateisystemen gemeinsam genutzt, wenn Sie diese Option mehrmals wählen.

    > **Note**
    >
    > Diese Option ist ausgegraut, wenn eine der letzten 64 IP-Adressen im primären CIDR-Bereich einer VPC von einem Subnetz verwendet wird. In diesem Fall können Sie immer noch einen In-VPC-Adressbereich auswählen (d. h. einen Bereich, der nicht am Ende Ihres primären CIDR-Bereichs liegt, oder einen Bereich, der sich in einem sekundären CIDR Ihrer VPC befindet), indem Sie die Option Einen IP-Adressbereich eingeben auswählen.

  - Floating-IP-Adressbereich außerhalb Ihrer VPC — Amazon FSx wählt einen 198.19.x.0/24-Adressbereich, der noch nicht von anderen Dateisystemen mit derselben VPC und Routing-Tabellen verwendet wird.
  - Geben Sie einen IP-Adressbereich ein — Sie können einen CIDR-Bereich Ihrer Wahl angeben. Der von Ihnen gewählte IP-Adressbereich kann entweder innerhalb oder außerhalb des IP-Adressbereichs der VPC liegen, sofern er sich nicht mit einem Subnetz überschneidet.

    > **Note**
    >
    > Wählen Sie keinen Bereich, der in die folgenden CIDR-Bereiche fällt, da diese nicht mit FSx for ONTAP kompatibel sind:
    >
    > - 0.0.0.0/8
    > - 127,0.0.0/8
    > - 198,19.0.0/20
    > - 224.0.0.0/4
    > - 240.0.0.0/4

- 255,255,255,255/32

7. Wählen Sie im Abschnitt Sicherheit und Verschlüsselung für Verschlüsselungsschlüssel den Verschlüsselungsschlüssel AWS Key Management Service (AWS KMS) aus, der die Daten Ihres Dateisystems im Ruhezustand schützt.
8. Geben Sie unter Administratorkennwort für das Dateisystem ein sicheres Passwort für den `fsxadmin` Benutzer ein. Bestätigen Sie das Passwort.

   Sie können den `fsxadmin` Benutzer verwenden, um Ihr Dateisystem mithilfe der ONTAP CLI und der REST-API zu verwalten. Weitere Informationen über den `fsxadmin` Benutzer finden Sie unter. Verwaltung von Dateisystemen mit der ONTAP CLI
9. Geben Sie im Abschnitt Standardkonfiguration für virtuelle Speichermaschinen die folgenden Informationen ein:

   - Geben Sie im Feld Name der virtuellen Speichermaschine einen Namen für die virtuelle Speichermaschine ein. Sie können maximal 47 alphanumerische Zeichen plus den Unterstrich (_) als Sonderzeichen verwenden.
   - Als Administratorkennwort für die SVM können Sie optional Passwort angeben wählen und ein Passwort für den SVM-Benutzer angeben. `vsadmin` Sie können den `vsadmin` Benutzer verwenden, um die SVM mithilfe der ONTAP CLI oder der REST-API zu verwalten. Weitere Informationen über den `vsadmin` Benutzer finden Sie unter. Verwaltung von SVMs mit der CLI ONTAP

     Wenn Sie Kein Passwort angeben (Standardeinstellung) wählen, können Sie trotzdem den `fsxadmin` Benutzer des Dateisystems verwenden, um Ihr Dateisystem mithilfe der ONTAP CLI oder der REST-API zu verwalten, aber Sie können nicht den `vsadmin` Benutzer Ihrer SVM dafür verwenden.
   - Im Bereich Active Directory können Sie der SVM ein Active Directory hinzufügen. Weitere Informationen finden Sie unter Arbeiten mit Microsoft Active Directory in FSx für ONTAP.

     Wenn Sie Ihre SVM nicht zu einem Active Directory hinzufügen möchten, wählen Sie Nicht einem Active Directory beitreten.

     Wenn Sie Ihre SVM einer selbstverwalteten Active Directory-Domäne hinzufügen möchten, wählen Sie Einem Active Directory beitreten und geben Sie die folgenden Informationen für Ihr Active Directory an:

- Der NetBIOS-Name des Active Directory-Computerobjekts, das für Ihre SVM erstellt werden soll. Der NetBIOS-Name darf 15 Zeichen nicht überschreiten.
- Der vollqualifizierte Domänenname Ihres Active Directory. Der Domänenname darf 255 Zeichen nicht überschreiten.
- IP-Adressen von DNS-Servern — Die IPv4-Adressen der DNS-Server (Domain Name System) für Ihre Domain.
- 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.
- Passwort bestätigen — Das Passwort für das Dienstkonto.
- (Optional) Organizational Unit (OU) — Der definierte Pfadname der Organisationseinheit, mit der Sie Ihr Dateisystem verbinden möchten.
- Gruppe delegierter Dateisystemadministratoren — Der Name der Gruppe in Ihrem Active Directory, die Ihr Dateisystem verwalten kann.

  Wenn Sie verwenden AWS Managed Microsoft AD, müssen Sie eine Gruppe wie AWS Delegated FSx Administrators, Delegated Administrators oder eine benutzerdefinierte Gruppe mit AWS delegierten Berechtigungen für die OU angeben.

  Wenn Sie einem selbstverwalteten AD beitreten, verwenden Sie den Namen der Gruppe in Ihrem AD. Die Standardgruppe ist`Domain Admins`.

10. Geben Sie im Abschnitt Standard-Volume-Konfiguration die folgenden Informationen für das Standardvolume an, das mit Ihrem Dateisystem erstellt wird:

    - Geben Sie im Feld Volumenname einen Namen für das Volume ein. Sie können bis zu 203 alphanumerische Zeichen oder Unterstriche (_) verwenden.
    - (Nur Dateisysteme hochskalieren) Wählen Sie für den Volume-Stil entweder oder. FlexVolFlexGroup FlexVolVolumen sind Allzweckvolumen, die eine Größe von bis zu 300 TiB haben können. FlexGroupVolumes sind für Hochleistungs-Workloads vorgesehen und können eine Größe von bis zu 20 PiB haben.
    - Geben Sie für Volumengröße eine beliebige ganze Zahl im Bereich von 800 Gibibyte (GiB) bis 2.000 Pebibyte (PiB) ein.
    - Wählen Sie für Volumetyp die Option Read-Write (RW), um ein Volumen zu erstellen, das lesbar und beschreibbar ist, oder Data Protection (DP), um ein Volume zu erstellen, das

schreibgeschützt ist und als Ziel einer Oder-Beziehung verwendet werden kann. NetApp SnapMirror SnapVault Weitere Informationen finden Sie unter Volume-Typen.

- Geben Sie für Junction Path einen Speicherort im Dateisystem ein, an dem das Volume bereitgestellt werden soll. Dem Namen muss beispielsweise `/vol3` ein Schrägstrich vorangestellt werden.
- Wählen Sie für Speichereffizienz Enabled, um die ONTAP-Speichereffizienzfunktionen (Deduplizierung, Komprimierung und Verdichtung) zu aktivieren. Weitere Informationen finden Sie unter FSx für ONTAP-Speichereffizienz.
- Wählen Sie für das Volume Security Style zwischen Unix (Linux), NTFS und Mixed für das Volume. Weitere Informationen finden Sie unter Sicherheitsstil des Volumes.
- Wählen Sie unter Snapshot-Richtlinie eine Snapshot-Richtlinie für das Volume aus. Weitere Informationen zu Snapshot-Richtlinien finden Sie unterSnapshot-Richtlinien.

  Wenn Sie „Benutzerdefinierte Richtlinie“ wählen, müssen Sie den Namen der Richtlinie im Feld „Benutzerdefinierte Richtlinie“ angeben. Die benutzerdefinierte Richtlinie muss bereits auf der SVM oder im Dateisystem vorhanden sein. Sie können mit der ONTAP CLI oder der REST API eine benutzerdefinierte Snapshot-Richtlinie erstellen. Weitere Informationen finden Sie unter Erstellen einer Snapshot-Richtlinie in der NetApp ONTAP-Produktdokumentation.

11. Wählen Sie im Abschnitt Standard Volume Storage Tiering für Capacity Pool Tiering Policy die Storage-Pool-Tiering-Richtlinie für das Volume aus. Dabei kann es sich um Automatisch (Standardeinstellung), Nur Snapshot, Alle oder Keine handeln. Weitere Informationen zu Richtlinien für das Tiering von Kapazitätspools finden Sie unter. Richtlinien für das Volumen-Tiering

    Wenn Sie für die Abkühlungszeit bei der Staffelung von Richtlinien die Option Speicherstufenzuweisung oder `Snapshot-only` Richtlinien festgelegt haben. Gültige Werte `Auto` liegen zwischen 2 und 183 Tagen. Die Abkühlperiode eines Volumes definiert die Anzahl der Tage, bevor Daten, auf die nicht zugegriffen wurde, als kalt markiert und in den Capacity-Pool-Speicher verschoben werden.

12. Unter Backup und Wartung — optional können Sie die folgenden Optionen festlegen:

    - Wählen Sie für Tägliches automatisches Backup die Option Aktiviert für automatische tägliche Backups aus. Diese Option ist standardmäßig aktiviert.
    - Geben Sie unter Tägliches automatisches Backup-Fenster die Uhrzeit in koordinierter Weltzeit (UTC) an, zu der das tägliche automatische Backup-Fenster gestartet werden soll. Ab dieser

angegebenen Uhrzeit beträgt das Zeitfenster 30 Minuten. Dieses Fenster darf sich nicht mit dem wöchentlichen Backup-Fenster für Wartungsarbeiten überschneiden.

- Legen Sie für den Aufbewahrungszeitraum für automatische Backups einen Zeitraum von 1—90 Tagen fest, für den Sie automatische Backups aufbewahren möchten.
- Für das wöchentliche Wartungsfenster können Sie die Uhrzeit festlegen, zu der das Wartungsfenster beginnen soll. Tag 1 ist Montag, 2 ist Dienstag usw. Ab diesem angegebenen Zeitpunkt beträgt das Zeitfenster 30 Minuten. Dieses Fenster darf sich nicht mit dem täglichen automatischen Backup-Fenster überschneiden.

13. Unter Tags — optional können Sie einen Schlüssel und einen Wert eingeben, 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.

    Wählen Sie Weiter aus.

14. Prüfen Sie die Dateisystemkonfiguration, die auf der Seite Create File System (Dateisystem erstellen) angezeigt wird. Notieren Sie sich zu Referenzzwecken, welche Dateisystemeinstellungen Sie nach der Erstellung des Dateisystems ändern können.
15. Wählen Sie Create file system (Dateisystem erstellen) aus.

Um ein Dateisystem (CLI) zu erstellen

- Um ein FSx for ONTAP-Dateisystem zu erstellen, verwenden Sie den create-file-systemCLI-Befehl (oder die entsprechende CreateFileSystemAPI-Operation), wie im folgenden Beispiel gezeigt.

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \

    --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
    --ontap-configuration DeploymentType=MULTI_AZ_1,
        ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

Nach erfolgreicher Erstellung des Dateisystems gibt Amazon FSx die Beschreibung des Dateisystems im JSON-Format zurück, wie im folgenden Beispiel gezeigt.


```
{
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
                "Mode": "AUTOMATIC",
                "Iops": 3072
      },
      "PreferredSubnetId": "subnet-abcdef1234567890b",
      "RouteTableIds": [
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
      ],
      "ThroughputCapacity": 512,
```

```
      "WeeklyMaintenanceStartTime": "4:10:00"
    }
  }
}
```

> **Note**
>
> Im Gegensatz zur Erstellung eines Dateisystems in der Konsole erstellen der `create-file-system` CLI-Befehl und die `CreateFileSystem` API-Operation keine Standard-SVM oder kein Standardvolume. Informationen zum Erstellen einer SVM finden Sie unterErstellen einer virtuellen Speichermaschine; Informationen zum Erstellen eines Volumes finden Sie unter. Volumen erstellen

FSx für ONTAP-Dateisysteme in gemeinsam genutzten Subnetzen erstellen

VPC-Sharing ermöglicht es mehreren AWS-Konten , Ressourcen in gemeinsam genutzten, zentral verwalteten Virtual Private Clouds (VPCs) zu erstellen. In diesem Modell teilt sich das Konto, dem die VPC gehört (Eigentümer), ein oder mehrere Subnetze mit anderen Konten (Teilnehmern), die derselben Organisation angehören. AWS Organizations

Teilnehmerkonten können FSx für ONTAP Single-AZ- und Multi-AZ-Dateisysteme in einem VPC-Subnetz erstellen, das das Eigentümerkonto mit ihnen geteilt hat. Damit ein Teilnehmerkonto ein Multi-AZ-Dateisystem erstellen kann, muss das Besitzerkonto Amazon FSx außerdem die Erlaubnis erteilen, Routing-Tabellen in den gemeinsam genutzten Subnetzen im Namen des Teilnehmerkontos zu ändern. Weitere Informationen finden Sie unter Verwaltung der gemeinsamen VPC-Unterstützung für Multi-AZ-Dateisysteme.

> **Note**
>
> Es liegt in der Verantwortung des Teilnehmerkontos, sich mit dem VPC-Eigentümer abzustimmen, um zu verhindern, dass nachfolgende VPC-Subnetze erstellt werden, die sich mit dem VPC-internen CIDR der Dateisysteme des Teilnehmers überschneiden. Wenn sich Subnetze überschneiden, kann der Datenverkehr zum Dateisystem unterbrochen werden.

Anforderungen und Überlegungen für gemeinsam genutzte Subnetze

Beachten Sie beim Erstellen von FSx for ONTAP-Dateisystemen in gemeinsam genutzten Subnetzen Folgendes:

- Der Besitzer des VPC-Subnetzes muss ein Subnetz mit einem Teilnehmerkonto teilen, bevor dieses Konto darin ein FSx for ONTAP-Dateisystem erstellen kann.
- Sie können keine Ressourcen mit der Standardsicherheitsgruppe für die VPC starten, da diese dem Eigentümer gehört. Darüber hinaus können Teilnehmerkonten keine Ressourcen mithilfe von Sicherheitsgruppen starten, die anderen Teilnehmern oder dem Eigentümer gehören.
- In einem gemeinsam genutzten Subnetz kontrollieren der Teilnehmer und der Eigentümer die Sicherheitsgruppen innerhalb des jeweiligen Kontos separat. Das Besitzerkonto kann Sicherheitsgruppen sehen, die von den Teilnehmern erstellt wurden, kann jedoch keine Aktionen für sie ausführen. Wenn das Besitzerkonto diese Sicherheitsgruppen entfernen oder ändern möchte, muss der Teilnehmer, der die Sicherheitsgruppe erstellt hat, die Aktion ausführen.
- Teilnehmerkonten können Single-AZ-Dateisysteme und die zugehörigen Ressourcen in Subnetzen, die das Besitzerkonto mit ihnen geteilt hat, anzeigen, erstellen, ändern und löschen.
- Teilnehmerkonten können Multi-AZ-Dateisysteme und die zugehörigen Ressourcen in Subnetzen, die das Eigentümerkonto mit ihnen geteilt hat, erstellen, anzeigen, ändern und löschen. Darüber hinaus muss das Besitzerkonto dem Amazon FSx-Service auch Berechtigungen zur Änderung von Routing-Tabellen in den gemeinsam genutzten Subnetzen im Namen des Teilnehmerkontos gewähren. Weitere Informationen finden Sie unter Verwaltung der gemeinsamen VPC-Unterstützung für Multi-AZ-Dateisysteme.
- Der Besitzer einer gemeinsam genutzten VPC kann Ressourcen, die ein Teilnehmer im gemeinsam genutzten Subnetz erstellt, nicht anzeigen, ändern oder löschen. Dies gilt zusätzlich zu den VPC-Ressourcen, auf die jedes Konto unterschiedlich zugreifen kann. Weitere Informationen finden Sie unter Verantwortlichkeiten und Berechtigungen für Eigentümer und Teilnehmer im Amazon VPC-Benutzerhandbuch.

Weitere Informationen finden Sie unter Teilen Ihrer VPC mit anderen Konten im Amazon VPC-Benutzerhandbuch.

Bei der gemeinsamen Nutzung eines VPC-Subnetzes

Wenn Sie Ihre Subnetze mit Teilnehmerkonten teilen, die FSx for ONTAP-Dateisysteme in den gemeinsam genutzten Subnetzen erstellen, müssen Sie wie folgt vorgehen:

- Der VPC-Besitzer muss VPCs und Subnetze sicher mit anderen teilen. AWS Resource Access Manager AWS-Konten Weitere Informationen finden Sie im Benutzerhandbuch unter Gemeinsame Nutzung Ihrer AWS Ressourcen. AWS Resource Access Manager
- Der VPC-Besitzer muss eine oder mehrere VPCs mit einem Teilnehmerkonto teilen. Weitere Informationen finden Sie unter Teilen Ihrer VPC mit anderen Konten im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.
- Damit Teilnehmerkonten FSx für ONTAP Multi-AZ-Dateisysteme erstellen können, muss der VPC-Besitzer dem Amazon FSx-Service auch Berechtigungen zum Erstellen und Ändern von Routing-Tabellen in den gemeinsam genutzten Subnetzen im Namen der Teilnehmerkonten gewähren. Dies liegt daran, dass FSx for ONTAP Multi-AZ-Dateisysteme Floating-IP-Adressen verwenden, sodass verbundene Clients während eines Failover-Ereignisses nahtlos zwischen dem bevorzugten und dem Standby-Dateiserver wechseln können. Wenn ein Failover-Ereignis eintritt, aktualisiert Amazon FSx alle Routen in allen Routentabellen, die dem Dateisystem zugeordnet sind, sodass sie auf den aktuell aktiven Dateiserver verweisen.

Verwaltung der gemeinsamen VPC-Unterstützung für Multi-AZ-Dateisysteme

Besitzerkonten können verwalten, ob Teilnehmerkonten Multi-AZ-FSx für ONTAP-Dateisysteme in VPC-Subnetzen erstellen können, die der Eigentümer mithilfe der API, und mit Teilnehmern geteilt hat AWS Management Console AWS CLI, wie in den folgenden Abschnitten beschrieben.

So verwalten Sie die VPC-Sharing für Multi-AZ-Dateisysteme (Konsole)

Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.

1. Wählen Sie im Navigationsbereich Settings (Einstellungen).
2. Suchen Sie auf der Seite Einstellungen nach den Einstellungen für gemeinsam genutzte Multi-AZ-VPC-Einstellungen.
   - Um VPC-Sharing für Multi-AZ-Dateisysteme in von Ihnen gemeinsam VPC VPC-Subnetzen zu aktivieren, wählen Sie Routentabellenaktualisierungen von Teilnehmerkonten aktivieren aus.
   - Um die VPC-Sharing für Multi-AZ-Dateisysteme in allen VPCs, die Sie besitzen, zu deaktivieren, wählen Sie Routentabellenaktualisierungen von Teilnehmerkonten deaktivieren aus. Der Bestätigungsbildschirm wird angezeigt.

> **Important**
>
> Wir empfehlen dringend, von Teilnehmern erstellte Multi-AZ-Dateisysteme in der gemeinsam genutzten VPC zu löschen, bevor Sie diese Funktion deaktivieren. Sobald die Funktion deaktiviert ist, gehen diese Dateisysteme in einen `MISCONFIGURED` Zustand über und es besteht die Gefahr, dass sie nicht mehr verfügbar sind.

3. Geben Sie ein **`confirm`** und wählen Sie Bestätigen, um die Funktion zu deaktivieren.

So verwalten Sie die VPC-Sharing für Multi-AZ-Dateisysteme ()AWS CLI

1. Um die aktuelle Einstellung für Multi-AZ-VPC-Sharing anzuzeigen, verwenden Sie den describe-shared-vpc-configurationCLI-Befehl oder den entsprechenden DescribeSharedVpcConfigurationAPI-Befehl, der wie folgt dargestellt wird:

   ```
   $ aws fsx describe-shared-vpc-configuration
   ```

   Der Dienst reagiert auf eine erfolgreiche Anfrage wie folgt:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
   }
   ```

2. Verwenden Sie den update-shared-vpc-configurationCLI-Befehl oder den entsprechenden UpdateSharedVpcConfigurationAPI-Befehl, um die gemeinsam genutzte Multi-AZ-VPC-Konfiguration zu verwalten. Das folgende Beispiel aktiviert VPC-Sharing für Multi-AZ-Dateisysteme.

   ```
   $ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
   ```

   Der Dienst reagiert auf eine erfolgreiche Anfrage wie folgt:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
   }
   ```

3. Um die Funktion zu deaktivieren, stellen Sie `EnableFsxRouteTableUpdatesFromParticipantAccountsfalse`, wie im folgenden Beispiel gezeigt, auf ein.

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-
participant-accounts false
```

Der Dienst reagiert auf eine erfolgreiche Anfrage wie folgt:

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

Aktualisierung eines Dateisystems

In diesem Thema wird erklärt, welche Eigenschaften eines vorhandenen Dateisystems Sie aktualisieren können, und es werden Verfahren beschrieben, wie Sie dies mithilfe der Konsole und der CLI tun können.

Sie können die folgenden FSx for ONTAP-Dateisystemeigenschaften mithilfe der Amazon FSx-Konsole AWS CLI, der und der Amazon FSx-API aktualisieren:

- Automatische tägliche Backups. Schaltet automatische tägliche Backups ein oder aus, ändert das Backup-Fenster und den Aufbewahrungszeitraum für Backups. Weitere Informationen über Sicherungen finden Sie unter Arbeiten Sie mit automatischen täglichen Backups.
- Wöchentliches Wartungsfenster. Legt den Wochentag und die Uhrzeit fest, an dem Amazon FSx Dateisystemwartungen und -aktualisierungen durchführt. Weitere Informationen zum Wartungsfenster finden Sie unterLeistungsoptimierung mit Amazon FSx-Wartungsfenstern.
- Administratorkennwort für das Dateisystem. Ändert das Passwort für den `fsxadmin` Benutzer des Dateisystems. Sie können den `fsxadmin` Benutzer verwenden, um Ihr Dateisystem mithilfe der ONTAP CLI und der REST-API zu verwalten. Weitere Informationen über den `fsxadmin` Benutzer finden Sie unter. Verwaltung von Dateisystemen mit der ONTAP CLI
- Amazon VPC-Routing-Tabellen. Mit Multi-AZ FSx für ONTAP-Dateisysteme verwenden die Endpunkte, die Sie für den Zugriff auf Daten über NFS oder SMB verwenden, und die Management-Endpunkte für den Zugriff auf die ONTAP CLI, API und BlueXP Floating-IP-Adressen in den Amazon VPC-Routing-Tabellen, die Sie Ihrem Dateisystem zuordnen. Sie können neue

Routing-Tabellen, die Sie erstellen, mit Ihren vorhandenen Multi-AZ-Dateisystemen verknüpfen. Auf diese Weise können Sie konfigurieren, welche Clients auf Ihre Daten zugreifen können, auch wenn sich Ihr Netzwerk weiterentwickelt. Sie können auch bestehende Routing-Tabellen von Ihrem Dateisystem trennen (entfernen).

> **Note**
>
> Amazon FSx verwaltet VPC-Routing-Tabellen für Multi-AZ-Dateisysteme mithilfe von Tag-basierter Authentifizierung. Diese Routing-Tabellen sind mit gekennzeichnet. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Wenn Sie FSx für ONTAP Multi-AZ-Dateisysteme mithilfe von FSx erstellen oder aktualisieren, empfehlen AWS CloudFormation wir, das Tag manuell hinzuzufügen. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Um ein Dateisystem (Konsole) zu aktualisieren

Die folgenden Verfahren enthalten Anweisungen zum Aktualisieren eines vorhandenen FSx for ONTAP-Dateisystems mithilfe von. AWS Management Console

Um automatische tägliche Backups zu aktualisieren

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 linken Navigationsbereich Dateisysteme und dann das FSx for ONTAP-Dateisystem aus, das Sie aktualisieren möchten.
3. Wählen Sie im zweiten Bereich der Seite die Registerkarte Backups.
4. Wählen Sie Aktualisieren.
5. Ändern Sie die Einstellungen für das automatische tägliche Backup für dieses Dateisystem.
6. Wählen Sie Speichern, um Ihre Änderungen zu speichern.

Um das wöchentliche Wartungsfenster zu aktualisieren

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 linken Navigationsbereich Dateisysteme und dann das FSx for ONTAP-Dateisystem aus, das Sie aktualisieren möchten.
3. Wählen Sie im zweiten Bereich der Seite die Registerkarte Administration aus.

4. Wählen Sie im Wartungsbereich die Option Update aus.
5. Ändern Sie, wann das wöchentliche Wartungsfenster für dieses Dateisystem beginnt.
6. Wählen Sie Speichern, um Ihre Änderungen zu speichern.

Um das Administratorkennwort für das Dateisystem zu ändern

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 linken Navigationsbereich Dateisysteme und dann das FSx for ONTAP-Dateisystem aus, das Sie aktualisieren möchten.
3. Wählen Sie die Registerkarte Administration.
4. Wählen Sie im ONTAP-Administrationsbereich unter ONTAP-Administratorkennwort die Option Update aus.
5. Geben Sie im Dialogfeld ONTAP-Administratoranmeldedaten aktualisieren ein neues Passwort in das Feld ONTAP-Administratorkennwort ein.
6. Verwenden Sie das Feld Passwort bestätigen, um das Passwort zu bestätigen.
7. Wählen Sie Anmeldeinformationen aktualisieren, um Ihre Änderung zu speichern.

> **Note**
>
> Wenn Sie eine Fehlermeldung erhalten, die besagt, dass das neue Passwort die Kennwortanforderungen nicht erfüllt, können Sie den `security login role config show`ONTAPCLI-Befehl verwenden, um die Einstellungen für die Kennwortanforderungen im Dateisystem anzuzeigen. Weitere Informationen, einschließlich Anweisungen zum Ändern der Kennworteinstellung, finden Sie unterDas Aktualisieren des `fsxadmin` Kontopassworts schlägt fehl.

Um VPC-Routing-Tabellen auf Multi-AZ-Dateisystemen zu aktualisieren

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 linken Navigationsbereich Dateisysteme und dann das FSx for ONTAP-Dateisystem aus, das Sie aktualisieren möchten.
3. Wählen Sie unter Aktionen die Option Routentabellen verwalten aus. Diese Option ist nur für Multi-AZ-Dateisysteme verfügbar.
4. Führen Sie im Dialogfeld „Routentabellen verwalten“ einen der folgenden Schritte aus:

- Um eine neue VPC-Routing-Tabelle zuzuordnen, wählen Sie eine Routing-Tabelle aus der Dropdownliste Neue Routing-Tabellen zuordnen aus und wählen Sie dann Zuordnen aus.
- Um die Zuordnung einer vorhandenen VPC-Routentabelle aufzuheben, wählen Sie im Bereich Aktuelle Routing-Tabellen eine Routing-Tabelle aus, und klicken Sie dann auf Zuordnung trennen.

5. Klicken Sie auf Schließen.

So aktualisieren Sie ein Dateisystem (CLI)

Das folgende Verfahren veranschaulicht, wie Sie mithilfe von Aktualisierungen an einem vorhandenen FSx for ONTAP-Dateisystem vornehmen. AWS CLI

1. Um die Konfiguration eines FSx for ONTAP-Dateisystems zu aktualisieren, verwenden Sie den update-file-systemCLI-Befehl (oder den entsprechenden UpdateFileSystemAPI-Vorgang), wie im folgenden Beispiel gezeigt.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
      FsxAdminPassword=new-fsx-admin-password
```

2. Um automatische tägliche Backups zu deaktivieren, setzen Sie die `AutomaticBackupRetentionDays` Eigenschaft auf 0.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

Löschen eines Dateisystems

Sie können ein FSx for ONTAP-Dateisystem mithilfe der Amazon FSx-Konsole, der und der Amazon AWS CLI FSx-API und -SDKs löschen.

Um ein Dateisystem zu löschen:

- Konsole verwenden — Folgen Sie dem unter beschriebenen VerfahrenSchritt 3: Bereinigen von Ressourcen.
- Verwenden der CLI oder API — Löschen Sie zunächst alle Volumes und SVMs in Ihrem Dateisystem. Verwenden Sie dann den delete-file-systemCLI-Befehl oder die DeleteFileSystemAPI-Operation.

Dateisystemdetails anzeigen

Sie können detaillierte Konfigurationsinformationen für Ihr FSx for ONTAP-Dateisystem mithilfe der Amazon FSx-Konsole, der AWS CLI, der API und der unterstützten SDKs anzeigen. AWS

Um detaillierte Dateisysteminformationen anzuzeigen:

- Verwenden der Konsole — Wählen Sie ein Dateisystem aus, um die Detailseite für Dateisysteme anzuzeigen. Im Übersichtsbereich werden die ID, der Lebenszyklusstatus, der Bereitstellungstyp, die SSD-Speicherkapazität, die Durchsatzkapazität, die bereitgestellten IOPS, die Availability Zones und die Erstellungszeit des Dateisystems angezeigt.

  Auf den folgenden Registerkarten finden Sie detaillierte Konfigurationsinformationen und Bearbeitungsmöglichkeiten für Eigenschaften, die geändert werden können:
  - Netzwerk und Sicherheit
  - Überwachung und Leistung — Zeigt von Ihnen erstellte CloudWatch Alarme sowie Messwerte und Warnungen für die folgenden Kategorien an:
    - Zusammenfassung — Zusammenfassung der Kennzahlen zur Dateisystemaktivität auf oberster Ebene
    - Speicherkapazität des Dateisystems
    - Leistung von Dateiserver und Festplatte

    Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch.
  - Administration — Zeigt die folgenden Informationen zur Dateisystemadministration an:
    - Die DNS Namen und IP Adressen der Verwaltungs- und Cluster-Endpunkte des Dateisystems.
    - Der ONTAP Administrator-Benutzername.
    - Die Option zum Aktualisieren des ONTAP Administratorkennworts.
  - Liste der SVMs des Dateisystems

  - Liste der Volumes des Dateisystems
  - Backup-Einstellungen — ändern Sie die automatische tägliche Backup-Einstellung des Dateisystems.
  - Updates — zeigt den Status der vom Benutzer initiierten Aktualisierungen der Dateisystemkonfiguration an.
  - Tags — Tag-Schlüssel/Wert-Paare anzeigen, bearbeiten, hinzufügen und entfernen.
- Verwenden der CLI oder API — Verwenden Sie den describe-file-systemsCLI-Befehl oder die DescribeFileSystemsAPI-Operation.

FSx for ONTAP Dateisystemstatus

Sie können den Status eines Amazon FSx-Dateisystems mithilfe der Amazon FSx-Konsole, des AWS CLI Befehls describe-file-systemsoder der API-Operation anzeigen. DescribeFileSystems

Status des Dateisystems	Beschreibung
VERFÜGBAR	Das Dateisystem wurde erfolgreich erstellt und kann verwendet werden.
WIRD ERSTELLT	Amazon FSx erstellt ein neues Dateisystem.
WIRD GELÖSCHT	Amazon FSx löscht ein vorhandenes Dateisyst em.
FALSCH KONFIGURIERT	Das Dateisystem befindet sich in einem falsch konfigurierten, aber wiederherstellbaren Zustand.
FEHLGESCHLAGEN	1. Das Dateisystem ist ausgefallen und Amazon FSx kann es nicht wiederherstellen. 2. Beim Erstellen eines neuen Dateisystems konnte Amazon FSx kein neues Dateisystem erstellen.

Verwalten virtueller FSx-für-ONTAP-Speichermaschinen

In FSx für ONTAP werden Volumes auf virtuellen Dateiservern gehostet, die als virtuelle Speichermaschinen (SVMs) bezeichnet werden. Eine SVM ist ein isolierter Dateiserver mit eigenen Administratoranmeldeinformationen und Endpunkten für die Verwaltung und den Zugriff auf Daten. Wenn Sie auf Daten in FSx für ONTAP zugreifen, mounten Ihre Clients und Workstations ein Volume, eine SMB-Freigabe oder eine iSCSI LUN, die von einer SVM mithilfe des Endpunkts (IP-Adresse) der SVM gehostet wird.

Amazon FSx erstellt automatisch eine Standard-SVM auf Ihrem Dateisystem, wenn Sie ein Dateisystem mit der erstellen AWS Management Console. Sie können zusätzliche SVMs auf Ihrem Dateisystem jederzeit über die Konsole AWS CLI oder die Amazon-FSx-API und SDKs erstellen. Sie können SVMs nicht mit der ONTAP-CLI oder REST-API erstellen.

Sie können Ihre SVMs zu einem Microsoft Active Directory für die Authentifizierung und Autorisierung des Dateizugriffs hinzufügen. Weitere Informationen finden Sie unter Arbeiten mit Microsoft Active Directory in FSx für ONTAP.

Maximale Anzahl von SVMs pro Dateisystem

In der folgenden Tabelle ist die maximale Anzahl von SVMs aufgeführt, die Sie für ein Dateisystem erstellen können. Die maximale Anzahl von SVMs hängt von der Durchsatzkapazität ab, die in Megabyte pro Sekunde (MBps bereitgestellt wird.

Deployment type (Bereitstellungstyp)	Menge der Durchsatzkapazität (MBps	Maximale Anzahl von SVMs pro Dateisystem
Single-AZ (Skalierung) und Multi-AZ (Skalierung)	128	6
	256	6
	512	14
	1,024	14
	2 048	24
	4.096	24
Single-AZ (Aufskalierung)	Any	5

Themen

- Erstellen einer virtuellen Speichermaschine
- Aktualisieren einer virtuellen Speichermaschine
- Löschen einer virtuellen Speichermaschine (SVM)
- Anzeigen der Konfigurationsdetails der virtuellen Speichermaschine

Erstellen einer virtuellen Speichermaschine

Sie können ein FSx für ONTAP SVM mithilfe der AWS Management Console AWS CLI, und API erstellen.

Die maximale Anzahl von SVMs, die Sie für ein Dateisystem erstellen können, hängt vom Bereitstellungstyp Ihres Dateisystems und der Menge der bereitgestellten Durchsatzkapazität ab. Weitere Informationen finden Sie unter Maximale Anzahl von SVMs pro Dateisystem.

SVM-Eigenschaften

Beim Erstellen einer SVM definieren Sie die folgenden Eigenschaften:

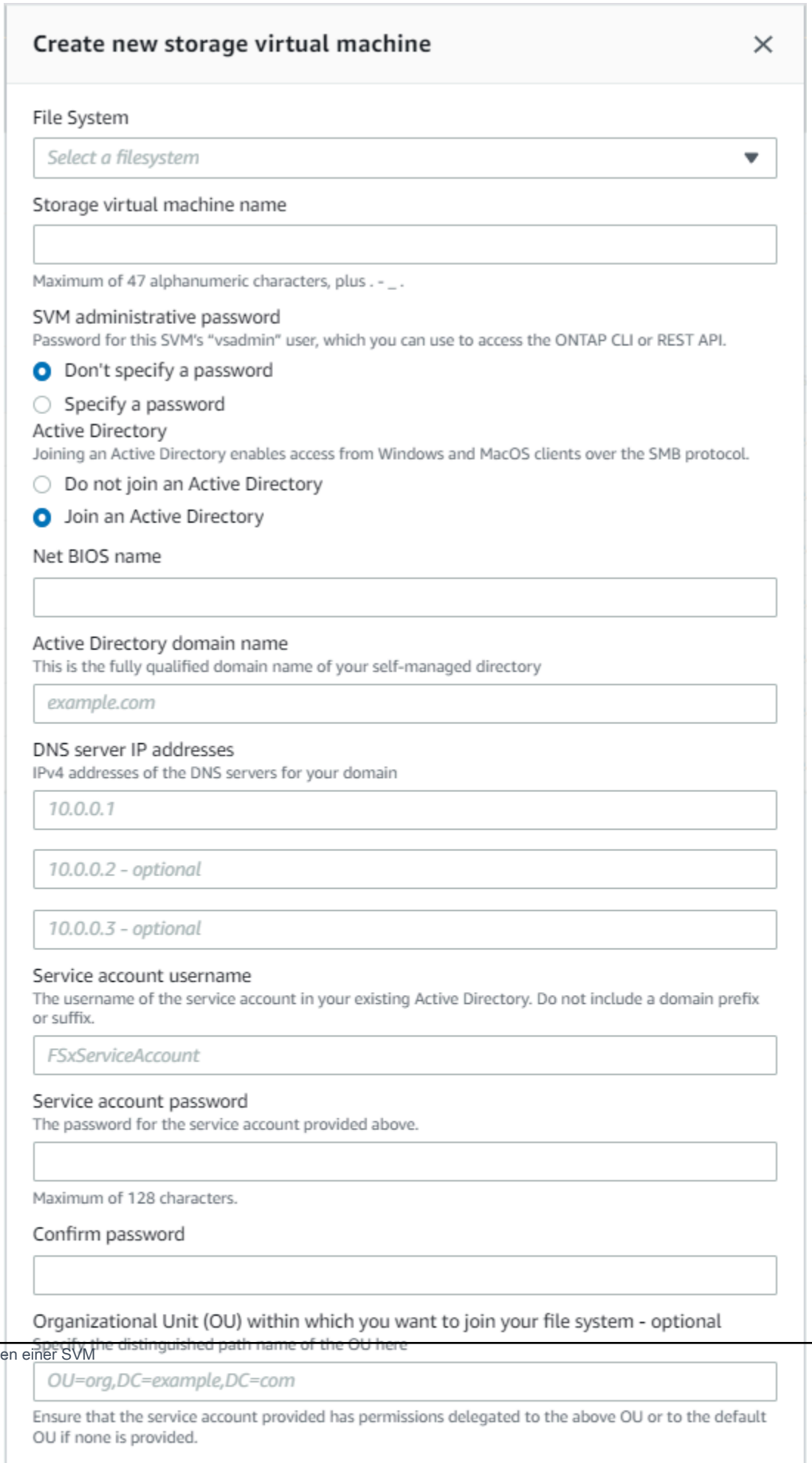
- Das FSx-für-ONTAP-Dateisystem, zu dem es gehört.
- Die Microsoft Active Directory (AD)-Konfiguration – Sie können Ihre SVM optional zu einem selbstverwalteten AD für die Authentifizierung und Zugriffskontrolle von Windows- und macOS-Clients hinzufügen. Weitere Informationen finden Sie unter Arbeiten mit Microsoft Active Directory in FSx für ONTAP.
- Der Sicherheitsstil des Root-Volumes – Legen Sie den Sicherheitsstil des Root-Volumes (Unix, NTFS oder Mixed) fest, damit er an den Client-Typ angepasst wird, den Sie für den Zugriff auf Ihre Daten innerhalb der SVM verwenden. Weitere Informationen finden Sie unter Sicherheitsstil des Volumes.
- Das SVM-Administratorpasswort – Sie können optional das Passwort für den `vsadmin` Benutzer der SVM festlegen. Weitere Informationen finden Sie unter Verwaltung von SVMs mit der CLI ONTAP.

So erstellen Sie eine virtuelle Speichermaschine (Konsole)

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich Virtuelle Speichermaschinen aus.

3. Wählen Sie Neue virtuelle Speichermaschine erstellen aus.

   Das Dialogfeld Neue virtuelle Speichermaschine erstellen wird angezeigt.


Create new storage virtual machine
File System
Select a filesystem
Storage virtual machine name
Maximum of 47 alphanumeric characters, plus . - _ .
SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.
Don't specify a password
Specify a password
Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.
Do not join an Active Directory
Join an Active Directory
Net BIOS name
Active Directory domain name
This is the fully qualified domain name of your self-managed directory
example.com
DNS server IP addresses
IPv4 addresses of the DNS servers for your domain
10.0.0.1
10.0.0.2 - optional
10.0.0.3 - optional
Service account username
The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
FSxServiceAccount
Service account password
The password for the service account provided above.
Maximum of 128 characters.
Confirm password
Organizational Unit (OU) within which you want to join your file system - optional
Specify the distinguished path name of the OU here
OU=org,DC=example,DC=com
Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

4. Wählen Sie für Dateisystem das Dateisystem aus, auf dem die virtuelle Speichermaschine erstellt werden soll.
5. Geben Sie im Feld Name der virtuellen Speichermaschine einen Namen für die virtuelle Speichermaschine ein. Sie können maximal 47 alphanumerische Zeichen sowie den Unterstrich (_) verwenden.
6. Für das Administratorpasswort von SVM können Sie optional Passwort angeben auswählen und ein Passwort für den `vsadmin` Benutzer dieser SVM angeben. Sie können den `vsadmin` Benutzer verwenden, um die SVM mithilfe der ONTAP-CLI oder REST-API zu verwalten. Weitere Informationen zum `vsadmin` Benutzer finden Sie unter Verwaltung von SVMs mit der CLI ONTAP.

   Wenn Sie Kein Passwort angeben (Standard) wählen, können Sie weiterhin den `fsxadmin` Benutzer des Dateisystems verwenden, um Ihr Dateisystem mit der ONTAP-CLI oder REST-API zu verwalten, aber Sie können den `vsadmin` Benutzer Ihrer SVM nicht verwenden, um dasselbe zu tun.
7. Für Active Directory haben Sie die folgenden Optionen:

   - Wenn Sie Ihr Dateisystem nicht mit einem Active Directory (AD) verbinden, wählen Sie Keinen Active Directory verbinden aus.
   - Wenn Sie Ihre SVM mit einer selbstverwalteten AD-Domain verbinden, wählen Sie Ein Active Directory beitreten und geben Sie die folgenden Details für Ihr AD an. Weitere Informationen finden Sie unter Voraussetzungen für das Verbinden einer SVM mit einem selbstverwalteten Microsoft AD.
     - Der NetBIOS-Name des Active-Directory-Computerobjekts, das für Ihre SVM erstellt werden soll. Der NetBIOS-Name darf 15 Zeichen nicht überschreiten. Dies ist der Name dieser SVM in Active Directory.
     - Der vollqualifizierte Domänenname (FQDN) Ihres Active Directory. Der FQDN darf 255 Zeichen nicht überschreiten.
     - IP-Adressen des DNS-Servers – Die IPv4-Adressen der DNS-Server für Ihre Domain.
     - Benutzername des Servicekontos – Der Benutzername des Servicekontos in Ihrem vorhandenen Active Directory. Geben Sie kein Domänenpräfix oder Suffix an. Geben Sie als `EXAMPLE\ADMIN` `ADMIN`ein.
     - Servicekonto-Passwort – Das Passwort für das Servicekonto.
     - Passwort bestätigen – Das Passwort für das Servicekonto.

- (Optional) Organisationseinheit (OU) – Der eindeutige Pfadname der Organisationseinheit, der Sie Ihr Dateisystem beitreten möchten.
- Delegierte Dateisystem-Administratorgruppe – Der Name der Gruppe in Ihrem AD, die Ihr Dateisystem verwalten kann.

  Wenn Sie verwenden AWS Managed Microsoft AD, müssen Sie eine Gruppe wie AWS Delegierte FSx-Administratoren, AWS Delegierte Administratoren oder eine benutzerdefinierte Gruppe mit delegierten Berechtigungen an die Organisationseinheit angeben.

  Wenn Sie einem selbstverwalteten AD beitreten, verwenden Sie den Namen der Gruppe in Ihrem AD. Die Standardgruppe ist `Domain Admins`.

8. Wählen Sie für den Sicherheitsstil des SVM-Root-Volumes den Sicherheitsstil für die SVM aus, abhängig von der Art der Clients, die auf Ihre Daten zugreifen. Wählen Sie Unix (Linux) ,wenn Sie hauptsächlich über Linux-Clients auf Ihre Daten zugreifen. Wählen Sie NTFS, wenn Sie hauptsächlich über Windows-Clients auf Ihre Daten zugreifen. Weitere Informationen finden Sie unter Sicherheitsstil des Volumes.
9. Wählen Sie Bestätigen, um die virtuelle Speichermaschine zu erstellen.

Sie können den Aktualisierungsfortschritt auf der Detailseite Dateisysteme in der Spalte Status des Bereichs Virtuelle Speichermaschinen überwachen. Die virtuelle Speichermaschine ist einsatzbereit, wenn ihr Status Erstellt lautet.

So erstellen Sie eine virtuelle Speichermaschine (CLI)

- Um eine virtuelle Speichermaschine (SVM) von FSx für ONTAP zu erstellen, verwenden Sie den create-storage-virtual-machine CLI-Befehl (oder die entsprechende CreateStorageVirtualMachine API-Operation), wie im folgenden Beispiel gezeigt.

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name svm1 \
    --svm-admin-password password \
    --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
 \
UserName="FSxService",Password="password", \
```

```
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Nachdem die virtuelle Speichermaschine erfolgreich erstellt wurde, gibt Amazon FSx ihre Beschreibung im JSON-Format zurück, wie im folgenden Beispiel gezeigt.


```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
```

```
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Aktualisieren einer virtuellen Speichermaschine

Sie können die folgenden SVM-Konfigurationseigenschaften (Storage Virtual Machine) mithilfe der Amazon-FSx-Konsole AWS CLI und der Amazon-FSx-API aktualisieren:

- Passwort für das Administratorkonto von SVM.
- SVM Active Directory (AD)-Konfiguration – Sie können eine SVM mit einem AD verbinden oder die AD-Konfiguration einer SVM ändern, die bereits mit einem AD verbunden ist. Weitere Informationen finden Sie unter Verwalten von SVM-Active-Directory-Konfigurationen.

So aktualisieren Sie die Anmeldeinformationen des SVM-Administratorkontos (Konsole)

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie die zu aktualisierende SVM wie folgt aus:
   - Wählen Sie im linken Navigationsbereich Dateisysteme und dann das ONTAP-Dateisystem aus, für das Sie eine SVM aktualisieren möchten.
   - Wählen Sie die Registerkarte Virtuelle Speichermaschinen aus.

     – Oder –
   - Um eine Liste aller in Ihrem AWS-Konto in der aktuellen verfügbaren SVMs anzuzeigen AWS-Region, erweitern Sie ONTAP und wählen Sie Virtuelle Speichermaschinen aus.
3. Wählen Sie die virtuelle Speichermaschine aus, die Sie aktualisieren möchten.
4. Wählen Sie Aktionen > Administratorpasswort aktualisieren aus. Das Fenster Aktualisieren von SVM-Administratoranmeldeinformationen wird angezeigt.

5. Geben Sie das neue Passwort für den `vsadmin` Benutzer ein und bestätigen Sie es.
6. Wählen Sie Anmeldeinformationen aktualisieren, um das neue Passwort zu speichern.

So aktualisieren Sie die Anmeldeinformationen des SVM-Administratorkontos (CLI)

- Um die Konfiguration einer FSx for ONTAP SVM zu aktualisieren, verwenden Sie den update-storage-virtual-machine CLI-Befehl (oder die entsprechende UpdateStorageVirtualMachine API-Operation), wie im folgenden Beispiel gezeigt.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

Nachdem die virtuelle Speichermaschine erfolgreich erstellt wurde, gibt Amazon FSx ihre Beschreibung im JSON-Format zurück, wie im folgenden Beispiel gezeigt.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
```

```
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
    "StorageVirtualMachineId": "svm-abcdef01234567890",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Löschen einer virtuellen Speichermaschine (SVM)

Sie können eine FSx-für-ONTAP-SVM nur mithilfe der Amazon-FSx-Konsole AWS CLI, der und der API löschen. Bevor Sie eine SVM löschen können, müssen Sie zuerst alle Nicht-Root-Volumes löschen, die an die SVM angehängt sind.

> **Important**
>
> Sie können eine SVM nicht mithilfe der NetApp ONTAP-CLI oder -API löschen.

> **Note**
>
> Bevor Sie eine virtuelle Speichermaschine löschen, stellen Sie sicher, dass keine Anwendungen auf die Daten in der SVM zugreifen und dass Sie alle Nicht-Root-Volumes gelöscht haben, die an die SVM angehängt sind.

So löschen Sie eine virtuelle Speichermaschine (Konsole)

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie die SVM, die Sie löschen möchten, wie folgt aus:

   - Wählen Sie im linken Navigationsbereich Dateisysteme und dann das ONTAP-Dateisystem aus, für das Sie eine SVM löschen möchten.
   - Wählen Sie die Registerkarte Virtuelle Speichermaschinen aus.

   – Oder –

   - Um eine Liste aller verfügbaren SVMs anzuzeigen, erweitern Sie ONTAP und wählen Sie Virtuelle Speichermaschinen aus.

   Wählen Sie die SVM, die Sie löschen möchten, aus der Liste aus.
3. Zeigen Sie auf der Registerkarte Volumes die Liste der Volumes an, die an die SVM angehängt sind. Wenn der SVM Nicht-Root-Volumes zugeordnet sind, müssen Sie diese löschen, bevor Sie die SVM löschen können. Weitere Informationen finden Sie unter Löschen eines Volumes.
4. Wählen Sie im Menü Aktionen die Option Virtuelle Speichermaschine löschen aus.
5. Wählen Sie im Dialogfeld Bestätigung löschen die Option Virtuelle Speichermaschine löschen aus.

So löschen Sie eine virtuelle Speichermaschine (CLI)

- Um eine virtuelle FSx-für-ONTAP-Speichermaschine zu löschen, verwenden Sie den delete-storage-virtual-machine CLI-Befehl (oder die entsprechende DeleteStorageVirtualMachine API-Operation), wie im folgenden Beispiel gezeigt.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

Anzeigen der Konfigurationsdetails der virtuellen Speichermaschine

Sie können die virtuellen FSx-für-ONTAP-Speichermaschinen, die sich derzeit auf Ihrem Dateisystem befinden, mithilfe der Amazon-FSx-Konsole AWS CLI, der und der Amazon-FSx-API anzeigen.

So zeigen Sie eine virtuelle Speichermaschine in Ihrem Dateisystem an:

- Verwenden der Konsole – Wählen Sie ein Dateisystem aus, um die Detailseite des Dateisystems anzuzeigen. Um alle virtuellen Speichermaschinen im Dateisystem aufzulisten, wählen Sie die Registerkarte Virtuelle Speichermaschinen und dann die virtuelle Speichermaschine aus, die Sie anzeigen möchten.
- Verwenden der CLI oder API – Verwenden Sie den describe-storage-virtual-machines CLI-Befehl oder die DescribeStorageVirtualMachines API-Operation .

  Die Systemantwort ist eine Liste mit vollständigen Beschreibungen aller SVMs in Ihrem Konto in dieser AWS-Region.

Verwaltung von FSx für ONTAP-Volumes

Jede virtuelle Speichermaschine (SVM) auf einem FSx for ONTAP-Dateisystem kann über ein oder mehrere Volumes verfügen. Ein Volume ist ein isolierter Datencontainer für Dateien, Verzeichnisse oder logische iSCSI-Speichereinheiten (LUNs). Volumes sind Thin Provisioning, was bedeutet, dass sie nur Speicherkapazität für die darin gespeicherten Daten verbrauchen.

Sie können von Linux-, Windows- oder macOS-Clients aus über das Network File System (NFS) -Protokoll, das Server Message Block (SMB) -Protokoll oder über das Internet Small Computer Systems Interface (iSCSI) -Protokoll auf ein Volume zugreifen, indem Sie eine iSCSI-LUN (Shared Block Storage) erstellen. FSx for ONTAP unterstützt auch den Multiprotokollzugriff (gleichzeitiger NFS- und SMB-Zugriff) auf dasselbe Volume.

Sie können Volumes mithilfe der AWS Management Console, AWS CLI, der Amazon FSx-API oder NetApp BlueXP erstellen. Sie können auch den administrativen Endpunkt Ihres Dateisystems oder Ihrer SVM verwenden, um Volumes mithilfe der NetApp ONTAP CLI oder der REST-API zu erstellen, zu aktualisieren und zu löschen.

Sie können bis zu 500 Volumes pro Scale-up-Dateisystem und 1.000 Volumes pro Scale-Out-Dateisystem erstellen.

Wenn Sie ein Volume erstellen, definieren Sie die folgenden Eigenschaften:

- Volumenstil — Der Volumenstil kann entweder FlexVol oder sein FlexGroup.
- Datenträgername — Der Name des Volumes.
- Datenträgertyp — Der Volumetyp kann entweder Read-Write (RW) oder Data Protection (DP) sein. DP-Volumes sind schreibgeschützt und werden als Ziel in einer Oder-Beziehung verwendet. NetApp SnapMirror SnapVault
- Datenträgergröße — Dies ist die maximale Datenmenge, die das Volume speichern kann, unabhängig von der Speicherebene.
- Verbindungspfad — Dies ist der Ort im Namespace der SVM, an dem das Volume bereitgestellt wird.
- Speichereffizienz — Funktionen zur Speichereffizienz, einschließlich Datenkomprimierung, Komprimierung und Deduplizierung, ermöglichen typische Speichereinsparungen von 65% für allgemeine Filesharing-Workloads.
- Volume-Sicherheitsstil (Unix, NTFS oder Mixed) — Legt fest, welche Art von Berechtigungen für den Datenzugriff auf dem Volume verwendet werden, wenn Benutzer autorisiert werden.
- Datenklassifizierung — Die Tiering-Richtlinie definiert, welche Daten in der kostengünstigen Kapazitätspoolstufe gespeichert werden.
- Abkühlungszeitraum für Tiering-Policys — Definiert, wann Daten als „kalt“ markiert und in den Capacity-Pool-Speicher verschoben werden.
- Snapshot-Richtlinie — Snapshot-Richtlinien definieren, wie das System Snapshots für ein Volume erstellt. Sie können aus drei vordefinierten Richtlinien wählen oder eine benutzerdefinierte Richtlinie verwenden, die Sie mit der ONTAP CLI oder der REST API erstellt haben.
- Tags in Backups kopieren — Amazon FSx kopiert mit dieser Option automatisch alle Tags von Ihren Volumes in Backups. Sie können diese Option mithilfe der AWS CLI oder der Amazon FSx-API festlegen.

Themen

- Lautstärkestile
- Volume-Typen
- Sicherheitsstil des Volumes
- Volumen erstellen
- Ein Volume aktualisieren
- Löschen eines Volumes
- Ein Volume anzeigen

Lautstärkestile

FSx for ONTAP bietet zwei Arten von Volumes, die Sie für unterschiedliche Zwecke verwenden können. Sie können entweder FlexVol oder FlexGroup Volumes mit der Amazon FSx-Konsole AWS CLI, der und der Amazon FSx-API erstellen.

- FlexVolVolumes bieten die einfachste Bedienung für Dateisysteme mit einem Hochverfügbarkeitspaar (HA) und sind der Standard-Volume-Stil für Scale-up-Dateisysteme. Die Mindestgröße eines FlexVol Volumes beträgt 20 Mebibyte (MiB) und die maximale Größe beträgt 314.572.800 MiB.
- FlexGroupVolumes bestehen aus mehreren einzelnen FlexVol Volumes, wodurch sie eine höhere Leistung und Speicherskalierbarkeit bieten als FlexVol Volumes für Dateisysteme mit mehreren HA-Paaren. FlexGroupVolumes sind der Standard-Volume-Stil für Scale-Out-Dateisysteme. Die Mindestgröße eines FlexGroup Volumes beträgt 100 Gibibyte (GiB) pro Bestandteil und die maximale Größe beträgt 20 Pebibyte (PiB).

Sie können ein Volume mit dem FlexVol Stil mit der ONTAP CLI in den FlexGroup Stil konvertieren, wodurch ein Volume FlexGroup mit einem einzigen Bestandteil erstellt wird. Wir empfehlen jedoch, Daten zwischen einem FlexVol Volume und einem neuen FlexGroup Volume AWS DataSync zu verschieben, um sicherzustellen, dass die Daten gleichmäßig auf die FlexGroup's einzelnen Komponenten verteilt sind. Weitere Informationen finden Sie unter FlexGroupBestandteile.

> **Note**
>
> Wenn Sie die ONTAP CLI verwenden möchten, um ein Volume in ein FlexVol Volume zu konvertieren, stellen Sie sicher, dass Sie alle Backups des FlexVol Volumes löschen, bevor Sie es konvertieren. FlexGroup ONTAPführt im Rahmen der Konvertierung nicht automatisch eine Neuverteilung der Daten durch, sodass die Daten zwischen den einzelnen Komponenten möglicherweise unausgewogen sind. FlexGroup

FlexGroupBestandteile

Ein FlexGroup Volumen besteht aus Bestandteilen, bei denen es sich um Volumen handeltFlexVol. Standardmäßig weist FSx for ONTAP einem FlexGroup Volume acht Komponenten pro HA-Paar zu.

Wenn Sie Ihr FlexGroup Volume erstellen, wird dessen Größe gleichmäßig auf seine Bestandteile aufgeteilt. Wenn Sie beispielsweise ein 800 Gigabyte (GB) großes FlexGroup Volume mit acht

Komponenten erstellen, hat jede Komponente eine Größe von 100 GB. Ein FlexGroup Volumen kann zwischen 100 GB und 20 PiB groß sein, aber die Gesamtgröße hängt von der Größe der Bestandteile ab. Jede Komponente hat eine Mindestgröße von 100 GB und eine Maximalgröße von 300 TiB. Ein FlexGroup Volume mit acht Komponenten hat beispielsweise eine Mindestgröße von 800 GB und eine Maximalgröße von 20 PiB.

ONTAP verteilt Daten auf Dateiebene auf die einzelnen Komponenten. Sie können bis zu zwei Milliarden Dateien in jeder Komponente Ihres Volumes speichern. FlexGroup

Wenn Sie die Größe Ihres FlexGroup Volumes aktualisieren, wird die neue Größe gleichmäßig auf die vorhandenen Bestandteile verteilt.

Sie können Ihrem FlexGroup Volume auch mithilfe der ONTAP CLI oder der REST-API weitere Komponenten hinzufügen. Wir empfehlen Ihnen jedoch, dies nur zu tun, wenn Sie zusätzliche Speicherkapazität benötigen und alle Ihre Komponenten bereits ihre maximale Größe erreicht haben (300 TiB pro Bestandteil). Das Hinzufügen von Komponenten kann zu einem Ungleichgewicht von Daten und I/O zwischen den Komponenten führen. Solange die Komponenten nicht ausgewogen sind, ist es möglich, dass der Schreibdurchsatz um 5 bis 10% niedriger ist als bei einem ausgewogenen Volumen. FlexGroup Wenn neue Daten auf das FlexGroup Volume geschrieben werden, verteilt ONTAP sie nach Priorität auf die neuen Komponenten, bis die Komponenten ausgeglichen sind. Wenn Sie neue Bestandteile hinzufügen, empfehlen wir, eine gerade Zahl zu wählen und acht pro Aggregat nicht zu überschreiten.

> **Note**
>
> Wenn Sie neue Komponenten hinzufügen, werden Ihre vorhandenen Snapshots zu Teilschnappschüssen. Daher können sie nicht verwendet werden, um Ihr FlexGroup Volume vollständig auf einen früheren Zustand zurückzusetzen. Die vorherigen Schnappschüsse bieten kein vollständiges point-in-time Bild Ihres FlexGroup Volumes, da die neuen Bestandteile noch nicht existierten. Die Teilschnappschüsse können jedoch verwendet werden, um einzelne Dateien und Verzeichnisse wiederherzustellen, ein neues Volume zu erstellen oder um mit ihnen zu replizieren. SnapMirror

Volume-Typen

FSx for ONTAP bietet zwei Arten von Volumes, die Sie mit der Amazon FSx-Konsole erstellen können: die und die AWS CLI Amazon FSx-API.

- In den meisten Fällen werden Read-Write-Volumes (RW) verwendet. Wie ihr Name schon sagt, sind sie lesbar und schreibbar.
- Data Protection (DP) -Volumes sind schreibgeschützte Volumes, die Sie als Ziel einer OR-Beziehung verwenden. NetApp SnapMirror SnapVault Sie sollten DP-Volumes verwenden, wenn Sie die Daten eines einzelnen Volumes migrieren oder schützen möchten.

FlexVolund FlexGroup Volumes können entweder RW oder DP sein.

> **Note**
>
> Sie können den Typ eines Volumes nicht aktualisieren, nachdem das Volume erstellt wurde.

Sicherheitsstil des Volumes

FSx for ONTAP unterstützt 3 verschiedene Volumesicherheitsstile: Unix, NTFS und gemischt. Jeder Sicherheitsstil hat unterschiedliche Auswirkungen darauf, wie mit Berechtigungen für Daten umgegangen wird. Sie müssen die verschiedenen Auswirkungen verstehen, um sicherzustellen, dass Sie den für Ihre Zwecke geeigneten Sicherheitsstil auswählen.

Es ist wichtig zu verstehen, dass Sicherheitsstile nicht bestimmen, welche Clienttypen auf Daten zugreifen können und welche nicht. Sicherheitsstile bestimmen nur, welche Art von Berechtigungen FSx for ONTAP zur Steuerung des Datenzugriffs verwendet und welcher Clienttyp diese Berechtigungen ändern kann.

Die beiden Faktoren, anhand derer Sie den Sicherheitsstil für ein Volume bestimmen, sind die Art der Administratoren, die das Dateisystem verwalten, und die Art der Benutzer oder Dienste, die auf die Daten auf dem Volume zugreifen.

Beim Erstellen eines Volumes in der Amazon FSx-Konsole, CLI und API wird der Sicherheitsstil automatisch auf den Sicherheitsstil des Root-Volumes festgelegt. Sie können den Sicherheitsstil eines Volumes mithilfe der API AWS CLI oder ändern. Sie können diese Einstellung ändern, nachdem das Volume erstellt wurde. Weitere Informationen finden Sie unter Ein Volume aktualisieren.

Wenn Sie den Sicherheitsstil für ein Volume konfigurieren, sollten Sie die Anforderungen Ihrer Umgebung berücksichtigen, um sicherzustellen, dass Sie den besten Sicherheitsstil auswählen, um Probleme bei der Verwaltung von Berechtigungen zu vermeiden. Beachten Sie, dass der

Sicherheitsstil nicht bestimmt, welche Clienttypen auf Daten zugreifen können. Der Sicherheitsstil bestimmt die Berechtigungen, die für den Datenzugriff verwendet werden, und die Clienttypen, die diese Berechtigungen ändern können. Im Folgenden finden Sie Überlegungen, die Ihnen bei der Entscheidung helfen können, welchen Sicherheitsstil Sie für ein Volume wählen sollten:

- Unix (Linux) — Wählen Sie diesen Sicherheitsstil, wenn das Dateisystem von einem Unix-Administrator verwaltet wird, die meisten Benutzer NFS-Clients sind und eine Anwendung, die auf die Daten zugreift, einen Unix-Benutzer als Dienstkonto verwendet. Nur Linux-Clients können Berechtigungen im Unix-Sicherheitsstil ändern, und die für Dateien und Verzeichnisse verwendeten Berechtigungstypen sind Modus-Bits oder NFS v4.x-ACLs.
- NTFS — Wählen Sie diesen Sicherheitsstil, wenn das Dateisystem von einem Windows-Administrator verwaltet wird, die meisten Benutzer SMB-Clients sind und eine Anwendung, die auf die Daten zugreift, einen Windows-Benutzer als Dienstkonto verwendet. Wenn Windows-Zugriff auf ein Volume erforderlich ist, empfehlen wir, den NTFS-Sicherheitsstil zu verwenden. Nur Windows-Clients können Berechtigungen im NTFS-Sicherheitsstil ändern, und die für Dateien und Verzeichnisse verwendeten Berechtigungstypen sind NTFS-ACLs.
- Gemischt — Dies ist eine erweiterte Einstellung. Weitere Informationen finden Sie im NetApp Documentation Center im Thema Welche Sicherheitsstile und welche Auswirkungen sie haben.

Volumen erstellen

Sie können einen FSx für ONTAP FlexVol oder ein FlexGroup Volume mithilfe der Amazon FSx-Konsole AWS CLI, der und der Amazon FSx-API sowie der NetApp ONTAP-Befehlszeilenschnittstelle (CLI) und der REST-API erstellen.

Um ein Volume (Konsole) zu erstellen FlexVol

> **Note**
>
> Der Sicherheitsstil des Volumes wird automatisch auf den Sicherheitsstil des Root-Volumes festgelegt.

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich Volumes aus.
3. Wählen Sie Create Volume (Volume erstellen) aus.
4. Wählen Sie als Dateisystemtyp Amazon FSx for NetApp ONTAP.

5. Geben Sie im Abschnitt Dateisystemdetails die folgenden Informationen ein:

   - Wählen Sie unter Dateisystem das Dateisystem aus, auf dem das Volume erstellt werden soll.
   - Wählen Sie unter Virtuelle Speichermaschine die virtuelle Speichermaschine (SVM) aus, auf der das Volume erstellt werden soll.

6. Wählen Sie im Bereich Volume-Stil die Option FlexVol.

7. Geben Sie im Abschnitt Volumendetails die folgenden Informationen ein:

   - Geben Sie im Feld Datenträgername einen Namen für das Volume ein. Sie können bis zu 203 alphanumerische Zeichen oder Unterstriche (_) verwenden.
   - Geben Sie für Volumengröße eine beliebige ganze Zahl im Bereich von 20—314572800 ein, um die Größe in Mebibyte (MiB) anzugeben.
   - Wählen Sie für Volumetyp die Option Lesen-Schreiben (RW), um ein Volumen zu erstellen, das lesbar und beschreibbar ist, oder Data Protection (DP), um ein Volume zu erstellen, das schreibgeschützt ist und als Ziel einer Oder-Beziehung verwendet werden kann. NetApp SnapMirror SnapVault Weitere Informationen finden Sie unter Volume-Typen.
   - Geben Sie für Junction Path einen Speicherort im Dateisystem ein, an dem das Volume bereitgestellt werden soll. Dem Namen muss beispielsweise `/vol3` ein Schrägstrich vorangestellt werden.
   - Wählen Sie für Speichereffizienz Enabled, um die ONTAP-Speichereffizienzfunktionen (Deduplizierung, Komprimierung und Verdichtung) zu aktivieren. Weitere Informationen finden Sie unter FSx für ONTAP-Speichereffizienz.
   - Wählen Sie für das Volume Security Style zwischen Unix (Linux), NTFS und Mixed für das Volume. Weitere Informationen finden Sie unter Sicherheitsstil des Volumes.
   - Wählen Sie unter Snapshot-Richtlinie eine Snapshot-Richtlinie für das Volume aus. Weitere Informationen zu Snapshot-Richtlinien finden Sie unterSnapshot-Richtlinien.

     Wenn Sie „Benutzerdefinierte Richtlinie“ wählen, müssen Sie den Namen der Richtlinie im Feld „Benutzerdefinierte Richtlinie“ angeben. Die benutzerdefinierte Richtlinie muss bereits auf der SVM oder im Dateisystem vorhanden sein. Sie können mit der ONTAP CLI oder der REST API eine benutzerdefinierte Snapshot-Richtlinie erstellen. Weitere Informationen finden Sie unter Erstellen einer Snapshot-Richtlinie in der NetApp ONTAP-Produktdokumentation.

8. Geben Sie im Abschnitt Speicherstufenzuweisung die folgenden Informationen an:

   - Wählen Sie unter Capacity Pool Tiering Policy die Storage-Pool-Tiering-Richtlinie für das Volume aus. Dabei kann es sich um Automatisch (Standardeinstellung), Nur Snapshot, Alle

oder Keine handeln. Weitere Informationen finden Sie unter Richtlinien für das Volumen-Tiering.

- Wenn Sie „Automatisch“ oder „Nur Snapshot“ wählen, können Sie den Kühlzeitraum für die Tiering-Richtlinie festlegen, um die Anzahl der Tage zu definieren, nach der Daten, auf die nicht zugegriffen wurde, als kalt markiert und in den Speicher des Kapazitätspools verschoben werden. Sie können einen Wert zwischen 2 und 183 Tagen angeben. Die Standardeinstellung ist 31 Tage.

9. Wählen Sie im Bereich Erweitert für SnapLockKonfiguration zwischen Aktiviert und Deaktiviert. Weitere Informationen zur Konfiguration eines SnapLock Compliance-Volumes oder eines SnapLock Enterprise-Volumes finden Sie unter Erstellen eines SnapLock Compliance-Volumes undErstellen eines SnapLock Enterprise-Volumes. Mehr über SnapLock erfahren Sie unter Schützen Ihrer Daten mit SnapLock.
10. Wählen Sie Bestätigen, um das Volume zu erstellen.

Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme in der Spalte Status des Bereichs Volumes überwachen. Das Volume ist einsatzbereit, wenn sein Status „Erstellt“ lautet.

Um ein FlexGroup Volume (Konsole) zu erstellen

> **Note**
>
> Mit der Amazon FSx-Konsole können Sie nur FlexGroup Volumes für Scale-Out-Dateisysteme erstellen. Verwenden Sie die Amazon FSx-API oder NetApp die Verwaltungstools, um FlexVol Volumes für Ihre Scale-Out-Dateisysteme zu erstellen. AWS CLI

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich Volumes aus.
3. Wählen Sie Create Volume (Volume erstellen) aus.
4. Wählen Sie als Dateisystemtyp Amazon FSx for NetApp ONTAP.
5. Geben Sie im Abschnitt Dateisystemdetails die folgenden Informationen ein:

   - Wählen Sie unter Dateisystem das Dateisystem aus, auf dem das Volume erstellt werden soll.
   - Wählen Sie unter Virtuelle Speichermaschine die virtuelle Speichermaschine (SVM) aus, auf der das Volume erstellt werden soll.

6. Wählen Sie im Bereich Volume-Stil die Option FlexGroup.
7. Geben Sie im Abschnitt Volumendetails die folgenden Informationen ein:

   - Geben Sie im Feld Datenträgername einen Namen für das Volume ein. Sie können bis zu 203 alphanumerische Zeichen oder Unterstriche (_) verwenden.
   - Geben Sie für Volumengröße eine beliebige ganze Zahl im Bereich von 800 Gibibyte (GiB) bis 2.000 Pebibyte (PiB) ein.
   - Wählen Sie für Volumetyp die Option Read-Write (RW), um ein Volumen zu erstellen, das lesbar und beschreibbar ist, oder Data Protection (DP), um ein Volume zu erstellen, das schreibgeschützt ist und als Ziel einer Oder-Beziehung verwendet werden kann. NetApp SnapMirror SnapVault Weitere Informationen finden Sie unter Volume-Typen.
   - Geben Sie für Junction Path einen Speicherort im Dateisystem ein, an dem das Volume bereitgestellt werden soll. Dem Namen muss beispielsweise `/vol3` ein Schrägstrich vorangestellt werden.
   - Wählen Sie für Speichereffizienz Enabled, um die ONTAP-Speichereffizienzfunktionen (Deduplizierung, Komprimierung und Verdichtung) zu aktivieren. Weitere Informationen finden Sie unter FSx für ONTAP-Speichereffizienz.
   - Wählen Sie für das Volume Security Style zwischen Unix (Linux), NTFS und Mixed für das Volume. Weitere Informationen finden Sie unter Sicherheitsstil des Volumes.

     > **Note**
     >
     > Der Sicherheitsstil des Volumes wird automatisch auf den Sicherheitsstil des Root-Volumes festgelegt.

   - Wählen Sie unter Snapshot-Richtlinie eine Snapshot-Richtlinie für das Volume aus. Weitere Informationen zu Snapshot-Richtlinien finden Sie unterSnapshot-Richtlinien.

     Wenn Sie „Benutzerdefinierte Richtlinie“ wählen, müssen Sie den Namen der Richtlinie im Feld „Benutzerdefinierte Richtlinie“ angeben. Die benutzerdefinierte Richtlinie muss bereits auf der SVM oder im Dateisystem vorhanden sein. Sie können mit der ONTAP CLI oder der REST API eine benutzerdefinierte Snapshot-Richtlinie erstellen. Weitere Informationen finden Sie unter Erstellen einer Snapshot-Richtlinie in der NetApp ONTAP-Produktdokumentation.
8. Geben Sie im Abschnitt Speicherstufenzuweisung die folgenden Informationen an:

   - Wählen Sie unter Capacity Pool Tiering Policy die Storage-Pool-Tiering-Richtlinie für das Volume aus. Dabei kann es sich um Automatisch (Standardeinstellung), Nur Snapshot, Alle

oder Keine handeln. Weitere Informationen finden Sie unter Richtlinien für das Volumen-Tiering.

- Wenn Sie „Automatisch“ oder „Nur Snapshot“ wählen, können Sie den Kühlzeitraum für die Tiering-Richtlinie festlegen, um die Anzahl der Tage zu definieren, nach der Daten, auf die nicht zugegriffen wurde, als kalt markiert und in den Speicher des Kapazitätspools verschoben werden. Sie können einen Wert zwischen 2 und 183 Tagen angeben. Die Standardeinstellung ist 31 Tage.

9. Wählen Sie im Bereich Erweitert für SnapLockKonfiguration zwischen Aktiviert und Deaktiviert. Weitere Informationen zur Konfiguration eines SnapLock Compliance-Volumes oder eines SnapLock Enterprise-Volumes finden Sie unter Erstellen eines SnapLock Compliance-Volumes undErstellen eines SnapLock Enterprise-Volumes. Mehr über SnapLock erfahren Sie unter Schützen Ihrer Daten mit SnapLock.
10. Wählen Sie Bestätigen, um das Volume zu erstellen.

Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme in der Spalte Status des Bereichs Volumes überwachen. Das Volume ist einsatzbereit, wenn sein Status „Erstellt“ lautet.

So erstellen Sie ein Volume (CLI)

- Um ein FSx for ONTAP-Volume zu erstellen, verwenden Sie den CLI-Befehl create-volume (oder den entsprechenden CreateVolumeAPI-Vorgang), wie im folgenden Beispiel gezeigt.

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
          SizeInMegabytes=1024,SnapshotPolicy=default, \
          StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
          StorageEfficiencyEnabled=true
```

Nach erfolgreicher Erstellung des Volumes gibt Amazon FSx seine Beschreibung im JSON-Format zurück, wie im folgenden Beispiel gezeigt.

```
{
    "Volume": {
        "CreationTime": "2022-08-12T13:03:37.625000-04:00",
        "FileSystemId": "fs-abcdef0123456789c",
```

```
        "Lifecycle": "CREATING",
        "Name": "vol1",
        "OntapConfiguration": {
            "CopyTagsToBackups": true,
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "NTFS",
            "SizeInMegabytes": 1024,
            "SnapshotPolicy": "default",
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abcdef0123456789a",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "NONE"
            },
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
        "VolumeId": "fsvol-abcdef0123456789b",
        "VolumeType": "ONTAP"


    }
}
```

Sie können auch ein neues Volume erstellen, indem Sie ein Backup eines Volumes auf einem neuen Volume wiederherstellen. Weitere Informationen finden Sie unter Backups auf einem neuen Volume wiederherstellen.

Ein Volume aktualisieren

Sie können die Konfiguration eines FSx for ONTAP-Volumes mithilfe der Amazon FSx-Konsole AWS CLI, der und der Amazon FSx-API sowie der NetApp ONTAP-Befehlszeilenschnittstelle (CLI) und der REST-API aktualisieren. Sie können die folgenden Eigenschaften eines vorhandenen FSx for ONTAP-Volumes ändern:

- Name des Volumes
- Verbindungspfad
- Volume-Größe
- Speichereffizienz

- Richtlinie zur Staffelung von Kapazitätspools
- Art der Volumensicherheit
- Snapshot-Richtlinie
- Abkühlungszeitraum für gestaffelte Richtlinien
- Tags in Backups kopieren (mithilfe der AWS CLI und der Amazon FSx-API)

Weitere Informationen finden Sie unter Verwaltung von FSx für ONTAP-Volumes.

Um eine Volume-Konfiguration (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 ONTAP-Dateisystem aus, für das Sie ein Volume aktualisieren möchten.
3. Wählen Sie die Registerkarte Volumes.
4. Wählen Sie das Volume aus, das Sie aktualisieren möchten.
5. Wählen Sie unter Aktionen die Option Volume aktualisieren aus.

   Das Dialogfeld „Lautstärke aktualisieren“ wird mit den aktuellen Einstellungen des Volumes angezeigt.
6. Geben Sie als Verbindungspfad einen vorhandenen Speicherort innerhalb des Dateisystems ein, an dem das Volume bereitgestellt werden soll. Dem Namen muss ein Schrägstrich vorangestellt sein, z. B. `/vol5`
7. Für die Volume-Größe können Sie die Größe des Volumes innerhalb des in der Amazon FSx-Konsole angegebenen Bereichs erhöhen oder verringern. Für FlexVol Volumen beträgt die maximale Größe 300 TiB. Für FlexGroup Volumes beträgt die maximale Größe 300 TiB multipliziert mit der Gesamtzahl der vorhandenen Volumes, bis zu einem Maximum von 20 PiB. FlexGroup
8. Wählen Sie für Speichereffizienz Aktiviert, um die ONTAP-Speichereffizienzfunktionen (Deduplizierung, Komprimierung und Komprimierung) zu aktivieren, oder wählen Sie Deaktiviert, um sie zu deaktivieren.
9. Wählen Sie für die Richtlinie „Kapazitätspool-Tiering“ eine neue Speicherpool-Tiering-Richtlinie für das Volume aus. Diese kann „Automatisch“ (Standardeinstellung), „Nur Snapshot“, „Alle“ oder „Keine“ lauten. Weitere Informationen zu Richtlinien für die Staffelung von Kapazitätspools finden Sie unter. Richtlinien für das Volumen-Tiering

10. Wählen Sie für den Sicherheitsstil Volume entweder Unix (Linux), NTFS oder Mixed. Der Sicherheitsstil eines Volumes bestimmt, ob NTFS- oder UNIX-ACLs für den Zugriff über mehrere Protokolle bevorzugt werden. Der MIXED-Modus ist für den Zugriff über mehrere Protokolle nicht erforderlich und wird nur erfahrenen Benutzern empfohlen.
11. Wählen Sie unter Snapshot-Richtlinie eine Snapshot-Richtlinie für das Volume aus. Weitere Informationen zu Snapshot-Richtlinien finden Sie unterSnapshot-Richtlinien.

    Wenn Sie „Benutzerdefinierte Richtlinie“ wählen, müssen Sie den Namen der Richtlinie im Feld „Benutzerdefinierte Richtlinie“ angeben. Die benutzerdefinierte Richtlinie muss bereits auf der SVM oder im Dateisystem vorhanden sein. Sie können mit der ONTAP CLI oder der REST API eine benutzerdefinierte Snapshot-Richtlinie erstellen. Weitere Informationen finden Sie unter Erstellen einer Snapshot-Richtlinie in der NetApp ONTAP-Produktdokumentation.
12. Die gültigen Werte für die Kühlperiode der Tiering-Richtlinie liegen zwischen 2 und 183 Tagen. Die Abkühlperiode eines Volumes definiert die Anzahl der Tage, bevor Daten, auf die nicht zugegriffen wurde, als kalt markiert und in den Capacity-Pool-Speicher verschoben werden. Diese Einstellung wirkt sich nur auf die `Snapshot-only` Richtlinien `Auto` und aus.
13. Wählen Sie „Aktualisieren“, um das Volume zu aktualisieren.

So aktualisieren Sie die Konfiguration eines Volumes (CLI)

- Um die Konfiguration eines FSx for ONTAP-Volumes zu aktualisieren, verwenden Sie den CLI-Befehl update-volume (oder den entsprechenden UpdateVolumeAPI-Vorgang), wie im folgenden Beispiel gezeigt.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Löschen eines Volumes

Sie können ein FSx for ONTAP-Volume mit der Amazon FSx-Konsole AWS CLI, der und der Amazon FSx-API sowie mit der NetApp ONTAP-Befehlszeilenschnittstelle (CLI) und der REST-API löschen.

> **Important**
>
> Sie können Volumes mit der Amazon FSx-Konsole, API oder CLI nur löschen, wenn für das Volume Amazon FSx-Backups aktiviert sind.

> **Important**
>
> Wenn Sie ein Volume mithilfe der Amazon FSx-Konsole löschen, haben Sie die Möglichkeit, eine endgültige Sicherungskopie des Volumes zu erstellen. Sie können neue Volumes aus Backups erstellen. 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 Volume-Backups löschen. Wenn Sie ein Volume mithilfe des `delete-volume` CLI-Befehls löschen, erstellt Amazon FSx standardmäßig ein letztes Backup.

Bevor Sie ein Volume löschen, stellen Sie sicher, dass keine Anwendungen auf die Daten in dem Volume zugreifen, das Sie löschen möchten.

Um ein Volume zu löschen (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich Dateisysteme und dann das ONTAP-Dateisystem aus, aus dem Sie ein Volume löschen möchten.
3. Wählen Sie die Registerkarte Volumes.
4. Wählen Sie das Volume aus, das Sie löschen möchten.
5. Wählen Sie unter Aktionen die Option Volume löschen aus.
6. Im Bestätigungsdialogfeld haben Sie unter Endgültiges Backup erstellen zwei Optionen:
   - Wählen Sie Ja, um eine endgültige Sicherungskopie des Volumes zu erstellen. Der Name der endgültigen Sicherung wird angezeigt.
   - Wählen Sie Nein, wenn Sie keine endgültige Sicherung des Volumes wünschen. Sie werden aufgefordert, zu bestätigen, dass nach dem Löschen des Volumes keine automatischen Backups mehr verfügbar sind.

7. Bestätigen Sie das Löschen des Volumes, indem Sie im Feld Löschen bestätigen den Text Löschen eingeben.
8. Wählen Sie Volume (s) löschen.

Um ein Volume zu löschen (CLI)

- Um ein FSx for ONTAP-Volume zu löschen, verwenden Sie den CLI-Befehl delete-volume (oder den entsprechenden DeleteVolumeAPI-Vorgang), wie im folgenden Beispiel gezeigt.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Ein Volume anzeigen

Sie können die FSx for ONTAP-Volumes, die sich derzeit in Ihrem Dateisystem befinden, mithilfe der Amazon FSx-Konsole, der und der Amazon AWS CLI FSx-API und -SDKs anzeigen.

So zeigen Sie die Volumes in Ihrem Dateisystem an:

- Mithilfe der Konsole — Wählen Sie ein Dateisystem aus, um die Detailseite für Dateisysteme anzuzeigen. Wählen Sie die Registerkarte Volumes, um alle Volumes im Dateisystem aufzulisten, und wählen Sie dann das Volume aus, das Sie anzeigen möchten.
- Verwenden der CLI oder API — Verwenden Sie den CLI-Befehl describe-volumes oder den DescribeVolumesAPI-Vorgang.

Eine iSCSI-LUN erstellen

Dieser Prozess beschreibt, wie Sie mithilfe des ONTAP CLI-Befehls eine iSCSI-LUN auf einem Amazon FSx for NetApp ONTAP Scale-up-Dateisystem erstellen. NetApp lun create Weitere Informationen finden Sie im ONTAP Documentation Center lun create. NetApp

> **Note**
>
> Das iSCSI-Protokoll wird für Scale-Out-Dateisysteme nicht unterstützt.

Bei diesem Vorgang wird davon ausgegangen, dass Sie bereits ein Volume in Ihrem Dateisystem erstellt haben. Weitere Informationen finden Sie unter Volumen erstellen.

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *management_endpoint_ip*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Erstellen Sie mit dem lun create NetApp CLI-Befehl eine LUN und ersetzen Sie dabei die folgenden Werte:

   - ***svm_name***- Der Name der virtuellen Speichermaschine (SVM), die das iSCSI-Ziel bereitstellt. Der Host verwendet diesen Wert, um die LUN zu erreichen.
   - ***vol_name***- Der Name des Volumes, das die LUN hostet.
   - ***lun_name***- Der Name, den Sie der LUN zuweisen möchten.
   - ***size***- Die Größe der LUN in Byte. Die maximale Größe der LUN, die Sie erstellen können, beträgt 128 TB.

     > **Note**
     >
     > Wir empfehlen, dass Sie ein Volume verwenden, das mindestens 5% größer ist als Ihre LUN-Größe. Dieser Rand lässt Platz für Volume-Snapshots.

   - ***ostype***— Das Betriebssystem des Hosts, entweder `windows_2008` oder`linux`. Wird `windows_2008` für alle Versionen von Windows verwendet. Dadurch wird sichergestellt, dass die LUN über den richtigen Blockoffset für das Betriebssystem verfügt, und die Leistung wird optimiert.

     > **Note**
     >
     > Wir empfehlen, die Speicherzuweisung auf Ihrer LUN zu aktivieren. Wenn die Speicherzuweisung aktiviert ist, kann ONTAP Ihren Host informieren, wenn die LUN keine Kapazität mehr hat, und Speicherplatz zurückgewinnen, wenn Sie Daten aus der LUN löschen.

Weitere Informationen finden Sie `lun create`in der NetApp ONTAP CLI-Dokumentation.

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
ostype ostype -space-allocation enabled
```

```
Created a LUN of size 10g (10737418240)
```

3. Vergewissern Sie sich, dass die LUN erstellt, online und zugeordnet ist.

```
> lun show
```

Das System antwortet mit der folgenden Ausgabe:

```
Vserver   Path                            State   Mapped   Type         Size
--------- ------------------------------- ------- -------- ------------ --------
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

Nächste Schritte

Nachdem Sie eine iSCSI-LUN erstellt haben, besteht der nächste Schritt bei der Verwendung einer iSCSI-LUN als Blockspeicher darin, die LUN einer zuzuordnen. `igroup` Weitere Informationen finden Sie unter Mounting von iSCSI LUNs an einen Linux-Client oder Mounting von iSCSI LUNs an einen Windows-Client.

Verwaltung von SMB-Aktien

Um SMB-Dateifreigaben auf Ihrem Amazon FSx-Dateisystem zu verwalten, können Sie die Microsoft Windows Shared Folders-GUI verwenden. Die Benutzeroberfläche für gemeinsame Ordner bietet einen zentralen Ort für die Verwaltung aller freigegebenen Ordner auf Ihrer virtuellen Speichermaschine (SVM). In den folgenden Verfahren wird detailliert beschrieben, wie Sie Ihre Dateifreigaben erstellen, aktualisieren und entfernen.

> **Note**
>
> Sie können SMB-Dateifreigaben auch mit dem NetApp System Manager verwalten. Weitere Informationen finden Sie unter Verwenden von NetApp System Manager mit BlueXP.

Um geteilte Ordner mit Ihrem Amazon FSx-Dateisystem zu verbinden

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 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 Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance im Amazon EC2-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 einen anderen Computer beispielsweise **`netbios_name.corp.example.com`** den DNS-Namen für Ihre virtuelle Speichermaschine (SVM) ein.

   Um den DNS-Namen Ihrer SVM auf der Amazon FSx-Konsole zu finden, wählen Sie Virtuelle Speichermaschinen, wählen Sie Ihre SVM aus und scrollen Sie dann nach unten zu Endpoints, bis Sie den SMB-DNS-Namen finden. Sie können den DNS-Namen auch in der Antwort auf den API-Vorgang abrufen. DescribeStorageVirtualMachines
6. Wählen Sie OK aus. Ein Eintrag für Ihr Amazon FSx-Dateisystem erscheint dann in der Liste für das Tool Shared Folders.

Nachdem Shared Folders mit Ihrem Amazon FSx-Dateisystem verbunden ist, können Sie die Windows-Dateifreigaben auf dem Dateisystem mit den folgenden Aktionen verwalten:

> **Note**
>
> Wir empfehlen, dass Sie Ihre SMB-Shares auf einem anderen Volume als Ihrem Root-Volume speichern.

- 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. Volumes werden in dem Pfad angezeigt, der bei der Erstellung des Volumes ausgewählt wurde. 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: Wählen Sie Durchsuchen, wenn Sie einen lokalen Ordnerpfad angeben, und wählen Sie Neuen Ordner erstellen, um den lokalen Ordner zu erstellen.
  - Verwenden Sie die Befehlszeile:

    ```
    New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
    $volume_path\MyNewFolder
    ```

- 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**
  >
  > Das Entfernen von Dateifreigaben aus der GUI ist nur möglich, wenn Sie mit dem DNS-Namen des Amazon FSx-Dateisystems eine Verbindung zu fsmgmt.msc hergestellt haben. Wenn Sie die Verbindung über die IP-Adresse oder den DNS-Aliasnamen des Dateisystems hergestellt haben, funktioniert die Option „Teilen beenden“ nicht und die Dateifreigabe wird nicht entfernt.

Überwachen des Dateizugriffs

Amazon FSx for NetApp ONTAP unterstützt die Überwachung von Endbenutzerzugriffen auf Dateien und Verzeichnisse in einer virtuellen Speichermaschine (SVM).

Themen

- Überblick über die Dateizugriffsüberwachung
- Überblick über die Aufgaben zur Einrichtung der Dateizugriffskontrolle

Überblick über die Dateizugriffsüberwachung

Mit der Dateizugriffsüberwachung können Sie die Zugriffe von Endbenutzern auf einzelne Dateien und Verzeichnisse auf der Grundlage der von Ihnen definierten Überwachungsrichtlinien aufzeichnen. Die Prüfung des Dateizugriffs kann Ihnen helfen, die Sicherheit Ihres Systems zu verbessern und das Risiko eines unbefugten Zugriffs auf Ihre Systemdaten zu verringern. Die Prüfung des Dateizugriffs hilft Ihrem Unternehmen, die Datenschutzanforderungen einzuhalten, potenzielle Bedrohungen frühzeitig zu erkennen und das Risiko einer Datenschutzverletzung zu verringern.

Bei Datei- und Verzeichniszugriffen unterstützt Amazon FSx die Protokollierung erfolgreicher Versuche (z. B. dass ein Benutzer mit ausreichenden Berechtigungen erfolgreich auf eine Datei zugreift), fehlgeschlagener Versuche oder beides. Sie können die Überprüfung des Dateizugriffs auch jederzeit deaktivieren.

Standardmäßig werden Audit-Ereignisprotokolle im`EVTX` Dateiformat gespeichert, sodass Sie sie mit Microsoft Event Viewer anzeigen können.

SMB-Zugriffsereignisse, die überprüft werden können

In der folgenden Tabelle sind die SMB-Datei- und Ordnerzugriffsereignisse aufgeführt, die überwacht werden können.

Ereignis-ID (EVT/ EVTX)	Veranstaltung	Beschreibung	Kategorie
560/4656	Objekt öffnen/Objekt erstellen	OBJECT ACCESS: Objekt (Datei oder Verzeichnis) geöffnet	Dateizugriff

Ereignis-ID (EVT/ EVTX)	Veranstaltung	Beschreibung	Kategorie
563/4659	Objekt mit der Absicht öffnen, es zu löschen	OBJEKTZUGRIFF: Ein Handle für ein Objekt (Datei oder Verzeichnis) wurde mit der Absicht angefordert, es zu löschen	Dateizugriff
564/460	Objekt löschen	OBJEKTZUGRIFF: Objekt löschen (Datei oder Verzeichnis). ONTAP generiert dieses Ereignis, wenn ein Windows-Client versucht, das Objekt (Datei oder Verzeichnis) zu löschen.	Dateizugriff

Ereignis-ID (EVT/EVTX)	Veranstaltung	Beschreibung	Kategorie
567/4663	Objekt lesen/Objekt schreiben/Objektattribute abrufen/Objektattribute setzen	OBJEKTZUGRIFF: Versuch, auf das Objekt zuzugreifen (lesen, schreiben, Attribut abrufen, Attribut setzen). **Note** Für dieses Ereignis überprüft ONTAP nur den ersten SMB-Lese- und den ersten SMB-Schreibvorgang (Erfolg oder Misserfolg) für ein Objekt. Dadurch wird verhindert, dass ONTAP übermäßig viele Protokolleinträge erstellt, wenn ein einzelner Client ein Objekt öffnet und viele aufeinand	Dateizugriff

Ereignis-ID (EVT/ EVTX)	Veranstaltung	Beschreibung	Kategorie
		erfolgende Lese- oder Schreibvo rgänge für dasselbe Objekt ausführt.	
NICHT ZUTREFFEN D, 4664	Harter Link	OBJEKTZUGRIFF: Es wurde versucht, einen Hardlink zu erstellen	Dateizugriff
N/A/N/A ONTAP Ereignis-ID 9999	Objekt umbenennung	OBJECT ACCESS: Objekt wurde umbenannt. Dies ist eine ONTAP-Ver anstaltung. Es wird derzeit von Windows nicht als einzelnes Ereignis unterstützt.	Dateizugriff
N/A/N/A ONTAP Ereignis-ID 9998	Objekt trennen	OBJEKTZUGRIFF: Die Verknüpfung zum Objekt wurde aufgehoben. Dies ist eine ONTAP-Ver anstaltung. Es wird derzeit von Windows nicht als einzelnes Ereignis unterstützt.	Dateizugriff

NFS-Zugriffsereignisse, die geprüft werden können

Die folgenden NFS-Datei- und Ordnerzugriffsereignisse können überwacht werden.

- READ
- OPEN
- CLOSE
- READDIR
- WRITE
- SETATTR
- CREATE
- VERKNÜPFUNG
- OPENATTR
- REMOVE
- GETATTR
- VERIFIZIEREN
- NVERIFIZIEREN
- RENAME

Überblick über die Aufgaben zur Einrichtung der Dateizugriffskontrolle

Die Einrichtung von FSx für ONTAP für die Dateizugriffskontrolle umfasst die folgenden allgemeinen Aufgaben:

1. Machen Sie sich mit den Anforderungen und Überlegungen zur Dateizugriffskontrolle vertraut.
2. Erstellen Sie eine Überwachungskonfiguration auf einer bestimmten SVM.
3. Aktivieren Sie das Auditing auf dieser SVM.
4. Konfigurieren Sie die Überwachungsrichtlinien für Ihre Dateien und Verzeichnisse.
5. Sehen Sie sich die Audit-Ereignisprotokolle an, nachdem FSx for ONTAP sie ausgegeben hat.

Einzelheiten zur Aufgabe finden Sie in den folgenden Verfahren.

Wiederholen Sie die Aufgaben für jede andere SVM in Ihrem Dateisystem, für die Sie die Dateizugriffskontrolle aktivieren möchten.

Audit-Parameteranforderungen

Bevor Sie die Überwachung auf einer SVM konfigurieren und aktivieren, beachten Sie Folgendes beachten und beachten, dass Sie die folgenden Anforderungen und Überlegungen beachten.

- Das NFS-Auditing unterstützt als Typ definierte Audit Access Control Entries (ACEs)u, die einen Audit-Logeintrag generieren, wenn versucht wird, auf das Objekt zuzugreifen. Für das NFS-Auditing gibt es keine Zuordnung zwischen Modusbits und Audit-ACEs. Bei der Konvertierung von ACLs in Modusbits werden Audit-ACEs übersprungen. Bei der Konvertierung von Modusbits in ACLs werden keine Audit-ACEs generiert.
- Die Prüfung hängt vom verfügbaren Speicherplatz in den Staging-Volumes ab. (Ein Staging-Volume ist ein dediziertes Volume, das von ONTAP zum Speichern von Staging-Dateien erstellt wurde. Dabei handelt es sich um binäre Zwischendateien auf einzelnen Knoten, auf denen Audit-Datensätze vor der Konvertierung in ein EVTX- oder XML-Dateiformat gespeichert werden.) Sie müssen sicherstellen, dass in Aggregaten, die die geprüften Volumina enthalten, ausreichend Speicherplatz für die Staging-Volumina vorhanden ist.
- Die Überwachung hängt davon ab, ob auf dem Volume, das das Verzeichnis enthält, in dem die konvertierten Audit-Ereignisprotokolle gespeichert werden, verfügbaren Speicherplatz verfügbar ist. Sie müssen sicherstellen, dass auf den Datenträgern, die zum Speichern von Ereignisprotokollen verwendet werden, ausreichend Speicherplatz vorhanden ist. Sie können die Anzahl der Audit-Logs angeben, die im Audit-Verzeichnis aufbewahrt werden sollen, indem Sie den `-rotate-limit` Parameter beim Erstellen einer Überwachungskonfiguration verwenden. Dadurch können Sie sicherstellen, dass auf dem Volume genügend Speicherplatz für die Audit-Logs verfügbar ist.

Auditkonfigurationen auf SVMs erstellen

Bevor Sie mit der Überwachung von Datei- und Verzeichnisereignissen beginnen können, müssen Sie eine Überwachungskonfiguration auf der Storage Virtual Machine (SVM) erstellen. Wenn Sie die Audit-Parameterkonfiguration erstellt haben, müssen Sie auf der SVM aktivieren.

Bevor Sie den`vserver audit create` Befehl zum Erstellen der Überwachungskonfiguration verwenden, stellen Sie sicher, dass Sie ein Verzeichnis erstellt haben, das als Ziel für Protokolle verwendet werden soll, und dass das Verzeichnis keine Symlinks enthält. Sie geben das Zielverzeichnis mit dem`-destination` Parameter an.

Sie können eine Überwachungskonfiguration erstellen, die Audit-Logs je nach Protokollgröße oder einem Zeitplan rotiert, wie folgt:

- Verwenden Sie diesen Befehl, um Audit-Logs basierend auf der Protokollgröße zu rotieren:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

Im folgenden Beispiel wird eine Überwachungskonfiguration für die SVM mit dem Namen erstelltsvm1, die Dateivorgänge und CIFS- (SMB) -Anmelde- und Abmeldeereignisse (Standard) anhand der größenabhängigen Rotation überwacht. Das Protokollformat istEVTX (Standard), die Protokolle werden im/audit_log Verzeichnis gespeichert und Sie haben jeweils eine einzelne Protokolldatei (bis zu 200 MB groß).

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- Verwenden Sie diesen Befehl, um die Audit-Logs nach einem Zeitplan zu rotieren:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]
        [-rotate-limit integer] [-rotate-schedule-month chron_month]
        [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-
day chron_dayofmonth]
        [-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

Der-rotate-schedule-minute Parameter ist erforderlich, wenn Sie die zeitbasierte Rotation von Audit-Logs konfigurieren.

Im folgenden Beispiel wird eine Auditing-Konfiguration für die benannte SVMsvm2 mit zeitbasierter Rotation erstellt. Das Protokollformat istEVTX (die Standardeinstellung) und die Prüfprotokolle werden monatlich um 12:30 Uhr an allen Wochentagen rotiert.

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB  -
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -
rotate-schedule-minute 30
```

Mit dem-format Parameter können Sie angeben, ob die Audit-Logs im konvertiertenEVTX Format (Standard) oder imXML Dateiformat erstellt werden. DasEVTX Format ermöglicht es Ihnen, die Protokolldateien mit Microsoft Event Viewer anzusehen.

Standardmäßig sind die zu überwachenden Ereigniskategorien Dateizugriffsereignisse (sowohl SMB als auch NFS), CIFS- (SMB) -Anmelde- und Abmeldeereignisse sowie Ereignisse zur Änderung der

Autorisierungsrichtlinie. Mithilfe des`-events` Parameters, der das folgende Format hat, können Sie besser steuern, welche Ereignisse protokolliert werden sollen:

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-
account|authorization-policy-change|security-group}
```

Beispielsweise`-events file-share` ermöglicht die Verwendung die Überwachung von Fileshare-Ereignissen.

Weitere Informationen zu dem`vserver audit create` Befehl finden Sie unter Erstellen einer Auditkonfiguration.

Auditing auf einer SVM aktivieren

Nachdem Sie die Einrichtung der Überwachungskonfiguration abgeschlossen haben, müssen Sie die Überwachung auf der SVM aktivieren. Verwenden Sie dazu den folgenden Befehl:

```
vserver audit enable -vserver svm_name
```

Verwenden Sie z. B. den folgenden Befehl, um die Überprüfung auf der genannten SVM zu aktivieren`svm1`.

```
vserver audit enable -vserver svm1
```

Sie können die Zugriffsüberwachen jederzeit deaktivieren. Verwenden Sie beispielsweise den folgenden Befehl, um die Überwachung auf der genannten SVM zu deaktivieren`svm4`.

```
vserver audit disable -vserver svm4
```

Wenn Sie die Überwachung deaktivieren, wird die Audit-Konfiguration auf der SVM nicht gelöscht, was bedeutet, dass Sie die Überwachung auf dieser SVM jederzeit wieder aktivieren können.

Konfiguration von Datei- und Ordnerüberwachungsrichtlinien

Sie müssen die Überwachungsrichtlinien für die Dateien und Ordner konfigurieren, die auf Benutzerzugriffsversuche überprüft werden sollen. Sie können Überwachungsrichtlinien konfigurieren, um sowohl erfolgreiche als auch fehlgeschlagene Zugriffsversuche zu überwachen.

Sie können sowohl SMB- als auch NFS-Auditrichtlinien konfigurieren. Für SMB- und NFS-Auditrichtlinien gelten je nach Sicherheitsstil des Volumes unterschiedliche Konfigurationsanforderungen und Auditfunktionen.

Prüfungsrichtlinien für Dateien und Verzeichnisse im NTFS-Sicherheitsstil

Sie können NTFS-Auditrichtlinien mithilfe der Registerkarte Windows-Sicherheit oder der ONTAP CLI konfigurieren.

So konfigurieren Sie NTFS-Überwachungsrichtlinien (Registerkarte „Windows-Sicherheit“)

Sie konfigurieren NTFS-Auditrichtlinien, indem Sie Einträge zu NTFS-SACLs hinzufügen, die mit einer NTFS-Sicherheitsbeschreibung verknüpft sind. Die Sicherheitsbeschreibung wird dann auf NTFS-Dateien und -Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows-GUI ausgeführt. Die Sicherheitsbeschreibung kann diskretionäre Zugriffskontrolllisten (DACLs) für die Anwendung von Datei- und Ordnerzugriffsberechtigungen, SACLs für die Datei- und Ordnerüberwachung oder sowohl SACLs als auch DACLs enthalten.

1. Wählen Sie im Windows Explorer im Menü Tools die Option Netzlaufwerk zuordnen aus.
2. Füllen Sie das Feld Netzlaufwerk zuordnen aus:

   a. Wählen Sie einen Drive-Buchstaben.
   b. Geben Sie im Feld Ordner den Namen des SMB-Servers (CIFS) ein, der die Freigabe enthält und die Daten enthält, die Sie überprüfen möchten, sowie den Namen der Freigabe.
   c. Wählen Sie Finish (Abschließen).

   Das von Ihnen gewählte Laufwerk ist gemountet und bereit. Im Windows Explorer-Fenster werden die im Share enthaltenen Dateien und Ordner angezeigt.
3. Wählen Sie die Datei oder das Verzeichnis aus, für das Sie den Audit-Parameterzugriff aktivieren möchten.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis und wählen Sie Eigenschaften.
5. Wählen Sie die Registerkarte Sicherheit aus.
6. Klicken Sie auf Erweitert.
7. Wählen Sie den Tab Auditing.
8. Führen Sie die gewünschten Aktionen aus:

Wenn Sie …	Gehen Sie wie folgt vor
Richten Sie die Überwachung für einen neuen Benutzer oder eine neue Gruppe ein	1. Wählen Sie Add (Hinzufügen) aus. 2. Geben Sie im Feld Geben Sie den zu wählenden Objektnamen den Namen des Benutzers oder der Gruppe ein, den Sie hinzufügen möchten. 3. Wählen Sie OK.
Überwachung für einen Benutzer oder eine Gruppe entfernen	1. Wählen Sie im Feld Geben Sie den zu wählenden Objektnamen ein und wählen Sie den Benutzer oder die Gruppe aus, die Sie entfernen möchten. 2. Wählen Sie Remove (Entfernen) aus. 3. Wählen Sie OK. 4. Überspringen Sie den Rest dieses Verfahrens.
Auditing für einen Benutzer oder eine Gruppe ändern	1. Wählen Sie im Feld Geben Sie den zu wählenden Objektnamen ein und wählen Sie den Benutzer oder die Gruppe aus, die Sie ändern möchten. 2. Wählen Sie Edit (Bearbeiten) aus. 3. Wählen Sie OK.

Wenn Sie die Überwachung für einen Benutzer oder eine Gruppe einrichten oder die Überwachung für einen vorhandenen Benutzer oder eine bestehende Gruppe ändern, wird das Feld Auditing-Eintrag für ein ***Objekt*** geöffnet.

9. Wählen Sie im Feld Anwenden auf aus, wie Sie diesen Auditing-Eintrag anwenden möchten.

   Wenn Sie die Überwachung für eine einzelne Datei einrichten, ist das Feld Anwenden auf nicht aktiv, da es standardmäßig auf Nur dieses Objekt gesetzt ist.

10. Wählen Sie im Feld Zugriff aus, was Sie überprüfen möchten und ob Sie erfolgreiche Ereignisse, Fehlerereignisse oder beides überwachen möchten.

    - Um erfolgreiche Ereignisse zu überprüfen, wählen Sie das Feld Erfolg aus.
    - Um Fehlerereignisse zu überprüfen, wählen Sie das Feld Fehler aus.

Wählen Sie die Aktionen aus, die Sie überwachen müssen, um Ihre Sicherheitsanforderungen zu erfüllen. Weitere Informationen über diese überprüfbaren Ereignisse finden Sie in Ihrer Windows-Dokumentation. Sie können die folgenden Ereignisse überprüfen:

- Volle Kontrolle
- Ordner durchqueren/Datei ausführen
- Ordner auflisten/Daten lesen
- Attribute lesen
- Lesen erweiterter Attribute
- Dateien erstellen/Daten schreiben
- Ordner erstellen/Daten anhängen
- Schreiben von Attributen
- Schreiben erweiterter Attribute
- Unterordner und Dateien löschen
- Löschen
- Lesen von Zugriffsberechtigungen
- Berechtigungen ändern
- Überwachen Sie die Verantwortung

11. Wenn Sie nicht möchten, dass die Auditing-Einstellung auf nachfolgende Dateien und Ordner des ursprünglichen Containers übertragen wird, wählen Sie das Feld Diese Auditing-Einträge nur auf Objekte und/oder Container innerhalb dieses Containers anwenden.
12. Wählen Sie Apply (Anwenden) aus.
13. Wenn Sie mit dem Hinzufügen, Entfernen oder Bearbeiten von Audit-Einträgen fertig sind, wählen Sie OK.

    Das Feld Auditing-Eintrag für ***das Objekt*** wird geschlossen.
14. Wählen Sie im Feld Auditing die Vererbungseinstellungen für diesen Ordner aus. Wählen Sie nur die Minimalebene, die die Audit-Ereignisse bereitstellt, die Ihren Sicherheitsanforderungen entsprechen.

    Sie können eine der folgenden Optionen auswählen:

- Wählen Sie das Feld Vererbbare Prüfungseinträge aus dem übergeordneten Objekt einbeziehen.
- Wählen Sie das Feld Alle vorhandenen vererbbaren Audit-Einträge auf allen untergeordneten Objekten durch vererbbare Audit-Einträge aus diesem Objekt ersetzen.
- Wählen Sie beide Felder aus.
- Wähle keine der beiden Boxen.

Wenn Sie SACLs für eine einzelne Datei festlegen, ist das Feld Alle vorhandenen vererbbaren Auditing-Einträge auf allen untergeordneten Objekten durch vererbbare Auditing-Einträge aus diesem Objekt ersetzen im Feld Auditing nicht vorhanden.

15. Wählen Sie OK.

So konfigurieren Sie NTFS-Auditrichtlinien (ONTAP CLI)

Mithilfe der ONTAP CLI können Sie NTFS-Auditrichtlinien konfigurieren, ohne dass Sie über einen SMB-Share auf einem Windows-Client eine Verbindung zu den Daten herstellen müssen.

- Sie können NTFS-Auditrichtlinien mithilfe der Befehlsfamilie vserver security file-directory konfigurieren.

Der folgende Befehl wendet beispielsweise eine Sicherheitsrichtlinie mit dem Namenp1 auf die benannte SVM an`vs0`.

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

Prüfungsrichtlinien für Dateien und Verzeichnisse im UNIX-Sicherheitsstil

Sie konfigurieren die Überwachung von Dateien und Verzeichnissen im UNIX-Sicherheitsstil, indem Sie Audit-ACEs (Zugriffskontrollausdrücke) zu NFS v4.x-ACLs (Zugriffskontrolllisten) hinzufügen. Auf diese Weise können Sie aus Sicherheitsgründen bestimmte NFS-Datei- und Verzeichniszugriffsereignisse überwachen.

> **Note**
>
> Für NFS v4.x werden sowohl diskretionäre als auch System-ACEs in derselben ACL gespeichert. Daher müssen Sie beim Hinzufügen von Audit-ACEs zu einer vorhandenen ACL

vorsichtig sein, um zu vermeiden, dass eine vorhandene ACL überschrieben und verloren geht. Die Reihenfolge, in der Sie die Audit-ACEs zu einer vorhandenen ACL hinzufügen, spielt keine Rolle.

So konfigurieren Sie UNIX-Audit-Richtlinien

1. Rufen Sie die vorhandene ACL für die Datei oder das Verzeichnis ab, indem Sie den Befehl`nfs4_getfacl` oder einen entsprechenden Befehl verwenden.
2. Hängen Sie die gewünschten Audit-ACEs an.
3. Wenden Sie die aktualisierte ACL auf die Datei oder das Verzeichnis an, indem Sie den Befehl`nfs4_setfacl` oder einen entsprechenden Befehl verwenden.

   In diesem Beispiel wird die`-a` Option verwendet, um einem Benutzer (benannt`testuser`) Leseberechtigungen für die benannte Datei zu gewähren`file1`.

   ```
   nfs4_setfacl -a "A::testuser@example.com:R" file1
   ```

Anzeigen von Audit-Parameterprotokollen

Sie können Audit-Ereignisprotokolle anzeigen, die in den`XML` Dateiformaten`EVTX` oder gespeichert sind.

- `EVTX`Dateiformat — Sie können die konvertierten`EVTX` Audit-Ereignisprotokolle als gespeicherte Dateien mit Microsoft Event Viewer öffnen.

  Es gibt zwei Optionen, die Sie beim Anzeigen von Ereignisprotokollen mit der Ereignisanzeige verwenden können:

  - Allgemeine Ansicht: Informationen, die allen Ereignissen gemeinsam sind, werden für den Ereignisdatensatz angezeigt. Die ereignisspezifischen Daten für den Ereignisdatensatz werden nicht angezeigt. Sie können die Detailansicht verwenden, um ereignisspezifische Daten anzuzeigen.
  - Detailansicht: Eine benutzerfreundliche Ansicht und eine XML-Ansicht sind verfügbar. In der benutzerfreundlichen Ansicht und in der XML-Ansicht werden sowohl die Informationen angezeigt, die allen Ereignissen gemeinsam sind, als auch die ereignisspezifischen Daten für den Ereignisdatensatz.

- `XML`Dateiformat — Sie können XML-Auditereignisprotokolle in Anwendungen von Drittanbietern, die das XML-Dateiformat unterstützen, anzeigen und verarbeiten. Tools zur XML-Anzeige können zum Anzeigen der Prüfprotokolle verwendet werden, sofern Sie über das XML-Schema und Informationen zu den Definitionen für die XML-Felder verfügen.

Skalierung der SSD-Speicherkapazität und der bereitgestellten IOPS

Wenn Sie zusätzlichen Speicherplatz für den aktiven Teil Ihres Datensatzes benötigen, können Sie die Solid-State-Drive-Speicherkapazität (SSD) Ihres Amazon FSx for NetApp ONTAP-Dateisystems erhöhen. Sie können dies tun, indem Sie die Amazon FSx-Konsole, die Amazon FSx-API oder AWS Command Line Interface ()AWS CLI verwenden.

Sie können auch die bereitgestellten SSD-IOPS für Ihr Dateisystem ändern, entweder wenn Sie die primäre SSD-Speicherkapazität erhöhen oder als eigenständige Aktion. Weitere Informationen zur Skalierung der primären SSD-Speicherkapazität eines Dateisystems und zur Anzahl der bereitgestellten IOPS finden Sie unter. Aktualisierung des Dateisystems, des SSD-Speichers und der IOPS

Verwaltung der Durchsatzkapazität

FSx for ONTAP konfiguriert die Durchsatzkapazität, wenn Sie das Dateisystem erstellen. Sie können die Durchsatzkapazität Ihres Scale-up-Dateisystems jederzeit ändern, aber Sie können die Durchsatzkapazität Ihres Scale-out-Dateisystems nicht ändern. Denken Sie daran, dass Ihr Dateisystem eine bestimmte Konfiguration erfordert, um die maximale Durchsatzkapazität zu erreichen. Um beispielsweise 4 Gbit/s Durchsatzkapazität für ein Scale-up-Dateisystem bereitzustellen, benötigt Ihr Dateisystem eine Konfiguration mit mindestens 5.120 GiB SSD-Speicherkapazität und 160.000 SSD-IOPS. Weitere Informationen finden Sie unter Auswirkungen der Durchsatzkapazität auf die Leistung.

Die Durchsatzkapazität ist ein Faktor, der die Geschwindigkeit bestimmt, mit der der Dateiserver, der das Dateisystem hostet, die Dateidaten bereitstellen kann. Höhere Durchsatzkapazitäten sind mit einem höheren Maß an Netzwerk, Festplatten-Lese-I/O-Vorgängen pro Sekunde (IOPS) und Daten-Cache-Kapazität auf dem Dateiserver verbunden. Weitere Informationen finden Sie unter Leistung.

Wenn Sie die Durchsatzkapazität Ihres Dateisystems ändern, schaltet Amazon FSx den Dateiserver aus, der Ihr Dateisystem mit Strom versorgt. Sowohl bei Single-AZ- als auch bei Multi-AZ-

Dateisystemen kommt es während dieses Vorgangs zu einem automatischen Failover und Failback, der in der Regel einige Minuten in Anspruch nimmt. Die Failover- und Failback-Prozesse sind für NFS- (Network File Sharing) -, SMB- (Server Message Block) - und iSCSI-Clients (Internet Small Computer Systems Interface) transparent, sodass Ihre Workloads ohne Unterbrechung oder manuelles Eingreifen weiterlaufen können. Die neue Menge an Durchsatzkapazität wird Ihnen in Rechnung gestellt, sobald sie für Ihr Dateisystem verfügbar ist.

> **Note**
>
> Um die Datenintegrität während der Wartungsaktivitäten zu gewährleisten, schließt FSx for ONTAP alle opportunistischen Sperren und schließt alle ausstehenden Schreibvorgänge auf den zugrunde liegenden Speichervolumes ab, die Ihr Dateisystem hosten, bevor die Wartung beginnt. Während eines geplanten Wartungsfensters für das Dateisystem können Systemänderungen (z. B. Änderungen an Ihrer Durchsatzkapazität) verzögert werden. Die Systemwartung kann dazu führen, dass diese Änderungen in die Warteschlange gestellt werden, bis sie verarbeitet werden. Weitere Informationen finden Sie unter the section called “Wartungsfenster”.

Themen

- Wann muss die Durchsatzkapazität geändert werden
- Wie werden gleichzeitige Durchsatz- und Speicherskalierungsanforderungen behandelt
- Wie ändert man die Durchsatzkapazität
- Überwachung von Änderungen der Durchsatzkapazität

Wann muss die Durchsatzkapazität geändert werden

Amazon FSx ist in Amazon integriert CloudWatch, sodass Sie die laufende Durchsatznutzung Ihres Dateisystems überwachen können. Der Durchsatz und die IOPS-Leistung, die Sie in Ihrem Dateisystem erzielen können, hängen neben der Durchsatzkapazität Ihres Dateisystems auch von den Eigenschaften Ihres spezifischen Workloads ab. In der Regel sollten Sie genügend Durchsatzkapazität bereitstellen, um den Lesedurchsatz Ihres Workloads plus den doppelten Schreibdurchsatz Ihres Workloads zu unterstützen. Mithilfe von CloudWatch Metriken können Sie bestimmen, welche dieser Dimensionen geändert werden müssen, um die Leistung zu verbessern. Weitere Informationen finden Sie unter the section called “So verwenden Sie FSx für ONTAP CloudWatch-Metriken”.

> **Note**
>
> Sie können die Durchsatzkapazität für Scale-Out-Dateisysteme nicht ändern.

Wie werden gleichzeitige Durchsatz- und Speicherskalierungsanforderungen behandelt

Sie können eine Aktualisierung der Durchsatzkapazität anfordern, kurz bevor ein Workflow zur Aktualisierung von SSD-Speicherkapazität und bereitgestellter IOPS beginnt oder während dieser ausgeführt wird. Die Reihenfolge, in der Amazon FSx die beiden Anfragen verarbeitet, ist wie folgt:

- Wenn Sie ein SSD/IOPS-Update und ein Update der Durchsatzkapazität gleichzeitig einreichen, werden beide Anfragen akzeptiert. Das SSD/IOPS-Update wird vor dem Update der Durchsatzkapazität priorisiert.
- Wenn Sie ein Update der Durchsatzkapazität einreichen, während ein SSD/IOPS-Update ausgeführt wird, wird die Anfrage zur Aktualisierung der Durchsatzkapazität akzeptiert und in die Warteschlange gestellt, sodass sie nach dem SSD/IOPS-Update erfolgt. Die Aktualisierung der Durchsatzkapazität beginnt nach der Aktualisierung von SSD/IOPS (neue Werte sind verfügbar) und während des Optimierungsschritts. Dies dauert in der Regel weniger als 10 Minuten.
- Wenn Sie ein SSD/IOPS-Update einreichen, während eine Aktualisierung der Durchsatzkapazität durchgeführt wird, wird die SSD/IOPS-Speicheraktualisierungsanforderung akzeptiert und in die Warteschlange gestellt, um sie zu starten, nachdem die Durchsatzkapazitätsaktualisierung abgeschlossen ist (neue Durchsatzkapazität ist verfügbar). Dies dauert in der Regel 20 Minuten.

Weitere Informationen zu SSD-Speicher und bereitgestellten IOPS-Updates finden Sie unter. Verwaltung der Speicherkapazität

Wie ändert man die Durchsatzkapazität

Sie können die Durchsatzkapazität eines Dateisystems mithilfe der Amazon FSx-Konsole, der AWS Command Line Interface (AWS CLI) oder der Amazon FSx-API ändern.

Um die Durchsatzkapazität eines Dateisystems 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 ONTAP-Dateisystem aus, für das Sie die Durchsatzkapazität erhöhen möchten.
3. Wählen Sie für Aktionen die Option Durchsatzkapazität aktualisieren aus. Oder wählen Sie im Übersichtsbereich neben der Durchsatzkapazität des Dateisystems die Option Aktualisieren aus.
4. Wählen Sie den neuen Wert für die Durchsatzkapazität aus der Liste aus.

   > **Note**
   >
   > Sie können die Durchsatzkapazität für jedes FSx for ONTAP-Dateisystem ändern. Allerdings können nur Dateisysteme, die am oder nach dem 9. Dezember 2021 erstellt wurden, eine Durchsatzkapazität von 128 MB/s oder 256 MB/s unterstützen.

5. Wählen Sie Update, um die Aktualisierung der Durchsatzkapazität zu starten.
6. Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme auf der Registerkarte Updates überwachen.

   Sie können den Fortschritt des Updates mithilfe der Amazon FSx-KonsoleAWS CLI, der und der API überwachen. Weitere Informationen finden Sie unter Überwachung von Änderungen der Durchsatzkapazität.

So ändern Sie die Durchsatzkapazität (CLI) eines Dateisystems

Verwenden Sie den AWS CLI Befehl, um die Durchsatzkapazität eines Dateisystems zu ändern 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-KonsoleAWS CLI, der und der API überwachen. 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 überwachen.

Überwachung von Änderungen der Durchsatzkapazität in der Konsole

Auf der Registerkarte Updates im Fenster mit den Dateisystemdetails können Sie die 10 neuesten Aktualisierungsaktionen für jeden Aktualisierungsaktionstyp anzeigen.

Für Aktionen zur Aktualisierung der Durchsatzkapazität können Sie sich die folgenden Informationen anzeigen lassen.

Art der Aktualisierung

Unterstützte Typen sind Durchsatzkapazität, Speicherkapazität und Speicheroptimierung.

Zielwert

Der gewünschte Wert, auf den die Durchsatzkapazität des Dateisystems geändert werden soll.

Status

Der aktuelle Status des Updates. Für Aktualisierungen der Durchsatzkapazität 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 — Die Aktualisierung der Durchsatzkapazität wurde erfolgreich abgeschlossen.
- Fehlgeschlagen — Die Aktualisierung der Durchsatzkapazität ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Einzelheiten darüber zu erhalten, warum die Durchsatzaktualisierung fehlgeschlagen ist.

Uhrzeit der Anfrage

Der Zeitpunkt, zu dem Amazon FSx die Aktualisierungsanfrage erhalten hat.

Überwachung von Änderungen mit der AWS CLI AND-API

Sie können Anfragen zur Änderung der Kapazität des Dateisystemdurchsatzes mithilfe des describe-file-systemsCLI-Befehls und der DescribeFileSystemsAPI-Aktion anzeigen und überwachen. Das `AdministrativeActions` Array listet die 10 neuesten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die Durchsatzkapazität eines Dateisystems ändern, wird eine `FILE_SYSTEM_UPDATE` Verwaltungsaktion generiert.

Das folgende Beispiel zeigt den Antwortausschnitt eines `describe-file-systems` CLI-Befehls. Das Dateisystem hat eine Durchsatzkapazität von 128 MB/s und eine Zieldurchsatzkapazität von 256 MB/s.

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Wenn Amazon FSx die Aktion erfolgreich verarbeitet, ändert sich der Status in`COMPLETED`. Die neue Durchsatzkapazität ist dann für das Dateisystem verfügbar und wird in der `ThroughputCapacity` Eigenschaft angezeigt. Dies wird im folgenden Antwortauszug eines describe-file-systems CLI-Befehls gezeigt.

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Wenn die Änderung der Durchsatzkapazität fehlschlägt, ändert sich der Status in`FAILED`, und die `FailureDetails` Eigenschaft enthält Informationen über den Fehler.

Leistungsoptimierung mit Amazon FSx-Wartungsfenstern

Als vollständig verwalteter Service führt FSx for ONTAP regelmäßig Wartungsarbeiten und Updates an Ihrem Dateisystem durch. Diese Wartung hat für die meisten Workloads keine Auswirkungen. Bei leistungsabhängigen Workloads kann es in seltenen Fällen vorkommen, dass Sie bei Wartungsarbeiten eine kurze (<60 Sekunden) Beeinträchtigung der Leistung feststellen. Amazon FSx ermöglicht es Ihnen, das Wartungsfenster zu verwenden, um zu kontrollieren, wann solche potenziellen Wartungsaktivitäten stattfinden.

Das Patchen erfolgt selten, in der Regel einmal alle paar Wochen. Bei Scale-up-Dateisystemen dauert das Patchen in der Regel nur 30 Minuten ab Beginn des Wartungsfensters. Bei Dateisystemen mit horizontaler Skalierung dauert das Patchen bis zu 90 Minuten ab Beginn des Wartungsfensters. Während dieser wenigen Minuten führen Ihre Dateisysteme automatisch einen Failover und ein Failback durch. Sie wählen das Wartungsfenster bei der Erstellung des Dateisystems. Wenn Sie keine Zeitpräferenz haben, wird eine Startzeit von 30 Minuten zugewiesen.

FSx for ONTAP ermöglicht es Ihnen, Ihr Wartungsfenster nach Bedarf an Ihre Arbeitslast und Betriebsanforderungen anzupassen. Sie können Ihr Wartungsfenster beliebig oft verschieben, vorausgesetzt, dass mindestens einmal alle 14 Tage ein Wartungsfenster geplant ist. Wenn ein Patch veröffentlicht wird und Sie innerhalb von 14 Tagen kein Wartungsfenster geplant haben, wird FSx for ONTAP mit der Wartung des Dateisystems fortfahren, um dessen Sicherheit und Zuverlässigkeit zu gewährleisten.

> **Note**
>
> Um die Datenintegrität während der Wartungsaktivitäten zu gewährleisten, schließt FSx for ONTAP alle opportunistischen Sperren und schließt alle ausstehenden Schreibvorgänge auf den zugrunde liegenden Speichervolumes ab, die Ihr Dateisystem hosten, bevor die Wartung beginnt.

Sie können die Amazon FSx Management ConsoleAWS CLI, AWS API oder eines der AWS SDKs verwenden, um das Wartungsfenster für Ihre Dateisysteme zu ändern.

Um das wöchentliche Wartungsfenster (Konsole) zu ändern

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie in der linken Navigationsspalte Dateisysteme aus.
3. Wählen Sie das Dateisystem aus, für das Sie das wöchentliche Wartungsfenster ändern möchten. Die Seite mit den Details zum Dateisystem mit der Zusammenfassung wird angezeigt.
4. Wählen Sie Administration, um den Bereich Einstellungen für die Dateisystemverwaltung aufzurufen.
5. Wählen Sie „Aktualisieren“, um das Fenster „Wartung ändern“ aufzurufen.
6. Geben Sie den neuen Tag und die 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 den Einstellungen der Dateisystemadministration angezeigt.

Informationen zum Ändern des wöchentlichen Wartungsfensters mithilfe des update-file-systemCLI-Befehls finden Sie unterSo aktualisieren Sie ein Dateisystem (CLI).

Markieren Sie Ihre Amazon FSx-Ressourcen mit Tags

Zur einfacheren Verwaltung Ihrer Dateisysteme und anderer Amazon FSx-Ressourcen können Sie den einzelnen Ressourcen bei Bedarf eigene Metadaten in Form von Tags zuweisen. Mithilfe von Tags können Sie Ihre AWS -Ressourcen auf verschiedene Arten kategorisieren, z. B. nach Zweck, Besitzer oder Umgebung. Diese Kategorisierung ist nützlich, wenn Sie viele Ressourcen desselben Typs haben — In diesem Fall können Sie schnell bestimmte Ressourcen basierend auf den zugewiesenen Tags bestimmen. In diesem Thema werden Tags (Markierungen) und deren Erstellung beschrieben.

Themen

- Grundlagen zu Tags (Markierungen)
- Markieren Ihrer -Ressourcen
- Kopieren von Tags in Backups
- Tag (Markierung)-Einschränkungen
- Berechtigungen und Tagging

Grundlagen zu Tags (Markierungen)

Ein Tag ist eine Markierung, die Sie einer AWS Ressource zuordnen. Jedes Tag besteht aus zwei Teilen, die Sie definieren:

- einem Tag-Schlüssel (z. B. `CostCenter`, `Environment` oder `Project`). Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.
- Einem Tag-Wert (z. B. `111122223333` oder `Production`). Wie bei Tag-Schlüsseln wird auch bei Tag-Werten zwischen Groß- und Kleinschreibung unterschieden. Tag-Werte sind optional.

Sie können Tags verwenden, um Ihre AWS -Ressourcen auf verschiedene Arten zu kategorisieren, z. B. nach Zweck, Besitzer oder Umgebung. Sie können zum Beispiel eine Reihe von Tags für die Amazon FSx-Dateisysteme Ihres Kontos definieren, die Ihnen dabei helfen, den 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 durchsuchen und filtern. Weitere Informationen zum Implementieren einer effektiven Ressourcen-Markierungs-Strategie finden Sie unter Tagging AWS Ressourcen im. Allgemeine AWS-Referenz

Beachten Sie Sie Sie Sie Sie Sie Sie Sie Sie Sie Sie Sie Sie Sie Sie Sie Sie Sie

- Tags haben keine semantische Bedeutung für Amazon FSx und werden ausschließlich als Zeichenfolgen interpretiert.
- Tags werden 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 auf eine leere Zeichenfolge setzen, aber Sie können den Wert eines Tags nicht auf setzen`null`.
- 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, die AWS Command Line Interface (AWS CLI) oder ein AWS SDK verwenden, können Sie Folgendes tun:
  - Sie können die `TagResource` API-Aktion, um Tags auf vorhandene Ressourcen anzuwenden.
  - Für einige Aktionen zur Ressourcenerstellung können Sie Tags für eine Ressource angeben, wenn die Ressource erstellt wird. Indem Sie Ressourcen zum Erstellungszeitpunkt markieren, müssen Sie anschließend keine benutzerdefinierten Skripts ausführen.

    Wenn Tags nicht während der Ressourcenerstellung angewendet werden können, wird die Ressourcenerstellung von Amazon FSx rückgängig gemacht. Dieses Verhalten trägt dazu bei, dass Ressourcen entweder mit Tags oder überhaupt nicht erstellt werden und dass keine Ressourcen zu irgendeinem Zeitpunkt unmarkiert bleiben.

    > **Note**
    >
    > Sie AWS Identity and Access Management sind für die Erstellung taggen Ressourcen bei der Erstellung mit Tags versehen können. Weitere Informationen 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 vorhanden sind. Wenn Sie die Amazon FSx-Konsole verwenden, können Sie Tags auf der Registerkarte Tags auf dem entsprechenden Ressourcenbildschirm Tags auf Ressourcen anwenden. Wenn Sie Ressourcen erstellen, können Sie den Namensschlüssel mit einem Wert anwenden, und Sie können beim Erstellen eines neuen Dateisystems Tags Ihrer Wahl anwenden. Obwohl die Konsole Ressourcen nach dem Name -Schlüssel organisiert, hat dieser Schlüssel keine semantische Bedeutung für den Amazon FSx-Service.

Zur granulare Kontrolle über die Benutzer und Gruppen zu implementieren, die Ressourcen bei der Erstellung taggen können, können Sie Tag-basierte Berechtigungen auf Ressourcenebene in Ihren IAM-Richtlinien auf die Amazon FSx-API-Aktionen anwenden, die das Tagging bei der Erstellung unterstützen. Wenn Sie diese Berechtigungen in Ihren -Richtlinien verwenden, erhalten Sie die die die folgenden Vorteile:

- Ihre Ressourcen sind vor der Erstellung ordnungsgemäß gesichert.

- Da Tags sofort auf Ihre Ressourcen angewendet werden, sind alle Tag-basierten Berechtigungen auf Ressourcenebene, die die Verwendung von Ressourcen steuern, sofort wirksam.
- 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.

Um die Tag-Schlüssel und -Werte zu steuern, die für Ihre bestehenden Ressourcen festgelegt sind, können Sie Berechtigungen auf Ressourcenebene auf die - `TagResource` und `UntagResource` - Amazon FSx-API-Aktionen in den IAM-Richtlinien anwenden.

Weitere Informationen zu den Berechtigungen, die zum Tagging von Amazon FSx-Ressourcen bei der Erstellung mit Tags versehen können, finden Sie unterErteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung.

Weitere Informationen zur Verwendung von Tags zum Beschränken des Zugriffs auf Amazon-FSx-Ressourcen in IAM-Richtlinien finden Sie unter. Verwenden von Tags zur Steuerung des Zugriffs auf Ihre Amazon FSx-Ressourcen

Informationen zum Markieren von Ressourcen für die Fakturierung finden Sie unter Verwendung von Kostenzuordnungs-Tags im AWS BillingBenutzerhandbuch.

Kopieren von Tags in Backups

Wenn Sie ein Volume in der Amazon FSx-API oder aktualisieren, können Sie aktivieren AWS CLI`CopyTagsToBackups`, dass alle Tags automatisch von Ihren Volumes in Backups kopiert werden.

> **Note**
>
> Wenn Sie bei der Erstellung eines benutzerinitiierten Backups Tags angeben (einschließlich des Name-Tags, wenn Sie ein Backup mit der Amazon FSx-Konsole erstellen), werden Tags nicht vom Volume kopiert, selbst wenn Sie dies aktiviert haben. `CopyTagsToBackups`

Weitere Informationen über Sicherungen finden Sie unter Arbeiten mit Backups. Weitere Informationen zur Aktivierung `CopyTagsToBackups` finden Sie unter So erstellen Sie ein Volume (CLI) und So aktualisieren Sie die Konfiguration eines Volumes (CLI) im Amazon FSx for NetApp

ONTAP-Benutzerhandbuch oder CreateVolumeUpdateVolumein der Amazon FSx for NetApp ONTAP-API-Referenz.

Tag (Markierung)-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Die maximale Anzahl an Tags pro Ressource beträgt 50.
- Die maximale Schlüssellänge beträgt 128 Unicode-Zeichen in UTF-8.
- Die maximale Wertelänge beträgt 256 Unicode-Zeichen in UTF-8.
- Die zulässigen Zeichen sind Buchstaben, Zahlen und Leerzeichen, die in UTF-8 darstellbar sind, und die die folgenden Zeichen: `+ - (Bindestrich) (Unterstrich) = . _ . : / @`
- Jeder Tag (Markierung) muss für jede Ressource eindeutig sein. Jeder Tag (Markierung) kann nur einen Wert haben.
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden.
- Das Präfix `aws:` ist zur Verwendung in AWS reserviert. Wenn das Tag über einen Tag-Schlüssel mit diesem Präfix verfügt, können Sie den Schlüssel oder Wert des Tags 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 die Ressourcenbezeichner angeben. Um beispielsweise ein Dateisystem zu löschen, das Sie mit dem Tag-Schlüssel markiert haben`DeleteMe`, müssen Sie die `DeleteFileSystem` -Aktion mit der Ressourcenbezeichner des -Dateisystems verwenden, z. B.`fs-1234567890abcdef0`.

Wenn Sie öffentliche oder gemeinsam genutzte Ressourcen markieren, sind die von Ihnen zugewiesenen Tags nur für Sie AWS-Konto verfügbar. Kein anderer AWS-Konto hat Zugriff auf diese Tags. Für die tagbasierte Zugriffskontrolle auf freigegebene Ressourcen AWS-Konto muss jede ihren eigenen Satz von Tags zuweisen, um den Zugriff auf die Ressource zu kontrollieren.

Berechtigungen und Tagging

Weitere Informationen zu den Berechtigungen, die zum Tagging von Amazon FSx-Ressourcen bei der Erstellung mit Tags versehen können, finden Sie unterErteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung.

Weitere Informationen zur Verwendung von Tags zum Beschränken des Zugriffs auf Amazon-FSx-Ressourcen in IAM-Richtlinien finden Sie unter. Verwenden von Tags zur Steuerung des Zugriffs auf Ihre Amazon FSx-Ressourcen

Verwaltung von FSx for ONTAP-Ressourcen mithilfe von Anwendungen NetApp

Neben der AWS Management Console AWS CLI, und AWS API und den SDKs können Sie auch diese NetApp Verwaltungstools und -anwendungen verwenden, um Ihre FSx for ONTAP-Ressourcen zu verwalten:

Themen

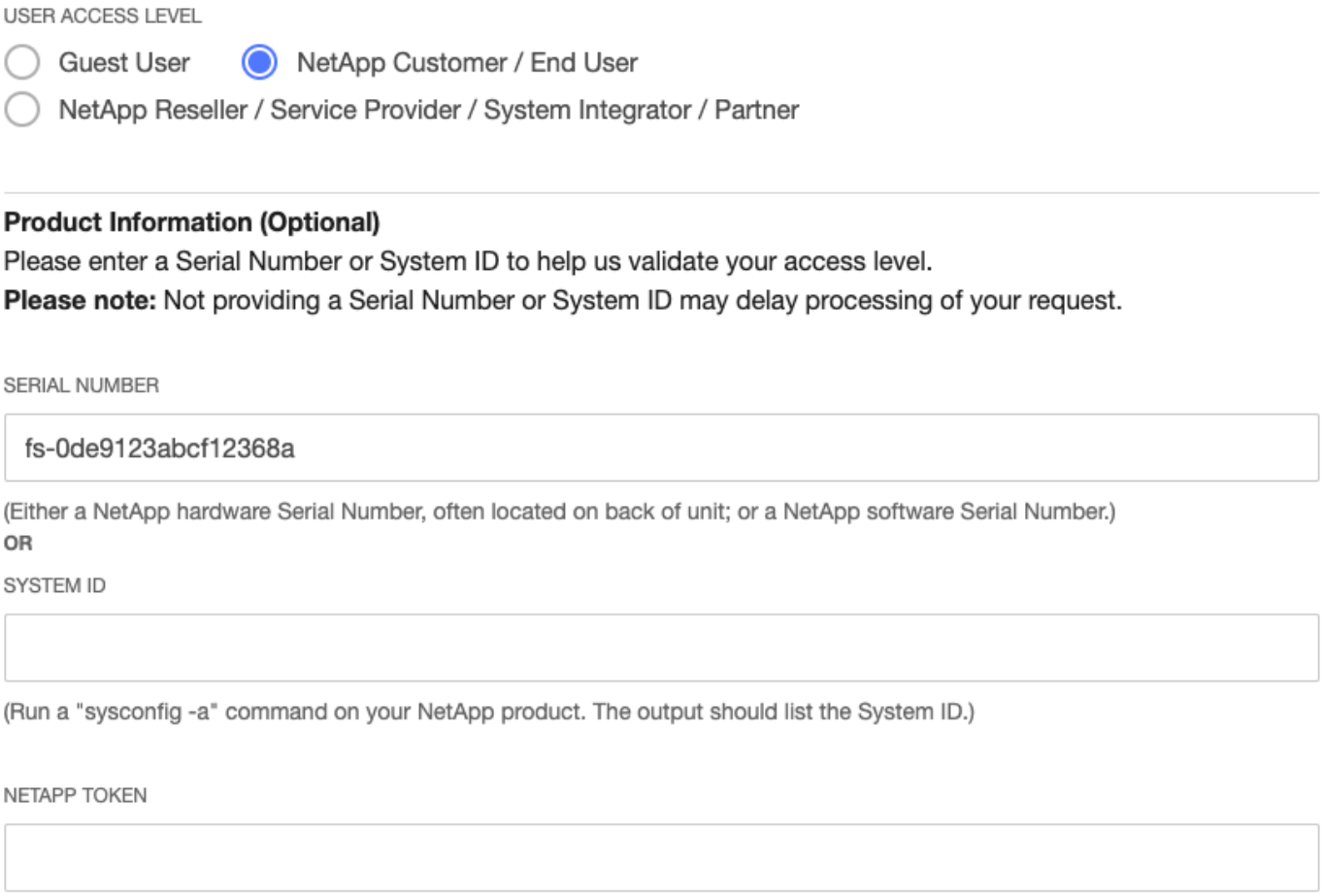
- Eröffnen Sie ein Konto NetApp
- Verwenden von NetApp BlueXP
- Verwenden der NetApp ONTAP-CLI
- Verwendung der ONTAP REST-API

> **Important**
>
> Amazon FSx synchronisiert sich regelmäßig mit, ONTAP um Konsistenz zu gewährleisten. Wenn Sie Volumes mithilfe von NetApp Anwendungen erstellen oder ändern, kann es mehrere Minuten dauern, bis diese Änderungen in der AWS Management Console, AWS CLI, API und den SDKs übernommen werden.

Eröffnen Sie ein Konto NetApp

Um NetApp Software wieBlueXP, SnapCenter und den ONTAP Antivirus-Connector herunterzuladen, benötigen Sie ein NetApp Konto. Gehen Sie wie folgt vor, um ein NetApp Konto zu eröffnen:

1. Gehen Sie zur Seite NetAppBenutzerregistrierung und registrieren Sie sich für ein neues NetApp Benutzerkonto.
2. Füllen Sie das/die Formular (e) mit Ihren Daten aus. Achten Sie darauf, die NetAppZugriffsebene Kunde/Endbenutzer auszuwählen. Kopieren Sie im Feld SERIENNUMMER die Dateisystem-ID für Ihr FSx for ONTAP-Dateisystem und fügen Sie sie ein. Sehen Sie sich das folgende Beispiel an:



Was erwartet Sie nach der Registrierung

Bei Kunden mit bestehenden NetApp Produkten wird ihr NSS-Konto innerhalb eines Werktages auf Kundenebene hochgestuft. Kunden, die neu bei uns sind, NetApp werden nach den üblichen Geschäftspraktiken aufgenommen und ihr NSS-Konto wird zusätzlich zum Zugang auf Kundenebene hochgestuft. Durch die Angabe der Dateisystem-ID kann dieser Vorgang beschleunigt werden. Sie können den Status Ihres NSS-Kontos überprüfen, indem Sie sich bei mysupport.netapp.com anmelden und zur Willkommensseite navigieren. Die Zugriffsebene Ihres Kontos sollte Kundenzugang sein.

Verwenden von NetApp BlueXP

NetApp BlueXP ist eine einheitliche Steuerungsebene, die die Verwaltung von Speicher- und Datendiensten in lokalen und Cloud-Umgebungen vereinfacht. BlueXP bietet eine zentrale Benutzeroberfläche zur Verwaltung, Überwachung und Automatisierung von ONTAP-Bereitstellungen

innerhalb und vor Ort. AWS Weitere Informationen finden Sie in der NetApp BlueXP-Dokumentation und in der NetApp BlueXP for Amazon FSx for ONTAP-Dokumentation. NetApp

> **Note**
>
> NetApp BlueXPwird für Scale-Out-Dateisysteme nicht unterstützt.

Verwenden von NetApp System Manager mit BlueXP

Sie können Ihre Amazon FSx for NetApp ONTAP-Dateisysteme mit System Manager direkt von aus verwalten. BlueXP BlueXPermöglicht es Ihnen, dieselbe System Manager-Oberfläche zu verwenden, die Sie gewohnt sind, sodass Sie Ihre hybride Multi-Cloud-Infrastruktur von einer einzigen Steuerungsebene aus verwalten können. Sie haben auch Zugriff auf die anderen Funktionen von BlueXP. Weitere Informationen finden Sie im Thema System Manager-Integration mit BlueXP in der ONTAP-Dokumentation. NetApp

> **Note**
>
> NetApp System Manager wird für Scale-Out-Dateisysteme nicht unterstützt.

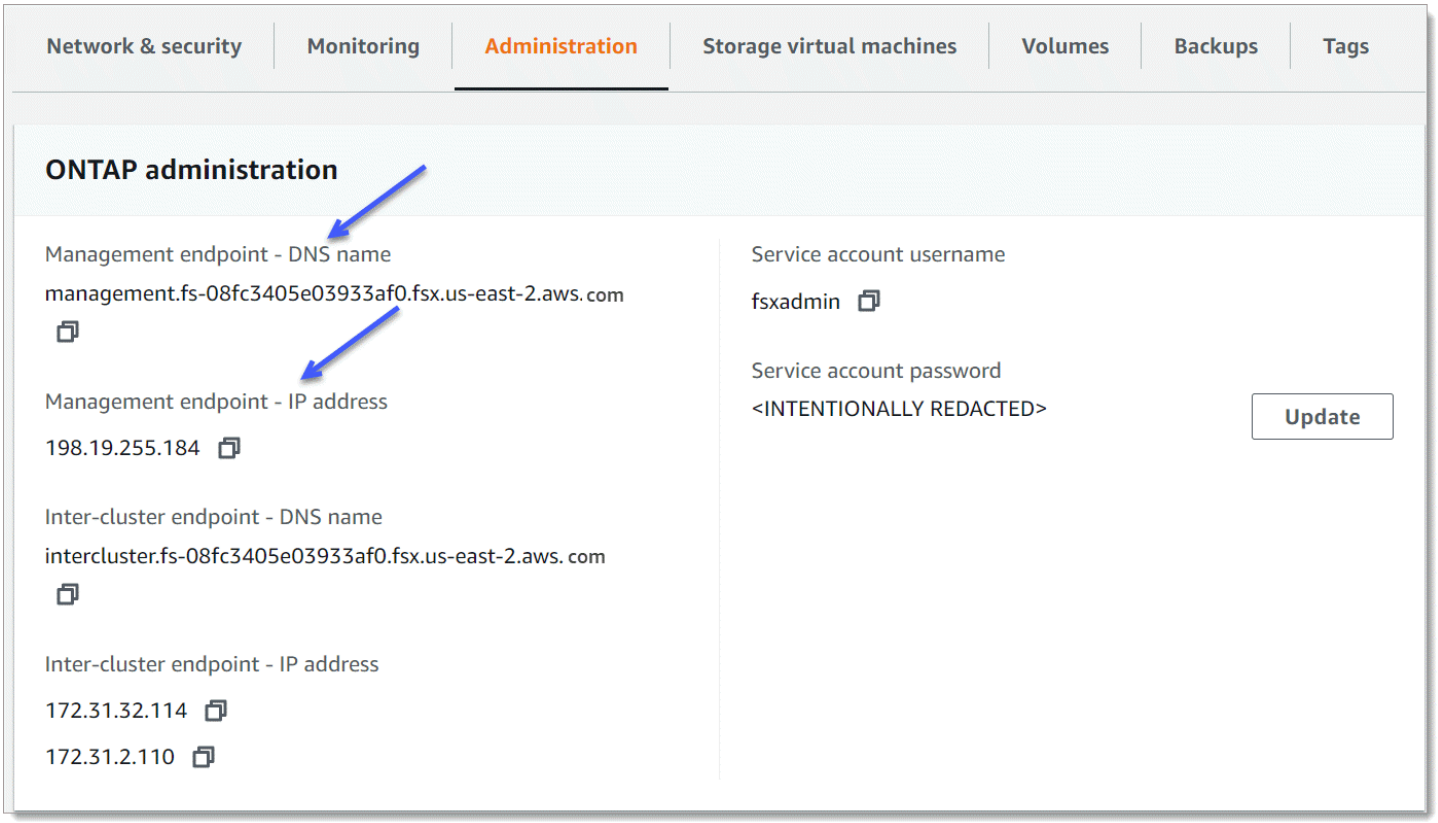
Verwenden der NetApp ONTAP-CLI

Sie können Ihre Amazon FSx for NetApp ONTAP-Ressourcen mit der NetApp ONTAP CLI verwalten. Sie können Ressourcen auf Dateisystemebene (analog zum NetApp ONTAP-Cluster) und auf SVM-Ebene verwalten.

Verwaltung von Dateisystemen mit der ONTAP CLI

Sie können ONTAP CLI-Befehle auf Ihrem FSx for ONTAP-Dateisystem ausführen, analog zur Ausführung auf einem Cluster. NetApp ONTAP Sie greifen auf die ONTAP CLI in Ihrem Dateisystem zu, indem Sie eine Secure Shell (SSH) -Verbindung zum Verwaltungsendpunkt des Dateisystems herstellen und sich mit dem `fsxadmin` Benutzernamen und dem Passwort anmelden. Sie haben die Möglichkeit, das Passwort festzulegen, wenn Sie das Dateisystem mit dem benutzerdefinierten Erstellungsablauf oder mit dem AWS CLI erstellen. Wenn Sie das Dateisystem mit der Option Quick Create erstellt haben, wurde das `fsxadmin` Passwort nicht festgelegt. Sie müssen also eines festlegen, um sich bei der ONTAP CLI anzumelden. Weitere Informationen finden Sie

unter Aktualisierung eines Dateisystems. Sie finden den DNS-Namen und die IP-Adresse des Verwaltungsendpunkts Ihres Dateisystems in der Amazon FSx-Konsole auf der Registerkarte Administration auf der Detailseite des FSx for ONTAP-Dateisystems, wie in der folgenden Grafik dargestellt.



Verwenden Sie den `fsxadmin` Benutzer und das Passwort, um mit SSH eine Verbindung zum Verwaltungsendpunkt des Dateisystems herzustellen. Sie können von einem Client aus, der sich in derselben VPC wie das Dateisystem befindet, per SSH auf die IP-Adresse oder den DNS-Namen des Verwaltungsendpunkts des Dateisystems zugreifen, wie in den folgenden Beispielen gezeigt.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

Der SSH-Befehl mit Beispielwerten:

```
ssh fsxadmin@198.51.100.0
```

Der SSH-Befehl, der den DNS-Namen des Verwaltungsendpunkts verwendet:

```
ssh fsxadmin@file-system-management-endpoint-dns-name
```

Der SSH-Befehl mit einem DNS-Beispielnamen:

```
$ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Umfang der verfügbaren ONTAP CLI-Befehle für **`fsxadmin`**

Die `fsxadmin` Administratoransicht befindet sich auf Dateisystemebene, die alle SVMs und Volumes im Dateisystem umfasst. Die `fsxadmin` Rolle erfüllt die Rolle des ONTAP Clusteradministrators. Da Amazon FSx for NetApp ONTAP-Dateisysteme vollständig verwaltet werden, kann die `fsxadmin` Rolle eine Teilmenge der verfügbaren ONTAP CLI-Befehle ausführen.

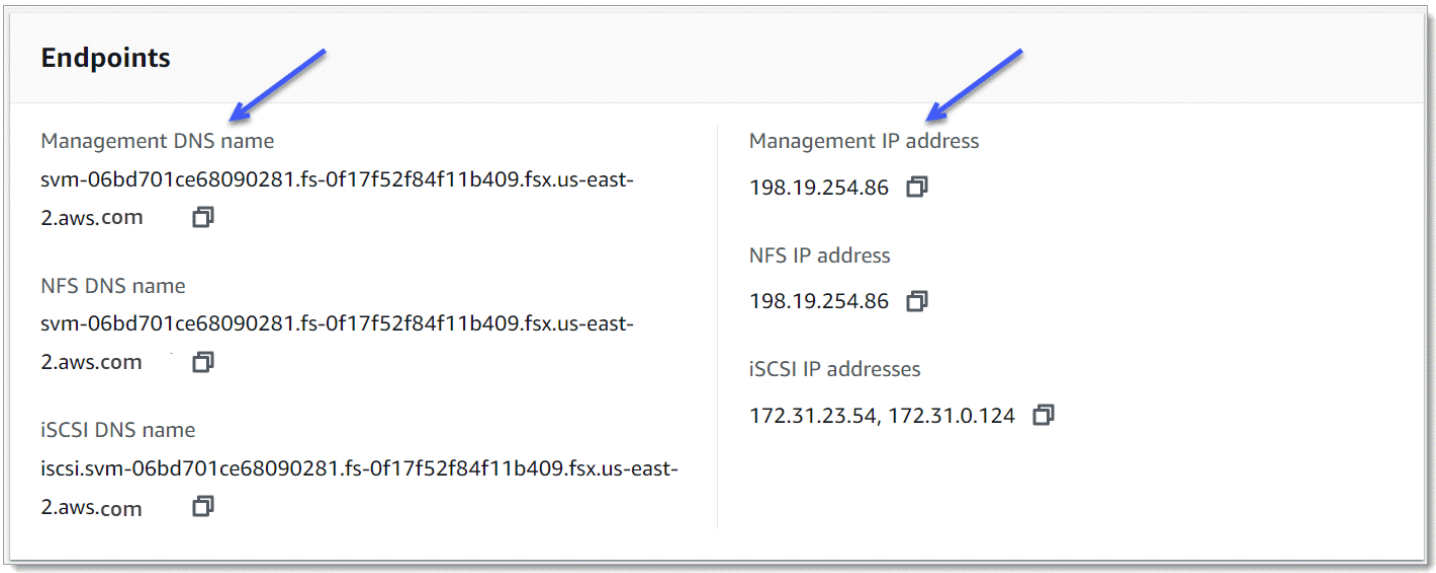
Verwenden Sie den folgenden `security login role show`ONTAPCLI-Befehl, um eine Liste der Befehle anzuzeigen, die ausgeführt werden `fsxadmin` können:

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
           Role          Command/                                    Access
Vserver    Name          Directory                          Query    Level
---------- ------------- --------- ---------------------------------- --------
FsxId0abcdef123456789
           fsxadmin      application                                   all
                         cluster application-record                    all
                         cluster date show                             readonly
                         cluster ha modify                             readonly
                         cluster ha show                               readonly
                         cluster identity modify                       readonly
                         cluster identity show                         readonly
                         cluster log-forwarding           -port !55555 all
                         cluster modify                                readonly
                         cluster peer                                  all
                         cluster show                                  readonly
                         cluster statistics show                       readonly
                         cluster time-service ntp server create        readonly
                         cluster time-service ntp server delete        readonly
                         cluster time-service ntp server modify        readonly
                         cluster time-service ntp server show          readonly
                         debug network tcpdump       -ipspace !Cluster all
                         debug san lun                                 all
                         df         -vserver !FsxId* -vserver !Cluster readonly
                         echo                                          all
```

```
                          event catalog show                              readonly
                          event config                                    all
.
.
.
363 entries were displayed.
```

Verwaltung von SVMs mit der CLI ONTAP

Sie können auf die ONTAP CLI auf Ihrer SVM zugreifen, indem Sie eine Secure Shell (SSH) - Verbindung zum Verwaltungsendpunkt der SVM herstellen, indem Sie entweder den `fsxadmin` oder den `vsadmin` Benutzernamen und das Passwort verwenden. Den DNS-Namen und die IP-Adresse des Verwaltungsendpunkts der SVM finden Sie in der Amazon FSx-Konsole im Bereich Endpoints auf der Detailseite für virtuelle Speichermaschinen, wie in der folgenden Abbildung dargestellt.



Um mit SSH eine Verbindung zum Verwaltungsendpunkt der SVM herzustellen, können Sie entweder den `fsxadmin` Benutzernamen und das Passwort `vsadmin` oder verwenden. Falls Sie bei der Erstellung der SVM kein Passwort für den `vsadmin` Benutzer festgelegt haben, können Sie das `vsadmin` Passwort jederzeit festlegen. Weitere Informationen finden Sie unter Aktualisieren einer virtuellen Speichermaschine. Sie können von einem Client aus, der sich in derselben VPC wie das Dateisystem befindet, per SSH auf die SVM zugreifen, indem Sie die IP-Adresse oder den DNS-Namen des Verwaltungsendpunkts verwenden.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

Der Befehl mit Beispielwerten:

```
ssh vsadmin@198.51.100.10
```

Der SSH-Befehl, der den DNS-Namen des Verwaltungsendpunkts verwendet:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

Der SSH-Befehl mit einem DNS-Beispielnamen:

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Amazon FSx for NetApp ONTAP unterstützt die NetApp ONTAP CLI-Befehle.

Eine vollständige Referenz der NetApp ONTAP CLI-Befehle finden Sie unter ONTAP Commands: Manual Page Reference.

Verwendung der ONTAP REST-API

Wenn Sie über die ONTAP REST-API mit den `fsxadmin` Anmeldeinformationen auf Ihr FSx for ONTAP-Dateisystem zugreifen, gehen Sie wie folgt vor:

- Deaktivieren Sie die TLS-Validierung.

  Oder

- Vertrauen Sie den AWS Zertifizierungsstellen (CAs) — Das Zertifikatspaket für die Zertifizierungsstellen in jeder Region finden Sie unter den folgenden URLs:
  - fsx-aws-certificates*https://.s3.amazonaws.com/bundle- aws-region .pem für die Öffentlichkeit* AWS-Regionen
  - https://fsx-aws-us-gov-certificates.s3. us-gov-west*-1.amazonaws.com/bundle- aws-region .pem für Regionen* AWS GovCloud
  - https://fsx-aws-cn-certificates. s3.cn-north-1.amazonaws.com .cn/bundle- *aws-region* .pem für chinesische Regionen AWS

Eine vollständige Referenz der REST-API-Befehle finden Sie in der NetApp ONTAP REST-API-Online-Referenz. NetApp ONTAP

Sicherheit in Amazon FSx für ONTAP NetApp

Cloud-Sicherheit hat höchste AWS Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon FSx for NetApp ONTAP gelten, finden Sie unter AWS Services in Scope by Compliance Program AWS 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 anwenden können. In den folgenden Themen erfahren Sie, wie Sie Amazon FSx konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Amazon FSx-Ressourcen zu überwachen und zu sichern.

Themen

- Datenschutz in Amazon FSx for NetApp ONTAP
- Identitäts- und Zugriffsmanagement für Amazon FSx for ONTAP NetApp
- AWS verwaltete Richtlinien für Amazon FSx
- Dateisystem-Zugriffskontrolle mit Amazon VPC
- Konformitätsprüfung für Amazon FSx for ONTAP NetApp
- Amazon FSx für NetApp ONTAP und VPC-Schnittstellen-Endpunkte ()AWS PrivateLink
- Resilienz in Amazon FSx für ONTAP NetApp
- Infrastruktursicherheit in Amazon FSx for ONTAP NetApp

- Verwenden Sie NetApp ONTAP Vscan mit FSx für ONTAP
- Rollen und Benutzer in Amazon FSx for ONTAP NetApp

Datenschutz in Amazon FSx for NetApp ONTAP

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz in Amazon FSx for NetApp ONTAP. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen. AWS Cloud Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon FSx oder anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten.

Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung in FSx für ONTAP

Amazon FSx for NetApp ONTAP unterstützt die Verschlüsselung von Daten im Ruhezustand und die Verschlüsselung von Daten während der Übertragung. Die Verschlüsselung von Daten im Ruhezustand wird automatisch aktiviert, wenn ein Amazon FSx-Dateisystem erstellt wird. Amazon FSx for NetApp ONTAP unterstützt Kerberos-basierte Verschlüsselung bei der Übertragung über die Protokolle NFS und SMB, wenn Sie auf Daten in einer Storage Virtual Machine (SVM) zugreifen, die mit einem Active Directory oder einer Domain über das Lightweight Directory Access Protocol (LDAP) verbunden ist.

Verwendung von Verschlüsselung

Wenn Ihr Unternehmen Unternehmens- oder behördlichen Richtlinien unterliegt, die die Verschlüsselung von Daten und Metadaten im Ruhezustand vorschreiben, werden Ihre Daten im Ruhezustand automatisch verschlüsselt. Wir empfehlen Ihnen außerdem, die Verschlüsselung von Daten während der Übertragung zu aktivieren, indem Sie Ihr Dateisystem mithilfe der Verschlüsselung von Daten während der Übertragung einbinden.

Weitere Informationen zur Datenverschlüsselung mit Amazon FSx for NetApp ONTAP finden Sie unter Verschlüsselung gespeicherter Daten und. Verschlüsseln von Daten während der Übertragung

Verschlüsselung gespeicherter Daten

Alle Dateisysteme von Amazon FSx for NetApp ONTAP 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 KMS-Schlüssel, 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. Dieser KMS-Schlüssel kann einer der beiden folgenden Typen sein:

- AWS-verwalteter KMS-Schlüssel — Dies ist der Standard-KMS-Schlüssel, der kostenlos verwendet werden kann.
- Vom Kunden verwalteter KMS-Schlüssel — Dies ist der flexibelste zu verwendende KMS-Schlüssel, da Sie die wichtigsten Richtlinien und Berechtigungen für mehrere Benutzer oder Dienste konfigurieren können. Weitere Informationen zum Erstellen von KMS-Schlüsseln finden Sie unter Creating Keys im AWS Key Management Service Developer Guide.

> **Important**
>
> Amazon FSx akzeptiert nur KMS-Schlüssel mit symmetrischer Verschlüsselung. Sie können keine asymmetrischen KMS-Schlüssel mit Amazon FSx verwenden.

Wenn Sie einen vom Kunden verwalteten KMS-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 KMS-Schlüssel jederzeit wählen, wann Sie den Zugriff auf Ihren KMS-Schlüssel deaktivieren, erneut aktivieren, löschen oder widerrufen möchten. Weitere Informationen finden Sie im Entwicklerhandbuch unter Drehen, Aktivieren AWS KMS keys und Deaktivieren von Schlüsseln.AWS Key Management Service

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. Chiffretext 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 Code AWS KMS key, ohne dass der Klartext der Daten auf der Clientseite offengelegt wird. Die Daten werden zuerst entschlüsselt und dann neu verschlüsselt. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.
- kms: GenerateDataKeyWithoutPlaintext — (Erforderlich) Gibt einen mit einem KMS-Schlüssel verschlüsselten Datenverschlüsselungsschlüssel zurück. Diese Berechtigung ist in der Standardschlüsselrichtlinie unter kms: GenerateDataKey * enthalten.
- kms: CreateGrant — (Erforderlich) Fügt einem Schlüssel einen Zuschuss hinzu, um anzugeben, wer den Schlüssel verwenden kann und unter welchen Bedingungen. Erteilungen sind eine alternative Berechtigungsmethode zu Schlüsselrichtlinien. Weitere Informationen zu Grants finden Sie unter Verwendung von Grants 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 Schlüsselaliase 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.

Verschlüsseln von Daten während der Übertragung

In diesem Thema werden die verschiedenen Optionen erklärt, die für die Verschlüsselung Ihrer Dateidaten während der Übertragung zwischen einem FSx for ONTAP-Dateisystem und verbundenen

Clients verfügbar sind. Es enthält auch Anleitungen, die Ihnen bei der Auswahl der für Ihren Workflow am besten geeigneten Verschlüsselungsmethode helfen sollen.

Alle Daten, die AWS-Regionen über das AWS globale Netzwerk übertragen werden, werden auf der physischen Ebene automatisch verschlüsselt, bevor sie AWS gesicherte Einrichtungen verlassen. Der gesamte Verkehr zwischen Availability Zones ist verschlüsselt. Zusätzliche Verschlüsselungsebenen, einschließlich der in diesem Abschnitt aufgeführten, bieten zusätzlichen Schutz. Weitere Informationen zum AWS Schutz von Daten AWS-Regionen, die zwischen Available Zones und Instances fließen, finden Sie unter Verschlüsselung bei der Übertragung im Amazon Elastic Compute Cloud-Benutzerhandbuch für Linux-Instances.

Amazon FSx for NetApp ONTAP unterstützt die folgenden Methoden zur Verschlüsselung von Daten bei der Übertragung zwischen FSx for ONTAP-Dateisystemen und verbundenen Clients:

- Automatische Nitro-basierte Verschlüsselung für alle unterstützten Protokolle und Clients, die auf unterstützten Amazon EC2 EC2-Linux - und Windows-Instance-Typen ausgeführt werden.
- Kerberos-basierte Verschlüsselung über NFS- und SMB-Protokolle.
- IPSec-basierte Verschlüsselung über NFS-, iSCSI- und SMB-Protokolle

Alle unterstützten Methoden zur Verschlüsselung von Daten während der Übertragung verwenden kryptografische AES-256-Algorithmen nach Industriestandard, die eine sichere Verschlüsselung für Unternehmen bieten.

Themen

- Auswahl einer Methode zur Verschlüsselung von Daten bei der Übertragung
- Verschlüsselung von Daten während der Übertragung mit AWS Nitro System
- Verschlüsselung von Daten während der Übertragung mit Kerberos-basierter Verschlüsselung
- Verschlüsselung von Daten während der Übertragung mit IPSec-Verschlüsselung
- Aktivieren Sie die SMB-Verschlüsselung von Daten bei der Übertragung
- Konfiguration von IPSec mithilfe der PSK-Authentifizierung
- Konfiguration von IPSec mithilfe der Zertifikatsauthentifizierung

Auswahl einer Methode zur Verschlüsselung von Daten bei der Übertragung

Dieser Abschnitt enthält Informationen, anhand derer Sie entscheiden können, welche der unterstützten Verschlüsselungsmethoden bei der Übertragung für Ihren Workflow am besten geeignet

ist. Schauen Sie sich diesen Abschnitt an, wenn Sie sich mit den unterstützten Optionen befassen, die in den folgenden Abschnitten ausführlich beschrieben werden.

Bei der Entscheidung, wie Sie Daten bei der Übertragung zwischen Ihrem FSx for ONTAP-Dateisystem und verbundenen Clients verschlüsseln möchten, sind mehrere Faktoren zu berücksichtigen. Zu diesen Faktoren gehören:

- AWS-Region Das, in dem Ihr FSx for ONTAP-Dateisystem läuft.
- Der Instanztyp, auf dem der Client läuft.
- Der Standort des Clients, der auf Ihr Dateisystem zugreift.
- Anforderungen an die Netzwerkleistung.
- Das Datenprotokoll, das Sie verschlüsseln möchten.
- Wenn Sie Microsoft Active Directory verwenden.

AWS-Region

Die Art und Weise AWS-Region , in der Ihr Dateisystem ausgeführt wird, bestimmt, ob Sie die Amazon Nitro-basierte Verschlüsselung verwenden können oder nicht. Die Verschlüsselung auf Nitrobasis ist in den folgenden Fällen verfügbar: AWS-Regionen

- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Oregon)
- Europa (Irland)

Darüber hinaus ist Nitro-basierte Verschlüsselung für Scale-Out-Dateisysteme im asiatisch-pazifischen Raum (Sydney) verfügbar. AWS-Region

Typ der Client-Instanz

Sie können die Amazon Nitro-basierte Verschlüsselung verwenden, wenn der Client, der auf Ihr Dateisystem zugreift, auf einem der unterstützten Amazon EC2 EC2-Instance-Typen für Mac, Linux oder Windows läuft und Ihr Workflow alle anderen Anforderungen für die Verwendung der Nitro-basierten Verschlüsselung erfüllt. Für die Verwendung der Kerberos- oder IPSec-Verschlüsselung bestehen keine Anforderungen an den Client-Instance-Typ.

Kundenstandort

Der Standort des Clients, der in Bezug auf den Speicherort Ihres Dateisystems auf Daten zugreift, wirkt sich darauf aus, welche Verschlüsselungsmethoden während der Übertragung verwendet

werden können. Sie können jede der unterstützten Verschlüsselungsmethoden verwenden, wenn sich der Client und das Dateisystem in derselben VPC befinden. Das Gleiche gilt, wenn sich der Client und das Dateisystem in Peer-VPCs befinden, sofern der Datenverkehr nicht über ein virtuelles Netzwerkgerät oder einen virtuellen Netzwerkdienst, z. B. ein Transit-Gateway, geleitet wird. Nitrobasierte Verschlüsselung ist keine verfügbare Option, wenn sich der Client nicht in derselben oder einer Peering-VPC befindet oder wenn der Datenverkehr über ein virtuelles Netzwerkgerät oder einen virtuellen Netzwerkdienst geleitet wird.

Netzwerkleistung

Die Verwendung von Amazon Nitro-basierter Verschlüsselung hat keine Auswirkungen auf die Netzwerkleistung. Dies liegt daran, dass die unterstützten Amazon EC2 EC2-Instances die Offload-Funktionen der zugrunde liegenden Nitro System-Hardware nutzen, um den während der Übertragung befindlichen Verkehr zwischen Instances automatisch zu verschlüsseln.

Die Verwendung von Kerberos- oder IPSec-Verschlüsselung wirkt sich auf die Netzwerkleistung aus. Dies liegt daran, dass diese beiden Verschlüsselungsmethoden softwarebasiert sind, was bedeutet, dass der Client und der Server Rechenressourcen verwenden müssen, um den während der Übertragung befindlichen Verkehr zu verschlüsseln und zu entschlüsseln.

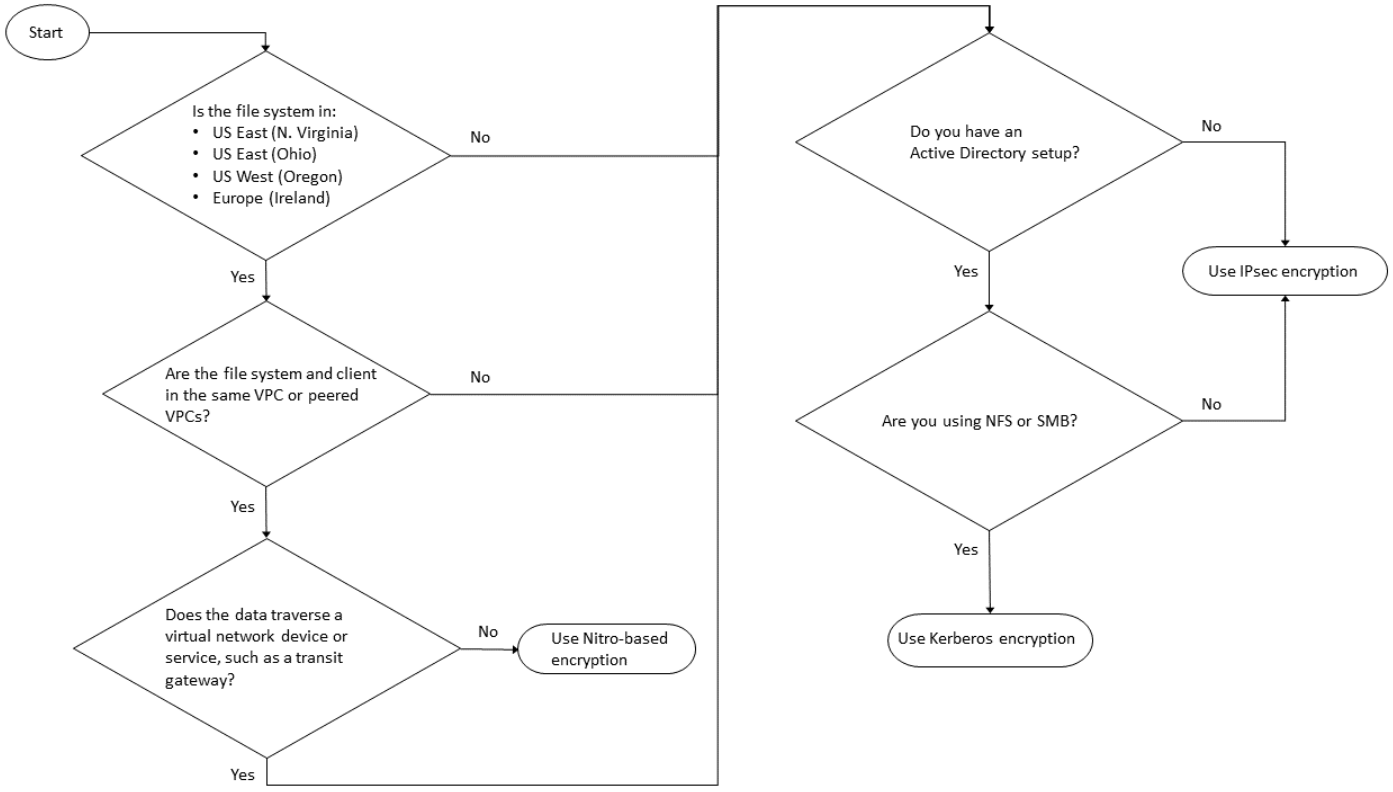
Datenprotokoll

Sie können Amazon Nitro-basierte Verschlüsselung und IPSec-Verschlüsselung mit allen unterstützten Protokollen — NFS, SMB und iSCSI — verwenden. Sie können die Kerberos-Verschlüsselung mit den Protokollen NFS und SMB (mit einem Active Directory) verwenden.

Active Directory

Wenn Sie Microsoft Active Directory verwenden, können Sie die Kerberos-Verschlüsselung über die Protokolle NFS und SMB verwenden.

Verwenden Sie das folgende Diagramm, um zu entscheiden, welche Verschlüsselungsmethode bei der Übertragung verwendet werden soll.



Die IPSec-Verschlüsselung ist die einzige verfügbare Option, wenn alle der folgenden Bedingungen auf Ihren Workflow zutreffen:

- Sie verwenden das NFS-, SMB- oder iSCSI-Protokoll.
- Ihr Workflow unterstützt die Verwendung von Amazon Nitro-basierter Verschlüsselung nicht.
- Sie verwenden keine Microsoft Active Directory-Domäne.

Verschlüsselung von Daten während der Übertragung mit AWS Nitro System

Bei der Nitro-basierten Verschlüsselung werden Daten während der Übertragung automatisch verschlüsselt, wenn Clients, die auf Ihre Dateisysteme zugreifen, auf unterstützten Amazon EC2 EC2-Linux - oder Windows-Instance-Typen ausgeführt werden.

Die Verwendung von Amazon Nitro-basierter Verschlüsselung hat keine Auswirkungen auf die Netzwerkleistung. Dies liegt daran, dass die unterstützten Amazon EC2 EC2-Instances die Offload-Funktionen der zugrunde liegenden Nitro System-Hardware nutzen, um den während der Übertragung befindlichen Verkehr zwischen Instances automatisch zu verschlüsseln.

Die Nitro-basierte Verschlüsselung wird automatisch aktiviert, wenn sich die unterstützten Client-Instance-Typen in derselben AWS-Region und derselben VPC oder in einer VPC befinden, die mit der VPC des Dateisystems über Peering verbunden ist. Wenn sich der Client in einer Peering-VPC befindet, können Daten außerdem kein virtuelles Netzwerkgerät oder einen virtuellen Netzwerkdienst (z. B. ein Transit-Gateway) passieren, sodass die Nitro-basierte Verschlüsselung automatisch aktiviert wird. Weitere Informationen zur Nitro-basierten Verschlüsselung finden Sie im Abschnitt Verschlüsselung bei der Übertragung im Amazon EC2-Benutzerhandbuch für Linux - oder Windows-Instance-Typen.

Nitro-basierte Verschlüsselung bei der Übertragung ist für Dateisysteme verfügbar, die nach dem 28. November 2022 erstellt wurden, und zwar im Folgenden: AWS-Regionen

- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Oregon)
- Europa (Irland)

Darüber hinaus ist Nitro-basierte Verschlüsselung für Scale-Out-Dateisysteme im asiatisch-pazifischen Raum (Sydney) verfügbar. AWS-Region

Weitere Informationen darüber, AWS-Regionen wo FSx for ONTAP erhältlich ist, finden Sie unter Amazon FSx for NetApp ONTAP — Preise.

Weitere Informationen zu den Leistungsspezifikationen für FSx für ONTAP-Dateisysteme finden Sie unter. Auswirkungen der Durchsatzkapazität auf die Leistung

Verschlüsselung von Daten während der Übertragung mit Kerberos-basierter Verschlüsselung

Wenn Sie Microsoft Active Directory verwenden, können Sie die Kerberos-basierte Verschlüsselung über die Protokolle NFS und SMB verwenden, um Daten während der Übertragung für untergeordnete Volumes von SVMs zu verschlüsseln, die mit einem Microsoft Active Directory verbunden sind.

Verschlüsselung von Daten bei der Übertragung über NFS mit Kerberos

Die Verschlüsselung von Daten während der Übertragung mit Kerberos wird für die Protokolle NFSv3 und NFSv4 unterstützt. Informationen zur Aktivierung der Verschlüsselung bei der Übertragung mit

Kerberos für das NFS-Protokoll finden Sie im Documentation Center unter Verwenden von Kerberos mit NFS für hohe Sicherheit. NetApp ONTAP

Verschlüsselung von Daten bei der Übertragung über SMB mithilfe von Kerberos

Die Verschlüsselung von Daten bei der Übertragung über das SMB-Protokoll wird auf Dateifreigaben unterstützt, die einer Recheninstanz zugeordnet sind, die das SMB-Protokoll 3.0 oder neuer unterstützt. Dies umfasst alle Microsoft Windows Versionen von Microsoft Windows Server 2012 und höher sowie Microsoft Windows 8 und höher. Wenn diese Option aktiviert ist, verschlüsselt FSx for ONTAP automatisch Daten während der Übertragung mithilfe der SMB-Verschlüsselung, wenn Sie auf Ihr Dateisystem zugreifen, ohne dass Sie Ihre Anwendungen ändern müssen.

FSx for ONTAP SMB unterstützt 128- und 256-Bit-Verschlüsselung, die durch die Client-Sitzungsanfrage bestimmt wird. Eine Beschreibung der verschiedenen Verschlüsselungsstufen finden Sie im Abschnitt Mindestsicherheitsstufe für die SMB-Serverauthentifizierung festlegen unter SMB mit der CLI verwalten im NetApp ONTAP Documentation Center.

> **Note**
>
> Der Client bestimmt den Verschlüsselungsalgorithmus. Sowohl die NTLM- als auch die Kerberos-Authentifizierung funktionieren sowohl mit 128- als auch mit 256-Bit-Verschlüsselung. Der FSx for ONTAP SMB Server akzeptiert alle standardmäßigen Windows-Client-Anfragen, und die detaillierten Steuerungen werden von Microsoft-Gruppenrichtlinien oder Registrierungseinstellungen übernommen.

Sie verwenden die ONTAP CLI, um die Einstellungen für die Verschlüsselung bei der Übertragung auf SVMs und Volumes von FSx for ONTAP zu verwalten. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf der SVM ein, auf der Sie die Verschlüsselung in den Transiteinstellungen vornehmen, wie unter beschrieben. Verwaltung von SVMs mit der CLI ONTAP

Anweisungen zur Aktivierung der SMB-Verschlüsselung auf einer SVM oder einem Volume finden Sie unter. Aktivieren Sie die SMB-Verschlüsselung von Daten bei der Übertragung

Verschlüsselung von Daten während der Übertragung mit IPSec-Verschlüsselung

FSx for ONTAP unterstützt die Verwendung des IPSec-Protokolls im Transportmodus, um sicherzustellen, dass Daten während der Übertragung kontinuierlich sicher und verschlüsselt sind. IPSec bietet end-to-end Verschlüsselung von Daten während der Übertragung zwischen Clients

und FSx for ONTAP-Dateisystemen für den gesamten unterstützten IP-Verkehr — NFS-, iSCSI- und SMB-Protokolle. Mit der IPSec-Verschlüsselung richten Sie einen IPSec-Tunnel zwischen einer FSx for ONTAP SVM, die mit aktiviertem IPSec konfiguriert ist, und einem IPSec-Client ein, der auf dem verbundenen Client ausgeführt wird und auf die Daten zugreift.

Wir empfehlen Ihnen, IPSec zu verwenden, um Daten während der Übertragung über die Protokolle NFS, SMB und iSCSI zu verschlüsseln, wenn Sie von Clients auf Ihre Daten zugreifen, die keine Nitro-basierte Verschlüsselung unterstützen, und wenn Ihr Client und Ihre SVMs nicht mit einem Active Directory verbunden sind, was für die Kerberos-basierte Verschlüsselung erforderlich ist. IPSec-Verschlüsselung ist die einzige verfügbare Option für die Verschlüsselung von Daten während der Übertragung für iSCSI-Verkehr, wenn Ihr iSCSI-Client keine Nitro-basierte Verschlüsselung unterstützt.

Für die IPSec-Authentifizierung können Sie entweder Pre-Shared Keys (PSKs) oder Zertifikate verwenden. Wenn Sie ein PSK verwenden, muss der von Ihnen verwendete IPSec-Client Internet Key Exchange Version 2 (IKEv2) mit einem PSK unterstützen. Die allgemeinen Schritte zur Konfiguration der IPSec-Verschlüsselung sowohl auf FSx for ONTAP als auch auf dem Client lauten wie folgt:

1. Aktivieren und konfigurieren Sie IPSec auf Ihrem Dateisystem.
2. Installieren und konfigurieren Sie IPSec auf Ihrem Client
3. Konfigurieren Sie IPSec für den Zugriff mehrerer Clients

Weitere Informationen zur Konfiguration von IPSec mit PSK finden Sie im Dokumentationscenter unter IP-Sicherheit (IPSec) über Drahtverschlüsselung konfigurieren. NetApp ONTAP

Weitere Informationen zur Konfiguration von IPSec mithilfe von Zertifikaten finden Sie unter. Konfiguration von IPSec mithilfe der Zertifikatsauthentifizierung

Aktivieren Sie die SMB-Verschlüsselung von Daten bei der Übertragung

Wenn Sie eine SVM erstellen, ist die SMB-Verschlüsselung standardmäßig ausgeschaltet. Sie können entweder die SMB-Verschlüsselung aktivieren, die für einzelne Shares erforderlich ist, oder auf einer SVM, wodurch sie für alle Shares auf dieser SVM aktiviert wird.

> **Note**
>
> Wenn SMB-Verschlüsselung erforderlich auf einer SVM oder Share aktiviert ist, können SMB-Clients, die keine Verschlüsselung unterstützen, keine Verbindung zu dieser SVM oder Share herstellen.

Um SMB-Verschlüsselung für eingehenden SMB-Verkehr auf einer SVM vorzuschreiben

Gehen Sie wie folgt vor, um die SMB-Verschlüsselung auf einer SVM mithilfe der NetApp ONTAP CLI zu verlangen.

1. Um mit SSH eine Verbindung zum SVM-Verwaltungsendpunkt herzustellen, verwenden Sie den Benutzernamen `vsadmin` und das vsadmin-Passwort, das Sie bei der Erstellung der SVM festgelegt haben. Wenn Sie kein vsadmin-Passwort festgelegt haben, verwenden Sie den Benutzernamen und das fsxadmin-Passwort. `fsxadmin` Sie können von einem Client aus, der sich in derselben VPC wie das Dateisystem befindet, per SSH auf die SVM zugreifen, indem Sie die IP-Adresse oder den DNS-Namen des Verwaltungsendpunkts verwenden.

   ```
   ssh vsadmin@svm-management-endpoint-ip-address
   ```

   Der Befehl mit Beispielwerten:

   ```
   ssh vsadmin@198.51.100.10
   ```

   Der SSH-Befehl, der den DNS-Namen des Verwaltungsendpunkts verwendet:

   ```
   ssh vsadmin@svm-management-endpoint-dns-name
   ```

   Der SSH-Befehl unter Verwendung eines Beispiel-DNS-Namens:

   ```
   ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-
   east-2.aws.com
   ```

   ```
   Password: vsadmin-password

   This is your first recorded login.
   FsxIdabcdef01234567892::>
   ```

2. Verwenden Sie den `vserver cifs security modify`NetApp ONTAPCLI-Befehl, um eine SMB-Verschlüsselung für den eingehenden SMB-Verkehr zur SVM vorzuschreiben.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
```

3. Verwenden Sie den folgenden Befehl, um die SMB-Verschlüsselung für eingehenden SMB-Verkehr nicht mehr zu verlangen.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required
 false
```

4. Um die aktuellen `is-smb-encryption-required` Einstellungen auf einer SVM zu sehen, verwenden Sie den `vserver cifs security show`NetApp ONTAPCLI-Befehl:

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

Weitere Informationen zur Verwaltung der SMB-Verschlüsselung auf einer SVM finden Sie im Documentation Center unter Konfiguration der erforderlichen SMB-Verschlüsselung auf SMB-Servern für Datenübertragungen über SMB. NetApp ONTAP

So aktivieren Sie die SMB-Verschlüsselung auf einem Volume

Gehen Sie wie folgt vor, um die SMB-Verschlüsselung auf einem Share mithilfe der NetApp ONTAP CLI zu aktivieren.

1. Stellen Sie eine Secure Shell (SSH) -Verbindung zum Verwaltungsendpunkt der SVM her, wie unter beschrieben. Verwaltung von SVMs mit der CLI ONTAP
2. Verwenden Sie den folgenden NetApp ONTAP CLI-Befehl, um eine neue SMB-Freigabe zu erstellen und für den Zugriff auf diese Freigabe eine SMB-Verschlüsselung vorzuschreiben.

```
vserver cifs share create -vserver vserver_name -share-name share_name -
path share_path -share-properties encrypt-data
```

   Weitere Informationen finden Sie `vserver cifs share create`in den Manpages für NetApp ONTAP CLI Command.

3. Verwenden Sie den folgenden Befehl, um eine SMB-Verschlüsselung für eine bestehende SMB-Freigabe zu verlangen.

```
vserver cifs share properties add -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

   Weitere Informationen finden Sie vserver cifs share createin den Manpages für NetApp ONTAP CLI Command.

4. Verwenden Sie den folgenden Befehl, um die SMB-Verschlüsselung auf einer vorhandenen SMB-Freigabe zu deaktivieren.

```
vserver cifs share properties remove -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

   Weitere Informationen finden Sie vserver cifs share properties removein den Manpages für NetApp ONTAP CLI Command.

5. Verwenden Sie den folgenden NetApp ONTAP CLI-Befehl, um die aktuelle `is-smb-encryption-required` Einstellung auf einer SMB-Freigabe anzuzeigen:

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -
fields share-properties
```

   Wenn eine der vom Befehl zurückgegebenen Eigenschaften die Eigenschaft ist, gibt diese `encrypt-data` Eigenschaft an, dass beim Zugriff auf diese Freigabe SMB-Verschlüsselung verwendet werden muss.

   Weitere Informationen finden Sie vserver cifs share properties showin den Manpages für NetApp ONTAP CLI Command.

Konfiguration von IPSec mithilfe der PSK-Authentifizierung

Wenn Sie PSK für die Authentifizierung verwenden, lauten die Schritte zur Konfiguration der IPSec-Verschlüsselung sowohl auf FSx for ONTAP als auch auf dem Client wie folgt:

1. Aktivieren und konfigurieren Sie IPSec in Ihrem Dateisystem.
2. Installieren und konfigurieren Sie IPSec auf Ihrem Client
3. Konfigurieren Sie IPSec für den Zugriff mehrerer Clients

Einzelheiten zur Konfiguration von IPSec mit PSK finden Sie im Dokumentationscenter unter IP-Sicherheit (IPSec) über Drahtverschlüsselung konfigurieren. NetApp ONTAP

Konfiguration von IPSec mithilfe der Zertifikatsauthentifizierung

Die folgenden Themen enthalten Anweisungen zur Konfiguration der IPSec-Verschlüsselung mithilfe der Zertifikatsauthentifizierung auf einem FSx for ONTAP-Dateisystem und einem Client, auf dem Libreswan IPSec ausgeführt wird. Diese Lösung verwendet AWS Certificate Manager und, um eine private Zertifizierungsstelle AWS Private Certificate Authority zu erstellen und die Zertifikate zu generieren.

Die allgemeinen Schritte zur Konfiguration der IPSec-Verschlüsselung mithilfe der Zertifikatsauthentifizierung auf FSx for ONTAP-Dateisystemen und verbundenen Clients lauten wie folgt:

1. Richten Sie eine Zertifizierungsstelle für die Ausstellung von Zertifikaten ein.
2. Generieren und exportieren Sie CA-Zertifikate für das Dateisystem und den Client.
3. Installieren Sie das Zertifikat und konfigurieren Sie IPSec auf der Client-Instanz.
4. Installieren Sie das Zertifikat und konfigurieren Sie IPSec auf Ihrem Dateisystem.
5. Definieren Sie die Sicherheitsrichtlinien-Datenbank (SPD).
6. Konfigurieren Sie IPSec für den Zugriff mehrerer Clients.

CA-Zertifikate erstellen und installieren

Für die Zertifikatsauthentifizierung müssen Sie Zertifikate von einer Zertifizierungsstelle auf Ihrem FSx for ONTAP-Dateisystem und den Clients, die auf die Daten in Ihrem Dateisystem zugreifen, generieren und installieren. Im folgenden Beispiel wird AWS Private Certificate Authority eine private Zertifizierungsstelle eingerichtet und die Zertifikate für die Installation im Dateisystem und auf dem Client generiert. Mit dieser AWS Private Certificate Authority Methode können Sie eine vollständig AWS gehostete Hierarchie von Stamm- und untergeordneten Zertifizierungsstellen (CAs) für den internen Gebrauch in Ihrer Organisation erstellen. Dieser Prozess besteht aus fünf Schritten:

1. Erstellen Sie eine private Zertifizierungsstelle (CA) mit AWS Private CA
2. Stellen Sie das Stammzertifikat auf der privaten CA aus und installieren Sie es
3. Fordern Sie ein privates Zertifikat AWS Certificate Manager für Ihr Dateisystem und Ihre Clients an
4. Exportieren Sie das Zertifikat für das Dateisystem und die Clients.

Weitere Informationen finden Sie unter Private CA-Administration im AWS Private Certificate Authority Benutzerhandbuch.

Um die private Root-CA zu erstellen

1. Wenn Sie eine Zertifizierungsstelle erstellen, müssen Sie die CA-Konfiguration in einer von Ihnen bereitgestellten Datei angeben. Der folgende Befehl verwendet den Nano-Texteditor, um die `ca_config.txt` Datei zu erstellen, in der die folgenden Informationen angegeben sind:

   - Den Namen des Algorithmus
   - Der Signaturalgorithmus, den die CA zum Signieren verwendet
   - X.500-Themeninformationen

   ```
   $ > nano ca_config.txt
   ```

   Der Texteditor wird angezeigt.
2. Bearbeiten Sie die Datei mit den Spezifikationen für Ihre CA.

   ```
   {
      "KeyAlgorithm":"RSA_2048",
      "SigningAlgorithm":"SHA256WITHRSA",
      "Subject":{
         "Country":"US",
         "Organization":"Example Corp",
         "OrganizationalUnit":"Sales",
         "State":"WA",
         "Locality":"Seattle",
         "CommonName":"*.ec2.internal"
      }
   }
   ```
3. Speichern und schließen Sie die Datei und beenden Sie den Texteditor. Weitere Informationen finden Sie im AWS Private Certificate Authority Benutzerhandbuch unter Verfahren zum Erstellen einer Zertifizierungsstelle.
4. Verwenden Sie den create-certificate-authority AWS Private CA CLI-Befehl, um eine private CA zu erstellen.

   ```
   ~/home > aws acm-pca create-certificate-authority \
        --certificate-authority-configuration file://ca_config.txt \
   ```

```
    --certificate-authority-type "ROOT" \
    --idempotency-token 01234567 --region aws-region
```

Bei Erfolg gibt dieser Befehl den Amazon-Ressourcennamen (ARN) der CA aus.

```
{
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Um ein Zertifikat für Ihre private Root-CA (AWS CLI) zu erstellen und zu installieren

1. Generieren Sie mit dem [get-certificate-authority-csr](#) AWS CLI-Befehl eine Certificate Signing Request (CSR).

```
$ aws acm-pca get-certificate-authority-csr \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --output text \
    --endpoint https://acm-pca.aws-region.amazonaws.com \
    --region eu-west-1 > ca.csr
```

Die resultierende Datei`ca.csr`, eine im Base64-Format codierte PEM-Datei, hat das folgende Aussehen.

```
-----BEGIN CERTIFICATE-----
 MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
 VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
 BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
 MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
 VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
 b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
 YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
 rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
 Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
 FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
 NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
```

```
-----END CERTIFICATE-----
```

Weitere Informationen finden Sie im Benutzerhandbuch unter Installation eines Root-CA-Zertifikats. AWS Private Certificate Authority

2. Verwenden Sie den `issue-certificate` AWS CLI Befehl, um das Root-Zertifikat auszustellen und auf Ihrer privaten CA zu installieren.

```
$ aws acm-pca issue-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --csr file://ca.csr \
     --signing-algorithm SHA256WITHRSA \
     --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
     --validity Value=3650,Type=DAYS --region aws-region
```

3. Laden Sie das Stammzertifikat mit dem `get-certificate` AWS CLI Befehl herunter.

```
$ aws acm-pca get-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
    --output text --region aws-region > rootCA.pem
```

4. Installieren Sie das Stammzertifikat mit dem `import-certificate-authority-certificate` AWS CLI Befehl auf Ihrer privaten CA.

```
$ aws acm-pca import-certificate-authority-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --certificate file://rootCA.pem --region aws-region
```

Generieren und exportieren Sie das Dateisystem und das Client-Zertifikat

1. Verwenden Sie den `request-certificate` AWS CLI Befehl, um ein AWS Certificate Manager Zertifikat für Ihr Dateisystem und Ihre Clients anzufordern.

```
$ aws acm request-certificate \
    --domain-name *.ec2.internal \
```

```
    --idempotency-token 12345 \
    --region aws-region \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

Wenn die Anfrage erfolgreich ist, wird der ARN des ausgestellten Zertifikats zurückgegeben.

2. Aus Sicherheitsgründen müssen Sie dem privaten Schlüssel beim Exportieren eine Passphrase zuweisen. Erstellen Sie eine Passphrase und speichern Sie sie in einer Datei mit dem Namen `passphrase.txt`
3. Verwenden Sie den `export-certificate` AWS CLI Befehl, um das zuvor ausgestellte private Zertifikat zu exportieren. Die exportierte Datei enthält das Zertifikat, die Zertifikatskette und den verschlüsselten privaten 2048-Bit-RSA-Schlüssel, der dem öffentlichen Schlüssel zugeordnet ist, der in das Zertifikat eingebettet ist. Aus Sicherheitsgründen müssen Sie dem privaten Schlüssel beim Exportieren eine Passphrase zuweisen. Das folgende Beispiel bezieht sich auf eine Linux EC2-Instance.

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
     --passphrase $(cat passphrase.txt | base64)) --region aws-region >
 exported_cert.json
```

4. Verwenden Sie die folgenden `jq` Befehle, um den privaten Schlüssel und das Zertifikat aus der JSON-Antwort zu extrahieren.

```
$ cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

5. Verwenden Sie den folgenden `openssl` Befehl, um den privaten Schlüssel aus der JSON-Antwort zu entschlüsseln. Nach Eingabe des Befehls werden Sie zur Eingabe der Passphrase aufgefordert.

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

Installation und Konfiguration von Libreswan IPSec auf einem Amazon Linux 2-Client

Die folgenden Abschnitte enthalten Anweisungen zur Installation und Konfiguration von Libreswan IPSec auf einer Amazon EC2 EC2-Instance, auf der Amazon Linux 2 ausgeführt wird.

Um Libreswan zu installieren und zu konfigurieren

1. Stellen Sie über SSH eine Connect zu Ihrer EC2-Instance her. Spezifische Anweisungen dazu finden Sie unter Herstellen einer Connect zu Ihrer Linux-Instance mithilfe eines SSH-Clients im Amazon Elastic Compute Cloud-Benutzerhandbuch für Linux-Instances.
2. Führen Sie zur Installation `libreswan` den folgenden Befehl aus:

   ```
   $ sudo yum install libreswan
   ```

3. (Optional) Bei der Überprüfung von IPSec in einem späteren Schritt werden diese Eigenschaften möglicherweise ohne diese Einstellungen gekennzeichnet. Wir empfehlen, Ihr Setup zunächst ohne diese Einstellungen zu testen. Wenn bei Ihrer Verbindung Probleme auftreten, kehren Sie zu diesem Schritt zurück und nehmen Sie die folgenden Änderungen vor.

   Verwenden Sie nach Abschluss der Installation Ihren bevorzugten Texteditor, um der `/etc/sysctl.conf` Datei die folgenden Einträge hinzuzufügen.

   ```
   net.ipv4.ip_forward=1
   net.ipv4.conf.all.accept_redirects = 0
   net.ipv4.conf.all.secure_redirects = 0
   net.ipv4.conf.all.send_redirects = 0
   net.ipv4.conf.default.accept_redirects = 0
   net.ipv4.conf.default.send_redirects = 0
   net.ipv4.conf.lo.accept_redirects = 0
   net.ipv4.conf.lo.send_redirects = 0
   net.ipv4.conf.all.rp_filter = 0
   net.ipv4.conf.default.rp_filter = 0
   net.ipv4.conf.eth0.rp_filter = 0
   ```

   Speichern Sie die Änderungen und beenden Sie den Texteditor.
4. Übernehmen Sie die Änderungen.

   ```
   $ sudo sysctl -p
   ```

5. Überprüfen Sie die IPSec-Konfiguration.

```
$ sudo ipsec verify
```

Stellen Sie sicher, dass die Version von `Libreswan` Ihnen installiert ist, läuft.

6. Initialisieren Sie die IPSec-NSS-Datenbank.

```
$ sudo ipsec checknss
```

Um das Zertifikat auf dem Client zu installieren

1. Kopieren Sie das Zertifikat, das Sie für den Client generiert haben, in das Arbeitsverzeichnis auf der EC2-Instance. Sie
2. Exportieren Sie das zuvor generierte Zertifikat in ein Format, das mit `libreswan` kompatibel ist.

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \
    -certfile rootCA.pem -out certkey.p12 -name fsx
```

3. Importieren Sie den neu formatierten Schlüssel und geben Sie die Passphrase an, wenn Sie dazu aufgefordert werden.

```
$ sudo ipsec import certkey.p12
```

4. Erstellen Sie mit dem bevorzugten Texteditor eine IPSec-Konfigurationsdatei.

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

Fügen Sie der Konfigurationsdatei die folgenden Einträge hinzu:

```
conn fsxn
    authby=rsasig
    left=172.31.77.6
    right=198.19.254.13
    auto=start
    type=transport
    ikev2=insist
    keyexchange=ike
    ike=aes256-sha2_384;dh20
    esp=aes_gcm_c256
    leftcert=fsx
```

```
    leftrsasigkey=%cert
    leftid=%fromcert
    rightid=%fromcert
    rightrsasigkey=%cert
```

Sie starten IPSec auf dem Client, nachdem Sie IPSec auf Ihrem Dateisystem konfiguriert haben.

Konfiguration von IPSec auf Ihrem Dateisystem

Dieser Abschnitt enthält Anweisungen zur Installation des Zertifikats auf Ihrem FSx for ONTAP-Dateisystem und zur Konfiguration von IPSec.

Um das Zertifikat auf Ihrem Dateisystem zu installieren

1. Kopieren Sie das Stammzertifikat ()`rootCA.pem`), das Client-Zertifikat (`cert.pem`) und die entschlüsselten Schlüsseldateien (`decrypted.key`) in Ihr Dateisystem. Sie müssen die Passphrase für das Zertifikat kennen.
2. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.
3. Verwenden Sie es cat auf einem Client (nicht in Ihrem Dateisystem), um den Inhalt der `decrypted.key` Dateien aufzulisten`rootCA.pem`, `cert.pem` sodass Sie die Ausgabe jeder Datei kopieren und einfügen können, wenn Sie in den folgenden Schritten dazu aufgefordert werden.

   ```
   $ > cat cert.pem
   ```

   Kopieren Sie den Inhalt des Zertifikats.
4. Sie müssen alle CA-Zertifikate, die während der gegenseitigen Authentifizierung verwendet wurden, einschließlich der lokalen und der clientseitigen Zertifizierungsstellen, in der ONTAP Zertifikatsverwaltung installieren, sofern sie nicht bereits installiert ist (wie es bei einer selbstsignierten ONTAP-Root-CA der Fall ist).

Verwenden Sie den `security certificate install` NetApp CLI-Befehl wie folgt, um das Client-Zertifikat zu installieren:

```
FSxID123:: > security certificate install -vserver dr -type client -cert-name
 ipsec-client-cert
```

```
Please enter Certificate: Press <Enter> when done
```

Fügen Sie den Inhalt der `cert.pem` Datei ein, die Sie zuvor kopiert haben, und drücken Sie die Eingabetaste.

```
Please enter Private Key: Press <Enter> when done
```

Fügen Sie den Inhalt der `decrypted.key` Datei ein und drücken Sie die Eingabetaste.

```
Do you want to continue entering root and/or intermediate certificates {y|n}:
```

Geben Sie n die Eingabetaste ein, um die Eingabe des Client-Zertifikats abzuschließen.

5. Erstellen und installieren Sie ein Zertifikat zur Verwendung durch die SVM. Die ausstellende Zertifizierungsstelle dieses Zertifikats muss bereits in IPSec installiert ONTAP und zu IPSec hinzugefügt worden sein.

   Verwenden Sie den folgenden Befehl, um das Stammzertifikat zu installieren.

   ```
   FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
    ipsec-ca-cert
   ```

   ```
   Please enter Certificate: Press <Enter> when done
   ```

   Fügen Sie den Inhalt der `rootCA.pem` Datei ein und drücken Sie die Eingabetaste.

6. Um sicherzustellen, dass sich die installierte Zertifizierungsstelle während der Authentifizierung innerhalb des IPSec-CA-Suchpfads befindet, fügen Sie die ONTAP Zertifizierungsstellen für die Zertifikatsverwaltung mithilfe des Befehls „security ipsec ca-certificate add“ zum IPSec-Modul hinzu.

   Geben Sie den folgenden Befehl ein, um das Stammzertifikat hinzuzufügen.

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. Geben Sie den folgenden Befehl ein, um die erforderliche IPSec-Richtlinie in der Security Policy Database (SPD) zu erstellen.

```
security ipsec policy create -vserver dr -name policy-name -local-ip-
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
 ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
 "CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. Verwenden Sie den folgenden Befehl, um die IPSec-Richtlinie für das Dateisystem zur Bestätigung anzuzeigen.

```
FSxID123:: > security ipsec policy show -vserver dr -instance

                                 Vserver: dr
                             Policy Name: promise
                          Local IP Subnets: 198.19.254.13/32
                         Remote IP Subnets: 172.31.0.0/16
                               Local Ports: 0-0
                              Remote Ports: 0-0
                                 Protocols: any
                                    Action: ESP_TRA
                              Cipher Suite: SUITEB_GCM256
          IKE Security Association Lifetime: 86400
        IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
                         Is Policy Enabled: true
                            Local Identity: CN=*.ec2.internal
                           Remote Identity: CN=*.ec2.internal
                    Authentication Method: PKI
             Certificate for Local Identity: ipsec-client-cert
```

Starten Sie IPSec auf dem Client

Jetzt ist IPSec sowohl auf dem FSx for ONTAP-Dateisystem als auch auf dem Client konfiguriert. Sie können IPSec auf dem Client starten.

1. Stellen Sie über SSH eine Connect zu Ihrem Clientsystem her.
2. Starten Sie IPSec.

```
$ sudo ipsec start
```

3. Überprüfen Sie den Status von IPSec.

```
$ sudo ipsec status
```

4. Hängen Sie ein Volume in Ihr Dateisystem ein.

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. Überprüfen Sie das IPSec-Setup, indem Sie die verschlüsselte Verbindung auf Ihrem FSx for ONTAP-Dateisystem anzeigen.

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ---------------- -----------
dr          policy-name
                   198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                   198.19.254.38   172.31.65.193   4fd3f22c993e60c5 ESTABLISHED
2 entries were displayed.
```

IPSec für mehrere Clients einrichten

Wenn eine kleine Anzahl von Clients IPSec nutzen muss, ist die Verwendung eines einzigen SPD-Eintrags für jeden Client ausreichend. Wenn jedoch Hunderte oder sogar Tausende von Clients IPSec nutzen müssen, empfehlen wir, die IPSec-Konfiguration für mehrere Clients zu verwenden.

FSx for ONTAP unterstützt die Verbindung mehrerer Clients in vielen Netzwerken mit einer einzigen SVM-IP-Adresse mit aktiviertem IPSec. Sie können dies entweder mithilfe der `subnet` Konfiguration oder der Konfiguration erreichen, die `Allow all clients` in den folgenden Verfahren erläutert werden:

So konfigurieren Sie IPSec für mehrere Clients mithilfe einer Subnetzkonfiguration

Damit alle Clients in einem bestimmten Subnetz (z. B. 192.168.134.0/24) über einen einzigen SPD-Richtlinieneintrag eine Verbindung zu einer einzigen SVM-IP-Adresse herstellen können, müssen Sie

das im Subnetzformat angeben. `remote-ip-subnets` Darüber hinaus müssen Sie das Feld mit der `remote-identity` richtigen clientseitigen Identität angeben.

> **Important**
>
> Bei Verwendung der Zertifikatsauthentifizierung kann jeder Client entweder sein eigenes eindeutiges Zertifikat oder ein gemeinsames Zertifikat zur Authentifizierung verwenden. FSx for ONTAP IPSec überprüft die Gültigkeit des Zertifikats anhand der CAs, die in seinem lokalen Trust Store installiert sind. FSx for ONTAP unterstützt auch die Überprüfung von Zertifikatssperrlisten (CRL).

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Verwenden Sie den `security ipsec policy create` NetApp ONTAP CLI-Befehl wie folgt und ersetzen Sie die *`Beispielwerte`* durch Ihre spezifischen Werte.

   ```
   FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
     -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
     -local-ports 2049 -protocols tcp -auth-method PSK \
     -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
     -remote-identity client_side_identity
   ```

So konfigurieren Sie IPSec für mehrere Clients mithilfe der Konfiguration „Alle Clients zulassen“

Damit jeder Client unabhängig von seiner Quell-IP-Adresse eine Verbindung zu der IPsec-fähigen IP-Adresse der SVM herstellen kann, verwenden Sie bei der Angabe des Felds den `0.0.0.0/0` Platzhalter. `remote-ip-subnets`

Darüber hinaus müssen Sie das `remote-identity` Feld mit der richtigen clientseitigen Identität angeben. Für die Zertifikatsauthentifizierung können Sie Folgendes eingeben`ANYTHING`.

Wenn der Platzhalter 0.0.0.0/0 verwendet wird, müssen Sie außerdem eine bestimmte lokale oder Remote-Portnummer konfigurieren, die verwendet werden soll. Zum Beispiel NFS-Port 2049.

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Verwenden Sie den `security ipsec policy create` NetApp ONTAP CLI-Befehl wie folgt und ersetzen Sie die *`Beispielwerte`* durch Ihre spezifischen Werte.

   ```
   FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
     -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
     -local-ports 2049 -protocols tcp -auth-method PSK \
     -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
     -local-ports 2049 -remote-identity client_side_identity
   ```

Identitäts- und Zugriffsmanagement für Amazon FSx for ONTAP NetApp

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon FSx-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So funktioniert Amazon FSx for NetApp ONTAP mit IAM

- Beispiele für identitätsbasierte Richtlinien für Amazon FSx for ONTAP NetApp
- Fehlerbehebung bei Amazon FSx for NetApp ONTAP Identity and Access
- Verwenden von Tags mit Amazon FSx
- Verwenden von serviceverknüpften Rollen für Amazon FSx

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Amazon FSx ausführen.

Servicebenutzer — Wenn Sie den Amazon FSx-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Amazon FSx-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf eine Funktion in Amazon FSx nicht zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei Amazon FSx for NetApp ONTAP Identity and Access.

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Amazon FSx-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon FSx. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Amazon FSx Ihre Servicebenutzer 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 darüber, wie Ihr Unternehmen IAM mit Amazon FSx verwenden kann, finden Sie unter. So funktioniert Amazon FSx for NetApp ONTAP mit IAM

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon FSx zu verwalten. Beispiele für identitätsbasierte Amazon FSx-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon FSx for ONTAP NetApp

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, 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 einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, 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

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf 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 Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten 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 innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. 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 innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. 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 Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (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 auszuführen AWS, gelten Sie als Principal. Bei einigen Services können Sie Aktionen ausführen, 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 Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. 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 API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt 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 kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden 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 mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff 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 von der AWS Management Console AWS CLI, der 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 System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. 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, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete 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 Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte 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. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. 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. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Amazon FSx for NetApp ONTAP mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon FSx zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für Amazon FSx verfügbar sind.

IAM-Funktionen, die Sie mit Amazon FSx for ONTAP verwenden können NetApp

IAM-Feature	Amazon FSx-Unterstützung
Identitätsbasierte Richtlinien	Ja

IAM-Feature	Amazon FSx-Unterstützung
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Amazon FSx und andere AWS Services mit den meisten IAM-Funktionen funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Services, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für Amazon 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 Amazon FSx

Beispiele für identitätsbasierte Richtlinien von Amazon FSx finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon FSx for ONTAP NetApp

Ressourcenbasierte Richtlinien innerhalb von Amazon FSx

Unterstützt ressourcenbasierte Richtlinien	Nein

Politische Maßnahmen für Amazon FSx

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff 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 der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation 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 Amazon FSx-Aktionen finden Sie unter Von Amazon FSx definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen in Amazon 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 Richtlinien von Amazon FSx finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon FSx for ONTAP NetApp

Richtlinienressourcen für Amazon FSx

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff 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 Amazon FSx-Ressourcentypen und ihrer ARNs finden Sie unter Von Amazon FSx definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen

Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon FSx definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von Amazon FSx finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon FSx for ONTAP NetApp

Schlüssel für Richtlinienbedingungen für Amazon FSx

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff 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 Bedingungsschlüssel 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 Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Amazon FSx-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon FSx in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit

denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon FSx definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von Amazon FSx finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon FSx for ONTAP NetApp

Zugriffskontrolllisten (ACLs) in Amazon FSx

Unterstützt ACLs	Nein

Attributbasierte Zugriffskontrolle (ABAC) mit Amazon FSx

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden diese AWS Attribute Tags genannt. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. 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 Bedingungselement 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.

Weitere Informationen zum Taggen von Amazon FSx-Ressourcen finden Sie unter. Markieren Sie Ihre Amazon FSx-Ressourcen mit Tags

Ein Beispiel für eine identitätsbasierte Richtlinie zur Einschränkung des Zugriffs auf eine Ressource auf der Grundlage der Markierungen dieser Ressource finden Sie unter Verwenden von Tags zur Steuerung des Zugriffs auf Ihre Amazon FSx-Ressourcen.

Temporäre Anmeldeinformationen mit Amazon FSx verwenden

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. 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.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Zugriffssitzungen für Amazon FSx weiterleiten

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services können Sie Aktionen ausführen, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste

AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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 Amazon FSx

Unterstützt Servicerollen	Nein

Servicebezogene Rollen für Amazon FSx

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten 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 ONTAP NetApp

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Amazon FSx-Ressourcen zu erstellen oder zu ändern. 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 den von Amazon FSx definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FSx in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Amazon 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 diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu 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 speziell auf Ihre Anwendungsfälle zugeschnitten 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 Serviceaktionen zu gewähren, wenn

diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. 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 Richtlinienvalidierung 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 System 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 Amazon FSx-Konsole

Um auf die Amazon FSx for NetApp ONTAP-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon FSx-Ressourcen in Ihrem AWS-Konto aufzulisten und anzuzeigen. 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.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. 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 Amazon FSx-Konsole verwenden können, fügen Sie den Entitäten auch die `AmazonFSxConsoleReadOnlyAccess` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Sie können die `AmazonFSxConsoleReadOnlyAccess` und andere Amazon FSx Managed Service-Richtlinien unter einsehen. AWS verwaltete Richtlinien für Amazon FSx

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 beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI API oder. AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Fehlerbehebung bei Amazon FSx for NetApp ONTAP Identity and Access

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon FSx und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Amazon FSx durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon FSx-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in Amazon FSx durchzuführen

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 berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon FSx übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene 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 von mir den Zugriff AWS-Konto auf meine Amazon FSx-Ressourcen ermöglichen

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 darüber, ob Amazon FSx diese Funktionen unterstützt, finden Sie unterSo funktioniert Amazon FSx for NetApp ONTAP mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- 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 kontrollieren und die attributebasierte Zugriffskontrolle (ABAC) zu implementieren. Um während der Erstellung Tags auf Amazon FSx-Ressourcen anzuwenden, müssen Benutzer über bestimmte AWS Identity and Access Management (IAM-) Berechtigungen verfügen.

Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung

Bei einigen ressourcenschaffenden Amazon FSx-API-Aktionen können Sie Tags angeben, wenn Sie die Ressource erstellen. Sie können diese Ressourcen-Tags verwenden, um die attributebasierte Zugriffskontrolle (ABAC) zu implementieren. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

Damit Benutzer Ressourcen bei der Erstellung taggen können, müssen sie über die Berechtigung verfügen, die Aktion zu verwenden, mit der die Ressource erstellt wird, z. B. `fsx:CreateFileSystem`fsx:CreateStorageVirtualMachine, oder`fsx:CreateVolume`. Wenn bei der Aktion zur Erstellung von Ressourcen Tags angegeben werden, führt IAM eine zusätzliche Autorisierung für die `fsx:TagResource` Aktion durch, um zu überprüfen, ob Benutzer berechtigt sind, Tags zu erstellen. Daher benötigen die Benutzer außerdem die expliziten Berechtigungen zum Verwenden der `fsx:TagResource`-Aktion.

Die folgende Beispielrichtlinie ermöglicht es Benutzern, Dateisysteme und virtuelle Speichermaschinen (SVMs) zu erstellen und ihnen während der Erstellung in einem bestimmten Bereich Tags zuzuweisen. AWS-Konto

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:CreateStorageVirtualMachine",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*",
         "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
```

```
  ]
}
```

In ähnlicher Weise ermöglicht die folgende Richtlinie Benutzern, Backups auf einem bestimmten Dateisystem zu erstellen und während der Backup-Erstellung beliebige Tags auf die Sicherung anzuwenden.

```
{
  "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 während der Aktion zur Erstellung der Ressource Tags angewendet werden. Daher benötigt ein Benutzer, der berechtigt ist, eine Ressource zu erstellen (vorausgesetzt, es gibt keine Tagging-Bedingungen), keine Erlaubnis, die `fsx:TagResource` Aktion zu verwenden, wenn in der Anforderung keine Tags angegeben sind. 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 Taggen von Amazon FSx-Ressourcen finden Sie unter. Markieren Sie Ihre Amazon FSx-Ressourcen mit Tags Weitere Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf Amazon FSx-Ressourcen finden Sie unterVerwenden 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 kontrollieren, können Sie IAM-Richtlinien verwenden, die auf Tags basieren. Sie können diese Kontrolle auf zwei Arten ausüben:

- Sie können den Zugriff auf Amazon FSx-Ressourcen anhand der Tags auf diesen Ressourcen steuern.
- Sie können steuern, welche Tags in einer IAM-Anforderungsbedingung übergeben werden können.

Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf AWS Ressourcen finden Sie unter Steuern des Zugriffs mithilfe von Tags im IAM-Benutzerhandbuch. Weitere Informationen zum Taggen 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 Sie Ihre Amazon FSx-Ressourcen mit Tags.

Bestimmung des Zugriffs auf Ressourcen basierend auf Tags

Um zu kontrollieren, welche Aktionen ein Benutzer oder eine Rolle auf einer 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 Beispielrichtlinie — Erstellen Sie ein Dateisystem nur, wenn ein bestimmtes Tag verwendet wird

Diese Richtlinie ermöglicht es dem Benutzer, ein Dateisystem nur dann zu erstellen, wenn er es mit einem bestimmten Tag-Schlüssel-Wert-Paar kennzeichnet, 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 Beispielrichtlinie — Nur Backups von Amazon FSx für NetApp ONTAP-Volumes mit einem bestimmten Tag erstellen

Diese Richtlinie ermöglicht es Benutzern, nur Backups von FSx for ONTAP-Volumes zu erstellen, die mit dem Schlüssel-Wert-Paar gekennzeichnet sind. `key=Department` `value=Finance` 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:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example Beispielrichtlinie — Erstellen Sie ein Volume mit einem bestimmten Tag aus Backups mit einem bestimmten Tag

Diese Richtlinie ermöglicht es Benutzern, Volumes, die mit gekennzeichnet sind, `Department=Finance` nur aus Backups zu erstellen, die mit gekennzeichnet sind`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Beispielrichtlinie — Dateisysteme mit bestimmten Tags löschen

Diese Richtlinie ermöglicht es einem Benutzer, nur Dateisysteme zu löschen, die mit gekennzeichnet sind`Department=Finance`. Wenn sie ein letztes Backup erstellen, muss es mit gekennzeichnet 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"
                }
            }
        }
    ]
}
```

Example Beispielrichtlinie — Löschen Sie ein Volume mit bestimmten Tags

Diese Richtlinie ermöglicht es einem Benutzer, nur Volumes zu löschen, die mit gekennzeichnet sind`Department=Finance`. Wenn sie ein letztes Backup erstellen, muss es mit gekennzeichnet werden`Department=Finance`.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Verwenden von serviceverknüpften Rollen für Amazon FSx

Amazon FSx verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon FSx verknüpft ist. Servicebezogene Rollen sind von Amazon FSx vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon FSx, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon FSx definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur Amazon FSx seine 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 Zugriffsberechtigung für 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.

Servicebezogene Rollenberechtigungen für Amazon FSx

Amazon FSx verwendet die serviceverknüpfte Rolle mit dem Namen AWSServiceRoleForAmazonFSx—, die bestimmte Aktionen in Ihrem Konto ausführt, z. B. das Erstellen von Elastic Network Interfaces für Ihre Dateisysteme in Ihrer VPC und das Veröffentlichen von Dateisystem- und Volume-Metriken in. CloudWatch

Aktualisierungen dieser Richtlinie finden Sie unter AmazonF SxServiceRolePolicy

Details zu Berechtigungen

Details zu Berechtigungen

Die AWSServiceRoleForAmazonFSx Rollenberechtigungen werden durch die von AmazonF SxServiceRolePolicy AWS verwaltete Richtlinie definiert. Der AWSServiceRoleForAmazonFSx hat die folgenden Berechtigungen:

> **Note**
>
> Das AWSServiceRoleForAmazonFSx wird von allen Amazon FSx-Dateisystemtypen verwendet; einige der aufgelisteten Berechtigungen gelten nicht für FSx for ONTAP.

- `ds`— Ermöglicht Amazon FSx, Anwendungen in Ihrem Verzeichnis anzuzeigen, zu autorisieren und deren Autorisierung aufzuheben. AWS Directory Service
- `ec2`— Ermöglicht Amazon FSx, Folgendes zu tun:
  - Netzwerkschnittstellen, die mit einem Amazon FSx-Dateisystem verknüpft sind, anzeigen, erstellen und deren Zuordnung aufheben.
  - Zeigen Sie eine oder mehrere Elastic IP-Adressen an, die mit einem Amazon FSx-Dateisystem verknüpft sind.

  - Sehen Sie sich Amazon-VPCs, Sicherheitsgruppen und Subnetze an, die mit einem Amazon FSx-Dateisystem verknüpft sind.
  - Um eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.
  - Erstellen Sie eine Berechtigung für einen AWS-autorisierten Benutzer, bestimmte Operationen an einer Netzwerkschnittstelle auszuführen.
- `cloudwatch`— Ermöglicht Amazon FSx, metrische Datenpunkte CloudWatch unter dem AWS/FSx-Namespace zu veröffentlichen.
- `route53`— Ermöglicht Amazon FSx, eine Amazon VPC mit einer privaten gehosteten Zone zu verknüpfen.
- `logs`— Ermöglicht Amazon FSx, CloudWatch Log-Streams zu beschreiben und in sie zu schreiben. Auf diese Weise können Benutzer Dateizugriffs-Auditprotokolle für ein FSx for Windows File Server Server-Dateisystem an einen CloudWatch Logs-Stream senden.
- `firehose`— Ermöglicht Amazon FSx, Amazon Data Firehose-Lieferstreams zu beschreiben und in sie zu schreiben. Auf diese Weise können Benutzer die Dateizugriffs-Audit-Logs für ein Amazon FSx for Windows File Server Server-Dateisystem in einem Amazon Data Firehose-Lieferstream 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-Updates 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 Berechtigungen für dienstverknüpfte Rollen im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für Amazon FSx erstellen

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.

Bearbeitung einer serviceverknüpften Rolle für Amazon FSx

Amazon FSx erlaubt Ihnen nicht, die AWSServiceRoleForAmazonFSx serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname 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 serviceverknüpften 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

Verwenden Sie die IAM-Konsole, die IAM-CLI oder die IAM-API, um die serviceverknüpfte Rolle zu löschen. AWSServiceRoleForAmazonFSx 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.

AWS verwaltete Richtlinien für Amazon FSx

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AmazonF SxServiceRolePolicy

Ermöglicht Amazon FSx, AWS Ressourcen in Ihrem Namen zu verwalten. Weitere Informationen hierzu finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon FSx.

AWS verwaltete Richtlinie: AmazonF SxDeleteServiceLinkedRoleAccess

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 Service Linked Role für Amazon S3 S3-Zugriff zu löschen, die nur von Amazon FSx for Lustre verwendet wird.

Details zu Berechtigungen

Diese Richtlinie beinhaltet Berechtigungen, die es Amazon FSx ermöglichen, den Löschstatus für den Zugriff auf FSx Service Linked Roles für Amazon S3 einzusehen, zu löschen und einzusehen. `iam`

Die Berechtigungen für diese Richtlinie finden Sie unter AmazonF SxDeleteServiceLinkedRoleAccess im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonF SxFullAccess

Sie können AmazonF an Ihre SxFullAccess IAM-Entitäten anhängen. Amazon FSx verknüpft diese Richtlinie auch mit einer Servicerolle, die es Amazon FSx ermöglicht, Aktionen in Ihrem Namen durchzuführen.

Bietet vollen Zugriff auf Amazon FSx und Zugriff auf verwandte AWS Services.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Prinzipalen vollen Zugriff auf die Ausführung aller Amazon FSx-Aktionen, mit Ausnahme von. `BypassSnaplockEnterpriseRetention`
- `ds`— Ermöglicht Prinzipalen, Informationen über die Verzeichnisse einzusehen. AWS Directory Service
- `ec2`
  - Ermöglicht Prinzipalen das Erstellen von Tags unter den angegebenen Bedingungen.
  - Um eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.
- `iam`— Ermöglicht Principles, im Namen des Benutzers eine mit dem Amazon FSx Service verknüpfte Rolle zu erstellen. Dies ist erforderlich, damit Amazon FSx AWS Ressourcen im Namen des Benutzers verwalten kann.
- `logs`— Ermöglicht Prinzipalen, Protokollgruppen zu erstellen, Streams zu protokollieren und Ereignisse in Protokollstreams zu schreiben. Dies ist erforderlich, damit Benutzer FSx for Windows File Server Server-Dateisystemzugriff überwachen können, indem sie CloudWatch Audit-Zugriffsprotokolle an Logs senden.
- `firehose`— Ermöglicht Prinzipalen das Schreiben von Datensätzen in eine Amazon Data Firehose. Dies ist erforderlich, damit Benutzer FSx for Windows File Server Server-Dateisystemzugriff überwachen können, indem sie Audit-Zugriffsprotokolle an Firehose senden.

Die Berechtigungen für diese Richtlinie finden Sie unter AmazonF SxFullAccess im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonF SxConsoleFullAccess

Sie können die `AmazonFSxConsoleFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die den vollen Zugriff auf Amazon FSx und den Zugriff auf verwandte AWS Dienste über die AWS Management Console ermöglichen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Principals, alle Aktionen in der Amazon FSx-Managementkonsole auszuführen, mit Ausnahme von. `BypassSnaplockEnterpriseRetention`
- `cloudwatch`— Ermöglicht Principals, CloudWatch Alarme und Metriken in der Amazon FSx-Managementkonsole einzusehen.
- `ds`— Ermöglicht Prinzipalen, Informationen über ein Verzeichnis aufzulisten. AWS Directory Service
- `ec2`
  - Ermöglicht Principals, Tags für Routing-Tabellen zu erstellen, Netzwerkschnittstellen, Routing-Tabellen, Sicherheitsgruppen, Subnetze und die mit einem Amazon FSx-Dateisystem verknüpfte VPC aufzulisten.
  - Ermöglicht Prinzipalen die erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen, die mit einer VPC verwendet werden können.
- `kms`— Ermöglicht Prinzipalen, Aliase für Schlüssel aufzulisten. AWS Key Management Service
- `s3`— Ermöglicht Prinzipalen, einige oder alle Objekte in einem Amazon S3 S3-Bucket aufzulisten (bis zu 1000).
- `iam`— Erteilt die Erlaubnis, eine serviceverknüpfte Rolle zu erstellen, die es Amazon FSx ermöglicht, Aktionen im Namen des Benutzers durchzuführen.

Die Berechtigungen für diese Richtlinie finden Sie unter AmazonF SxConsoleFullAccess im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonF SxConsoleReadOnlyAccess

Sie können die `AmazonFSxConsoleReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Amazon FSx und verwandten AWS Diensten nur Leseberechtigungen, sodass Benutzer Informationen zu diesen Diensten in der einsehen können. AWS Management Console

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Prinzipalen, Informationen über Amazon FSx-Dateisysteme, einschließlich aller Tags, in der Amazon FSx Management Console einzusehen.
- `cloudwatch`— Ermöglicht Principals, CloudWatch Alarme und Metriken in der Amazon FSx Management Console einzusehen.

- `ds`— Ermöglicht Principals, Informationen über ein AWS Directory Service Verzeichnis in der Amazon FSx Management Console einzusehen.
- `ec2`
  - Ermöglicht Principals die Anzeige von Netzwerkschnittstellen, Sicherheitsgruppen, Subnetzen und der VPC, die einem Amazon FSx-Dateisystem zugeordnet sind, in der Amazon FSx Management Console.
  - Um eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.
- `kms`— Ermöglicht Prinzipalen, Aliase für AWS Key Management Service Schlüssel in der Amazon FSx Management Console einzusehen.
- `log`— Ermöglicht Principals, die Amazon CloudWatch Logs-Protokollgruppen zu beschreiben, die dem Konto zugeordnet sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit Prinzipale die bestehende Konfiguration für die Dateizugriffsüberwachung für ein FSx for Windows File Server Server-Dateisystem einsehen können.
- `firehose`— Ermöglicht Principals, die Amazon Data Firehose-Lieferdatenströme zu beschreiben, die dem Konto zugeordnet sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit Prinzipale die bestehende Konfiguration für die Dateizugriffsüberwachung für ein FSx for Windows File Server Server-Dateisystem einsehen können.

Die Berechtigungen für diese Richtlinie finden Sie unter AmazonF SxConsoleReadOnlyAccess im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonF SxReadOnlyAccess

Sie können die `AmazonFSxReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Prinzipalen, Informationen über Amazon FSx-Dateisysteme, einschließlich aller Tags, in der Amazon FSx Management Console einzusehen.
- `ec2`— Bereitstellung einer erweiterten Sicherheitsgruppenvalidierung aller Sicherheitsgruppen, die mit einer VPC verwendet werden können.

Die Berechtigungen für diese Richtlinie finden Sie unter AmazonF SxReadOnlyAccess im Referenzhandbuch für AWS verwaltete Richtlinien.

Amazon FSx-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon FSx an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf der Amazon FSx-Seite, um automatische Benachrichtigungen über Änderungen an dieser Dokumentverlauf für Amazon FSx für NetApp ONTAP Seite zu erhalten.

Änderung	Beschreibung	Datum
AmazonF SxServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	9. Januar 2024
AmazonF SxReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	9. Januar 2024
AmazonF SxConsoleReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidieru	9. Januar 2024

Änderung	Beschreibung	Datum
	ng aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	9. Januar 2024
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	9. Januar 2024
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, die es Benutzern ermöglicht, regionsübergreifende und kontoübergreifende Datenreplikation für FSx for OpenZFS-Dateisysteme durchzuführen.	20. Dezember 2023

Änderung	Beschreibung	Datum
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, die es Benutzern ermöglich t, regionsübergreifende und kontoübergreifende Datenrepl ikation für FSx for OpenZFS-D ateisysteme durchzuführen.	20. Dezember 2023
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, um Benutzern die On-Demand-Replikation von Volumes für FSx for OpenZFS-Dateisyste me zu ermöglichen.	26. November 2023
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, um Benutzern die On-Demand-Replikation von Volumes für FSx for OpenZFS-Dateisyste me zu ermöglichen.	26. November 2023
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefü gt, mit denen Benutzer die gemeinsame VPC-Unter stützung für FSx for ONTAP Multi-AZ-Dateisysteme anzeigen, aktivieren und deaktivieren können.	14. November 2023

Änderung	Beschreibung	Datum
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, mit denen Benutzer die gemeinsame VPC-Unterstützung für FSx for ONTAP Multi-AZ-Dateisysteme anzeigen, aktivieren und deaktivieren können.	14. November 2023
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Netzwerkkonfigurationen für FSx for OpenZFS Multi-AZ-Dateisysteme zu verwalten.	9. August 2023
AWS verwaltete Richtlinie: SxServiceRolePolicy AmazonF — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat die bestehende `cloudwatch:PutMetricData` Berechtigung geändert, sodass Amazon FSx CloudWatch Metriken im `AWS/FSx` Namespace veröffentlicht.	24. Juli 2023
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat die Richtlinie aktualisiert, um die `fsx:*` Genehmigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen.	13. Juli 2023
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat die Richtlinie aktualisiert, um die `fsx:*` Genehmigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen.	13. Juli 2023

Änderung	Beschreibung	Datum
AmazonF SxConsole ReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, mit denen Benutzer erweiterte Leistungskennzahlen und empfohlene Aktionen für FSx for Windows File Server Server-Dateisysteme in der Amazon FSx-Konsole einsehen können.	21. September 2022
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, mit denen Benutzer erweiterte Leistungskennzahlen und empfohlene Aktionen für FSx for Windows File Server Server-Dateisysteme in der Amazon FSx-Konsole einsehen können.	21. September 2022
AmazonF SxReadOnlyAccess — Tracking-Richtlinie gestartet	Diese Richtlinie gewährt Lesezugriff auf alle Amazon FSx-Ressourcen und alle damit verbundenen Tags.	4. Februar 2022
AmazonF SxDeleteServiceLinkedRoleAccess — Die Tracking-Richtlinie wurde gestartet	Diese Richtlinie gewährt Administratorberechtigungen, die es Amazon FSx ermöglichen, seine Service Linked Role für den Zugriff auf Amazon S3 zu löschen.	7. Januar 2022

Änderung	Beschreibung	Datum
AmazonF SxServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Netzwerkkonfigurationen für Amazon FSx for NetApp ONTAP-Dateisysteme zu verwalten.	2. September 2021
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Tags in EC2-Routing-Tabellen für Scoped-Down-Aufrufe zu erstellen.	2. September 2021
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Amazon FSx für NetApp ONTAP Multi-AZ-Dateisysteme erstellen kann.	2. September 2021
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Tags in EC2-Routing-Tabellen für Scoped-Down-Aufrufe zu erstellen.	2. September 2021

Änderung	Beschreibung	Datum
AmazonF SxServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, CloudWatch Log-Streams zu beschreiben und in sie zu schreiben. Dies ist erforderlich, damit Benutzer die Dateizugriffsprüfungsprotokolle für FSx for Windows File Server Server-Dateisysteme mithilfe von CloudWatch Logs anzeigen können.	8. Juni 2021
AmazonF SxServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Amazon Data Firehose-Lieferstreams zu beschreiben und in sie zu schreiben. Dies ist erforderlich, damit Benutzer die Dateizugriffs-Audit-Logs für ein FSx for Windows File Server Server-Dateisystem mit Amazon Data Firehose einsehen können.	8. Juni 2021

Änderung	Beschreibung	Datum
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Prinzipalen ermöglichen, Log-Log-Gruppen zu beschreiben und zu erstellen, Streams zu CloudWatch protokollieren und Ereignisse in Log-Streams zu schreiben. Dies ist erforderlich, damit Prinzipale die Dateizugriffsprüfungsprotokolle für FSx for Windows File Server Server-Dateisysteme mithilfe von CloudWatch Protokollen anzeigen können.	8. Juni 2021
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, um es Prinzipalen zu ermöglichen, Datensätze zu beschreiben und in eine Amazon Data Firehose zu schreiben. Dies ist erforderlich, damit Benutzer die Dateizugriffs-Audit-Logs für ein FSx for Windows File Server Server-Dateisystem mit Amazon Data Firehose einsehen können.	8. Juni 2021

Änderung	Beschreibung	Datum
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon CloudWatch Logs-Protokollgruppen beschreiben können, die dem Konto zugeordnet sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit Prinzipale bei der Konfiguration der Dateizugriffsüberwachung für ein FSx for Windows File Server-Dateisystem eine vorhandene CloudWatch Protokollgruppe auswählen können.	8. Juni 2021
AmazonF SxConsole FullAccess — Aktualisierung auf eine bestehende Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon Data Firehose-Lieferströme beschreiben können, die mit dem Konto verknüpft sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit Principals bei der Konfiguration der Dateizugriffsüberwachung für ein FSx for Windows File Server-Dateisystem einen vorhandenen Firehose-Lieferstream auswählen können.	8. Juni 2021

Änderung	Beschreibung	Datum
AmazonF SxConsole ReadOnlyAccess — Aktualisierung auf eine bestehende Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon CloudWatch Logs-Protokollgruppen beschreiben können, die dem Konto zugeordnet sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit Prinzipale die bestehende Konfiguration für die Dateizugriffsüberwachung für ein FSx for Windows File Server Server-Dateisystem einsehen können.	8. Juni 2021
AmazonF SxConsole ReadOnlyAccess — Aktualisierung auf eine bestehende Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon Data Firehose-Lieferströme beschreiben können, die mit dem Konto verknüpft sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit Prinzipale die bestehende Konfiguration für die Dateizugriffsüberwachung für ein FSx for Windows File Server Server-Dateisystem einsehen können.	8. Juni 2021

Änderung	Beschreibung	Datum
Amazon FSx hat begonnen, Änderungen zu verfolgen	Amazon FSx hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	8. Juni 2021

Dateisystem-Zugriffskontrolle mit Amazon VPC

Sie greifen auf Ihre Amazon FSx for NetApp ONTAP-Dateisysteme und SVMs über den DNS-Namen oder die IP-Adresse eines ihrer Endgeräte zu, je nachdem, um welche Art von Zugriff es sich handelt. Der DNS-Name ist der privaten IP-Adresse der elastic network interface des Dateisystems oder der SVM in Ihrer VPC zugeordnet. Nur Ressourcen innerhalb der zugehörigen VPC oder Ressourcen, die über AWS Direct Connect oder VPN mit der zugehörigen VPC verbunden sind, können über die Protokolle NFS, SMB oder iSCSI auf die Daten in Ihrem Dateisystem 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.

Amazon VPC-Sicherheitsgruppen

Eine Sicherheitsgruppe fungiert als virtuelle Firewall für Ihre FSx for ONTAP-Dateisysteme, um eingehenden und ausgehenden Datenverkehr zu kontrollieren. Eingehende Regeln kontrollieren den eingehenden Verkehr zu Ihrem Dateisystem, und ausgehende Regeln kontrollieren den ausgehenden Verkehr von Ihrem Dateisystem. Wenn Sie ein Dateisystem erstellen, geben Sie die VPC an, in der es erstellt wird, und die Standardsicherheitsgruppe für diese VPC wird angewendet. Sie können jeder Sicherheitsgruppe Regeln hinzufügen, die den Datenverkehr zu oder von den zugehörigen Dateisystemen und SVMs zulassen. Sie können die Regeln für eine Sicherheitsgruppe jederzeit ändern. Neue und geänderte Regeln werden automatisch auf alle Ressourcen angewendet, die der Sicherheitsgruppe zugeordnet sind. Wenn Amazon FSx entscheidet, ob Datenverkehr eine

Ressource erreichen darf, bewertet es alle Regeln aller Sicherheitsgruppen, die mit der Ressource verknüpft sind.

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 für Linux-Instances.

Erstellen einer VPC-Sicherheitsgruppe

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. Lassen Sie bei Regeln für ausgehenden Datenverkehr den gesamten Datenverkehr auf allen Ports zu.
7. Fügen Sie den eingehenden Ports Ihrer Sicherheitsgruppe die folgenden Regeln hinzu.
   Für das Quellfeld sollten Sie Benutzerdefiniert wählen und die Sicherheitsgruppen oder IP-Adressbereiche eingeben, die den Instances zugeordnet sind, die auf Ihr FSx for ONTAP-Dateisystem zugreifen müssen, einschließlich:

   - Linux-, Windows- und/oder macOS-Clients, die über NFS, SMB oder iSCSI auf Daten in Ihrem Dateisystem zugreifen.
   - Alle ONTAP-Dateisysteme/-Cluster, die Sie per Peering mit Ihrem Dateisystem verbinden (z. B. um,, oder zu verwenden). SnapMirror SnapVault FlexCache
   - Alle Clients, die Sie für den Zugriff auf die ONTAP REST API, CLI oder ZAPIs verwenden werden (z. B. eine Harvest/Grafana-Instanz, NetApp Connector oder BlueXP). NetApp

Protokoll	Ports	Rolle
Alle ICMP	Alle	Die Instanz anpingen
SSH	22	SSH-Zugriff auf die IP-Adresse der Cluster-Management-LIF oder einer Node-Management-LIF
TCP	111	Remote-Prozeduraufruf für NFS
TCP	135	Entfernter Prozeduraufruf für CIFS
TCP	139	NetBIOS-Servicesitzung für CIFS
TCP	161-162	Einfaches Netzwerkverwaltungsprotokoll (SNMP)
TCP	443	ONTAP REST API-Zugriff auf die IP-Adresse der Cluster-Management-LIF oder einer SVM-Management-LIF
TCP	445	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
TCP	635	NFS-Halterung
TCP	749	Kerberos
TCP	2049	NFS-Serverdaemon
TCP	3260	iSCSI-Zugriff über die iSCSI-Daten-LIF
TCP	4045	NFS-Sperrdaemon
TCP	4046	Netzwerkstatusmonitor für NFS
TCP	10000	Netzwerkdatenverwaltungsprotokoll (NDMP) und Cluster-Kommunikation NetApp SnapMirror
TCP	11104	Verwaltung der Kommunikation NetApp SnapMirror zwischen Clustern

Protokoll	Ports	Rolle
TCP	11105	SnapMirror Datenübertragung mit Intercluster-LIFs
UDP	111	Entfernter Prozeduraufruf für NFS
UDP	135	Entfernter Prozeduraufruf für CIFS
UDP	137	NetBIOS-Namensauflösung für CIFS
UDP	139	NetBIOS-Servicesitzung für CIFS
UDP	161-162	Einfaches Netzwerkverwaltungsprotokoll (SNMP)
UDP	635	NFS-Halterung
UDP	2049	NFS-Serverdaemon
UDP	4045	NFS-Sperrdaemon
UDP	4046	Netzwerkstatusmonitor für NFS
UDP	4049	NFS-Kontingentprotokoll

8. Fügen Sie die Sicherheitsgruppe zur elastic network interface des Dateisystems hinzu.

Verbieten Sie den Zugriff auf ein Dateisystem

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.

Konformitätsprüfung für Amazon FSx for ONTAP NetApp

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 herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen 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 Bereitstellung 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— Auf diese AWS-Service Weise erhalten Sie 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.

- 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 für NetApp ONTAP und VPC-Schnittstellen-Endpunkte ()AWS PrivateLink

Sie können die Sicherheitslage Ihrer VPC verbessern, indem Sie Amazon FSx so konfigurieren, dass es einen VPC-Endpunkt mit Schnittstelle verwendet. Interface-VPC-Endpunkte basieren auf einer Technologie AWS PrivateLink, mit der Sie privat auf Amazon FSx-APIs zugreifen können, ohne dass ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung erforderlich ist. AWS Direct Connect Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Amazon FSx-APIs zu kommunizieren. Der Verkehr zwischen Ihrer VPC und Amazon FSx verlässt das AWS Netzwerk nicht.

Jeder Schnittstellen-VPC-Endpunkt wird durch eine oder mehrere elastische Netzwerkschnittstellen in Ihren Subnetzen repräsentiert. Eine Netzwerkschnittstelle stellt eine private IP-Adresse bereit, die als Einstiegspunkt für den Datenverkehr zur Amazon FSx-API dient.

Überlegungen zu VPC-Endpunkten mit Amazon FSx-Schnittstelle

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Amazon FSx einrichten, sollten Sie die Eigenschaften und Einschränkungen von Interface VPC-Endpunkten im Amazon VPC-Benutzerhandbuch lesen.

Sie können alle Amazon FSx-API-Operationen von Ihrer VPC aus aufrufen. Sie können beispielsweise ein FSx for ONTAP-Dateisystem erstellen, indem Sie die CreateFileSystem API von Ihrer VPC aus aufrufen. Die vollständige Liste der Amazon FSx-APIs finden Sie unter Aktionen in der Amazon FSx-API-Referenz.

Überlegungen zum VPC-Peering

Sie können andere VPCs mithilfe von VPC-Peering mit der VPC über Schnittstellen-VPC-Endpunkte 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 Die VPCs können sich auch in zwei verschiedenen Versionen befinden. AWS-Regionen

Der Verkehr zwischen Peer-VPCs verbleibt im AWS Netzwerk und durchquert nicht das öffentliche Internet. Sobald VPCs miteinander verbunden sind, können Ressourcen wie Amazon Elastic Compute Cloud (Amazon EC2) -Instances in beiden VPCs über Schnittstellen-VPC-Endpunkte, die in einer der VPCs erstellt wurden, auf die Amazon FSx-API zugreifen.

Erstellen eines VPC-Schnittstellen-Endpunkts für Amazon FSx API

Sie können einen VPC-Endpunkt für die Amazon FSx-API entweder mit der Amazon VPC-Konsole oder mit () erstellen. AWS Command Line Interface AWS CLI Weitere Informationen finden Sie unter Erstellen eines Schnittstellen-VPC-Endpunkts im Amazon VPC-Benutzerhandbuch.

Verwenden Sie eine der folgenden Methoden, um einen VPC-Schnittstellen-Endpunkt für Amazon FSx zu erstellen:

- **`com.amazonaws.region.fsx`**— Erzeugt einen Endpunkt für Amazon FSx-API-Operationen.
- **`com.amazonaws.region.fsx-fips`**— Erstellt einen Endpunkt für die Amazon FSx-API, der dem Federal Information Processing Standard (FIPS) 140-2 entspricht.

Um die private DNS-Option zu verwenden, müssen Sie die `enableDnsSupport` Attribute `enableDnsHostnames` und für Ihre VPC festlegen. Weitere Informationen finden Sie unter DNS-Unterstützung für Ihre VPC anzeigen und aktualisieren im Amazon VPC-Benutzerhandbuch.

Mit Ausnahme AWS-Regionen von China können Sie, wenn Sie privates DNS für den Endpunkt aktivieren, API-Anfragen an Amazon FSx mit dem VPC-Endpunkt stellen AWS-Region, indem Sie beispielsweise seinen Standard-DNS-Namen für verwenden. `fsx.us-east-1.amazonaws.com` Für China (Peking) und China (Ningxia) AWS-Regionen können Sie API-Anfragen mit dem VPC-Endpunkt jeweils mit `fsx-api.cn-north-1.amazonaws.com.cn` und `fsx-api.cn-northwest-1.amazonaws.com.cn` stellen.

Weitere Informationen finden Sie unter Zugreifen auf einen Service über einen Schnittstellen-VPC-Endpunkt im Amazon VPC-Benutzerhandbuch.

Erstellen einer VPC-Endpunktrichtlinie für Amazon FSx

Um den Zugriff auf die Amazon FSx-API zu kontrollieren, können Sie Ihrem AWS Identity and Access Management VPC-Endpunkt eine (IAM-) Richtlinie hinzufügen. 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.

Resilienz in Amazon FSx für ONTAP NetApp

Die AWS globale Infrastruktur basiert AWS-Regionen auf Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet Amazon FSx mehrere Funktionen zur Unterstützung Ihrer Datenstabilität und Backup-Anforderungen.

Backup und Wiederherstellung

Amazon FSx erstellt und speichert automatische Backups der Volumes in Ihrem Amazon FSx for NetApp ONTAP-Dateisystem. Amazon FSx erstellt automatische Backups Ihrer Volumes während des Backup-Fensters Ihres Amazon FSx for NetApp ONTAP-Dateisystems. Amazon FSx speichert die automatisierten Backups Ihrer Volumes gemäß dem von Ihnen angegebenen Aufbewahrungszeitraum für Backups. Sie können Ihre Volumes auch manuell sichern, indem Sie ein vom Benutzer initiiertes Backup erstellen. Sie können ein Volume-Backup jederzeit wiederherstellen, indem Sie ein neues Volume mit dem als Quelle angegebenen Backup erstellen.

Weitere Informationen finden Sie unter Arbeiten mit Backups.

Snapshots

Amazon FSx erstellt Snapshot-Kopien der Amazon FSx for NetApp ONTAP-Volumes. Snapshot-Kopien bieten Schutz vor versehentlichem Löschen oder Ändern von Dateien in Ihren Volumes durch Endbenutzer. Weitere Informationen finden Sie unter Arbeiten mit Snapshots.

Availability Zones

Die Dateisysteme von Amazon FSx for NetApp ONTAP sind so konzipiert, dass Daten auch bei einem Serverausfall kontinuierlich verfügbar sind. Jedes Dateisystem wird von zwei Dateiservern in mindestens einer Availability Zone betrieben, von denen jeder über seinen eigenen Speicher verfügt. Amazon FSx repliziert Ihre Daten automatisch, um sie vor Komponentenausfällen zu schützen, sucht kontinuierlich nach Hardwareausfällen und ersetzt bei einem Ausfall automatisch Infrastrukturkomponenten. Dateisysteme führen bei Bedarf automatisch Failover und Backups durch (in der Regel innerhalb von 60 Sekunden), und Clients führen automatisch ein Failover mit dem Dateisystem durch.

Multi-AZ-Dateisysteme

Die Dateisysteme von Amazon FSx for NetApp ONTAP sind in allen AWS Availability Zones hochverfügbar und stabil. Sie sind so konzipiert, dass Daten auch dann kontinuierlich verfügbar sind, wenn eine Availability Zone nicht verfügbar ist.

Weitere Informationen finden Sie unter Verfügbarkeit und Beständigkeit.

Single-AZ-Dateisysteme

Amazon FSx for NetApp ONTAP-Dateisysteme sind innerhalb einer einzigen AWS Availability Zone hochverfügbar und dauerhaft und so konzipiert, dass sie bei einem Ausfall eines einzelnen Dateiservers oder einer Festplatte eine kontinuierliche Verfügbarkeit innerhalb dieser Availability Zone bieten.

Weitere Informationen finden Sie unter Verfügbarkeit und Beständigkeit.

Infrastruktursicherheit in Amazon FSx for ONTAP NetApp

Als verwalteter Service ist Amazon FSx for NetApp ONTAP durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon FSx zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.

- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Verwenden Sie NetApp ONTAP Vscan mit FSx für ONTAP

Sie können die Vscan-Funktion von NetApp ONTAP verwenden, um unterstützte Antivirensoftware von Drittanbietern auszuführen. Weitere Informationen finden Sie in den folgenden Ressourcen für jede der unterstützten Lösungen.

- McAfee — Leitfaden zu Antiviren-Lösungen für Clustered Data ONTAP: McAfee
- SentinelOne — Partnerlösungen von Vscan und SentinelOne Singularity Cloud Data Security
- Symantec — Vscan-Partnerlösungen und Symantec Protection Engine
- Trend Micro — Leitfaden für Antiviren-Lösungen für Clustered Data ONTAP: Trend Micro

Rollen und Benutzer in Amazon FSx for ONTAP NetApp

ONTAP bietet eine robuste und erweiterbare Funktion zur rollenbasierten Zugriffskontrolle (RBAC). Sie können Benutzern eine Rolle zuweisen, um ihren Zugriff auf die Ressourcen zu kontrollieren, die über die ONTAP REST API und CLI verfügbar gemacht werden. Die Rollen definieren verschiedene Ebenen des administrativen Zugriffs für die verschiedenen ONTAP-Benutzer. Sie können Rollen und Benutzer in FSx for ONTAP verwenden, um Benutzerfunktionen und -berechtigungen zu definieren, wenn Sie die ONTAP CLI und die REST API verwenden. Jede ONTAP-Rolle und jeder Benutzer ist Ihrem Dateisystem oder einer Storage Virtual Machine (SVM) zugeordnet.

Standardmäßig hat Ihr FSx for ONTAP-Dateisystem einen Benutzer auf Dateisystemebene namens fsxadmin, dem die Rolle zugewiesen ist. `fsxadmin` Auf Dateisystemebene können Sie nur neue Benutzer mit dieser Rolle erstellen. `fsxadmin` Sie können keine neuen Rollen erstellen oder die `fsxadmin` Rolle ändern.

Für jede SVM in Ihrem Dateisystem gibt es einen Standardbenutzer namens vsadmin, dem die Rolle zugewiesen ist. `vsadmin` Auf SVM-Ebene können Sie neue Benutzer und neue Rollen erstellen.

Zusätzlich zur `vsadmin` Rolle gibt es mehrere vordefinierte SVM-Rollen, die Sie SVM-Benutzern zuweisen können. Sie können auch Rollen erstellen, die die Ebene der Zugriffskontrolle bieten, die den Anforderungen Ihres Unternehmens entspricht.

Vordefinierte Rollen auf einer SVM

SVMs haben die folgenden vordefinierten Rollen:

Rollenname	Funktionen
`vsadmin`	• Verwalten Sie Ihr Benutzerkonto, Ihr lokales Passwort und wichtige Informationen • Verwalten Sie Volumen, mit Ausnahme von Volumenverschiebungen • Verwalten Sie Kontingente, Qtrees, Snapshot-Kopien und Dateien • LUNs verwalten • Führen Sie SnapLock Operationen aus, mit Ausnahme von privilegierten Löschvorg ängen • Protokolle konfigurieren: NFS, SMB und iSCSI • Dienste konfigurieren: DNS, LDAP und NIS • Aufträge überwachen • Überwachen Sie die Netzwerkverbindungen und die Netzwerkschnittstelle • Überwachen Sie den Zustand der SVM
`vsadmin-volume`	• Verwalten Sie Ihr Benutzerkonto, Ihr lokales Passwort und wichtige Informationen • Verwalten Sie Volumen, einschließlich Volumenverschiebungen • Verwalten Sie Kontingente, QTrees, Snapshot-Kopien und Dateien • LUNs verwalten

Rollenname	Funktionen
	• Protokolle konfigurieren: NFS, SMB und iSCSI • Dienste konfigurieren: DNS, LDAP und NIS • Überwachen Sie die Netzwerkschnittstelle • Überwachen Sie den Zustand der SVM
`vsadmin-protocol`	• Verwalten Sie Ihr Benutzerkonto, Ihr lokales Passwort und wichtige Informationen • LUNs verwalten • Protokolle konfigurieren: NFS, SMB und iSCSI • Dienste konfigurieren: DNS, LDAP und NIS • Überwachen Sie die Netzwerkschnittstelle • Überwachen Sie den Zustand der SVM
`vsadmin-backup`	• Verwalten Sie Ihr Benutzerkonto, Ihr lokales Passwort und wichtige Informationen • NDMP-Operationen verwalten • Lese- und Schreibzugriff auf ein wiederher gestelltes Volume • SnapMirror Beziehungen und Snapshot-Kopien verwalten • Volumes und Netzwerkinformationen anzeigen

Rollenname	Funktionen
`vsadmin-snaplock`	• Verwalten Sie Ihr Benutzerkonto, Ihr lokales Passwort und wichtige Informationen • Verwalten Sie Volumen, mit Ausnahme von Volumenverschiebungen • Verwalten Sie Kontingente, Qtrees, Snapshot-Kopien und Dateien • Führen Sie SnapLock Operationen aus, einschließlich privilegierter Löschvorgänge • Konfigurieren Sie die Protokolle: NFS und SMB • Dienste konfigurieren: DNS, LDAP und NIS • Aufträge überwachen • Überwachen Sie die Netzwerkverbindungen und die Netzwerkschnittstelle
`vsadmin-readonly`	• Verwalten Sie Ihr Benutzerkonto, Ihr lokales Passwort und wichtige Informationen • Überwachen Sie den Zustand der SVM • Überwachen Sie die Netzwerkschnittstelle • Volumes und LUNs anzeigen • Dienste und Protokolle anzeigen

Themen

- Neue Rollen oder Benutzer erstellen
- Das Aktualisieren des fsxadmin Kontopassworts schlägt fehl
- Neue Rollen für eine SVM mit der NetApp ONTAP CLI erstellen
- Verwenden Sie Active Directory-Benutzerkonten mit Ihrem Dateisystem
- Konfiguration der Authentifizierung mit öffentlichem Schlüssel

Neue Rollen oder Benutzer erstellen

Jeder Benutzer in FSx for ONTAP ist einer SVM oder dem Dateisystem selbst zugeordnet. Sie können neue Rollen oder Benutzer erstellen, indem Sie den `security login create` Befehl in der NetApp ONTAP CLI mit der `vsadmin` Rolle für SVMs und der `fsxadmin` Standardrolle für Ihr Dateisystem verwenden.

Der `security login create` Befehl erstellt eine Anmeldemethode für das Verwaltungsdienstprogramm. Eine Anmeldemethode besteht aus einem Benutzernamen, einer Anwendung (Zugriffsmethode) und einer Authentifizierungsmethode. Ein Benutzername kann mehreren Anwendungen zugeordnet werden. Er kann optional einen Rollennamen für die Zugriffskontrolle enthalten. Wenn ein Active Directory-, LDAP- oder NIS-Gruppenname verwendet wird, gewährt die Anmeldemethode Benutzern, die zu der angegebenen Gruppe gehören, Zugriff. Wenn der Benutzer Mitglied mehrerer Gruppen ist, die in der Sicherheitsanmeldetabelle bereitgestellt werden, erhält der Benutzer Zugriff auf eine kombinierte Liste der Befehle, die für die einzelnen Gruppen autorisiert sind. Weitere Informationen finden Sie `security login create`in der NetApp ONTAP Produktdokumentation.

Um einen neuen Benutzer für eine SVM oder ein Dateisystem (NetApp ONTAPCLI) zu erstellen

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Verwenden Sie den `security login create` ONTAP CLI-Befehl, um ein neues Benutzerkonto auf Ihrem FSx for ONTAP-Dateisystem oder SVM zu erstellen.

   ```
   Fsx0123456::> security login create -vserver vserver_name -user-or-group-
   name user_or_group_name -application login_application -authentication-
   method auth_method -role role_or_account_name
   ```

   Fügen Sie Ihre Daten für die Platzhalter im Beispiel ein, um die folgenden erforderlichen Eigenschaften zu definieren:

- `-vserver`— Gibt den Namen des Dateisystems oder der SVM an, in dem Sie die neue Rolle oder den neuen Benutzer erstellen möchten.
- `-user-or-group-name`— Gibt den Benutzernamen oder den Active Directory-Gruppennamen der Anmeldemethode an. Der Active Directory-Gruppenname kann nur mit der `domain` Authentifizierungsmethode `ontapi` und den `ssh` Anwendungen angegeben werden.
- `-application`— Gibt die Anwendung der Anmeldemethode an. Mögliche Werte sind http, ontapi und ssh.
- `-authentication-method`— Gibt die Authentifizierungsmethode für die Anmeldung an. Die folgenden Werte sind möglich:
  - domain — Wird für die Active Directory-Authentifizierung verwendet
  - Passwort — Wird für die Passwortauthentifizierung verwendet
  - publickey — Benutzer für die Authentifizierung mit öffentlichem Schlüssel
- `-role`— Gibt den Namen der Zugriffskontrollrolle für die Anmeldemethode an. Auf Dateisystemebene ist die einzige Rolle, die angegeben werden kann, `fsxadmin`

(Optional) Sie können auch einen oder mehrere der folgenden Parameter mit dem Befehl verwenden:

- `[-comment]`— Der Kommentartext für das Benutzerkonto. z. B. **`Guest account`**. Die maximale Länge beträgt 128 Zeichen.
- `[-second-authentication-method {none|publickey|password|nsswitch}]`— Gibt die zweite Faktor-Authentifizierungsmethode an. Sie können die folgenden Methoden angeben:
  - Passwort — Wird für die Passwortauthentifizierung verwendet
  - publickey — Wird für die Authentifizierung mit öffentlichem Schlüssel verwendet
  - nsswitch — Wird für die NIS- oder LDAP-Authentifizierung verwendet
  - none — Der Standardwert, wenn Sie keinen angeben

Das Aktualisieren des **`fsxadmin`** Kontopassworts schlägt fehl

Wenn Sie das Kennwort für den `fsxadmin` Benutzer aktualisieren, wird möglicherweise eine Fehlermeldung angezeigt, wenn es die im Dateisystem festgelegten Kennwortanforderungen nicht

erfüllt. Sie können die Kennwortanforderungen mithilfe des `security login role config show` ONTAP CLI- oder REST-API-Befehls anzeigen.

Um die Passwortanforderungen für das **`fsxadmin`** Konto einzusehen

1. Um auf die NetApp ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Management-Port des Amazon FSx for NetApp ONTAP-Dateisystems ein, indem Sie den folgenden Befehl ausführen. *`management_endpoint_ip`*Ersetzen Sie es durch die IP-Adresse des Management-Ports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

2. Der `security login role config show` Befehl gibt die Kennwortanforderungen für ein Konto zurück.

   ```
   FsxId0123456::> security login role config show -role fsxadmin -
   fields password_requirement_fields
   ```

   Geben Sie für den `-fields` Parameter eine oder alle der folgenden Angaben an:

   - `passwd-minlength`— Die Mindestlänge des Passworts.
   - `passwd-min-special-chars`— Die Mindestanzahl von Sonderzeichen im Passwort.
   - `passwd-min-lowercase-chars`— Die Mindestanzahl von Kleinbuchstaben im Passwort.
   - `passwd-min-uppercase-chars`— Die Mindestanzahl von Großbuchstaben im Passwort.
   - `passwd-min-digits`— Die Mindestanzahl von Ziffern im Passwort.
   - `passwd-alphanum`— Informationen zum Ein- oder Ausschließen von alphanumerischen Zeichen.
   - `passwd-expiry-time`— Die Ablaufzeit des Passworts.
   - `passwd-expiry-warn-time`— Die Uhrzeit der Warnung vor Ablauf des Kennworts.

3. Führen Sie den folgenden Befehl aus, um alle Passwortanforderungen zu sehen:

   ```
   Fsx0123456::> security login role config show -role fsxadmin -fields passwd-
   minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
   digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
   uppercase-chars
   ```

Sie erhalten eine Antwort ähnlich dem folgenden Beispiel, in dem die Informationen für die angegebenen Felder angezeigt werden.

```
vserver                role     passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
---------------------- -------- ---------------- --------------
 ------------------------ ------------------ --------------------------
 ------------------------- ----------------- ----------------------
FsxId0ae30e5b7f1a50b6a fsxadmin 3                 enabled         0
       unlimited          0                         0                          0
               unlimited
```

So ändern Sie die Kennwortanforderungen (ONTAPCLI)

- Um Ihre Passwortanforderungen zu ändern, verwenden Sie den `security login role config modify` Befehl mit den gewünschten Passwortfeldern. Das folgende Beispiel zeigt, wie Sie die Mindestlänge des Kennworts auf 4 und die Mindestanzahl von Sonderzeichen auf 1 für die `fsxadmin` Rolle in einem Dateisystem ändern.

```
Fsx0123456::> security login role config modify -role fsxadmin -passwd-minlength 4
 -passwd-min-special-chars 1
```

Neue Rollen für eine SVM mit der NetApp ONTAP CLI erstellen

Jede SVM, die Sie erstellen, hat einen Standard-SVM-Administrator, dem die vordefinierte `vsadmin` Rolle zugewiesen ist. Sie können jedoch keine neuen Rollen mithilfe von. `vsadmin` Wenn Sie neue Rollen für Ihre SVM erstellen müssen, verwenden Sie den `security login role create` Befehl mit der `fsxadmin` Rolle in der NetApp ONTAP CLI.

Um mit der NetApp ONTAP CLI eine neue Rolle auf Ihrer SVM zu erstellen

1. Kopieren Sie den folgenden Befehl: `security login role create`

```
Fsx0123456::> security login role create -role vol_role -cmddirname "volume"
```

2. Geben Sie im Befehl die folgenden erforderlichen Parameter an:

- `-role`— Der Name der Rolle.
- `-cmddirname`— Der Befehl oder das Befehlsverzeichnis, auf das die Rolle Zugriff gewährt. Schließen Sie die Namen der Befehlsunterverzeichnisse in doppelte Anführungszeichen ein. z. B. `"volume snapshot"`. Geben Sie die Eingabetaste ein`DEFAULT`, um alle Befehlsverzeichnisse anzugeben.

3. (Optional) Sie können dem Befehl auch einen der folgenden Parameter hinzufügen:

- `-vserver`— Der Name der SVM, die der Rolle zugeordnet ist.
- `-access`— Die Zugriffsebene für die Rolle. Für Befehlsverzeichnisse beinhaltet dies:
  - `none`— Verweigert den Zugriff auf Befehle im Befehlsverzeichnis. Dies ist der Standardwert für benutzerdefinierte Rollen.
  - `readonly`— Gewährt Zugriff auf die Show-Befehle im Befehlsverzeichnis und seinen Unterverzeichnissen.
  - `all`— Gewährt Zugriff auf alle Befehle im Befehlsverzeichnis und seinen Unterverzeichnissen. Um den Zugriff auf systeminterne Befehle zu gewähren oder zu verweigern, müssen Sie das Befehlsverzeichnis angeben.

  Für Befehle, die nicht systemimmanent sind (Befehle, die nicht auf`create`,, `modify` oder enden): `delete show`
  - `none`— Verweigert den Zugriff auf Befehle im Befehlsverzeichnis. Dies ist der Standardwert für benutzerdefinierte Rollen.
  - `readonly`— Nicht zutreffend. Nicht verwenden.
  - `all`— Gewährt Zugriff auf den Befehl.
- `-query`— Das Abfrageobjekt, das zum Filtern der Zugriffsebene verwendet wird, die in Form einer gültigen Option für den Befehl oder für einen Befehl im Befehlsverzeichnis angegeben wird. Schließen Sie das Abfrageobjekt in doppelte Anführungszeichen ein.

4. Führen Sie den Befehl `security login role create` aus.

Verwenden Sie Active Directory-Benutzerkonten mit Ihrem Dateisystem

Wenn Sie ein Dateisystemadministrator sind, können Sie den `security login domain-tunnel create` Befehl in der NetApp ONTAP CLI verwenden, um sich mit Active Directory-Konten bei Ihrem Dateisystem und Ihren SVMs zu authentifizieren.

Um sich mit Active Directory bei Ihrem Dateisystem oder Ihren SVMs zu authentifizieren

1. Um eine SSH-Verbindung zur NetApp ONTAP CLI Ihres Dateisystems herzustellen, folgen Sie den im Verwenden der NetApp ONTAP-CLI Abschnitt des FSx for ONTAP-Benutzerhandbuchs dokumentierten Schritten.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Um sich bei Ihrem Dateisystem mit Active Directory-Anmeldeinformationen anstelle einer einzelnen SVM zu authentifizieren, kopieren Sie den folgenden `security login domain-tunnel create` Befehl, um Domain-Tunneling einzurichten. Wählen Sie eine SVM aus, die mit Ihrem Active Directory verknüpft ist und als Domänentunnel für die Authentifizierung von Anmeldungen mit Ihrem Active Directory dient.

   ```
   FsxIdabcdef0123456789a::> security login domain-tunnel create -vserver svm01
   ```

3. Verwenden Sie den `security login create` Befehl, um ein oder mehrere Active Directory-Domänenbenutzerkonten zu erstellen, denen Zugriff auf das Dateisystem gewährt wird.
4. Geben Sie im Befehl die folgenden erforderlichen Parameter an:

   - `-vserver`— Der Name des Dateisystems oder der SVM, in dem die neue Rolle oder der neue Benutzer erstellt wird.
   - `-user-or-group-name`— Der Benutzername oder der Active Directory-Gruppenname der Anmeldemethode. Der Active Directory-Gruppenname kann nur mit der `domain` Authentifizierungsmethode `ontapi` und der `ssh` Anwendung angegeben werden.
   - `-application`— Die Anwendung der Login-Methode. Mögliche Werte sind http, ontapi und ssh.
   - `-authentication-method`— Die für die Anmeldung verwendete Authentifizierungsmethode. Die folgenden Werte sind möglich:
     - Domäne — für die Active Directory-Authentifizierung
     - Passwort — für die Passwortauthentifizierung
     - publickey — für die Authentifizierung mit öffentlichen Schlüsseln
   - `-role`— Der Name der Zugriffskontrollrolle für die Anmeldemethode. Auf Dateisystemebene kann nur die Rolle angegeben werden. `-role fsxadmin`
5. Das folgende Beispiel zeigt, wie Sie mit Ihren Active Directory-Anmeldeinformationen eine SSH-Verbindung zu Ihrem Dateisystem herstellen können, wenn Sie den Typ wählen`ssh`. `-`

`application` Der hat `username` das Format`"domain-name\user-name"`, das aus dem Domänennamen und dem Benutzernamen besteht, die Sie bei der Erstellung des Kontos angegeben haben, getrennt durch einen umgekehrten Schrägstrich und in Anführungszeichen eingeschlossen.

```
Fsx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
```

Wenn Sie zur Eingabe eines Kennworts aufgefordert werden, verwenden Sie das Kennwort des Active Directory-Benutzers.

> **Note**
>
> Auf der SVM, die für das Tunneling verwendet wird, muss CIFS aktiviert sein oder sie muss mit einem Active Directory verknüpft sein. Wenn Sie CIFS nicht aktivieren und nur die Tunnel-SVM mit einem Active Directory verbinden, stellen Sie sicher, dass Ihre SVM mit Ihrem Active Directory verbunden ist. Weitere Informationen finden Sie unter Verbinden von SVMs mit einem Microsoft Active Directory.

Konfiguration der Authentifizierung mit öffentlichem Schlüssel

Um die SSH-Authentifizierung mit öffentlichem Schlüssel zu aktivieren, müssen Sie zunächst einen SSH-Schlüssel generieren und ihn mithilfe des `security login publickey create` Befehls einem Administratorkonto zuordnen. Dadurch kann das Konto auf die SVM zugreifen. Der `security login publickey create` Befehl akzeptiert die folgenden Parameter.

Parameter	Beschreibung
`-vserver` (Optional)	Der Name der SVM, auf die das Konto zugreift.
`-username`	Der Benutzername des Kontos. Der Standardwert,`admin`, ist der Standardname des Clusteradministrators.
`-index`	Die Indexnummer des öffentlichen Schlüssels. Der Standardwert ist 0, wenn der Schlüssel der erste Schlüssel ist, der für das Konto

Parameter	Beschreibung
	erstellt wurde. Andernfalls ist der Standardw ert um eins höher als die höchste existierende Indexnummer für das Konto.
`-publickey`	Der öffentliche OpenSSH-Schlüssel. Schließen Sie den Schlüssel in doppelte Anführung szeichen ein.
`-role`	Die Zugriffskontrollrolle, die dem Konto zugewiesen ist.
`-comment` (Optional)	Beschreibender Text für den öffentlichen Schlüssel. Schließen Sie den Text in doppelte Anführungszeichen ein.

Das folgende Beispiel verknüpft einen öffentlichen Schlüssel mit dem SVM-Administratorkonto `svmadmin` für die SVM. `svm01` Dem öffentlichen Schlüssel wird eine Indexnummer zugewiesen. 5

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J/
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

> **Important**
>
> Sie müssen SVM- oder Dateisystemadministrator sein, um diese Aufgabe ausführen zu können.

Migration zu Amazon FSx für NetApp ONTAP

Die folgenden Abschnitte enthalten Informationen zum Migrieren Ihrer vorhandenen NetApp ONTAP-Dateisysteme zu Amazon FSx für NetApp ONTAP.

> **Note**
>
> Wenn Sie planen, die `All` Tiering-Richtlinie zu verwenden, um Ihre Daten auf die Kapazitätspool-Ebene zu migrieren, denken Sie daran, dass Dateimetadaten immer auf der SSD-Ebene gespeichert sind und dass alle neuen Benutzerdaten zuerst auf die SSD-Ebene geschrieben werden. Wenn Daten in die SSD-Ebene geschrieben werden, beginnt der Hintergrund-Tiering-Prozess mit dem Tiering Ihrer Daten in den Kapazitätspool-Speicher, aber der Tiering-Prozess ist nicht sofort und verbraucht Netzwerkressourcen. Sie müssen Ihre SSD-Stufe so dimensionieren, dass sie Dateimetadaten (3–7 % der Größe der Benutzerdaten) als Puffer für Benutzerdaten berücksichtigt, bevor sie auf Kapazitätspoolspeicher gestaffelt wird. Wir empfehlen, die Auslastung Ihrer SSD-Stufe von 80 % nicht zu überschreiten.
> Achten Sie bei der Migration von Daten darauf, Ihre SSD-Ebene mithilfe von CloudWatch Dateisystemmetriken zu überwachen, um sicherzustellen, dass sie nicht schneller aufgefüllt wird, als der Tiering-Prozess Daten in den Kapazitätspoolspeicher verschieben kann.

Themen

- Migrieren zu FSx für ONTAP mit NetApp SnapMirror
- Migrieren zu FSx für ONTAP mit AWS DataSync

Migrieren zu FSx für ONTAP mit NetApp SnapMirror

Sie können Ihre NetApp ONTAP-Dateisysteme mit zu Amazon FSx für NetApp ONTAP migrieren NetApp SnapMirror.

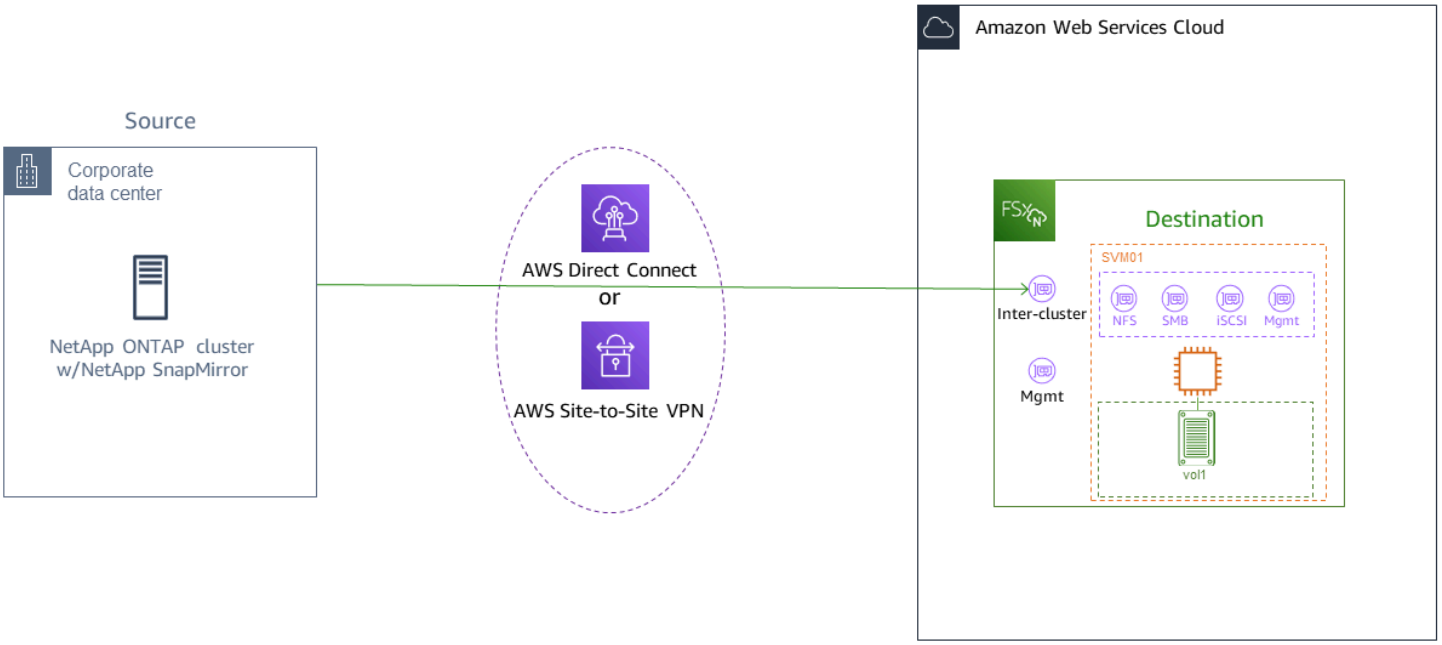
NetApp SnapMirror verwendet die Replikation auf Blockebene zwischen zwei ONTAP-Dateisystemen und repliziert Daten von einem angegebenen Quell-Volume auf ein Ziel-Volume. Wir empfehlen die Verwendung von SnapMirror , um On-Premises- NetApp ONTAP-Dateisysteme zu FSx für ONTAP zu migrieren. NetApp SnapMirrorDie Replikation auf Blockebene ist schnell und effizient, selbst für Dateisysteme mit:

- Komplexe Verzeichnisstrukturen
- Über 50 Millionen Dateien
- Sehr kleine Dateigrößen (in der Reihenfolge von Kilobyte)

Wenn Sie verwenden, SnapMirror um zu FSx für ONTAP zu migrieren, verbleiben deduplizierte und komprimierte Daten in diesen Zuständen, wodurch die Übertragungszeiten und die für die Migration erforderliche Bandbreite reduziert werden. Snapshots, die auf den ONTAP-Quell-Volumes vorhanden sind, werden beibehalten, wenn sie auf die Ziel-Volumes migriert werden. Die Migration Ihrer On-Premises- NetApp ONTAP-Dateisysteme zu FSx für ONTAP umfasst die folgenden allgemeinen Aufgaben:

1. Erstellen Sie das Ziel-Volume in Amazon FSx .
2. Erfassen Sie logische Quell- und Zielschnittstellen (LIFs).
3. Richten Sie Cluster-Peering zwischen den Quell- und Zieldateisystemen ein.
4. Erstellen Sie eine SVM-Peering-Beziehung.
5. Erstellen Sie die SnapMirror Beziehung.
6. Warten Sie einen aktualisierten Ziel-Cluster.
7. Wechseln Sie zu Ihrem FSx-für-ONTAP-Dateisystem.

Das folgende Diagramm veranschaulicht das in diesem Abschnitt beschriebene Migrationsszenario.



Themen

- Bevor Sie beginnen
- Erstellen des Ziel-Volumes
- Aufzeichnen der Quell- und Ziel-Cluster-übergreifenden LIFs
- Einrichten von Cluster-Peering zwischen Quelle und Ziel
- Erstellen einer SVM-Peering-Beziehung
- Erstellen der SnapMirror Beziehung
- Übertragen von Daten in Ihr FSx-für-ONTAP-Dateisystem
- Umstellung auf Amazon FSx

Bevor Sie beginnen

Bevor Sie mit den in den folgenden Abschnitten beschriebenen Verfahren beginnen, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllt haben:

- FSx für ONTAP priorisiert den Client-Datenverkehr gegenüber Hintergrundaufgaben wie Daten-Tiering, Speichereffizienz und Backups. Wir empfehlen Ihnen, bei der Migration von Daten und als allgemeine bewährte Methode die Kapazität Ihrer SSD-Ebene zu überwachen, um sicherzustellen, dass sie nicht mehr als 80 % ausgelastet ist. Sie können die Auslastung Ihrer SSD-Ebene mithilfe von CloudWatch Dateisystemmetriken überwachen. Weitere Informationen finden Sie unter Volume-Metriken.
- Wenn Sie die Daten-Tiering-Richtlinie des Ziel-Volumes `All` bei der Migration Ihrer Daten auf festlegen, werden alle Dateimetadaten auf der primären SSD-Speicherebene gespeichert. Dateimetadaten werden unabhängig von der Daten-Tiering-Richtlinie des Volumes immer auf der SSD-basierten primären Ebene gespeichert. Wir empfehlen Ihnen, ein Verhältnis von 1:10 für die Speicherkapazität der primären Ebene : Kapazitätspool-Ebene anzunehmen.
- Die Quell- und Zieldateisysteme sind in derselben VPC verbunden oder befinden sich in Netzwerken, die über Amazon VPC Peering, Transit Gateway AWS Direct Connect oder per Peering verbunden sindAWS VPN. Weitere Informationen finden Sie unter Zugriff auf Daten aus dem heraus AWS und Was ist VPC Peering? im Amazon-VPC-Peering-Handbuch.
- Die VPC-Sicherheitsgruppe für das FSx-für-ONTAP-Dateisystem verfügt über Regeln für ein- und ausgehenden Datenverkehr, die ICMP sowie TCP auf den Ports 443, 1000, 111104 und 111105 für Ihre Cluster-übergreifenden Endpunkte (LIFs) ermöglichen.

- Stellen Sie sicher, dass auf den Quell- und Ziel-Volumes kompatible NetApp ONTAP-Versionen ausgeführt werden, bevor Sie eine SnapMirror Datenschutzbeziehung erstellen. Weitere Informationen finden Sie unter Kompatible ONTAP-Versionen für SnapMirror Beziehungen in NetAppder ONTAP-Benutzerdokumentation von . Die hier vorgestellten Verfahren verwenden ein On-Premises- NetApp ONTAP-Dateisystem für die Quelle.
- Ihr On-Premises-Dateisystem (Quelle) NetApp ONTAP enthält eine SnapMirror Lizenz.
- Sie haben ein Ziel-FSx-für-ONTAP-Dateisystem mit einer SVM erstellt, aber Sie haben kein Ziel-Volume erstellt. Weitere Informationen finden Sie unter FSx für ONTAP-Dateisysteme erstellen.

Die Befehle in diesen Verfahren verwenden die folgenden Cluster-, SVM- und Volume-Aliase:

- *FSx-Dest* – die ID des Ziel-Clusters (FSx) (im Format F SxIdabcdef1234567890a).
- *OnPrem-Source* – die ID des Quell-Clusters.
- *DestSVM* – der SVM-Zielname.
- *SourceSVM* – der Quell-SVM-Name.
- Sowohl die Namen des Quell- als auch des Ziel-Volumes sind `vol1`.

> **Note**
>
> Ein FSx-für-ONTAP-Dateisystem wird in allen ONTAP-CLI-Befehlen als Cluster bezeichnet.

Die Verfahren in diesem Abschnitt verwenden die folgenden NetApp ONTAP-CLI-Befehle.

- -Volume-Befehl „Erstellen“
- -Cluster-Befehle
- vserver-Peer-Befehle
- Snapmirror-Befehle

Sie verwenden die NetApp ONTAP-CLI, um eine SnapMirror Konfiguration auf Ihrem FSx-für-ONTAP-Dateisystem zu erstellen und zu verwalten. Weitere Informationen finden Sie unter Verwenden der NetApp ONTAP-CLI.

Erstellen des Ziel-Volumes

Sie können ein Ziel-Volume für den Datenschutz (DP) mithilfe der Amazon-FSx-Konsole, der AWS CLIund der Amazon-FSx-API erstellen, zusätzlich zur NetApp ONTAP-CLI und REST-API. Informationen zum Erstellen eines Ziel-Volumes mit der Amazon-FSx-Konsole und finden Sie AWS CLIunter Volumen erstellen.

Im folgenden Verfahren verwenden Sie die NetApp ONTAP-CLI, um ein Ziel-Volume auf Ihrem FSx-für-ONTAP-Dateisystem zu erstellen. Sie benötigen das `fsxadmin` Passwort und die IP-Adresse oder den DNS-Namen des Verwaltungsports des Dateisystems.

1. Richten Sie eine SSH-Sitzung mit dem Zieldateisystem mithilfe des Benutzers `fsxadmin` und des Passworts ein, das Sie beim Erstellen des Dateisystems festgelegt haben.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Erstellen Sie ein Volume auf dem Ziel-Cluster, das über eine Speicherkapazität verfügt, die mindestens der Speicherkapazität des Quell-Volumes entspricht. Verwenden Sie `-type DP`, um sie als Ziel für eine SnapMirror Beziehung zu bezeichnen.

   Wenn Sie Daten-Tiering verwenden möchten, empfehlen wir Ihnen, `-tiering-policy` auf festzulegen`all`. Dadurch wird sichergestellt, dass Ihre Daten sofort in den Kapazitätspool-Speicher übertragen werden, und verhindert, dass Ihnen die Kapazität auf Ihrer SSD-Ebene ausgeht. Nach der Migration können Sie `-tiering-policy` zu wechseln`auto`.

   > **Note**
   >
   > Dateimetadaten werden unabhängig von der Daten-Tiering-Richtlinie des Volumes immer auf der SSD-basierten primären Ebene gespeichert.

   ```
   FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
   type DP -tiering-policy all
   ```

Aufzeichnen der Quell- und Ziel-Cluster-übergreifenden LIFs

SnapMirror verwendet logische Schnittstellen (LIFs) zwischen Clustern, die jeweils eine eindeutige IP-Adresse haben, um die Datenübertragung zwischen Quell- und Ziel-Clustern zu erleichtern.

1. Für die Ziel-FSx-für-ONTAP-Dateisysteme können Sie den Cluster-übergreifenden Endpunkt – IP-Adressen von der Amazon-FSx-Konsole abrufen, indem Sie auf der Detailseite Ihres Dateisystems zur Registerkarte Administration navigieren.
2. Rufen Sie für den NetApp ONTAP-Quell-Cluster die LIF-IP-Adressen zwischen Clustern mithilfe der ONTAP-CLI ab. Führen Sie den folgenden Befehl aus:

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

> **Note**
>
> Bei Scale-Out-Dateisystemen gibt es zwei Cluster-übergreifende IP-Adressen für jedes Hochverfügbarkeitspaar (HA). Speichern Sie diese Werte für später.

Speichern Sie die IP`inter_2`-Adressen `inter_1` und . Sie werden in der `FSx-Dest` als `dest_inter_1` und `dest_inter_2` und für `OnPrem-Source` als `source_inter_1` und referenziert`source_inter_2`.

Einrichten von Cluster-Peering zwischen Quelle und Ziel

Richten Sie eine Cluster-Peer-Beziehung auf dem Ziel-Cluster ein, indem Sie die IP-Adressen zwischen Clustern angeben. Sie müssen auch eine Passphrase erstellen, die Sie eingeben müssen, wenn Sie Cluster-Peering auf dem Quell-Cluster einrichten.

1. Richten Sie Peering auf dem Ziel-Cluster mit dem folgenden Befehl ein. Für Scale-Out-Dateisysteme müssen Sie jede Cluster-übergreifende IP-Adresse angeben.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
```

```
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. Richten Sie als Nächstes die Cluster-Peer-Beziehung auf dem Quell-Cluster ein. Sie müssen die oben erstellte Passphrase eingeben, um sich zu authentifizieren. Für Scale-Out-Dateisysteme müssen Sie jede Cluster-übergreifende IP-Adresse angeben.

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. Überprüfen Sie, ob das Peering erfolgreich war, indem Sie den folgenden Befehl auf dem Quell-Cluster verwenden. In der Ausgabe `Availability` sollte auf gesetzt werden`Available`.

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

Erstellen einer SVM-Peering-Beziehung

Wenn Cluster-Peering eingerichtet ist, besteht der nächste Schritt darin, die SVMs per Peering zu verbinden. Erstellen Sie mit dem `vserver peer` Befehl eine SVM-Peering-Beziehung auf dem Ziel-Cluster (FSx -Dest). Zusätzliche Aliase, die in den folgenden Befehlen verwendet werden, sind folgende:

- `DestLocalName` – Dies ist der Name, der verwendet wird, um die Ziel-SVM bei der Konfiguration von SVM-Peering auf der Quell-SVM zu identifizieren.
- `SourceLocalName` – Dies ist der Name, der zur Identifizierung der Quell-SVM bei der Konfiguration des SVM-Peerings auf der Ziel-SVM verwendet wird.

1. Verwenden Sie den folgenden Befehl, um eine SVM-Peering-Beziehung zwischen der Quell- und der Ziel-SVMs erstellen.

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName

 Info: [Job 207] 'vserver peer create' job queued
```

2. Akzeptieren Sie die Peering-Beziehung auf dem Quell-Cluster:

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. Überprüfen Sie den SVM-Peering-Status mit dem folgenden Befehl; `Peer State` sollte `peered` in der Antwort auf gesetzt werden.

```
OnPrem-Source::> vserver peer show

Peer    Peer     Peer   Peering  Remote
vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------ ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

Erstellen der SnapMirror Beziehung

Nachdem Sie nun die Quell- und Ziel-SVMs per Peering verbunden haben, bestehen die nächsten Schritte darin, die SnapMirror Beziehung auf dem Ziel-Cluster zu erstellen und zu initialisieren.

> **Note**
>
> Sobald Sie eine SnapMirror Beziehung erstellt und initialisiert haben, sind die Ziel-Volumes schreibgeschützt, bis die Beziehung unterbrochen ist.

- Verwenden Sie den `snapmirror create` Befehl , um die SnapMirror Beziehung auf dem Ziel-Cluster zu erstellen. Der `snapmirror create` Befehl muss von der Ziel-SVM aus verwendet werden.

  Sie können optional verwenden`-throttle`, um die maximale Bandbreite (in kB/s) für die SnapMirror Beziehung festzulegen.

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
path DestSVM:vol1 -vserver DestSVM -throttle unlimited

 Operation succeeded: snapmirror create for the relationship with destination
 "DestSVM:vol1".
```

Übertragen von Daten in Ihr FSx-für-ONTAP-Dateisystem

Nachdem Sie die SnapMirror Beziehung erstellt haben, können Sie Daten in das Zieldateisystem übertragen.

1. Sie können Daten in das Zieldateisystem übertragen, indem Sie den folgenden Befehl auf dem Zieldateisystem ausführen.

   > **Note**
   >
   > Sobald Sie diesen Befehl ausgeführt haben, SnapMirror beginnt mit der Übertragung von Snapshots von Daten vom Quell-Volume auf das Ziel-Volume.

   ```
   FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
   path SourceLocalName:vol1
   ```

2. Wenn Sie Daten migrieren, die aktiv verwendet werden, müssen Sie Ihren Ziel-Cluster aktualisieren, damit er mit Ihrem Quell-Cluster synchronisiert bleibt. Führen Sie den folgenden Befehl aus, um eine einmalige Aktualisierung des Ziel-Clusters durchzuführen.

   ```
   FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
   ```

3. Sie können auch stündliche oder tägliche Updates planen, bevor Sie die Migration abschließen und Ihre Clients zu FSx für ONTAP verschieben. Sie können einen SnapMirror Aktualisierungszeitplan mit dem `snapmirror modify` Befehl erstellen.

   ```
   FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
   ```

Umstellung auf Amazon FSx

Gehen Sie wie folgt vor, um den Cutover auf Ihr FSx-für-ONTAP-Dateisystem vorzubereiten:

- Trennen Sie alle Clients, die in den Quell-Cluster schreiben.
- Führen Sie eine endgültige SnapMirror Übertragung durch, um sicherzustellen, dass beim Cutover kein Datenverlust auftritt.
- Unterbrechen Sie die SnapMirror Beziehung.
- Verbinden Sie alle Clients mit Ihrem FSx-für-ONTAP-Dateisystem.

1. Um sicherzustellen, dass alle Daten aus dem Quell-Cluster in das FSx-für-ONTAP-Dateisystem übertragen werden, führen Sie eine endgültige Snapmirror-Übertragung durch.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. Stellen Sie sicher, dass die Datenmigration abgeschlossen ist`Snapmirrored`, indem Sie überprüfen, ob `Mirror State` auf und auf festgelegt `Relationship Status` ist`Idle`. Sie sollten auch sicherstellen, dass das `Last Transfer End Timestamp` Datum wie erwartet ist, da es anzeigt, wann die letzte Übertragung auf das Ziel-Volume stattgefunden hat.
3. Führen Sie den folgenden Befehl aus, um den SnapMirror Status anzuzeigen.

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      ---------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. Deaktivieren Sie alle zukünftigen SnapMirror Übertragungen mithilfe des `snapmirror quiesce` Befehls .

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. Stellen Sie sicher, dass sich der zu geändert `Relationship Status` hat, `Quiesced` indem Sie verwendensnapmirror show.

```
FSx-Dest::> snapmirror show

Source           Destination   Mirror        Relationship
```

```
Path             Path          State         Status
-----------      ------------  ------------ --------
sourcesvm1:vol1  svm01:DestVol Snapmirrored  Quiesced
```

6. Während der Migration ist das Ziel-Volume schreibgeschützt. Um das Lesen/Schreiben zu aktivieren, müssen Sie die SnapMirror Beziehung aufheben und auf Ihr FSx-für-ONTAP-Dateisystem umstellen. Unterbrechen Sie die SnapMirror Beziehung mit dem folgenden Befehl.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. Sobald die SnapMirror Replikation abgeschlossen ist und Sie die SnapMirror Beziehung unterbrochen haben, können Sie das Volume mounten, um die Daten verfügbar zu machen.

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

Das Volume ist jetzt verfügbar, wobei die Daten aus dem Quell-Volume vollständig auf das Ziel-Volume migriert wurden. Das Volume steht Clients auch zum Lesen und Schreiben zur Verfügung. Wenn Sie das `tiering-policy` dieses Volumes zuvor auf gesetzt haben`all`, können Sie es in `auto` oder ändern `snapshot-only` und Ihre Daten werden gemäß den Zugriffsmustern automatisch zwischen den Speicherebenen wechseln. Informationen zum Zugriff auf diese Daten für Clients und Anwendungen finden Sie unter Zugriff auf -Daten.

Migrieren zu FSx für ONTAP mit AWS DataSync

Wir empfehlen die Verwendung von , AWS DataSync um Daten zwischen FSx-für-ONTAP-Dateisystemen und Nicht-ONTAP-Dateisystemen zu übertragen, einschließlich FSx for Lustre, FSx for OpenZFS , FSx for Windows File Server, Amazon EFS , Amazon S3 und On-Premises-Dateisystemen. Wenn Sie Dateien zwischen FSx für ONTAP und NetApp ONTAP übertragen, empfehlen wir die Verwendung von NetApp SnapMirror. AWS DataSync ist ein Datenübertragungsservice, der das Verschieben und Replizieren von Daten zwischen selbstverwalteten Speichersystemen und AWS Speicherservices über das Internet vereinfacht, automatisiert und beschleunigt oder AWS Direct Connect. DataSync kann Ihre Dateisystemdaten und Metadaten wie Eigentum, Zeitstempel und Zugriffsberechtigungen übertragen.

Sie können verwenden DataSync , um Dateien zwischen zwei FSx-für-ONTAP-Dateisystemen zu übertragen und Daten auch in ein Dateisystem in einem anderen - AWS-Region oder -AWSKonto zu

verschieben. Sie können auch DataSync mit FSx-für-ONTAP-Dateisystemen 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 ist DataSyncein Speicherort ein Endpunkt für ein FSx-für-ONTAP-Dateisystem. Informationen zu bestimmten Übertragungsszenarien finden Sie unter Arbeiten mit Standorten im AWS DataSync -Benutzerhandbuch.

> **Note**
>
> Wenn Sie planen, die `All` Tiering-Richtlinie zu verwenden, um Ihre Daten auf die Kapazitätspool-Ebene zu migrieren, denken Sie daran, dass Dateimetadaten immer auf der SSD-Ebene gespeichert sind und dass alle neuen Benutzerdaten zuerst auf die SSD-Ebene geschrieben werden. Wenn Daten in die SSD-Ebene geschrieben werden, beginnt der Hintergrund-Tiering-Prozess mit dem Tiering Ihrer Daten in den Kapazitätspool-Speicher, aber der Tiering-Prozess ist nicht sofort und verbraucht Netzwerkressourcen. Sie müssen Ihre SSD-Stufe so dimensionieren, dass sie Dateimetadaten (3–7 % der Größe der Benutzerdaten) als Puffer für Benutzerdaten berücksichtigt, bevor sie auf Kapazitätspoolspeicher gestaffelt wird. Wir empfehlen, eine SSD-Auslastung von 80 % nicht zu überschreiten.
> Achten Sie bei der Migration von Daten darauf, Ihre SSD-Ebene mithilfe von CloudWatch Dateisystemmetriken zu überwachen, um sicherzustellen, dass sie nicht schneller aufgefüllt wird, als der Tiering-Prozess Daten in den Kapazitätspoolspeicher verschieben kann. Sie können DataSync Übertragungen auch auf eine Rate drosseln, die niedriger ist als die Rate, mit der Tiering stattfindet, um sicherzustellen, dass Ihre SSD-Stufe eine Auslastung von 80 % nicht überschreitet. Bei Dateisystemen mit einer Durchsatzkapazität von mindestens 512 MBpss gleicht eine Drosselung von 200 MBps beispielsweise die Datenübertragungs- und Datenübertragungs-Tiering-Raten aus.

Voraussetzungen

Um Daten in Ihr FSx-für-ONTAP-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.

Grundlegende Schritte für die Migration von Dateien mit DataSync

Das Übertragen von Dateien von einer Quelle an ein Ziel mit DataSync umfasst die folgenden grundlegenden Schritte:

- Laden Sie einen Agenten herunter, stellen Sie ihn in Ihrer Umgebung bereit und aktivieren Sie ihn (nicht erforderlich, wenn Sie zwischen übertragenAWS-Services).
- Erstellen Sie einen Quell- und Zielspeicherort.
- Erstellen Sie eine Aufgabe.
- Führen Sie die Aufgabe aus, um Dateien von der Quelle zum Ziel zu übertragen.

Weitere Informationen finden Sie in folgenden Themen im AWS DataSync-Benutzerhandbuch:

- Datenübertragung zwischen selbstverwaltetem Speicher und AWS
- Erstellen eines Speicherorts für Amazon FSx für NetApp ONTAP

Überwachen von Amazon FSx für NetApp ONTAP

Sie können die folgenden Services und Tools verwenden, um die Nutzung und Aktivität von Amazon FSx auf NetApp ONTAP zu überwachen:

- Amazon CloudWatch – Sie können Dateisysteme mit Amazon überwachen CloudWatch, das automatisch Rohdaten von FSx für ONTAP sammelt und zu lesbaren Metriken verarbeitet. Diese Statistiken werden für einen Zeitraum von 15 Monaten aufbewahrt, damit Sie auf historische Informationen zugreifen und sehen können, wie Ihr Dateisystem funktioniert. Sie können auch Alarme basierend auf Ihren Metriken über einen bestimmten Zeitraum festlegen und eine oder mehrere Aktionen basierend auf dem Wert der Metriken relativ zu den von Ihnen angegebenen Schwellenwerten ausführen.
- ONTAP -Ereignisse – Sie können Ihr FSx-für-ONTAP-Dateisystem überwachen, indem Sie Ereignisse verwenden, die vom ONTAP Events Management System (Speed) generiert wurden. sind Benachrichtigungen über Vorkommen in Ihrem Dateisystem, z. B. die iSCSI-LUN-Erstellung oder die automatische Größenanpassung von Volumes.
- NetApp Cloud Insights – Sie können Konfigurations-, Kapazitäts- und Leistungsmetriken für Ihre FSx-für-ONTAP-Dateisysteme mit dem NetApp Cloud-Insights-Service überwachen. Sie können Warnungen auch basierend auf Metrikbedingungen erstellen.
- NetApp Bolvest und NetApp Grafana – Sie können Ihr FSx-für-ONTAP-Dateisystem mithilfe von NetApp Bolvest und NetApp Grafana überwachen. NetApp Harvest überwacht ONTAP-Dateisysteme, indem es Leistungs-, Kapazitäts- und Hardwaremetriken von FSx-für-ONTAP-Dateisystemen sammelt. Grafana bietet ein Dashboard, in dem die erfasstenvest-Metriken angezeigt werden können.
- AWS CloudTrail – Sie können verwenden AWS CloudTrail , um alle API-Aufrufe für Amazon FSx als Ereignisse zu erfassen. Diese Ereignisse bieten eine Aufzeichnung der von einem Benutzer, einer Rolle oder AWS einem Service in Amazon FSx durchgeführten Aktionen.

Themen

- Überwachung mit Amazon CloudWatch
- Überwachen der Workload-Balance von FSx für ONTAP
- Überwachen von FSx-für-ONTAP- -Ereignissen
- Überwachung mit Cloud Insights
- Überwachen von FSx-für-ONTAP-Dateisystemen mitvest und Grafana

- Protokollieren von FSx für ONTAP-API-Aufrufe mitAWS CloudTrail

Überwachung mit Amazon CloudWatch

Sie können Dateisysteme mit Amazon überwachen CloudWatch, das Rohdaten von Amazon FSx für NetApp ONTAP sammelt und in lesbare Metriken verarbeitet, die nahezu in Echtzeit vorliegen. Diese Statistiken werden für einen Zeitraum von 15 Monaten aufbewahrt, sodass Sie auf historische Informationen zugreifen können, um die Leistung Ihres Dateisystems zu bestimmen. Metrikdaten von FSx für ONTAP werden standardmäßig automatisch CloudWatch in Abständen von 1 Minute an gesendet. Weitere Informationen zu CloudWatchfinden Sie unter Was ist Amazon CloudWatch? im Amazon- CloudWatch Benutzerhandbuch.

> **Note**
>
> Standardmäßig sendet FSx für ONTAP Metrikdaten an CloudWatch in Abständen von 1 Minute, mit Ausnahme der folgenden Metriken, die in Intervallen von 5 Minuten gesendet werden:
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch -Metriken für FSx für ONTAP sind in vier Kategorien unterteilt, die durch die Dimensionen definiert werden, die zum Abfragen jeder Metrik verwendet werden. Weitere Informationen zu Dimensionen finden Sie unter Dimensionen im Amazon- CloudWatch Benutzerhandbuch.

- Dateisystemmetriken: F-ile-system-level Leistungs- und Speicherkapazitätsmetriken.
- Detaillierte Dateisystemmetriken: F-ile-system-level Speichermetriken pro Speicherebene (SSD und Kapazitätspool).
- Volume-Metriken: Metriken zur Leistung und Speicherkapazität pro Volume.
- Detaillierte Volume-Metriken: Metriken zur Speicherkapazität pro Volume nach Speicherebene oder nach Datentyp (Benutzer, Snapshot oder andere).

Alle CloudWatch Metriken für FSx für ONTAP werden im `AWS/FSx` Namespace in veröffentlicht CloudWatch.

Themen

- So verwenden Sie FSx für ONTAP CloudWatch-Metriken
- Zugreifen auf CloudWatch Metriken
- Dateisystemmetriken
- Aufskalieren von Dateisystemmetriken
- Volume-Metriken
- Leistungswarnungen und Empfehlungen
- Erstellen von Amazon- CloudWatch Alarmen zur Überwachung von Amazon FSx

So verwenden Sie FSx für ONTAP CloudWatch-Metriken

Die von Amazon FSx gemeldeten CloudWatch Metriken liefern wertvolle Informationen über Ihre FSx-für-ONTAP-Dateisysteme und -Volumes.

Themen

- Überwachen von Dateisystemmetriken in der Amazon-FSx-Konsole
- Überwachen von Volume-Metriken in der Amazon-FSx-Konsole

Überwachen von Dateisystemmetriken in der Amazon-FSx-Konsole

Sie können das Bedienfeld Überwachung und Leistung im Dashboard Ihres Dateisystems in der Amazon-FSx-Konsole verwenden, um die in der folgenden Tabelle beschriebenen Metriken anzuzeigen. Weitere Informationen finden Sie unter Zugreifen auf CloudWatch Metriken.

Überwachung und Leistung	Wie kann ich ...	Tabelle	Relevante Metriken
Übersicht	... die Menge der verfügbaren Speicherkapazität in meinem Dateisystem ermitteln?	Verfügbare primäre Speicherkapazität (Byte)	`StorageCapacity {SSD} - StorageUsed {SSD}`

Überwachung und Leistung	Wie kann ich ...	Tabelle	Relevante Metriken
	... den Gesamtdurchsatz meines Dateisystems ermitteln?	Gesamter Client-Durchsatz (Byte/Sekunde)	SUM(`DataReadBytes + DataWriteBytes`)/ PERIOD (in Sekunden)
	... die Gesamt-Client-IOPS meines Dateisystems ermitteln?	Gesamt-Client-IOPS (Operationen/ Sekunde)	SUM(`DataReadOperations + DataWriteOperations + MetadataOperations`)/PERIOD (in Sekunden)
	... die durchschnittliche Latenz für die Lese-, Schreib- und Metadatenoperationen meines Dateisystems ermitteln?	Durchschnittliche Latenz (ms/ operation)	Durchschnittliche Leselatenz: `DataReadOperationTime * 1000/DataReadOperations` Durchschnittliche Schreiblatenz: `DataWriteOperationTime * 1000/DataWriteOperations` Durchschnittliche Metadatenlatenz: `MetadataOperationTime * 1000/MetadataOperations`

Überwachung und Leistung	Wie kann ich ...	Tabelle	Relevante Metriken
	... die Verteilung der verwendeten und freien Speicherkapazität auf meinem Dateisystem bestimmen?	Speicherverteilung	Primäre Stufe verfügbar: `StorageCapacity {SSD} – StorageUsed {SSD}` Verwendete primäre Stufe: `StorageUsed {SSD}` Verwendeter Kapazität spool: `StorageUsed {StandardCapacityPool }`
	... die Einsparungen durch Speichereffizienzen (Komprimierung, Deduplizierung und Verdichtung) ermitteln?	Einsparungen bei der Speichereffizienz	`StorageEfficiencySavings`
	... zu bestimmen, wie viel Primärspeicher verfügbar ist?	Verfügbare primäre Speicherkapazität (Byte)	`StorageCapacity {SSD} - StorageUsed {SSD}`
Speiche	... den Prozentsatz des verwendeten Primärspeichers für mein Dateisystem ermitteln?	Primäre Speicherkapazitätsauslastung (Prozent)	`StorageCapacity {SSD} * 100/StorageUsed {SSD}`

Überwachung und Leistung	Wie kann ich ...	Tabelle	Relevante Metriken
Dateiserver-Leistung	... festzustellen, ob sich mein Dateisystem seinem Netzwerkdurchsatzlimit nähert?	Netzwerkdurchsatz – Auslastung (Prozent)	`NetworkThroughputUtilization`
	... festzustellen, ob sich mein Dateisystem seinem Festplattendurchsatzlimit nähert?	Festplattendurchsatz – Auslastung (Prozent)	`FileServerDiskThroughputUtilization`
	... Feststellen, ob mein Dateisystem sein zulässiges Burst-Guthaben für den Festplattendurchsatz ausgeschöpft hat?	Festplattendurchsatz – Burst-Balance (Prozent)	`FileServerDiskThroughputBalance`
	... festzustellen, ob sich mein Dateisystem dem SSD-IOPS-Limit seiner Dateiserver nähert?	Festplatten-IOPS – Auslastung (Prozent)	`FileServerDiskIopsUtilization`

Überwachung und Leistung	Wie kann ich ...	Tabelle	Relevante Metriken
	... festzustellen, ob mein Dateisystem die zulässigen Burst-Guthaben für Festplatten-SSD-IOPS seiner Dateiserver ausgeschöpft hat?	Festplatten-IOPS – Burst-Balance (Prozent)	`FileServerDiskIopsBalance`
	... die durchschnittliche Auslastung der CPU des Dateisystems ermitteln?	CPU-Auslastung (Prozent)	`CPUUtilization`
	... festzustellen, ob meine Workload die RAM- und NVMe-Lese-Caches meines Dateisystems effizient nutzt?	Cache-Trefferverhältnis (Prozent)	`FileServerCacheHitRatio`
Festplattenleistung	... festzustellen, ob sich mein Dateisystem seiner derzeit bereitgestellten SSD-IOPS-Kapazität nähert?	Festplatten-IOPS – Auslastung (SSD) (Prozent)	`DiskIopsUtilization`

> **Note**
>
> Wir empfehlen Ihnen, eine durchschnittliche Durchsatzkapazitätsauslastung aller leistungsbezogenen Dimensionen wie Netzwerkauslastung, CPU-Auslastung und SSD-IOPS-Auslastung auf unter 50 % zu halten. Dadurch wird sichergestellt, dass Sie über genügend freie Durchsatzkapazität für unerwartete Spitzen in Ihrem Workload sowie für alle

Hintergrundspeichervorgänge (wie Speichersynchronisierung, Daten-Tiering oder Backups) verfügen.

Überwachen von Volume-Metriken in der Amazon-FSx-Konsole

Sie können den Bereich Überwachung im Dashboard Ihres Volumes in der Amazon-FSx-Konsole anzeigen, um zusätzliche Leistungsmetriken anzuzeigen. Weitere Informationen finden Sie unter Zugreifen auf CloudWatch Metriken.

Überwachen	Wie kann ich ...	Tabelle	Relevante Metriken
	... die verfügbare Speicherkapazität meines Volumes ermitteln?	Verfügbare Speicherkapazität	`StorageCapacity`
	... den gesamten Client-Durchsatz meines Volumes ermitteln?	Gesamter Client-Durchsatz (Byte/Sekunde)	SUM(`DataReadBytes` + `DataWriteBytes`)/ PERIOD (in Sekunden)
	... die Gesamt-Client-IOPS meines Volumes ermitteln?	Gesamt-Client-IOPS (Operationen/ Sekunde)	SUM(`DataReadOperations` + `DataWriteOperations` + `MetadataOperations`)/PERIOD (in Sekunden)
	... bestimmen, wie viele Lese- und Schreibvorgänge von der Kapazitätspool-Ebene kommen oder diese erreichen?	Kapazitätspool-IOPS (Operationen/ Sekunde)	Lesevorgänge: `CapacityPoolReadOperations` Schreibvorgänge: `CapacityPoolWriteOperations`

Überwac n	Wie kann ich ...	Tabelle	Relevante Metriken
	... die durchschnittliche Latenz für die Lese-, Schreib- und Metadatenoperationen meines Volumes ermitteln?	Durchschnittliche Latenz (ms/ operation)	Durchschnittliche Leselatenz: `DataReadOperationTime * 1000/DataReadOperations` Durchschnittliche Schreiblatenz: `DataWriteOperationTime * 1000/DataWriteOperations` Durchschnittliche Metadatenlatenz: `MetadataOperationTime * 1000/MetadataOperations`
	... die Anzahl der Dateien oder Knoten ermitteln, die auf meinem Volume verfügbar sind?	Verfügbare Dateien (Oliden)	`FilesCapacity - FilesUsed`
	... die Verteilung der verwendeten und freien Speicherkapazität auf meinem Volume bestimmen?	Speicherverteilung	`StorageCapacity - StorageUsed`

Zugreifen auf CloudWatch Metriken

Sie können Amazon- CloudWatch Metriken für Amazon FSx wie folgt anzeigen:

- Die Amazon-FSx-Konsole
- Die Amazon- CloudWatch Konsole
- Die AWS Command Line Interface (AWS CLI) für CloudWatch
- Die CloudWatch API

Im folgenden Verfahren wird erläutert, wie Sie die CloudWatch Metriken Ihres Dateisystems mit der Amazon-FSx-Konsole anzeigen.

So zeigen Sie CloudWatch Metriken für Ihr Dateisystem mit der Amazon-FSx-Konsole an

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich Dateisysteme und dann das Dateisystem aus, dessen Metriken Sie anzeigen möchten.
3. Wählen Sie auf der Seite Zusammenfassung im zweiten Bereich Überwachung und Leistung aus, um Diagramme für die Metriken Ihres Dateisystems anzuzeigen.

Es gibt vier Registerkarten im Bereich Überwachung und Leistung.

- Wählen Sie Zusammenfassung (Standardregisterkarte), um alle aktiven Warnungen, CloudWatch Alarme und Diagramme für Dateisystemaktivitäten anzuzeigen.
- Wählen Sie Speicher, um Speicherkapazitäts- und Auslastungsmetriken anzuzeigen.
- Wählen Sie Leistung, um die Metriken zur Dateiserver- und Speicherleistung anzuzeigen.
- Wählen Sie CloudWatch Alarme aus, um Diagramme aller Alarme anzuzeigen, die für Ihr Dateisystem konfiguriert sind.

Im folgenden Verfahren wird erläutert, wie Sie die CloudWatch Metriken Ihres Volumes mit der Amazon-FSx-Konsole anzeigen.

So zeigen Sie CloudWatch Metriken für Ihr Volume mit der Amazon-FSx-Konsole an

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich Volumes und dann das Volume aus, dessen Metriken Sie anzeigen möchten.
3. Wählen Sie auf der Seite Zusammenfassung im zweiten Bereich Überwachung (Standardregisterkarte), um Diagramme für die Metriken Ihres Volumes anzuzeigen.

Im folgenden Verfahren wird erläutert, wie Sie die CloudWatch Metriken Ihres Dateisystems mit der Amazon- CloudWatch Konsole anzeigen.

So zeigen Sie Metriken mit der Amazon- CloudWatch Konsole an

1. Wählen Sie auf der Seite Zusammenfassung Ihres Dateisystems im zweiten Bereich Überwachung und Leistung aus, um Diagramme für die Metriken Ihres Dateisystems anzuzeigen.
2. Wählen Sie im Aktionsmenü oben rechts im Diagramm, das Sie in der Amazon-Konsole anzeigen möchten, die Option In Metriken anzeigen aus. CloudWatch Dadurch wird die Seite Metriken in der Amazon- CloudWatch Konsole geöffnet.

Im folgenden Verfahren wird erläutert, wie Sie FSx-für-ONTAP-Dateisystemmetriken zu einem Dashboard in der Amazon- CloudWatch Konsole hinzufügen.

So fügen Sie Metriken zu einer Amazon- CloudWatch Konsole hinzu

1. Wählen Sie im Bereich Überwachung und Leistung der Amazon-FSx-Konsole die Metrikgruppe (Zusammenfassung , Speicher oder Leistung) aus. FSx
2. Wählen Sie oben rechts im Bereich Zum Dashboard hinzufügen aus. Dadurch wird die Amazon-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 Amazon- CloudWatch Dashboards im Amazon- CloudWatch Benutzerhandbuch.

Im folgenden Verfahren wird erläutert, wie Sie mit der auf die Metriken Ihres Dateisystems zugreifen AWS CLI.

So greifen Sie über die auf Metriken zu AWS CLI

- Verwenden Sie den CLI-Befehl CloudWatch list-metrics mit dem `--namespace "AWS/FSx"` Parameter . Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

Im folgenden Verfahren wird erläutert, wie Sie mit der - CloudWatch API auf die Metriken Ihres Dateisystems zugreifen.

So greifen Sie über die CloudWatch API auf Metriken zu

- Rufen Sie den GetMetricStatistics-API-Vorgang auf. Weitere Informationen finden Sie in der Amazon CloudWatch -API-Referenz .

Dateisystemmetriken

Ihre Amazon-FSx-für- NetApp ONTAP-Dateisystemmetriken werden entweder als Dateisystemmetriken oder Detaillierte Dateisystemmetriken klassifiziert.

- Dateisystemmetriken sind aggregierte Leistungs- und Speichermetriken für ein einzelnes Dateisystem, die eine einzelne Dimension annehmen, `FileSystemId`. Diese Metriken messen die Netzwerkleistung und die Speicherkapazitätsnutzung für Ihr Dateisystem.
- Detaillierte Dateisystemmetriken messen die Speicherkapazität und den verwendeten Speicher Ihres Dateisystems in jeder Speicherebene (z. B. SSD-Speicher und Kapazitätspool-Speicher). Jede Metrik enthält eine Dimension `StorageTier`, und `FileSystemIdDataType`.

Beachten Sie Folgendes darüber, wann Amazon FSx Datenpunkte für diese Metriken in veröffentlicht CloudWatch:

- Für die Auslastungsmetriken (jede Metrik, deren Name auf Auslastung endet, z. B. `NetworkThroughputUtilization`) wird für jeden aktiven Dateiserver oder Aggregat ein Datenpunkt ausgegeben. Amazon FSx gibt beispielsweise eine Metrik pro Minute pro aktivem Dateiserver für `FileServerDiskIopsUtilization`und eine Metrik pro Minute pro Aggregat für aus`DiskIopsUtilization`.
- Für alle anderen Metriken wird in jedem Zeitraum ein einzelner Datenpunkt ausgegeben, der dem Gesamtwert der Metrik über alle Ihre aktiven Dateiserver (z. B. `DataReadBytes` für Dateiservermetriken) oder alle Ihre Aggregate (z. B. `DiskReadBytes` für Speichermetriken) hinweg entspricht.

Themen

- Netzwerk-E/A-Metriken
- Dateiserver-Metriken
- Festplatten-I/O-Metriken
- Speicherkapazitätsmetriken
- Detaillierte Dateisystemmetriken

Netzwerk-E/A-Metriken

Alle diese Metriken haben eine Dimension, `FileSystemId`.

Metrik	Beschreibung
`NetworkThroughputUtilization`	Die prozentuale Auslastung des Netzwerkd urchsatzes für das Dateisystem. Die Statistik ist die `Average` durchschnittliche Netzwerkdurchsatzauslastung des Dateisyst ems über einen bestimmten Zeitraum. Die `Minimum` Statistik ist die niedrigste Netzwerkdurchsatzauslastung des Dateisyst ems über einen bestimmten Zeitraum. Die `Maximum` Statistik ist die höchste Netzwerkdurchsatzauslastung des Dateisyst ems über einen bestimmten Zeitraum. Einheiten: Prozent Gültige Statistiken: `Average`, `Minimum`, und `Maximum`
`NetworkSentBytes`	Die Anzahl der vom Dateisystem gesendeten Bytes (Netzwerk-E/A). Die `Sum` Statistik ist die Gesamtzahl der Bytes, die über einen bestimmten Zeitraum vom Dateisystem gesendet wurden. Um den gesendeten Durchsatz (Byte pro Sekunde) für eine beliebige Statistik zu berechnen, teilen Sie die Statistik durch die Sekunden im angegebenen Zeitraum. Einheiten: Byte Gültige Statistiken: `Sum`
`NetworkReceivedBytes`	Die Anzahl der vom Dateisystem empfangenen Bytes (Netzwerk-I/O).

Metrik	Beschreibung
	Die Sum Statistik ist die Gesamtzahl der Bytes, die das Dateisystem über einen bestimmten Zeitraum empfangen hat. Um den empfangenen Durchsatz (Byte pro Sekunde) für eine beliebige Statistik zu berechnen, dividieren Sie die Statistik durch die Sekunden im angegebenen Zeitraum. Einheiten: Byte Gültige Statistiken: Sum
DataReadBytes	Die Anzahl der Bytes (Netzwerk-E/A) von Lesevorgängen durch Clients zum Dateisyst em. Die Statistik ist die Gesamtzahl der BytesSum, die während des angegebenen Zeitraums mit Lesevorgängen verknüpft sind. Um den durchschnittlichen Durchsatz (Byte pro Sekunde) für einen Zeitraum zu berechnen, dividieren Sie die Sum Statistik durch die Anzahl der Sekunden im angegebenen Zeitraum. Einheiten: Byte Gültige Statistiken: Sum

Metrik	Beschreibung
`DataWriteBytes`	Die Anzahl der Bytes (Netzwerk-E/A) von Schreibvorgängen durch Clients in das Dateisystem. Die Statistik ist die Gesamtzahl der Bytes`Sum`, die während des angegebenen Zeitraums mit Schreibvorgängen verknüpft sind. Um den durchschnittlichen Durchsatz (Byte pro Sekunde) für einen Zeitraum zu berechnen, dividieren Sie die `Sum` Statistik durch die Anzahl der Sekunden im angegebenen Zeitraum. Einheiten: Byte Gültige Statistiken: `Sum`
`DataReadOperations`	Die Anzahl der Lesevorgänge (Netzwerk-E/A) von Lesevorgängen durch Clients zum Dateisystem. Die `Sum` Statistik ist die Gesamtzahl der E/A-Operationen, die über einen bestimmten Zeitraum stattgefunden haben. Um die `Sum` durchschnittlichen Lesevorgänge pro Sekunde für einen Zeitraum zu berechnen, dividieren Sie die Statistik durch die Anzahl der Sekunden im angegebenen Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`

Metrik	Beschreibung
`DataWriteOperations`	Die Anzahl der Schreibvorgänge (Netzwerk-E/A) von Schreibvorgängen durch Clients in das Dateisystem. Die `Sum` Statistik ist die Gesamtzahl der E/A-Operationen, die über einen bestimmte n Zeitraum stattgefunden haben. Um die `Sum` durchschnittlichen Schreibvorgänge pro Sekunde für einen Zeitraum zu berechnen, dividieren Sie die Statistik durch die Anzahl der Sekunden im angegebenen Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`
`MetadataOperations`	Die Anzahl der Metadatenoperationen (Netzwerk-E/A) durch Clients für das Dateisyst em. Die `Sum` Statistik ist die Gesamtzahl der E/A-Operationen, die über einen bestimmten Zeitraum stattgefunden haben. Um die `Sum` durchschnittlichen Metadatenoperationen pro Sekunde für einen Zeitraum zu berechnen, dividieren Sie die Statistik durch die Anzahl der Sekunden im angegebenen Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`

Metrik	Beschreibung
DataReadOperationTime	Die Gesamtzeit, die Clients im Dateisystem für Lesevorgänge (Netzwerk-E/A) auf Daten im Dateisystem zugreifen. Die Sum Statistik ist die Gesamtzahl der Sekunden, die von Lesevorgängen während des angegebenen Zeitraums aufgewend et wurden. Um die Sum durchschnittliche Leselatenz für einen Zeitraum zu berechnen , dividieren Sie die Statistik durch die Sum der DataReadOperations Metrik über denselben Zeitraum. Einheiten: Sekunden Gültige Statistiken: Sum
DataWriteOperationTime	Die Gesamtzeit, die Clients, die auf Daten im Dateisystem zugreifen, im Dateisystem für die Ausführung von Schreibvorgängen (Netzwerk-E/A) aufwenden. Die Statistik ist die Gesamtzahl der SekundenSum, die von Schreibvorgängen während des angegebenen Zeitraums aufgewendet wurden. Um die Sum durchschn ittliche Schreiblatenz für einen Zeitraum zu berechnen, dividieren Sie die Statistik durch die Sum der DataWriteOperations Metrik über denselben Zeitraum. Einheiten: Sekunden Gültige Statistiken: Sum

Metrik	Beschreibung
`CapacityPoolReadBytes`	Die Anzahl der aus der Kapazitätspool-Ebene des Dateisystems gelesenen Bytes (Netzwerk-I/O). Um die Datenintegrität zu gewährleisten, führt ONTAP unmittelbar nach der Ausführung eines Schreibvorgangs einen Lesevorgang für den Kapazitätspool durch. Die `Sum` Statistik ist die Gesamtzahl der Bytes, die über einen bestimmten Zeitraum aus der Kapazitätspool-Ebene des Dateisystems gelesen wurden. Um die Bytes des Kapazität spools pro Sekunde zu berechnen, dividiere n Sie die `Sum` Statistik durch die Sekunden in einem bestimmten Zeitraum. Einheiten: Byte Gültige Statistiken: `Sum`

Metrik	Beschreibung
`CapacityPoolReadOperations`	Die Anzahl der Lesevorgänge (Netzwerk-E/A) aus der Kapazitätspool-Ebene des Dateisyst ems. Dies wird in eine Leseanforderung für den Kapazitätspool übersetzt. Um die Datenintegrität zu gewährleisten, führt ONTAP unmittelbar nach der Ausführung eines Schreibvorgangs einen Lesevorgang für den Kapazitätspool durch. Die `Sum` Statistik ist die Gesamtzahl der Lesevorgänge aus der Kapazitätspool-Ebe ne des Dateisystems über einen bestimmten Zeitraum. Um Kapazitätspool-Anforderunge n pro Sekunde zu berechnen, teilen Sie die `Sum` Statistik durch die Sekunden in einem bestimmten Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`

Metrik	Beschreibung
`CapacityPoolWriteBytes`	Die Anzahl der Bytes, die auf die Kapazität spool-Ebene des Dateisystems geschrieben wurden (Netzwerk-E/A). Um die Datenintegrität zu gewährleisten, führt ONTAP unmittelbar nach der Ausführung eines Schreibvorgangs einen Lesevorgang für den Kapazitätspool durch. Die `Sum` Statistik ist die Gesamtzahl der Bytes, die über einen bestimmten Zeitraum auf die Kapazitätspool-Ebene des Dateisyst ems geschrieben wurden. Um die Bytes des Kapazitätspools pro Sekunde zu berechnen, teilen Sie die `Sum` Statistik durch die Sekunden in einem bestimmten Zeitraum. Einheiten: Byte Gültige Statistiken: `Sum`

Metrik	Beschreibung
`CapacityPoolWriteOperations`	Die Anzahl der Schreibvorgänge (Netzwerk -E/A) für das Dateisystem von der Kapazität spool-Ebene aus. Dies wird in eine Schreiban forderung übersetzt. Um die Datenintegrität zu gewährleisten, führt ONTAP unmittelbar nach der Ausführung eines Schreibvorgangs einen Lesevorgang für den Kapazitätspool durch. Die `Sum` Statistik ist die Gesamtzahl der Schreibvorgänge auf die Kapazitätspool-Ebe ne des Dateisystems über einen bestimmten Zeitraum. Um Kapazitätspool-Anforderunge n pro Sekunde zu berechnen, teilen Sie die `Sum` Statistik durch die Sekunden in einem bestimmten Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`

Dateiserver-Metriken

Alle diese Metriken haben eine Dimension, `FileSystemId`.

Metrik	Beschreibung
`CPUUtilization`	Die prozentuale Auslastung der CPU-Resso urcen des Dateisystems. Die Statistik ist die `Average` durchschnittliche CPU-Auslastung des Dateisystems über einen bestimmten Zeitraum.

Metrik	Beschreibung
	Die `Minimum` Statistik ist die niedrigste CPU-Auslastung des Dateisystems über einen bestimmten Zeitraum. Die `Maximum` Statistik ist die höchste CPU-Auslastung des Dateisystems über einen bestimmten Zeitraum. Einheiten: Prozent Gültige Statistiken: `Average`, `Minimum`, und `Maximum`
`FileServerDiskThroughputUtilization`	Der Festplattendurchsatz zwischen Ihrem Dateiserver und der primären Ebene als Prozentsatz des bereitgestellten Grenzwerts, der durch die Durchsatzkapazität bestimmt wird. Die Statistik ist die `Average` durchschnittliche prozentuale Auslastung des Festplattendurchsatzes der Dateiserver über einen bestimmten Zeitraum. Die `Minimum` Statistik ist die niedrigste prozentuale Auslastung des Festplattendurchsatzes der Dateiserver über einen bestimmten Zeitraum. Die `Maximum` Statistik ist die höchste Auslastung des Festplattendurchsatzes der Dateiserver über einen bestimmten Zeitraum. Einheiten: Prozent Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Metrik	Beschreibung
`FileServerDiskThroughputBalance`	Der Prozentsatz der verfügbaren Burst-Gut haben für den Festplattendurchsatz zwischen Ihrem Dateiserver und der primären Stufe. Dies gilt für Dateisysteme, die mit einer Durchsatz kapazität von 512 MBpss oder weniger bereitgestellt werden. Die Statistik ist die `Average` durchschnittliche Burst-Balance, die über einen bestimmten Zeitraum verfügbar ist. Die `Minimum` Statistik ist der minimale Burst-Balance, der über einen bestimmten Zeitraum verfügbar ist. Die `Maximum` Statistik ist die maximale Burst-Balance, die über einen bestimmten Zeitraum verfügbar ist. Einheiten: Prozent Gültige Statistiken: `AverageMinimum`, und `Maximum`

Metrik	Beschreibung
`FileServerDiskIopsBalance`	Der Prozentsatz der verfügbaren Burst-Gut haben für Festplatten-IOPS zwischen Ihrem Dateiserver und der primären Ebene. Dies gilt für Dateisysteme, die mit einer Durchsatz kapazität von 512 MBpss oder weniger bereitgestellt werden. Die Statistik ist die `Average` durchschnittliche Burst-Balance, die über einen bestimmten Zeitraum verfügbar ist. Die `Minimum` Statistik ist der minimale Burst-Balance, der über einen bestimmten Zeitraum verfügbar ist. Die `Maximum` Statistik ist die maximale Burst-Balance, die über einen bestimmten Zeitraum verfügbar ist. Einheiten: Prozent Gültige Statistiken: `AverageMinimum`, und `Maximum`

Metrik	Beschreibung
`FileServerDiskIopsUtilization`	Der Prozentsatz der IOPS-Auslastung der verfügbaren Festplatten-IOPS-Kapazität für Ihren Dateiserver. Die Statistik ist die `Average` durchschnittliche Festplatten-IOPS-Auslastung des Dateisystems über einen bestimmten Zeitraum. Die Statistik ist die minimale Festplatt en`Minimum`-IOPS-Auslastung des Dateisyst ems über einen bestimmten Zeitraum. Die Statistik ist die maximale Festplatt en`Maximum`-IOPS-Auslastung des Dateisyst ems über einen bestimmten Zeitraum. Einheiten: Prozent Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Metrik	Beschreibung
`FileServerCacheHitRatio`	Der Prozentsatz aller Leseanforderungen, die von Daten in den RAM- und NVMe-Caches des Dateisystems bedient werden. Ein höherer Prozentsatz bedeutet, dass mehr Lesevorgänge von den Lese-Caches des Dateisystems bereitgestellt werden. Einheiten: Prozent Die Statistik ist der `Average` durchschnittliche Cache-Trefferprozentsatz für das Dateisystem über einen bestimmten Zeitraum. Die `Minimum` Statistik ist der niedrigste Cache-Trefferprozentsatz für das Dateisystem über einen bestimmten Zeitraum. Die `Maximum` Statistik ist der höchste Cache-Trefferprozentsatz für das Dateisystem über einen bestimmten Zeitraum. Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Festplatten-I/O-Metriken

Alle diese Metriken haben eine Dimension, `FileSystemId`.

Metrik	Beschreibung
`DiskReadBytes`	Die Anzahl der Bytes (Festplatten-I/O) von allen Festplattenlesevorgängen auf der primären Ebene des Dateisystems.

Metrik	Beschreibung
	Die Sum Statistik ist die Gesamtzahl der Bytes, die über einen bestimmten Zeitraum aus dem Dateisystem gelesen wurden. Um den Lesedatenträgerdurchsatz (Bytes pro Sekunde) für eine beliebige Statistik zu berechnen, teilen Sie die Sum Statistik durch die Sekunden im angegebenen Zeitraum. Einheiten: Byte Gültige Statistiken: Sum
DiskWriteBytes	Die Anzahl der Bytes (Festplatten-I/O) von einem beliebigen Datenträger, der auf die primäre Ebene des Dateisystems schreibt. Die Statistik ist die Gesamtzahl der Bytes, die über einen bestimmten Zeitraum aus dem Dateisystem Sum geschrieben wurden. Um den Durchsatz des Schreibdatenträgers (Bytes pro Sekunde) für eine beliebige Statistik zu berechnen, dividieren Sie Sum die Statistik durch die Sekunden im angegebenen Zeitraum. Einheiten: Byte Gültige Statistiken: Sum

Metrik	Beschreibung
`DiskIopsUtilization`	Die Festplatten-IOPS zwischen Ihrem Dateiserver und Speicher-Volumes als Prozentsatz des IOPS-Limits für bereitgestellte Festplatten der primären Ebene. Die Statistik ist die `Average` durchschnittliche Festplatten-IOPS-Auslastung des Dateisystems über einen bestimmten Zeitraum. Die Statistik ist die minimale Festplatten`Minimum`-IOPS-Auslastung des Dateisystems über einen bestimmten Zeitraum. Die Statistik ist die maximale Festplatten`Maximum`-IOPS-Auslastung des Dateisystems über einen bestimmten Zeitraum. Einheiten: Prozent Gültige Statistiken: `Average`, `Minimum`, und `Maximum`
`DiskReadOperations`	Die Anzahl der Lesevorgänge (Festplatten-I/O) aus der primären Ebene des Dateisystems. Die `Sum` Statistik ist die Gesamtzahl der Lesevorgänge von der primären Ebene über einen bestimmten Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`

Metrik	Beschreibung
`DiskWriteOperations`	Die Anzahl der Schreibvorgänge (Festplatten-I/O) auf der primären Ebene des Dateisystems. Die `Sum` Statistik ist die Gesamtzahl der Schreibvorgänge auf der primären Ebene über einen bestimmten Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`

Speicherkapazitätsmetriken

Alle diese Metriken haben eine Dimension, `FileSystemId`.

Metrik	Beschreibung
`StorageEfficiencySavings`	Die Bytes, die durch Speichereffizienzf unktionen (Komprimierung, Deduplizierung und Verdichtung) gespeichert wurden. Die Statistik ist die `Average` durchschn ittliche Speichereffizienz über einen bestimmte n Zeitraum. Um die Speichereffizienze insparungen als Prozentsatz aller gespeiche rten Daten über einen Zeitraum von einer Minute zu berechnen, dividieren `StorageEf ficiencySavings` durch die Summe von `StorageEfficiencySavings` und die `StorageUsed` Dateisystemmetrik unter Verwendung der `Sum` -Statistik für `StorageUs ed` . Die `Minimum` Statistik ist die minimale Speichereffizienz über einen bestimmten Zeitraum.

Metrik	Beschreibung
	Die `Maximum` Statistik ist die maximale Speichereffizienz über einen bestimmten Zeitraum. Einheiten: Byte Gültige Statistiken: `Average`, `Minimum`, und `Maximum`
`StorageUsed`	Die Gesamtmenge der im Dateisystem gespeicherten physischen Daten, sowohl auf der primären Ebene (SSD) als auch auf der Kapazitätspool-Ebene. Diese Metrik beinhaltet Einsparungen durch Speichere ffizienzfunktionen wie Datenkomprimierung und Deduplizierung. Einheiten: Byte Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Metrik	Beschreibung
`LogicalDataStored`	Die Gesamtmenge der im Dateisystem gespeicherten logischen Daten unter Berücksichtigung der SSD-Ebene und der Kapazitätspool-Ebene. Diese Metrik umfasst die gesamte logische Größe von Snapshots und FlexClones, jedoch keine Speichereffizienzeinsparungen, die durch Komprimierung, Verdichtung und Deduplizierung erzielt werden. Um Speichereffizienzeinsparungen in Bytes zu berechnen, nehmen Sie die `Average` von `StorageUsed` über einen bestimmten Zeitraum und subtrahieren Sie sie von der `Average` von `LogicalDataStored` über denselben Zeitraum. Um Speichereffizienzeinsparungen als Prozentsatz der gesamten logischen Datengröße zu berechnen, nehmen Sie den `Average` von `StorageUsed` über einen bestimmten Zeitraum und subtrahieren Sie ihn von dem `Average` von `LogicalDataStored` über denselben Zeitraum. Teilen Sie dann die Differenz durch die `Average` von `LogicalDataStored` im gleichen Zeitraum. Einheiten: Byte Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Detaillierte Dateisystemmetriken

Detaillierte Dateisystemmetriken sind detaillierte Metriken zur Speicherauslastung für jede Ihrer Speicherebenen. Detaillierte Dateisystemmetriken haben alle die Dimensionen `FileSystemId`, `StorageTier`, und `DataType`.

- Die `StorageTier` Dimension gibt die Speicherebene an, die die Metrik misst, mit möglichen Werten von `SSD` und `StandardCapacityPool`.
- Die `DataType` Dimension gibt den Datentyp an, den die Metrik misst, mit dem möglichen Wert `All`.

Für jede eindeutige Kombination aus einer bestimmten Metrik und Dimensionalen Schlüssel-Wert-Paaren gibt es eine Zeile mit einer Beschreibung dessen, was diese Kombination misst.

Metrik	Beschreibung
`StorageCapacityUtilization`	Die Speicherkapazitätsauslastung für jedes Aggregat Ihres Dateisystems. Für jedes Aggregat Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die `Average` durchschnittliche Speicherkapazitätsauslastung für die Leistungs stufe Ihres Dateisystems im angegebenen Zeitraum. Die `Minimum` Statistik ist die niedrigste Speicherkapazitätsauslastung für die Leistungs stufe Ihres Dateisystems im angegebenen Zeitraum. Die `Maximum` Statistik ist die höchste Speicherk apazitätsauslastung für die Leistungsstufe Ihres Dateisystems im angegebenen Zeitraum. Einheiten: Byte

Metrik	Beschreibung
	Gültige Statistiken: `Average`, `Minimum`, und `Maximum`
`StorageCapacity`	Die Gesamtspeicherkapazität der primären Ebene (SSD). Einheiten: Byte Gültige Statistiken: `Maximum`

Metrik	Beschreibung
`StorageUsed`	Die verwendete physische Speicherkapazität in Byte, spezifisch für die Speicherstufe. Dieser Wert beinhaltet Einsparungen durch Speichere ffizienzfunktionen wie Datenkomprimierung und Deduplizierung. Gültige Dimensionswerte für `StorageTier` sind `SSD` und `StandardCapacityPool`, was der Speicherebene entspricht, die diese Metrik misst. Diese Metrik erfordert auch die `DataType` Dimension mit dem Wert `All`. Die `Maximum` Statistiken `Average`, `Minimum`und sind der Speicherverbrauch pro Stufe in Byte für den angegebenen Zeitraum. Um die Speicherkapazitätsauslastung Ihrer primären (SSD) Speicherebene zu berechnen , teilen Sie jede dieser Statistiken durch `Maximum` `StorageCapacity` den gleichen Zeitraum, wobei die `StorageTier` Dimension gleich ist`SSD`. Um die freie Speicherkapazität Ihrer primären (SSD) Speicherebene in Byte zu berechnen , subtrahieren Sie jede dieser Statistiken vom `Maximum` `StorageCapacity` über denselben Zeitraum, wobei die Dimension `StorageTier` gleich ist`SSD`. Einheiten: Byte Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Aufskalieren von Dateisystemmetriken

Die folgenden Metriken werden für FSx-für-ONTAP-Dateisysteme mit zwei oder mehr Hochverfügbarkeitspaaren (HA) bereitgestellt. Für die Metriken wird für jedes HA-Paar und für jedes Aggregat (für Speicherauslastungsmetriken) ein Datenpunkt ausgegeben.

> **Note**
>
> Wenn Sie ein Dateisystem mit mehreren HA-Paaren haben, können Sie auch die Einzel-HA-Paar-Dateisystemmetriken und die Volume-Metriken verwenden.

Themen

- Netzwerk-E/A-Metriken
- Dateiserver-Metriken
- Festplatten-I/O-Metriken
- Detaillierte Dateisystemmetriken

Netzwerk-E/A-Metriken

Alle diese Metriken haben zwei Dimensionen, `FileSystemId` und `FileServer`.

- `FileSystemId` – Die AWS Ressourcen-ID Ihres Dateisystems.
- `FileServer` – Der Name eines Dateiservers (oder Knotens) in ONTAP (z. B. `FsxId01234567890abcdef-01`). Odd-nummerierte Dateiserver sind bevorzugte Dateiserver (d. h. sie bedienen den Datenverkehr, es sei denn, das Dateisystem hat ein Failover auf den sekundären Dateiserver durchgeführt), während gerade nummerierte Dateiserver sekundäre Dateiserver sind (d. h. sie bedienen den Datenverkehr nur, wenn ihr Partner nicht verfügbar ist). Aus diesem Grund zeigen sekundäre Dateiserver in der Regel eine geringere Auslastung als bevorzugte Dateiserver.

Metrik	Beschreibung
`NetworkThroughputUtilization`	Netzwerkdurchsatzauslastung als Prozentsatz des verfügbaren Netzwerkdurchsatzes für Ihr Dateisystem. Diese Metrik entspricht dem

Metrik	Beschreibung
	Maximum von `NetworkSentBytes` und `NetworkReceivedBytes` als Prozentsatz der Netzwerkdurchsatzkapazität eines HA-Paares für Ihr Dateisystem. Der gesamte Datenverkehr wird in dieser Metrik berücksichtigt, einschließlich Hintergrundaufgaben (wie , SnapMirrorTiering und Backups). Für jeden Dateiserver Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die `Average` durchschnittliche Netzwerkdurchsatzauslastung für den angegebenen Dateiserver im angegebenen Zeitraum. Die `Minimum` Statistik ist die niedrigste Netzwerkdurchsatzauslastung für den angegebenen Dateiserver über eine Minute für den angegebenen Zeitraum. Die `Maximum` Statistik ist die höchste Netzwerkdurchsatzauslastung für den angegebenen Dateiserver über eine Minute für den angegebenen Zeitraum. Einheiten: Prozent Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Metrik	Beschreibung
`NetworkSentBytes`	Die Anzahl der von Ihrem Dateisystem gesendeten Bytes (Netzwerk-IO). Der gesamte Datenverkehr wird in dieser Metrik berücksic htigt, einschließlich Hintergrundaufgaben (wie , SnapMirrorTiering und Backups). Für jeden Dateiserver Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die Gesamtzahl der Bytes`Sum`, die vom angegebenen Dateiserver im angegebenen Zeitraum über das Netzwerk gesendet wurden. Die Statistik ist die `Average` durchschnittliche Anzahl von Bytes, die vom angegebenen Dateiserver im angegebenen Zeitraum über das Netzwerk gesendet wurden. Die `Minimum` Statistik ist die niedrigste Anzahl von Bytes, die über den angegebenen Dateiserver im angegebenen Zeitraum über das Netzwerk gesendet wurden. Die `Maximum` Statistik ist die höchste Anzahl von Bytes, die über den angegebenen Dateiserver im angegebenen Zeitraum über das Netzwerk gesendet wurden. Um den gesendeten Durchsatz (Byte pro Sekunde) für eine beliebige Statistik zu berechnen, dividieren Sie die Statistik durch die Sekunden im angegebenen Zeitraum. Einheiten: Byte

Metrik	Beschreibung
	Gültige Statistiken: `Sum`, `AverageMinimum`, und `Maximum`

Metrik	Beschreibung
`NetworkReceivedBytes`	Die Anzahl der von Ihrem Dateisystem empfangenen Bytes (Netzwerk-IO). Der gesamte Datenverkehr wird in dieser Metrik berücksichtigt, einschließlich Hintergrundaufgaben (wie , SnapMirrorTiering und Backups). Für jeden Dateiserver Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die `Sum` Statistik ist die Gesamtzahl der Bytes, die über den angegebenen Dateiserver im angegebenen Zeitraum über das Netzwerk empfangen wurden. Die Statistik ist die `Average` durchschnittliche Anzahl von Bytes, die der angegebene Dateiserver jede Minute im angegebenen Zeitraum über das Netzwerk empfangen hat. Die `Minimum` Statistik ist die niedrigste Anzahl von Bytes, die der angegebene Dateiserver jede Minute über den angegebenen Zeitraum über das Netzwerk empfangen hat. Die `Maximum` Statistik ist die höchste Anzahl von Bytes, die der angegebene Dateiserver jede Minute über den angegebenen Zeitraum über das Netzwerk empfangen hat. Um den empfangenen Durchsatz (Byte pro Sekunde) für eine beliebige Statistik zu berechnen, teilen Sie die Statistik durch die Sekunden im Zeitraum. Einheiten: Byte

Metrik	Beschreibung
	Gültige Statistiken: `Sum`, `AverageMinimum`, und `Maximum`

Dateiserver-Metriken

Alle diese Metriken haben zwei Dimensionen, `FileSystemId` und `FileServer`.

Metrik	Beschreibung
`CPUUtilization`	Die prozentuale Auslastung der CPU-Resso urcen des Dateisystems. Für jeden Dateiserv er Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die `Average` durchschnittliche CPU-Auslastung des Dateisystems über einen bestimmten Zeitraum. Die `Minimum` Statistik ist die niedrigste CPU-Auslastung für den angegebenen Dateiserver im angegebenen Zeitraum. Die `Maximum` Statistik ist die höchste CPU-Auslastung für den angegebenen Dateiserver im angegebenen Zeitraum. Einheiten: Prozent Gültige Statistiken: `AverageMinimum`, und `Maximum`
`FileServerDiskThroughputUti lization`	Der Festplattendurchsatz zwischen Ihrem Dateiserver und dem Aggregat als Prozentsa tz des bereitgestellten Limits, das durch die Durchsatzkapazität bestimmt wird. Der gesamte Datenverkehr wird in dieser Metrik

Metrik	Beschreibung
	berücksichtigt, einschließlich Hintergru ndaufgaben (wie , SnapMirrorTiering und Backups). Diese Metrik entspricht der Summe von `DiskReadBytes` und `DiskWrite Bytes` als Prozentsatz der Festplattendurchsa tzkapazität des Dateiservers von einem HA-Paar für Ihr Dateisystem. Für jeden Dateiserv er Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die `Average` durchschnittliche Durchsatzauslastung des Dateiserver-Datent rägers für den angegebenen Dateiserver im angegebenen Zeitraum. Die `Minimum` Statistik ist die niedrigste Auslastung des Dateiserver-Datenträgerdurc hsatzes für den angegebenen Dateiserver im angegebenen Zeitraum. Die `Maximum` Statistik ist die höchste Durchsatz auslastung für den Dateiserver für den angegebenen Dateiserver im angegebenen Zeitraum. Einheiten: Prozent Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Metrik	Beschreibung
`FileServerDiskIopsUtilization`	Die IOPS-Auslastung der verfügbaren Festplatten-IOPS-Kapazität für Ihren Dateiserver als Prozentsatz seines Festplatten-IOPS-Limits. Dies unterscheidet sich von `DiskIopsUtilization` dadurch, dass die Auslastung von Festplatten-IOPS außerhalb des Maximums liegt, das Ihr Dateiserver verarbeiten kann, im Gegensatz zu Ihren bereitgestellten Festplatten-IOPS. Der gesamte Datenverkehr wird in dieser Metrik berücksichtigt, einschließlich Hintergrundaufgaben (wie SnapMirror, Tiering und Backups). Für jeden Dateiserver Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die `Average` durchschnittliche Festplatten-IOPS-Auslastung für den angegebenen Dateiserver im angegebenen Zeitraum. Die Statistik ist die niedrigste Festplatten`Minimum`-IOPS-Auslastung für den angegebenen Dateiserver im angegebenen Zeitraum. Die Statistik ist die höchste Festplatten`Maximum`-IOPS-Auslastung für den angegebenen Dateiserver im angegebenen Zeitraum. Einheiten: Prozent Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Metrik	Beschreibung
`FileServerCacheHitRatio`	Der Prozentsatz aller Leseanforderungen, die von Daten bereitgestellt werden, die sich im RAM- oder NVMe-Cache Ihres Dateisystems für jedes Ihrer HA-Paare befinden (z. B. den aktiven Dateiserver in einem HA-Paar). Ein höherer Prozentsatz weist auf ein höheres Verhältnis zwischengespeicherter Lesevorgänge zu den gesamten Lesevorgängen hin. Alle E/A-Vorgänge werden berücksichtigt, einschließlich Hintergrundaufgaben (wie SnapMirror, Tiering und Backups). Für jeden Dateiserver Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Einheiten: Prozent Die Statistik ist die `Average` durchschnittliche Cache-Trefferquote für eines der HA-Paare Ihres Dateisystems im angegebenen Zeitraum. Die `Minimum` Statistik ist die niedrigste Cache-Trefferquote für eines der HA-Paare Ihres Dateisystems im angegebenen Zeitraum. Die `Maximum` Statistik ist die höchste Cache-Trefferquote für eines der HA-Paare Ihres Dateisystems im angegebenen Zeitraum. Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Festplatten-I/O-Metriken

Alle diese Metriken haben zwei Dimensionen, `FileSystemId` und `Aggregate`.

- `FileSystemId` – Die AWS Ressourcen-ID Ihres Dateisystems.

- `Aggregate` – Die Leistungsstufe Ihres Dateisystems besteht aus mehreren Speicherpools, die als Aggregate bezeichnet werden. Für jedes HA-Paar gibt es ein Aggregat. Beispielsweise wird Aggregat einem Dateiserver `FsxId01234567890abcdef-01` (dem aktiven Dateiserver) und einem Dateiserver `FsxId01234567890abcdef-02` (dem sekundären Dateiserver) in einem HA-Paar `aggr1` zugeordnet.

Metrik	Beschreibung
`DiskReadBytes`	Die Anzahl der Bytes (Festplatten-IO) von ay-Festplattenlesevorgängen aus diesem Aggregat. Der gesamte Datenverkehr wird in dieser Metrik berücksichtigt, einschließlich Hintergrundaufgaben (wie , SnapMirrorTiering und Backups). Für jedes Aggregat Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die `Sum` Statistik ist die Gesamtzahl der pro Minute aus dem angegebenen Aggregat über den angegebenen Zeitraum gelesenen Byte. Die Statistik ist die `Average` durchschnittliche Anzahl von Bytes, die pro Minute aus dem angegebenen Aggregat über den angegebenen Zeitraum gelesen werden. Die `Minimum` Statistik ist die niedrigste Anzahl von Bytes, die jede Minute aus dem angegeben en Aggregat über den angegebenen Zeitraum gelesen wurden. Die `Maximum` Statistik ist die höchste Anzahl von Bytes, die pro Minute aus dem angegeben en Aggregat über den angegebenen Zeitraum gelesen wurden.

Metrik	Beschreibung
	Um den Lesedatenträgerdurchsatz (Byte pro Sekunde) für eine beliebige Statistik zu berechnen, teilen Sie die Statistik durch die Sekunden im Zeitraum. Einheiten: Byte Gültige Statistiken: `Sum`, `AverageMinimum`, und `Maximum`

Metrik	Beschreibung
`DiskWriteBytes`	Die Anzahl der Bytes (Festplatten-IO) von Festplattenschreibvorgängen in dieses Aggregat. Der gesamte Datenverkehr wird in dieser Metrik berücksichtigt, einschließlich Hintergrundaufgaben (wie , SnapMirrorTiering und Backups). Für jedes Aggregat Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die Gesamtzahl der Bytes, die im angegebenen Zeitraum in das angegebene Aggregat `Sum` geschrieben wurden. Die Statistik ist die `Average` durchschn ittliche Anzahl von Bytes, die im angegeben en Zeitraum minütlich in das angegebene Aggregat geschrieben wurden. Die `Minimum` Statistik ist die niedrigste Anzahl von Bytes, die jede Minute im angegeben en Zeitraum in die angegebene Zusammenf assung geschrieben wurden. Die `Maximum` Statistik ist die höchste Anzahl von Bytes, die jede Minute im angegeben en Zeitraum in das angegebene Aggregat geschrieben wurden. Um den Durchsatz des Schreibdatenträgers (Bytes pro Sekunde) für eine beliebige Statistik zu berechnen, dividieren Sie die Statistik durch die Sekunden im angegebenen Zeitraum. Einheiten: Byte

Metrik	Beschreibung
	Gültige Statistiken: `Sum`, `AverageMinimum`, und `Maximum`

Metrik	Beschreibung
`DiskIopsUtilization`	Die Festplatten-IOPS-Auslastung eines Aggregats als Prozentsatz des Festplatten-IOPS-Limits des Aggregats (d. h. die Gesamt-IOPS des Dateisystems geteilt durch die Anzahl der HA-Paare für Ihr Dateisystem). Dies unterscheidet sich von `FileServerDiskIopsUtilization` dadurch, dass es sich um die Auslastung von bereitgestellten Festplatten-IOPS gegenüber Ihrem bereitgestellten IOPS-Limit handelt, im Gegensatz zu den maximalen Festplatten-IOPS, die vom Dateiserver unterstützt werden (d. h. durch Ihre konfigurierte Durchsatzkapazität pro HA-Paar bestimmt). Der gesamte Datenverkehr wird in dieser Metrik berücksichtigt, einschließlich Hintergrundaufgaben (wie SnapMirror, Tiering und Backups). Für jedes Aggregat Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die `Average` durchschnittliche Festplatten-IOPS-Auslastung für das angegebene Aggregat im angegebenen Zeitraum. Die Statistik ist die niedrigste Festplatten`Minimum`-IOPS-Auslastung für das angegebene Aggregat im angegebenen Zeitraum. Die Statistik gibt die höchste Festplatten`Maximum`-IOPS-Auslastung für das angegebene Aggregat im angegebenen Zeitraum an. Einheiten: Prozent

Metrik	Beschreibung
	Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Metrik	Beschreibung
`DiskReadOperations`	Die Anzahl der Lesevorgänge (Festplat ten-IO) für dieses Aggregat. Der gesamte Datenverkehr wird in dieser Metrik berücksic htigt, einschließlich Hintergrundaufgaben (wie , SnapMirrorTiering und Backups). Für jedes Aggregat Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die `Sum` Statistik ist die Gesamtzahl der Lesevorgänge, die von dem angegebenen Aggregat im angegebenen Zeitraum ausgeführ t wurden. Die Statistik ist die `Average` durchschnittliche Anzahl von Lesevorgängen, die pro Minute vom angegebenen Aggregat über den angegebenen Zeitraum ausgeführt werden. Die `Minimum` Statistik ist die niedrigste Anzahl von Lesevorgängen, die jede Minute vom angegebenen Aggregat über den angegebenen Zeitraum ausgeführt werden. Die `Maximum` Statistik ist die höchste Anzahl von Lesevorgängen, die pro Minute vom angegebenen Aggregat über den angegebenen Zeitraum ausgeführt werden. Um die durchschnittlichen Festplatten-IOPS über den Zeitraum zu berechnen, verwenden Sie die `Average` -Statistik und dividieren Sie das Ergebnis durch 60 (Sekunden). Einheiten: Anzahl

Metrik	Beschreibung
	Gültige Statistiken: `Sum`, `AverageMinimum`, und `Maximum`
`DiskWriteOperations`	Die Anzahl der Schreibvorgänge (Festplat ten-IO) für dieses Aggregat. Der gesamte Datenverkehr wird in dieser Metrik berücksic htigt, einschließlich Hintergrundaufgaben (wie , SnapMirrorTiering und Backups). Für jedes Aggregat Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die `Sum` Statistik ist die Gesamtzahl der Schreibvorgänge, die von dem angegebenen Aggregat im angegebenen Zeitraum ausgeführ t wurden. Die Statistik ist die `Average` durchschn ittliche Anzahl von Schreibvorgängen, die pro Minute vom angegebenen Aggregat über den angegebenen Zeitraum ausgeführt werden. Um die durchschnittlichen Festplatten-IOPS über den Zeitraum zu berechnen, verwenden Sie die `Average` -Statistik und dividieren Sie das Ergebnis durch 60 (Sekunden). Einheiten: Anzahl Gültige Statistiken: `Sum` und `Average`

Detaillierte Dateisystemmetriken

Detaillierte Dateisystemmetriken sind detaillierte Metriken zur Speicherauslastung für jede Ihrer Speicherebenen. Detaillierte Dateisystemmetriken haben entweder die `DataType` Dimensionen `FileSystemIdStorageTier`, und oder die `Aggregate` Dimensionen `FileSystemId`, `DataType`, und `StorageTier`.

- Wenn die `Aggregate` Dimension nicht angegeben wird, beziehen sich die Metriken auf Ihr gesamtes Dateisystem. Die `StorageCapacity` Metriken `StorageUsed` und verfügen jede Minute über einen einzelnen Datenpunkt, der dem gesamten verbrauchten Speicher des Dateisystems (pro Speicherstufe) und der gesamten Speicherkapazität (für die SSD-Stufe) entspricht. In der Zwischenzeit gibt die `StorageCapacityUtilization` Metrik pro Minute eine Metrik für jedes Aggregat aus.
- Wenn die `Aggregate` Dimension angegeben wird, gelten die Metriken für jedes Aggregat.

Die Dimensionen haben folgende Bedeutung:

- `FileSystemId` – Die AWS Ressourcen-ID Ihres Dateisystems.
- `Aggregate` – Die Leistungsstufe Ihres Dateisystems besteht aus mehreren Speicherpools, die als Aggregate bezeichnet werden. Für jedes HA-Paar gibt es ein Aggregat. Beispielsweise wird Aggregat einem Dateiserver `FsxId01234567890abcdef-01` (dem aktiven Dateiserver) und einem Dateiserver `FsxId01234567890abcdef-02` (dem sekundären Dateiserver) in einem HA-Paar `aggr1` zugeordnet.
- `StorageTier` – Gibt die Speicherebene an, die die Metrik misst, mit möglichen Werten von `SSD` und `StandardCapacityPool`.
- `DataType` – Gibt den Datentyp an, den die Metrik misst, mit dem möglichen Wert `All`.

Für jede eindeutige Kombination aus einer bestimmten Metrik und Dimensionalen Schlüssel-Wert-Paaren gibt es eine Zeile mit einer Beschreibung dessen, was diese Kombination misst.

Metrik	Beschreibung
`StorageCapacityUtilization`	Die Speicherkapazitätsauslastung für ein bestimmtes Dateisystemaggregat. Für jedes Aggregat Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die `Average` durchschn ittliche Speicherkapazitätsauslastung für ein bestimmtes Aggregat im angegebenen Zeitraum.

Metrik	Beschreibung
	Die `Minimum` -Statistik ist die minimale Speicherkapazitätsauslastung für ein bestimmtes Aggregat im angegebenen Zeitraum. Die `Maximum` Statistik ist die maximale Speicherkapazitätsauslastung für ein bestimmtes Aggregat im angegebenen Zeitraum. Einheiten: Byte Gültige Statistiken: `Average` `Minimum`, und `Maximum`
`StorageCapacity`	Die Speicherkapazität für ein bestimmtes Dateisystemaggregat. Für jedes Aggregat Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die `Average` durchschnittliche Speicherkapazität für ein bestimmtes Aggregat im angegebenen Zeitraum. Die `Minimum` Statistik ist die Mindestsp eicherkapazität für ein bestimmtes Aggregat im angegebenen Zeitraum. Die `Maximum` Statistik ist die maximale Speicherkapazität für ein bestimmtes Aggregat im angegebenen Zeitraum. Einheiten: Byte Gültige Statistiken: `Average` `Minimum`, und `Maximum`

Metrik	Beschreibung
`StorageUsed`	Die verwendete physische Speicherkapazität in Byte, spezifisch für die Speicherstufe. Dieser Wert beinhaltet Einsparungen durch Speichereffizienzfunktionen wie Datenkomprimierung und Deduplizierung. Gültige Dimensionswerte für `StorageTier` sind `SSD` und `StandardCapacityPool`, was der Speicherebene entspricht, die diese Metrik misst. Für jedes Aggregat Ihres Dateisystems wird jede Minute eine Metrik ausgegeben. Die Statistik ist die `Average` durchschnittliche physische Speicherkapazität, die auf der angegebenen Speicherebene vom angegebenen Aggregat im angegebenen Zeitraum verbraucht wird. Die `Minimum` Statistik ist die minimale physische Speicherkapazität, die auf der angegebenen Speicherebene vom angegebenen Aggregat im angegebenen Zeitraum verbraucht wird. Die `Maximum` Statistik ist die maximale Menge an physischer Speicherkapazität, die auf der angegebenen Speicherebene vom angegebenen Aggregat im angegebenen Zeitraum verbraucht wird. Einheiten: Byte Gültige Statistiken: `Average`, `Minimum`, und `Maximum`

Volume-Metriken

Ihr Dateisystem von Amazon FSx für NetApp ONTAP kann über ein oder mehrere Volumes verfügen, auf denen Ihre Daten gespeichert sind. Jedes dieser Volumes verfügt über eine Reihe von Metriken, die entweder als Volume-Metriken oder Detaillierte Volume-Metriken klassifiziert sind.

- Volume-Metriken sind Leistungs- und Speichermetriken pro Volume, die zwei Dimensionen annehmen, `FileSystemId` und `VolumeId`. `FileSystemId` wird dem Dateisystem zugeordnet, zu dem das Volume gehört.
- Detaillierte Volume-Metriken sind per-storage-tier Metriken, die den Speicherverbrauch pro Stufe mit der `StorageTier` Dimension (mit möglichen Werten von `SSD` und `StandardCapacityPool`) und pro Datentyp mit der `DataType` Dimension (mit möglichen Werten von `UserSnapshot`, und) messen`Other`. Diese Metriken haben die `DataType` Dimensionen `FileSystemId`, `VolumeIdStorageTier`, und .

Themen

- Netzwerk-E/A-Metriken
- Speicherkapazitätsmetriken
- Detaillierte Volume-Metriken

Netzwerk-E/A-Metriken

Alle diese Metriken haben zwei Dimensionen, `FileSystemId` und `VolumeId`.

Metrik	Beschreibung
`DataReadBytes`	Die Anzahl der Bytes (Netzwerk-E/A), die von Clients aus dem Volume gelesen wurden. Die `Sum` Statistik ist die Gesamtzahl der Bytes, die während des angegebenen Zeitraums mit Lesevorgängen verknüpft sind. Um den durchschnittlichen Durchsatz (Byte pro Sekunde) für einen Zeitraum zu berechnen, dividieren Sie die `Sum` Statistik durch die Anzahl der Sekunden im angegebenen Zeitraum.

Metrik	Beschreibung
	Einheiten: Byte Gültige Statistiken: `Sum`
`DataWriteBytes`	Die Anzahl der von Clients in das Volume geschriebenen Bytes (Netzwerk-E/A). Die Statistik ist die Gesamtzahl der Bytes`Sum`, die während des angegebenen Zeitraums mit Schreibvorgängen verknüpft sind. Um den durchschnittlichen Durchsatz (Byte pro Sekunde) für einen Zeitraum zu berechnen, dividieren Sie die `Sum` Statistik durch die Anzahl der Sekunden im angegebenen Zeitraum. Einheiten: Byte Gültige Statistiken: `Sum`
`DataReadOperations`	Die Anzahl der Lesevorgänge (Netzwerk-E/A) auf dem Volume durch Clients. Die `Sum` Statistik ist die Gesamtzahl der Lesevorgänge während des angegebenen Zeitraums. Um die `Sum` durchschnittlichen Lesevorgänge pro Sekunde für einen Zeitraum zu berechnen, dividieren Sie die Statistik durch die Anzahl der Sekunden im angegebenen Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`

Metrik	Beschreibung
`DataWriteOperations`	Die Anzahl der Schreibvorgänge (Netzwerk-E/A) auf dem Volume durch Clients. Die `Sum` Statistik ist die Gesamtzahl der Schreibvorgänge während des angegeben en Zeitraums. Um die `Sum` durchschnittlichen Schreibvorgänge pro Sekunde für einen Zeitraum zu berechnen, dividieren Sie die Statistik durch die Anzahl der Sekunden im angegebenen Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`
`MetadataOperations`	Die Anzahl der E/A-Operationen (Netzwerk-E/A) von Metadatenaktivitäten durch Clients auf das Volume. Die `Sum` Statistik ist die Gesamtzahl der Metadatenoperationen während des angegebenen Zeitraums. Um die `Sum` durchschnittlichen Metadatenoperationen pro Sekunde für einen Zeitraum zu berechnen, dividieren Sie die Statistik durch die Anzahl der Sekunden im angegebenen Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`

Metrik	Beschreibung
`DataReadOperationTime`	Die Gesamtzeit, die innerhalb des Volumes für Lesevorgänge (Netzwerk-E/A) von Clients auf Daten im Volume aufgewendet wurde. Die `Sum` Statistik ist die Gesamtzahl der Sekunden, die von Lesevorgängen während des angegebenen Zeitraums aufgewend et wurden. Um die `Sum` durchschnittliche Leselatenz für einen Zeitraum zu berechnen , dividieren Sie die Statistik durch die `Sum` der `DataReadOperations` Metrik über denselben Zeitraum. Einheiten: Sekunden Gültige Statistiken: `Sum`
`DataWriteOperationTime`	Die Gesamtzeit, die innerhalb des Volumes für die Ausführung von Schreibvorgängen (Netzwerk-E/A) von Clients auf Daten im Volume aufgewendet wurde. Die `Sum` Statistik ist die Gesamtzahl der Sekunden, die für Schreibvorgänge während des angegebenen Zeitraums aufgewend et wurden. Um die `Sum` durchschnittliche Schreiblatenz für einen Zeitraum zu berechnen , dividieren Sie die Statistik durch die `Sum` der `DataWriteOperations` Metrik über denselben Zeitraum. Einheiten: Sekunden Gültige Statistiken: `Sum`

Metrik	Beschreibung
`MetadataOperationTime`	Die Gesamtzeit, die innerhalb des Volumes für die Erfüllung von Metadatenoperation en (Netzwerk-E/A) von Clients aufgewendet wurde, die auf Daten im Volume zugreifen. Die `Sum` Statistik ist die Gesamtzahl der Sekunden, die von Lesevorgängen während des angegebenen Zeitraums aufgewendet wurden. Um die `Sum` durchschnittliche Latenz für einen Zeitraum zu berechnen, dividieren Sie die Statistik durch die `Sum` des `Metadata0 perations` im gleichen Zeitraum. Einheiten: Sekunden Gültige Statistiken: `Sum`
`CapacityPoolReadBytes`	Die Anzahl der aus der Kapazitätspool-Ebene des Volumes gelesenen Bytes (Netzwerk-E/A). Um die Datenintegrität zu gewährleisten, führt ONTAP unmittelbar nach der Ausführung eines Schreibvorgangs einen Lesevorgang für den Kapazitätspool durch. Die `Sum` Statistik ist die Gesamtzahl der Bytes, die über einen bestimmten Zeitraum aus der Kapazitätspool-Ebene des Volumes gelesen wurden. Um die Bytes des Kapazitätspools pro Sekunde zu berechnen, teilen Sie die `Sum` Statistik durch die Sekunden in einem bestimmten Zeitraum. Einheiten: Byte Gültige Statistiken: `Sum`

Metrik	Beschreibung
`CapacityPoolReadOperations`	Die Anzahl der Lesevorgänge (Netzwerk-E/A) aus der Kapazitätspool-Ebene des Volumes. Dies wird in eine Kapazitätspool-Leseanforderung übersetzt. Um die Datenintegrität zu gewährleisten, führt ONTAP unmittelbar nach der Ausführung eines Schreibvorgangs einen Lesevorgang für den Kapazitätspool durch. Die `Sum` Statistik ist die Gesamtzahl der Lesevorgänge aus der Kapazitätspool-Ebene des Volumes über einen bestimmten Zeitraum. Um Kapazitätspool-Anforderungen pro Sekunde zu berechnen, teilen Sie die `Sum` Statistik durch die Sekunden in einem bestimmten Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`

Metrik	Beschreibung
`CapacityPoolWriteBytes`	Die Anzahl der Bytes, die auf die Kapazität spool-Ebene des Volumes geschrieben wurden (Netzwerk-I/O). Um die Datenintegrität zu gewährleisten, führt ONTAP unmittelbar nach der Ausführung eines Schreibvorgangs einen Lesevorgang für den Kapazitätspool durch. Die `Sum` Statistik ist die Gesamtzahl der Bytes, die über einen bestimmten Zeitraum auf die Kapazitätspool-Ebene des Volumes geschrieb en wurden. Um die Bytes des Kapazitätspools pro Sekunde zu berechnen, teilen Sie die `Sum` Statistik durch die Sekunden in einem bestimmten Zeitraum. Einheiten: Byte Gültige Statistiken: `Sum`

Metrik	Beschreibung
`CapacityPoolWriteOperations`	Die Anzahl der Schreibvorgänge (Netzwerk-E/A) für das Volume von der Kapazitätspool-Ebene aus. Dies wird in eine Schreibanforderung übersetzt. Um die Datenintegrität zu gewährleisten, führt ONTAP unmittelbar nach der Ausführung eines Schreibvorgangs einen Lesevorgang für den Kapazitätspool durch. Die `Sum` Statistik ist die Gesamtzahl der Schreibvorgänge auf die Kapazitätspool-Ebene des Volumes über einen bestimmten Zeitraum. Um Kapazitätspool-Anforderungen pro Sekunde zu berechnen, teilen Sie die `Sum` Statistik durch die Sekunden in einem bestimmten Zeitraum. Einheiten: Anzahl Gültige Statistiken: `Sum`

Speicherkapazitätsmetriken

Alle diese Metriken haben zwei Dimensionen, `FileSystemId` und `VolumeId`.

Metrik	Beschreibung
`StorageCapacity`	Die Größe des Volumes in Byte. Einheiten: Byte Gültige Statistiken: `Maximum`
`StorageUsed`	Die verwendete logische Speicherkapazität des Volumes.

Metrik	Beschreibung
	Einheiten: Byte Gültige Statistiken: `Average`, `Minimum`, und `Maximum`
`StorageCapacityUtilization`	Die Speicherkapazitätsauslastung des Volumes. Einheiten: Prozent Gültige Statistiken: `Average`
`FilesUsed`	Die verwendeten Dateien (Anzahl der Dateien oder Inodes) auf dem Volume. Einheiten: Anzahl Gültige Statistiken: `Average`, `Minimum`, und `Maximum`
`FilesCapacity`	Die Gesamtzahl der Knoten, die auf dem Volume erstellt werden können. Einheiten: Anzahl Gültige Statistiken: `Maximum`

Detaillierte Volume-Metriken

Detaillierte Volume-Metriken haben mehr Dimensionen als Volume-Metriken, was detailliertere Messungen Ihrer Daten ermöglicht. Alle detaillierten Volume-Metriken haben die Dimensionen `FileSystemId`, `VolumeIdStorageTier`, und `DataType`.

- Die `StorageTier` Dimension gibt die Speicherebene an, die die Metrik misst, mit möglichen Werten von `AllSSD`, und `StandardCapacityPool`.
- Die `DataType` Dimension gibt den Datentyp an, den die Metrik misst, mit möglichen Werten von `All`, `UserSnapshot`, und `Other`.

Die folgende Tabelle definiert, was die `StorageUsed` Metrik für die aufgelisteten Dimensionen misst.

Metrik	Beschreibung
`StorageUsed`	Der verwendete logische Speicherplatz in Byte. Diese Metrik misst verschiedene Arten von Platzverbrauch, abhängig von den Dimension en, die mit dieser Metrik verwendet werden. Wenn Sie `StorageTier` auf `SSD` oder `StandardCapacityPool` und `DataType` auf festlegen`All`, misst diese Metrik die logische Speicherplatznutzung für dieses Volume für Ihre SSD- bzw. Kapazitätspool-Stu fen. Wenn Sie die `DataType` Dimension auf `User`, `Snapshot`oder `Other`und `StorageTi er` auf festlegen`All`, misst diese Metrik die logische Speicherplatznutzung für jeden jeweiligen Datentyp. Der `Snapshot` Datenverb rauch beinhaltet die Snapshot-Reservierung, die standardmäßig 5 % der Größe des Volumes entspricht. Einheiten: Byte Gültige Statistiken: `Average`, `Minimum`, und `Maximum`
`StorageCapacityUtilization`	Der Prozentsatz des belegten physischen Festplattenspeichers des Volumes. Einheiten: Prozent Gültige Statistiken: `Maximum`

Leistungswarnungen und Empfehlungen

FSx für ONTAP zeigt eine Warnung für CloudWatch Metriken an, wenn sich eine dieser Metriken einem vordefinierten Schwellenwert für mehrere aufeinanderfolgende Datenpunkte nähert oder

überschritten hat. Diese Warnungen bieten Ihnen umsetzbare Empfehlungen, mit denen Sie die Leistung Ihres Dateisystems optimieren können.

Auf Warnungen kann in mehreren Bereichen des Dashboards Überwachung und Leistung 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 im Abschnitt des Dashboards angezeigt, in dem das Metrikdiagramm angezeigt wird.

Sie können CloudWatch Alarme für jede der Amazon-FSx-Metriken erstellen. Weitere Informationen finden Sie unter Erstellen von Amazon- CloudWatch Alarmen zur Überwachung von Amazon FSx.

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 mit einem potenziellen Leistungsengpass umgehen können. Sie können die empfohlenen Maßnahmen ergreifen, wenn Sie erwarten, dass die Aktivität fortgesetzt wird oder wenn dies Auswirkungen auf die Leistung Ihres Dateisystems hat. Je nachdem, welche Metrik eine Warnung ausgelöst hat, können Sie sie auflösen, indem Sie entweder die Durchsatzkapazität oder die Speicherkapazität des Dateisystems erhöhen, wie in der folgenden Tabelle beschrieben.

Dashboard-Abschnitt	Wenn es eine Warnung für diese Metrik gibt	Vorgehensweise
Speicher	Auslastung der primären Speicherkapazität	Erhöhen Sie die primäre Speicherkapazität Ihres Dateisystems, wenn Ihr Dateisystem noch nicht über die maximale SSD-Speicherkapazität verfügt. Weitere Informationen finden Sie unter Änderung der SSD-Speicherkapazität und der bereitgestellten IOPS. Wenn Ihr Dateisystem mehrere HA-Paare hat und Ihre primäre Speicherkapazitätsauslastung nur für eine Teilmenge der Aggregate Ihres Dateisystems (die Speicherpools, aus denen Ihre primäre Speichere bene besteht) höher ist, können Sie Ihren Workload auch neu verteilen, sodass Ihre primäre Speicherk

Dashboard-Abschnitt	Wenn es eine Warnung für diese Metrik gibt	Vorgehensweise
		apazitätsauslastung gleichmäßiger auf Ihr Dateisyst em verteilt ist. Weitere Informationen zum Wiederher stellen des Gleichgewichts Ihrer Workloads finden Sie unter Überwachen der Workload-Balance von FSx für ONTAP.
Dateiserv er-Leistung	Netzwerkdurchsatz Festplattendurchsatz Festplatten-IOPS CPU-Auslastung	Erhöhen Sie die Durchsatzkapazität Ihres Dateisyst ems, wenn Ihr Dateisystem noch nicht über die maximale Durchsatzkapazität verfügt. Weitere Informati onen zum Aktualisieren der Durchsatzkapazität finden Sie unter Wie ändert man die Durchsatzkapazität. Wenn Ihr Dateisystem über mehrere HA-Paare verfügt und die Auslastung nur für eine Teilmenge von Dateiservern hoch ist, können Sie Ihren Workload auch neu ausgleichen, sodass Ihr Workload die Leistungs funktionen der einzelnen HA-Paare Ihres Dateisyst ems gleichmäßiger nutzt. Weitere Informationen zum Wiederherstellen des Gleichgewichts Ihrer Workloads finden Sie unter Überwachen der Workload-Balance von FSx für ONTAP.

Dashboard-Abschnitt	Wenn es eine Warnung für diese Metrik gibt	Vorgehensweise
Festplatt enleistung	Festplatten-IOPS	Erhöhen Sie SSD-IOPS, wenn Ihr Dateisystem noch nicht die maximale SSD-IOPS für die aktuelle Durchsatzkapazität Ihres Dateisystems erreicht hat. Weitere Informationen zum Aktualisieren der bereitgestellten IOPS Ihres Dateisystems finden Sie unter Änderung der SSD-Speicherkapazität und der bereitgestellten IOPS. Wenn Ihr Dateisystem mehrere HA-Paare hat und Ihre Festplatten-IOPS-Auslastung nur für eine Teilmenge der Aggregate Ihres Dateisystems (die Speicherpools, aus denen Ihre primäre Speicherebene besteht) höher ist, können Sie Ihren Workload auch neu ausgleich en, sodass Ihre Festplatten-IOPS in Ihrem Dateisyst em gleichmäßiger genutzt werden. Weitere Informati onen zum Wiederherstellen des Gleichgewichts Ihrer Workloads finden Sie unter Überwachen der Workload-Balance von FSx für ONTAP.

Weitere Informationen zur Leistung des Dateisystems finden Sie unter Leistung von Amazon FSx für NetApp ONTAP.

Erstellen von Amazon- CloudWatch Alarmen zur Überwachung von Amazon FSx

Sie können einen CloudWatch Alarm erstellen, der eine Amazon Simple Notification Service (Amazon SNS)-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum. Bei Bedarf führt der Alarm dann eine oder mehrere Aktionen basierend auf dem Wert der Metrik relativ zu einem bestimmten Schwellenwert über eine Reihe von Zeiträumen aus. Die Aktion ist eine Benachrichtigung, die an ein Amazon-SNS-Thema oder eine Auto-Scaling-Richtlinie gesendet wird.

Alarme rufen nur Aktionen für anhaltende Statusänderungen auf. CloudWatch Alarme rufen keine Aktionen auf, nur weil sie sich in einem bestimmten Status befinden. Der Status muss geändert und

für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Sie können einen Alarm über die Amazon-FSx-Konsole oder die Amazon- CloudWatch Konsole erstellen.

In den folgenden Verfahren wird beschrieben, wie Sie Alarme mithilfe der Amazon-FSx-Konsole, AWS Command Line Interface der (AWS CLI) und der API erstellen.

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 linken Navigationsbereich Dateisysteme und dann das Dateisystem aus, für das Sie den Alarm erstellen möchten.
3. Wählen Sie auf der Seite Zusammenfassung im zweiten Bereich Überwachung und Leistung aus.
4. Wählen Sie die Registerkarte CloudWatch Alarme aus.
5. Wählen Sie CloudWatch Alarm erstellen aus. Sie werden zur CloudWatch-Konsole umgeleitet.
6. Wählen Sie Select metric (Metrik auswählen) aus.
7. Wählen Sie im Abschnitt Metriken die Option FSx aus.
8. Wählen Sie eine Metrikkategorie aus:
   - Dateisystemmetriken
   - Detaillierte Dateisystemmetriken
   - Volume-Metriken
   - Detaillierte Volume-Metriken
9. Wählen Sie die Metrik aus, für die Sie den Alarm festlegen möchten, und wählen Sie dann Metrik auswählen aus.
10. Wählen Sie im Abschnitt Bedingungen die gewünschten Bedingungen für den Alarm und dann Weiter aus.

> **Note**
>
> Metriken werden möglicherweise während der Dateisystemwartung nicht veröffentlicht. Informationen zum Vermeiden unnötiger und betrügerischer Alarmbedingungsänderungen und zum Konfigurieren Ihrer Alarme so, dass sie gegenüber fehlenden Datenpunkten ausfallsicher sind, finden Sie unter Konfigurieren

der Reaktion von CloudWatch Alarmen auf fehlende Daten im Amazon- CloudWatch Benutzerhandbuch.

11. Wenn Sie eine E-Mail oder Amazon SNS-Benachrichtigung CloudWatch senden möchten, wenn der Alarmstatus die Aktion auslöst, wählen Sie einen Alarmstatus für Alarmstatusauslöser aus.

    Wählen Sie unter Benachrichtigung an das folgende SNS-Thema senden eine Option aus. Wenn Sie die Option Create topic (Thema erstellen) 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. 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 dieser Alarmzustands geändert wird, bevor die E-Mail Adressen überprüft wurden, erhalten sie keine Benachrichtigung.

12. Füllen Sie die Felder Alarmname und Alarmbeschreibung aus und wählen Sie dann Weiter aus.
13. Überprüfen Sie auf der Seite Vorschau und Erstellen den Alarm, den Sie gerade erstellen möchten, und wählen Sie dann Alarm erstellen aus.

So richten Sie Alarme mit der CloudWatch Konsole ein

1. 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. Folgen Sie den Anweisungen unter So richten Sie Alarme mithilfe der Amazon-FSx-Konsole ein, beginnend mit Schritt 6.

So richten Sie einen Alarm mithilfe der ein AWS CLI

- Rufen Sie den put-metric-alarm CLI-Befehl auf. Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

So richten Sie einen Alarm mithilfe der CloudWatch API ein

- Rufen Sie den PutMetricAlarm-API-Vorgang auf. Weitere Informationen finden Sie in der Amazon CloudWatch -API-Referenz .

Überwachen der Workload-Balance von FSx für ONTAP

Wenn Sie über ein Dateisystem mit mehreren HA-Paaren verfügen, wird dessen Leistung und Durchsatz auf jedes Ihrer HA-Paare verteilt. FSx für ONTAP gleicht Ihre Dateien automatisch aus, wenn sie in Ihr Dateisystem geschrieben werden. In seltenen Fällen ist es jedoch möglich, dass Ihre Workload-Daten oder E/A über HA-Paare hinweg unausgewogen werden können, was sich auf die Gesamtleistung Ihres Workloads auswirken kann. Sie können Ihren Workload überwachen, um sicherzustellen, dass er über die HA-Paare Ihres Dateisystems (und ihre entsprechenden Dateiserver und Aggregate – die Speicherpools, aus denen Ihre primäre Speicherebene besteht) verteilt bleibt.

Themen

- Auslastungssaldo des primären Speichers
- Ungleichgewicht bei der Dateiserver- und Festplattenleistung
- Zuordnen von CloudWatch Dimensionen zu ONTAP-CLI- und REST-API-Ressourcen
- Neuausgleich von Clients mit hohem Datenverkehr
- Wiederherstellen des Gleichgewichts von stark ausgelasteten Volumes

Auslastungssaldo des primären Speichers

Die primäre Speicherkapazität Ihres Dateisystems wird gleichmäßig auf jedes Ihrer HA-Paare in Speicherpools aufgeteilt, die als Aggregate bezeichnet werden. Jedes HA-Paar hat ein Aggregat. Wir empfehlen Ihnen, eine durchschnittliche Auslastung von nicht mehr als 80 % für Ihre primäre Speicherstufe kontinuierlich beizubehalten. Für Dateisysteme mit mehreren HA-Paaren empfehlen wir, für jedes Aggregat eine durchschnittliche Auslastung von bis zu 80 % beizubehalten.

Die Aufrechterhaltung einer Auslastung von 80 % stellt sicher, dass freier Speicherplatz für neue eingehende Daten vorhanden ist, und sorgt für einen fehlerfreien Overhead für Wartungsvorgänge, die vorübergehend freien Speicherplatz für Ihre Aggregate beanspruchen können.

Wenn Sie feststellen, dass Ihre Aggregate unausgewogen sind, können Sie entweder die primäre Speicherkapazität Ihres Dateisystems erhöhen (in der Regel die Speicherkapazität jedes Aggregats

erhöhen) oder Ihre Volumes mithilfe des Volume-Move-Befehls in der ONTAP-CLI zwischen Aggregaten verschieben.

Ungleichgewicht bei der Dateiserver- und Festplattenleistung

Die Gesamtleistungsfunktionen Ihres Dateisystems (z. B. Netzwerkdurchsatz, Dateiserver-zu-Datenträger-Durchsatz und IOPS sowie Festplatten-IOPS) werden gleichmäßig auf die HA-Paare Ihres Dateisystems aufgeteilt. Wir empfehlen Ihnen, eine durchschnittliche Auslastung unter 50 % (und eine maximale Spitzenauslastung unter 80 %) für alle Leistungsgrenzen kontinuierlich beizubehalten. Dies gilt sowohl für die Gesamtauslastung der Dateiserverressourcen Ihres Dateisystems über alle HA-Paare als auch für die pro Dateiserver.

Wenn Sie feststellen, dass Ihre Dateiserver-Leistungsauslastung unausgewogen ist und die Dateiserver, auf denen Ihr Workload unausgewogen ist, eine fortlaufende Auslastung von über 80 % aufweisen, können Sie die ONTAP-CLI und die REST-API verwenden, um die Ursache des Leistungsungleichgewichts weiter zu diagnostizieren und zu beheben. Im Folgenden finden Sie eine Tabelle möglicher Ungleichgewichtsindikatoren und der nächsten Schritte zur weiteren Diagnose.

Wenn Ihr Dateisystem ...	Dann …
Dateiserver-Festplattendurchsatz oder Dateiserver-Festplatten-IOPS sind unausgewogen	Möglicherweise treten bei einer Teilmenge von HA-Paaren (einer Teilmenge Ihrer Volumes mit einer übergroßen Datenmenge, auf die zugegriffen wird) E/A-Abschwächungen auf, wodurch die Gesamtleistung Ihres Workloads eingeschränkt werden kann, da sie bei einer Teilmenge von HA-Paaren Engpässe aufweist. Überprüfen Sie für jeden stark ausgelasteten Dateiserver die am häufigsten ausgelasteten Volumes, um zu sehen, welche Volumes innerhalb eines Aggregats am meisten aktiv sind. Weitere Informationen zu diesem Verfahren finden Sie unter Wiederherstellen des Gleichgewichts von stark ausgelasteten Volumes.
Der Netzwerkdurchsatz ist unausgewogen, aber Ihr Dateiserver-Festplattendurchsatz, Dateiserver-	Ihre Daten werden gleichmäßig auf HA-Paare verteilt, Ihre Clients jedoch nicht. Überprüfen Sie für die Dateiserver, die mehr Netzwerkdurchsatz als andere haben, die Top-Clients für jeden Dateiserver, und verteilen Sie diese Clients dann neu, indem Sie das Mounting aller Volumes von diesen Clients aufheben und sie mit einem anderen Endpunkt auf einem anderen HA-Paar erneut mounten. Weitere

Wenn Ihr Dateisyst em ...	Dann …
Festplatten-IOPS oder Festplatten-IOPS sind nicht unausgewogen	Informationen zu diesem Verfahren finden Sie unter Neuausgleich von Clients mit hohem Datenverkehr.

Zuordnen von CloudWatch Dimensionen zu ONTAP-CLI- und REST-API-Ressourcen

Ihr Scale-Out-Dateisystem verfügt über Amazon- CloudWatch Metriken mit der `Aggregate` Dimension `FileServer` oder . Um Fälle von Ungleichgewichten weiter zu diagnostizieren, müssen Sie diese Dimensionswerte bestimmten Dateiservern (oder Knoten) und Aggregaten in der ONTAP-CLI oder REST-API zuordnen.

- Bei Dateiservern wird jeder Dateiname einem Dateiservernamen (oder Knoten) in ONTAP zugeordnet (z. B. `FsxId01234567890abcdef-01`). Odd-nummerierte Dateiserver sind bevorzugte Dateiserver (d. h. sie bedienen den Datenverkehr, es sei denn, das Dateisystem hat ein Failover auf den sekundären Dateiserver durchgeführt), während gerade nummerierte Dateiserver sekundäre Dateiserver sind (d. h. sie bedienen den Datenverkehr nur, wenn ihr Partner nicht verfügbar ist). Aus diesem Grund zeigen sekundäre Dateiserver in der Regel eine geringere Auslastung als bevorzugte Dateiserver.
- Bei Aggregaten wird jeder Aggregatname einem Aggregat in ONTAP zugeordnet (z. B. `aggr1`). Für jedes HA-Paar gibt es ein Aggregat, d. h. das Aggregat `aggr1` wird von Dateiservern `FsxId01234567890abcdef-01` (dem aktiven Dateiserver) und `FsxId01234567890abcdef-02` (dem sekundären Dateiserver) in einem HA-Paar gemeinsam genutzt, das Aggregat `aggr2` wird von Dateiservern `FsxId01234567890abcdef-03` und `FsxId01234567890abcdef-04`usw. gemeinsam genutzt.

Sie können die Zuordnungen zwischen allen Aggregaten und Dateiservern mithilfe der ONTAP-CLI anzeigen.

1. Um eine SSH-Verbindung zur NetApp ONTAP-CLI Ihres Dateisystems herzustellen, befolgen Sie die im Verwenden der NetApp ONTAP-CLI Abschnitt des Benutzerhandbuchs zu Amazon FSx für NetApp ONTAP dokumentierten Schritte.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Verwenden Sie den Befehl storage aggregate show, wobei Sie den `-fields node` Parameter angeben.

```
::> storage aggregate show -fields node
aggregate                     node
----------------------------- ------------------------
aggr1                         FsxId01234567890abcdef-01
aggr2                         FsxId01234567890abcdef-03
aggr3                         FsxId01234567890abcdef-05
aggr4                         FsxId01234567890abcdef-07
aggr5                         FsxId01234567890abcdef-09
aggr6                         FsxId01234567890abcdef-11
6 entries were displayed.
```

Neuausgleich von Clients mit hohem Datenverkehr

Wenn Sie ein E/A-Ungleichgewicht zwischen den Dateiservern feststellen (insbesondere bei der Netzwerkdurchsatzauslastung), können hohe E/A-Clients die Ursache sein. Verwenden Sie die ONTAP-CLI, um Clients mit hohem Datenverkehr zu identifizieren.

1. Um eine SSH-Verbindung zur NetApp ONTAP-CLI Ihres Dateisystems herzustellen, befolgen Sie die im Verwenden der NetApp ONTAP-CLI Abschnitt des Benutzerhandbuchs zu Amazon FSx für NetApp ONTAP dokumentierten Schritte.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Um die Clients mit dem höchsten Datenverkehr anzuzeigen, verwenden Sie den Statistik-Top-Client, der den ONTAP-CLI-Befehl anzeigt. Sie können optional den `-node` Parameter angeben, um nur die Top-Clients für einen bestimmten Dateiserver anzuzeigen. Wenn Sie ein Ungleichgewicht für einen bestimmten Dateiserver diagnostizieren, verwenden Sie den `-node` Parameter und ersetzen Sie durch `node_name` den Namen des Dateiservers (z. B. `FsxId01234567890abcdef-01`).

   Sie können optional den `-interval` Parameter hinzufügen und das Intervall angeben, in dem gemessen werden soll (in Sekunden), bevor jeder Bericht ausgegeben wird. Eine Erhöhung des

Intervalls (z. B. auf maximal 300 Sekunden) bietet eine längerfristige Stichprobe für die Menge des Datenverkehrs, der zu jedem Volume geleitet wird. Der Standardwert ist 5 (Sekunden).

```
::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
```

In der Ausgabe werden die Top-Clients anhand ihrer IP-Adresse und ihres Ports angezeigt.

```
                                                      *Total     Total
            Client   Vserver          Node                Ops     (Bps)
------------------ --------- ------------------------ ------ ---------
 172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
```

3. Sie können eine Teilmenge der aufgelisteten Clients mit hohem Datenverkehr mit anderen Dateiservern ausgleichen. Heben Sie dazu das Mounting des Volumes vom Client auf und mounten Sie es mit dem DNS-Namen für den NFS/SMB-Endpunkt der SVM erneut. Dies gibt einen zufälligen Endpunkt zurück, der einem zufälligen HA-Paar entspricht.

   Wir empfehlen Ihnen, den DNS-Namen wiederzuverwenden, aber Sie haben die Möglichkeit, explizit auszuwählen, welches HA-Paar ein bestimmter Client-Mounts enthält. Um sicherzustellen, dass Sie einen Client an einem anderen Endpunkt mounten, können Sie stattdessen eine andere Endpunkt-IP-Adresse angeben als die, die dem Knoten entspricht, bei dem ein hoher Datenverkehr auftritt. Führen Sie dazu den folgenden Befehl aus:

   ```
   ::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
    address,curr-node
   vserver   lif                  address      curr-node
   --------- -------------------- ------------ -------------------------
   svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
   svm01 nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
   2 entries were displayed.
   ```

   Laut der Beispielausgabe für den `statistics top client show` Befehl `172.17.236.53` führt der Client einen hohen Datenverkehr zu durch`FsxId01234567890abcdef-01`.
   Die Ausgabe des `network interface show` Befehls gibt an, dass dies die Adresse ist`172.31.15.89`. Um an einen anderen Endpunkt zu mounten, wählen Sie eine andere Adresse aus (in diesem Beispiel ist die einzige andere Adresse `172.31.8.112`, entsprechend `FsxId01234567890abcdef-03`).

Wiederherstellen des Gleichgewichts von stark ausgelasteten Volumes

Wenn Sie einen E/A-Ungleichgewicht zwischen Ihren Volumes oder Aggregaten feststellen, können Sie die Volumes neu verteilen, um Ihren E/A-Datenverkehr auf Ihre Volumes umzuverteilen.

> **Note**
>
> Wenn Sie ein Ungleichgewicht der Speicherauslastung in Ihren Aggregaten feststellen, gibt es im Allgemeinen keine Auswirkungen auf die Leistung, es sei denn, die hohe Auslastung ist mit einem E/A-Ungleichgewicht verbunden. Obwohl Sie Volumes zwischen Aggregaten verschieben können, um die Speicherauslastung auszugleichen, empfehlen wir, Volumes nur zu verschieben, wenn Sie Leistungseinbußen feststellen, da das Verschieben von Volumes negative Auswirkungen auf die Leistung haben kann, wenn Sie nicht auch die E/A berücksichtigen, die für jedes Volume bestimmt ist, das Sie verschieben möchten.

1. Um SSH in die NetApp ONTAP-CLI Ihres Dateisystems zu übertragen, befolgen Sie die im Verwenden der NetApp ONTAP-CLI Abschnitt des Benutzerhandbuchs zu Amazon FSx für NetApp ONTAP dokumentierten Schritte.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Verwenden Sie das Statistik-Volume show ONTAP CLI-Befehl, um die Volumes mit dem höchsten Datenverkehr für ein bestimmtes Aggregat anzuzeigen, mit den folgenden Änderungen:

   - Ersetzen Sie *aggregate_name* durch den Namen des Aggregats (z. B. `aggr1`).
   - Sie können optional den `-interval` Parameter hinzufügen und das Intervall angeben, in dem gemessen werden soll (in Sekunden), bevor jeder Bericht ausgegeben wird. Eine Erhöhung des Intervalls (z. B. auf maximal 300 Sekunden) bietet eine längerfristige Stichprobe für die Menge des Datenverkehrs, der zu jedem Volume geleitet wird. Der Standardwert ist 5 (Sekunden).

   ```
   ::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
    [5,300]]
   ```

Je nach ausgewähltem Intervall kann es bis zu 5 Minuten dauern, bis Daten angezeigt werden. Der Befehl zeigt alle Volumes im Aggregat zusammen mit der Menge des Datenverkehrs an, der zu jedem Aggregat geleitet wird.

```
                          *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (us)
---------- ------- --------- ------ ---- ----- ----- --------- ----- -------
vol1__0007    svm1     aggr1   4078 4078     0     0 267255808     0    1092
vol1__0005    svm1     aggr1   4078 4078     0     0 267255808     0    1086
vol1__0003    svm1     aggr1   4077 4077     0     0 267223040     0    1086
vol1__0001    svm1     aggr1   4077 4077     0     0 267239424     0    1087
vol1__0008    svm1     aggr2   2314 2314     0     0 151650304     0    1112
vol1__0006    svm1     aggr2   2144 2144     0     0 140509184     0    1104
vol1__0002    svm1     aggr2   2183 2183     0     0 143065088     0    1106
vol1__0004    svm1     aggr2   2183 2183     0     0 143065088     0    1103
```

Die Volume-Statistiken werden pro Komponente angezeigt (z. B. `vol1__0015` ist der 15. Konstituent für FlexGroup `vol1`). Sie können aus der Beispielausgabe sehen, dass die Bestandteile für stärker ausgelastet `aggr1` sind als die Bestandteile für `aggr2`. Um den Datenverkehr zwischen Aggregaten auszugleichen, können Sie die zugehörigen Volumes zwischen Aggregaten verschieben, sodass der Datenverkehr gleichmäßiger verteilt wird.

3. Um ein Volume zwischen Aggregaten zu verschieben, verwenden Sie den ONTAP-CLI-Befehl start für die Volume-Verschiebung und ersetzen Sie die folgenden Werte:

   - Ersetzen Sie *`svm_name`* durch den Namen der SVM, die das Volume hostet, das Sie verschieben.
   - Ersetzen Sie *`volume_name`* durch den Namen des Volume-Kontingents (z. B. `vol1__0001`).
   - Ersetzen Sie *`aggregate_name`* durch den Namen des Zielaggregats für das Volume.

   > **Important**
   >
   > Volume-Verlagerung verbraucht Netzwerk- und Festplattenressourcen für die Quell- und Zieldateiserver. Infolgedessen kann die Leistung Ihres Workloads durch laufende Volume-Verschiebungen beeinträchtigt werden. Darüber hinaus gibt es eine Cut-over-Phase des Volume-Mounting-Prozesses, die die E/A für jeden Datenverkehr zum Volume vorübergehend pausiert.

```
::> volume move start -vserver svm_name -volume volume_name -
destination aggregate_name -foreground false
[Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".
Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the
 status of this operation.
```

Verwenden Sie den `volume move show` ONTAP-CLI-Befehl , um den Status der Volume-Verschiebungsoperation zu überprüfen.

```
::> volume move show -vserver svm_name -volume volume_name
                          Vserver Name: svm01
                           Volume Name: vol1__0001
                 Actual Completion Time: -
                        Bytes Remaining: 1.00TB
           Specified Action For Cutover: retry_on_failure
         Specified Cutover Time Window: 30
                 Destination Aggregate: aggr2
                      Destination Node: FsxId01234567890abcdef-03
                       Detailed Status: Transferring data: 12.23GB sent.
                    Percentage Complete: 1%
                             Move Phase: replicating
               Prior Issues Encountered: -
          Estimated Remaining Duration: 00:40:25
                Replication Throughput: 434.3MB/s
                      Duration of Move: 00:00:27
                      Source Aggregate: aggr2
                           Source Node: FsxId01234567890abcdef-01
                            Move State: healthy
```

Dieser Befehl zeigt die geschätzte Zeit für den Abschluss der Verschiebung als eines der Informationsfelder an. Wenn der Vorgang abgeschlossen ist, zeigt derselbe Befehl an, dass das `Move Phase` Feld abgeschlossen ist.

Sie sollten sicherstellen, dass jedes gleichmäßig auf Ihre Aggregate verteilt FlexGroup ist, idealerweise mit den empfohlenen 8 Komponenten pro Aggregat. Wenn Sie ein einzelnes einzelnes einzelnes Volume in ein anderes Aggregat für ein ansonsten ausgewogenes verschiebenFlexGroup, sollten Sie wiederum ein anderes (weniger ausgelastetes) einzelnes Volume in das Quellaggregat verschieben, um das Gleichgewicht aufrechtzuerhalten.

Überwachen von FSx-für-ONTAP- -Ereignissen

Sie können FSx-für-ONTAP-Dateisystemereignisse mit dem nativen Ereignisverwaltungssystem (Speed) von NetAPP ONTAP überwachen. Sie können diese Ereignisse mit der NetApp ONTAP-CLI anzeigen.

Themen

- Übersicht über
- Anzeigen von
- Weiterleitung von an einen Syslog-Server

Übersicht über

sind automatisch generierte Benachrichtigungen, die Sie warnen, wenn in Ihrem FSx-für-ONTAP-Dateisystem eine vordefinierte Bedingung auftritt. Diese Benachrichtigungen halten Sie auf dem Laufenden, damit Sie Probleme verhindern oder beheben können, die zu größeren Problemen führen können, z. B. Probleme mit der Storage Virtual Machine (SVM)-Authentifizierung oder vollständige Volumes.

Standardmäßig werden Ereignisse im Event Management System-Protokoll protokolliert. Mit können Sie Ereignisse wie Änderungen des Benutzerpassworts, einen Bestandteil innerhalb einer FlexGroup fast vollständigen Kapazität, eine Logical Unit Number (LUN) wurde manuell online oder offline gebracht oder die Größe eines Volumes wurde automatisch geändert überwachen.

Weitere Informationen zu ONTAP-Telefonieereignissen finden Sie in der ONTAP-Referenz im NetApp ONTAP-Dokumentationscenter. Um die Ereigniskategorien anzuzeigen, verwenden Sie den linken Navigationsbereich des Dokuments.

> **Note**
>
> Für FSx-für-ONTAP-Dateisysteme sind nur einige ONTAP- Bol-Nachrichten verfügbar.

Beschreibungen von enthalten Ereignisnamen, Schweregrade, mögliche Ursachen, Protokollmeldungen und Korrekturmaßnahmen, anhand derer Sie entscheiden können, wie Sie reagieren möchten. Beispielsweise tritt ein wafl.vol.autoSize.fail-Ereignis auf, wenn die

automatische Dimensionierung eines Volumes fehlschlägt. Laut der Ereignisbeschreibung besteht die Korrekturmaßnahme darin, die maximale Größe des Volumes zu erhöhen und gleichzeitig die automatische Größe festzulegen.

Anzeigen von

Verwenden Sie den NetApp ONTAP-CLI-event log showBefehl, um den Inhalt des Ereignisprotokolls anzuzeigen. Dieser Befehl ist verfügbar, wenn Sie die `-fsxadmin`Rolle auf Ihrem Dateisystem haben. Die Befehlssyntax lautet wie folgt:

```
event log show [event_options]
```

Die neuesten Ereignisse werden zuerst aufgeführt. Standardmäßig zeigt dieser Befehl Ereignisse mit den `ERROR` `EMERGENCY`Schweregraden `ALERT`, und mit den folgenden Informationen an:

- Uhrzeit – Die Uhrzeit des Ereignisses.
- Knoten – Der Knoten, auf dem das Ereignis aufgetreten ist.
- Schweregrad – Der Schweregrad des Ereignisses. Verwenden Sie die `-severity` Option `NOTICE`, oder `INFORMATIONAL`, um Ereignisse mit `DEBUG` Schweregrad anzuzeigen.
- Ereignis – Der Ereignisname und die Nachricht.

Um detaillierte Informationen zu Ereignissen anzuzeigen, verwenden Sie eine oder mehrere der in der folgenden Tabelle aufgeführten Ereignisoptionen.

Ereignisoption	Beschreibung
`-detail`	Zeigt zusätzliche Ereignisi nformationen an.
`-detailtime`	Zeigt detaillierte Ereignisi nformationen in umgekehrter chronologischer Reihenfolge an.
`-instance`	Zeigt detaillierte Informationen zu allen Feldern an.

Ereignisoption	Beschreibung
`-node` *`nodename`*`|local`	Zeigt eine Liste der Ereignisse für den von Ihnen angegeben en Knoten an. Verwenden Sie diese Option mit `-seqnum`, um detaillierte Informationen anzuzeigen.
`-seqnum` *`sequence_number`*	Wählt die Ereignisse aus, die dieser Zahl in der Sequenz entsprechen. Verwenden Sie mit `-node`, um detaillierte Informationen anzuzeigen.

Ereignisoption	Beschreibung

`-time` *`MM/DD/YYYY HH:MM:SS`*	Wählt die Ereignisse aus, die zu diesem bestimmten Zeitpunkt aufgetreten sind. Verwenden Sie das Format: MM/TT/JJJJ HH:MM:SS [+- HH:MM]. Sie können einen Zeitraum angeben, indem Sie den `-..`Operator zwischen zwei Zeitanwei sungen verwenden.
	`event log show - time "04/17/2023 05:55:00".."04/17/ 2023 06:10:00"`
	Vergleichbare Zeitwerte sind relativ zur aktuellen Zeit, zu der Sie den Befehl ausführen . Das folgende Beispiel zeigt, wie nur Ereignisse angezeigt werden, die innerhalb der letzten Minute aufgetreten sind:
	`event log show -time >1m`
	Die Felder Monat und Datum dieser Option sind nicht mit Null aufgefüllt. Diese Felder können einzelne Ziffern sein, z. B. `4/1/2023 06:45:00`.

Ereignisoption	Beschreibung
`-severity sev_level`	Wählt die Ereignisse aus, die mit dem Wert *sev_level* übereinstimmen, der eines der folgenden sein muss: • `EMERGENCY` – Unterbrechung • `ALERT` – Einzelne Fehlerquelle • `ERROR` – Verschlechterung • `NOTICE` – Informationen • `INFORMATIONAL` – Informationen • `DEBUG` – Debuggen von Informationen Um alle Ereignisse anzuzeigen, geben Sie den Schweregrad wie folgt an: `event log show -severity <=DEBUG`

Ereignisoption	Beschreibung
`-ems-severity` *ems_sev_level*	Wählt die Ereignisse aus, die mit dem Wert *ems_sev_level* übereinstimmen, der einer der folgenden sein muss: • `NODE_FAULT` – Datenbeschädigung wird erkannt oder der Knoten kann den Client-Service nicht bereitstellen. • `SVC_FAULT` – Es wird ein vorübergehender Serviceverlust – in der Regel ein vorübergehender Softwarefehler – erkannt. • `NODE_ERROR` – Ein Hardwarefehler, der nicht sofort fatal ist, wird erkannt. • `SVC_ERROR` – Ein Softwarefehler, der nicht sofort fatal ist, wird erkannt. • `WARNING` – Eine Meldung mit hoher Priorität, die keinen Fehler anzeigt. • `NOTICE` – Eine Meldung mit normaler Priorität, die keinen Fehler anzeigt. • `INFO` – Eine Meldung mit niedriger Priorität, die keinen Fehler anzeigt. • `DEBUG` – Eine Debugging-Nachricht. • `VAR` – Eine Nachricht mit variablem Schweregrad,

Ereignisoption	Beschreibung
	die zur Laufzeit ausgewählt wurde. Um alle Ereignisse anzuzeigen, geben Sie den Schweregrad wie folgt an: `event log show -ems-severity <=DEBUG`
`-source` *`text`*	Wählt die Ereignisse aus, die dem *`Textwert`* entsprechen. Die Quelle ist in der Regel ein Softwaremodul.
`-message-name` *`message_name`*	Wählt die Ereignisse aus, die mit dem Wert *`message_name`* übereinstimmen. Nachrichtennamen sind beschreibend, sodass beim Filtern der Ausgabe nach Nachrichtennamen Nachrichten eines bestimmten Typs angezeigt werden.
`-event` *`text`*	Wählt die Ereignisse aus, die dem *`Textwert`* entsprechen. Das `event` Feld enthält den vollständigen Text des Ereignisses, einschließlich aller Parameter.

Ereignisoption	Beschreibung
`-kernel-generation-num` *integer*	Wählt die Ereignisse aus, die dem *Ganzzahlwert* entsprechen. Nur Ereignisse, die aus dem Kernel stammen, haben Zahlen zur Kernelgen erierung.
`-kernel-sequence-num` *integer*	Wählt die Ereignisse aus, die dem *Ganzzahlwert* entsprechen. Nur Ereignisse, die aus dem Kernel stammen, haben Kernel-Sequenznumm ern.
`-action` *text*	Wählt die Ereignisse aus, die dem *Textwert* entsprechen. Das `action` Feld beschreibt, welche Korrekturmaßnahmen Sie ggf. ergreifen müssen, um die Situation zu beheben.
`-description` *text*	Wählt die Ereignisse aus, die dem *Textwert* entsprech en. Das `description` Feld beschreibt, warum das Ereignis eingetreten ist und was es bedeutet.
`-filter-name` *filter_name*	Wählt die Ereignisse aus, die dem Wert *filter_name* entsprechen. Nur Ereigniss e, die in vorhandenen Filtern enthalten sind, die diesem Wert entsprechen, werden angezeigt.

Ereignisoption	Beschreibung
`-fields fieldname ,...`	Gibt an, dass die Befehlsausgabe auch das angegebene Feld oder die angegebenen Felder enthält. Sie können verwenden `-fields ?`, um die Felder auszuwählen, die Sie angeben möchten.

So zeigen Sie an

1. Um eine SSH-Verbindung zur NetApp ONTAP-CLI Ihres Dateisystems herzustellen, führen Sie die im Verwenden der NetApp ONTAP-CLI Abschnitt des Benutzerhandbuchs zu Amazon FSx für NetApp ONTAP dokumentierten Schritte aus.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Verwenden Sie den `event log show` Befehl , um den Inhalt des Ereignisprotokolls anzuzeigen.

   ```
   ::> event log show
   Time                Node          Severity      Event
   ------------------- ------------- ------------- ------------------------
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0a.
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0d.
   ```

Weitere Informationen zu den vom `event log show` Befehl zurückgegebenen finden Sie in der ONTAP-Referenz im NetApp ONTAP-Dokumentationscenter.

Weiterleitung von an einen Syslog-Server

Sie können so konfigurieren, dass Benachrichtigungen an einen Syslog-Server weitergeleitet werden. Die wird für die Echtzeitüberwachung Ihres Dateisystems verwendet, um die Ursachen für eine Vielzahl von Problemen zu ermitteln und zu isolieren. Wenn Ihre Umgebung noch keinen Syslog-

Server für Ereignisbenachrichtigungen enthält, müssen Sie zunächst einen erstellen. DNS muss auf dem Dateisystem konfiguriert sein, um den Syslog-Servernamen aufzulösen.

So konfigurieren Sie , um Benachrichtigungen an einen Syslog-Server weiterzuleiten

1. Um eine SSH-Verbindung zur NetApp ONTAP-CLI Ihres Dateisystems herzustellen, führen Sie die im Verwenden der NetApp ONTAP-CLI Abschnitt des Benutzerhandbuchs zu Amazon FSx für NetApp ONTAP dokumentierten Schritte aus.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Verwenden Sie den Befehl create für das Ereignisbenachrichtigungsziel, um ein Ereignisbenachrichtigungsziel vom Typ zu erstellen`syslog`, das die folgenden Attribute angibt:

   - *`dest_name`* – Der Name des zu erstellenden Benachrichtigungsziels (z. B. `syslog-ems`). Ein Zielname für Ereignisbenachrichtigungen muss 2 bis 64 Zeichen lang sein. Gültige Zeichen sind die folgenden ASCII-Zeichen: A-Z, a-z, 0-9, „_“ und „-“. Der Name muss beginnen und mit enden: A-Z, a-z oder 0-9.
   - *`syslog_name`* – Der Hostname oder die IP-Adresse des Syslog-Servers, an die Syslog-Nachrichten gesendet werden.
   - *`transport_protocol`* – Das Protokoll, das zum Senden der Ereignisse verwendet wird:
     - `udp-unencrypted` – User Datagram Protocol ohne Sicherheit. Dies ist das Standardprotokoll.
     - `tcp-unencrypted` – Transmission Control Protocol ohne Sicherheit.
     - `tcp-encrypted` – Transmission Control Protocol mit Transport Layer Security (TLS). Wenn diese Option angegeben ist, überprüft FSx für ONTAP die Identität des Ziel-Hosts, indem es sein Zertifikat validiert.
   - *`port_number`* – Der Syslog-Serverport, an den Syslog-Nachrichten gesendet werden. Der `syslog-port` Standardwertparameter hängt von der Einstellung für den `syslog-transport` Parameter ab. Wenn auf gesetzt `syslog-transport` ist`tcp-encrypted`, ist der `syslog-port` Standardwert `6514`. Wenn auf gesetzt `syslog-transport` ist`tcp-unencrypted`, `syslog-port` hat den Standardwert `601`. Andernfalls ist der Standardport auf festgelegt`514`.

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. Verwenden Sie den Befehl zum Erstellen von Ereignisbenachrichtigungen, um eine neue Benachrichtigung über eine Reihe von Ereignissen zu erstellen, die durch einen Ereignisfilter für das im vorherigen Schritt erstellte Benachrichtigungsziel definiert werden, wobei die folgenden Attribute angegeben werden:

   - *node_name* – Der Name des Ereignisfilters. Ereignisse, die im Ereignisfilter enthalten sind, werden an die im `-destinations` Parameter angegebenen Ziele weitergeleitet.
   - *dest_name* – Der Name des vorhandenen Benachrichtigungsziels, an das die Ereignisbenachrichtigungen gesendet werden.

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. Verwenden Sie den `event notification destination check` Befehl , um eine Testnachricht zu generieren und zu überprüfen, ob Ihre Einrichtung funktioniert. Geben Sie die folgenden Attribute mit dem Befehl an:

   - *node_name* – Der Name des Knotens (z. B. `FsxId07353f551e6b557b4-01`).
   - *dest_name* – Der Name des vorhandenen Benachrichtigungsziels, an das die Ereignisbenachrichtigungen gesendet werden.

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

Überwachung mit Cloud Insights

NetApp Cloud Insights ist ein NetApp Service, mit dem Sie Ihre Dateisysteme von Amazon FSx für NetApp ONTAP zusammen mit Ihren anderen NetApp Speicherlösungen überwachen können. Mit Cloud Insights können Sie Konfigurations-, Kapazitäts- und Leistungsmetriken im Laufe der Zeit überwachen, um die Trends Ihres Workloads zu verstehen und zukünftige Leistungs- und Speicherkapazitätsanforderungen zu planen. Sie können Warnungen auch basierend auf Metrikbedingungen erstellen, die in Ihre vorhandenen Workflows und Produktivitätstools integriert werden können.

> **Note**
>
> Cloud Insights wird für Scale-Out-Dateisysteme nicht unterstützt.

Cloud Insights bietet:

- Eine Vielzahl von Metriken und Protokollen – Erfassen Sie Konfigurations-, Kapazitäts- und Leistungsmetriken. Verstehen Sie mit vordefinierten Dashboards, Warnungen und Berichten, wie Ihr Workload im Trend ist.
- Benutzeranalysen und Ransomware-Schutz – Mit Cloud Secure- und ONTAP-Snapshots können Sie Benutzerfehler und Ransomware prüfen, erkennen, stoppen und beheben.
- SnapMirror Berichterstellung – Machen Sie sich mit Ihren SnapMirror Beziehungen vertraut und legen Sie Warnungen zu Replikationsproblemen fest.
- Kapazitätsplanung – Machen Sie sich mit den Ressourcenanforderungen von On-Premises-Workloads vertraut, damit Sie Ihre Workload auf eine effizientere FSx-für-ONTAP-Konfiguration migrieren können. Sie können diese Erkenntnisse auch verwenden, um zu planen, wann für Ihre FSx-für-ONTAP-Bereitstellung mehr Leistung oder Kapazität benötigt wird.

Weitere Informationen zu Cloud Insights finden Sie unter NetApp Cloud Insights auf NetApp Cloud Central.

Überwachen von FSx-für-ONTAP-Dateisystemen mitvest und Grafana

NetApp Bolvest ist ein Open-Source-Tool zum Sammeln von Leistungs- und Kapazitätsmetriken von ONTAP-Systemen und ist mit FSx für ONTAP kompatibel. Sie könnenvest mit Grafana für eine Open-Source-Überwachungslösung verwenden.

Erste Schritte mitvest und Grafana

Im folgenden Abschnitt wird beschrieben, wie Sievest und Grafana einrichten und konfigurieren können, um die Leistung und Speicherkapazitätsauslastung Ihres FSx-für-ONTAP-Dateisystems zu messen.

Sie können Ihr Dateisystem von Amazon FSx für NetApp ONTAP mithilfe von Bolvest und Grafana überwachen. NetApp Die Überwachung von ONTAP-Rechenzentren erfolgt durch Erfassen von

Leistungs-, Kapazitäts- und Hardwaremetriken von FSx-für-ONTAP-Dateisystemen. Grafana bietet ein Dashboard, in dem die erfasstenvest-Metriken angezeigt werden können.

Unterstützte Bolvest-Dashboards

Amazon FSx für NetApp ONTAP stellt einen anderen Satz von Metriken bereit als On-Premises NetApp -ONTAP. Daher `fsx` werden derzeit nur die folgenden mit gekennzeichneten out-of-the-box Bolvest-Dashboards für die Verwendung mit FSx für ONTAP unterstützt. In einigen der Bereiche in diesen Dashboards fehlen möglicherweise Informationen, die nicht unterstützt werden.

- ONTAP: Compliance
- ONTAP: Datenschutz-Snapshots
- ONTAP: Sicherheit
- ONTAP: SVM
- ONTAP: Volume

AWS CloudFormation-Vorlage

Um zu beginnen, können Sie eine -AWS CloudFormationVorlage bereitstellen, die automatisch eine Amazon EC2-Instance startet, auf dervest und Grafana ausgeführt werden. Als Eingabe für die AWS CloudFormation Vorlage geben Sie den `fsxadmin` Benutzer und den Amazon-FSx-Verwaltungsendpunkt für das Dateisystem an, das im Rahmen dieser Bereitstellung hinzugefügt wird. Nachdem die Bereitstellung abgeschlossen ist, können Sie sich beim Grafana-Dashboard anmelden, um Ihr Dateisystem zu überwachen.

Diese Lösung verwendet AWS CloudFormation, um die Bereitstellung der Bolvest- und Grafana-Lösung zu automatisieren. Die Vorlage erstellt eine Amazon EC2-Linux-Instance und installiert Bolvest- und Grafana-Software. Um diese Lösung zu verwenden, laden Sie die fsx-ontap-harvest-grafana.template-AWS CloudFormationVorlage herunter.

> **Note**
>
> Bei der Implementierung dieser Lösung werden die zugehörigen AWS Services abgerechnet. Weitere Informationen finden Sie auf den Seiten mit den Preisdetails für diese Services.

Amazon EC2-Instance-Typen

Bei der Konfiguration der Vorlage geben Sie den Amazon EC2- NetAppInstance-Typ an. Die Empfehlung für die Instance-Größe hängt davon ab, wie viele Dateisysteme Sie überwachen und wie viele Metriken Sie erfassen möchten. Mit der Standardkonfiguration NetApp empfiehlt für jedes 10 Dateisystem, das Sie überwachen, Folgendes:

- CPU: 2 Kerne
- Speicher: 1 GB
- Festplatte: 500 MB (meist von Protokolldateien verwendet)

Im Folgenden finden Sie einige Beispielkonfigurationen und den `t3` Instance-Typ, den Sie wählen können.

Dateisysteme	CPU	Festplatte	Instance-Typ
Unter 10	2 Kerne	500 MB	`t3.micro`
10–40	4 Kerne	1 000 MB	`t3.xlarge`
Mehr als 40	8 Kerne	2 000 MB	`t3.2xlarge`

Weitere Informationen zu Amazon EC2-Instance-Typen finden Sie unter Allzweck-Instances im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Instance-Port-Regeln

Stellen Sie beim Einrichten Ihrer Amazon EC2-Instance sicher, dass die Ports 3000 und 9090 für eingehenden Datenverkehr für die Sicherheitsgruppe geöffnet sind, in der sich die Amazon EC2-vest- und Grafana-Instance befindet.

Bereitstellungsverfahren

Mit dem folgenden Verfahren wird die Bolvest/Grafana-Lösung konfiguriert und bereitgestellt. Die Bereitstellung dauert etwa fünf Minuten. Bevor Sie beginnen, müssen Sie ein FSx-für-ONTAP-Dateisystem in einer Amazon Virtual Private Cloud (Amazon VPC) in Ihrem AWS Konto und die Parameterinformationen für die unten aufgeführte Vorlage ausführen. Weitere Informationen zum Erstellen eines Dateisystems finden Sie unter FSx für ONTAP-Dateisysteme erstellen.

So starten Sie den Bolvest/Grafana-Lösungs-Stack

1. Laden Sie die fsx-ontap-harvest-grafana.template-AWS CloudFormationVorlage herunter. Weitere Informationen zum Erstellen eines -AWS CloudFormationStacks finden Sie unter Erstellen eines Stacks auf der -AWS CloudFormationKonsole im AWS CloudFormation - Benutzerhandbuch.

   > **Note**
   >
   > Standardmäßig wird diese Vorlage in der AWS Region USA Ost (Nord-Virginia) gestartet. Sie müssen diese Lösung in einer startenAWS-Region, in der Amazon FSx verfügbar ist. Weitere Informationen finden Sie unter Amazon-FSx-Endpunkte und -Kontingente im Allgemeine AWS-Referenz.

2. Überprüfen Sie für Parameter die Parameter für die Vorlage und ändern Sie sie entsprechend den Anforderungen Ihres Dateisystems. Diese Lösung verwendet die folgenden Standardwerte.

Parameter	Standard	Beschreibung
InstanceType	`t3.micro`	Der Amazon EC2-Instance-Typ. Im Folgenden sind die `t3` Instance-Typen aufgeführt. • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` Eine vollständige Liste der zulässigen Amazon EC2-Instance-Typwerte für diesen Parameter finden Sie unter

Parameter	Standard	Beschreibung
		fsx-ontap-harvest-grafana.template.
KeyPair	Kein Standardwert	Das Schlüsselpaar, das für den Zugriff auf die Amazon EC2 verwendet wird.
SecurityGroup	Kein Standardwert	Die Sicherheitsgruppen-ID für dievest/Grafana-Instance. Stellen Sie sicher, dass die eingehenden Ports 3000 und 9090 von den Clients aus geöffnet sind, die Sie für den Zugriff auf Ihr Grafana-Dashboard verwenden möchten.
Subnetztyp	Kein Standardwert	Geben Sie den Subnetztyp an, entweder `public` oder `private`. Verwenden Sie ein `public` Subnetz für Ressourcen, die mit dem Internet verbunden sein müssen, und ein privates Subnetz für Ressourcen, die nicht mit dem Internet verbunden sein werden. Weitere Informationen finden Sie unter Subnetztypen im Amazon-VPC-Benutzerhandbuch.

Parameter	Standard	Beschreibung
Subnetz	Kein Standardwert	Geben Sie dasselbe Subnetz an wie das bevorzugte Subnetz Ihres Amazon FSx for NetApp ONTAP-Dateisystems. Sie finden die bevorzugte Subnetz-ID des Dateisystems in der Amazon-FSx-Konsole auf der Registerkarte Netzwerk und Sicherheit der Detailseite des FSx-für-ONTAP-Dateisystems.
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	Die neueste Version des Amazon Linux 2-AMI in einer bestimmten AWS-Region.
FSxEndPoint	Kein Standardwert	Die IP-Adresse des Verwaltungsendpunkts des Dateisystems. Sie finden die IP-Adresse des Verwaltungsendpunkts des Dateisystems in der Amazon-FSx-Konsole auf der Registerkarte Administration der Seite mit den Details des FSx-für-ONTAP-Dateisystems.

Parameter	Standard	Beschreibung
SecretName	Kein Standardwert	AWS Secrets Manager Der geheime Name, der das Passwort für den `fsxadmin` Benutzer des Dateisyst ems enthält. Dies ist das Passwort, das Sie beim Erstellen des Dateisystems angegeben haben.

3. Wählen Sie Weiter aus.
4. Wählen Sie für Optionen die Option Weiter aus.
5. Überprüfen und bestätigen Sie für Überprüfen die Einstellungen. Sie müssen das Kontrollkästchen aktivieren, um zu bestätigen, 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 anzeigen. Sie sollten in etwa fünf Minuten den Status CREATE_COMPLETE sehen.

Anmelden bei Grafana

Nachdem die Bereitstellung abgeschlossen ist, verwenden Sie Ihren Browser, um sich am Grafana-Dashboard an der IP und Port 3000 der Amazon EC2-Instance anzumelden:

```
http://EC2_instance_IP:3000
```

Wenn Sie dazu aufgefordert werden, verwenden Sie den Grafana-Standardbenutzernamen (`admin`) und das Passwort (`pass`). Wir empfehlen Ihnen, Ihr Passwort zu ändern, sobald Sie sich anmelden.

Weitere Informationen finden Sie auf der NetApp Bolvest-Seite auf GitHub.

Fehlerbehebungvest und Grafana

Wenn Sie auf fehlende Daten stoßen, die in den Dashboards Bolvest und Grafana erwähnt werden, oder Probleme bei der Einrichtung vonvest und Grafana mit FSx für ONTAP haben, finden Sie in den folgenden Themen eine mögliche Lösung.

Themen

- SVM- und Volume-Dashboards sind leer
- CloudFormation Stack nach Timeout zurückgesetzt

SVM- und Volume-Dashboards sind leer

Wenn der AWS CloudFormationStack erfolgreich bereitgestellt wurde und Grafana kontaktieren kann, die SVM- und Volume-Dashboards jedoch leer sind, gehen Sie wie folgt vor, um Probleme in Ihrer Umgebung zu beheben. Sie benötigen SSH-Zugriff auf die Amazon EC2-Instance, auf der Bolvest und Grafana bereitgestellt werden.

1. SSH in die Amazon EC2-Instance, auf der Ihrevest- und Grafana-Clients ausgeführt werden.

   ```
   [~]$ ssh ec2-user@ec2_ip_address
   ```

2. Verwenden Sie den folgenden Befehl, um die `harvest.yml` Datei zu öffnen und:

   - Stellen Sie sicher, dass ein Eintrag für Ihre FSx-für-ONTAP-Instance als erstellt wurde`Cluster-2`.
   - Stellen Sie sicher, dass die Einträge für Benutzername und Passwort mit Ihren -`fsxadmin`Anmeldeinformationen übereinstimmen.

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/
   harvest.yml
   ```

3. Wenn das Passwortfeld leer ist, öffnen Sie die Datei in einem Editor und aktualisieren Sie sie mit dem `fsxadmin` Passwort wie folgt:

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
   harvest.yml
   ```

4. Stellen Sie sicher, dass die `fsxadmin` Benutzeranmeldeinformationen in Secrets Manager im folgenden Format für zukünftige Bereitstellungen gespeichert sind, und ersetzen Sie durch *`fsxadmin_password`* Ihr Passwort.

   ```
   {"username" : "fsxadmin", "password" : "fsxadmin_password"}
   ```

CloudFormation Stack nach Timeout zurückgesetzt

Wenn Sie den CloudFormation Stack nicht erfolgreich bereitstellen können und er mit Fehlern zurückgesetzt wird, gehen Sie wie folgt vor, um das Problem zu beheben. Sie benötigen SSH-Zugriff auf die EC2-Instance, die vom CloudFormation Stack bereitgestellt wird.

1. Stellen Sie den CloudFormation Stack erneut bereit und stellen Sie sicher, dass das automatische Rollback deaktiviert ist.
2. SSH in die Amazon EC2-Instance, auf der Ihrevest- und Grafana-Clients ausgeführt werden.

   ```
   [~]$ ssh ec2-user@ec2_ip_address
   ```

3. Überprüfen Sie, ob die Docker-Container erfolgreich gestartet wurden, indem Sie den folgenden Befehl verwenden.

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
   ```

   In der Antwort sollten Sie fünf Container wie folgt sehen:

   ```
   CONTAINER ID   IMAGE                  COMMAND                  CREATED
    STATUS                          PORTS                    NAMES
   6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
    Restarting (1) 20 seconds ago                            harvest_cluster-2
   3cf3e3623fde   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago   Up
    About a minute                                           harvest_cluster-1
   708f3b7ef6f8   grafana/grafana         "/run.sh"                8 minutes ago   Up
    8 minutes                   0.0.0.0:3000->3000/tcp   harvest_grafana
   0febee61cab7   prom/alertmanager       "/bin/alertmanager -…"   8
    minutes ago   Up 8 minutes                    0.0.0.0:9093->9093/tcp
    harvest_prometheus_alertmanager
   1706d8cd5a0c   prom/prometheus         "/bin/prometheus --c…"   8 minutes ago   Up
    8 minutes                   0.0.0.0:9090->9090/tcp   harvest_prometheus
   ```

4. Wenn die Docker-Container nicht ausgeführt werden, überprüfen Sie wie folgt, ob in der `/var/log/cloud-init-output.log` Datei Fehler auftreten.

   ```
   [ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
        PLAY [Manage Harvest]
    ***********************************************************

   TASK [Gathering Facts] ***********************************************************
   ```

```
ok: [localhost]

TASK [Verify images] ************************************************************
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
 "changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
 ('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
 "changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP **********************************************************************
localhost                  : ok=1    changed=0    unreachable=0    failed=1
 skipped=0    rescued=0    ignored=0
```

5. Wenn es Fehler gibt, führen Sie die folgenden Befehle aus, um die Bolvest- und Grafana-Container bereitzustellen.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
     [ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml --tags api
```

6. Validieren Sie die Container, die erfolgreich gestartet wurden, indem Sie ausführen sudo docker ps und eine Verbindung zu Ihrervest- und Grafana-URL herstellen.

Protokollieren von FSx für ONTAP-API-Aufrufe mitAWS CloudTrail

Amazon FSx ist integriert mitAWS CloudTrailEin Service, der die Aktionen eines Benutzers, einer Rolle oder eines Benutzers oder einer Rolle protokolliert.AWSService in Amazon FSx. CloudTrail erfasst alle Amazon FSx API-Aufrufe für Amazon FSx für NetApp ONTAP als Ereignisse. Zu erfassten Anrufen gehören Aufrufe von der Amazon FSx-Konsole und Codeaufrufe von Amazon FSx API-Operationen.

Wenn Sie einen Trail erstellen, aktivieren Sie die kontinuierliche Bereitstellung von CloudTrail Ereignisse in einem Amazon S3 S3-Bucket, einschließlich Ereignissen für Amazon FSx. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole inEreignisverlaufaus. Mit den von CloudTrail erfassten Informationen können Sie ermitteln, welche Anforderung an Amazon FSx gestellt wurde. Sie können auch die IP-Adresse, von der die Anforderung ausging, den Ersteller und den Erstellungszeitpunkt sowie weitere Details bestimmen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Amazon FSx Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Erfolgen API-Aktivitäten im Amazon FSx, werden diese als CloudTrail Event zusammen mit anderenAWS-Service-Ereignisse inEreignisverlaufaus. Sie können die neusten Ereignisse in Ihr AWS-Konto downloaden und dort suchen und anzeigen. Weitere Informationen finden Sie unterAnzeigen von Ereignissen mit CloudTrail Ereignisverlaufaus.

Für eine kontinuierliche Aufzeichnung von Ereignissen in IhremAWSErstellen Sie einen Trail, einschließlich Ereignissen für Amazon FSx. EINWanderwegaktiviert CloudTrail um Protokolldateien an einen Amazon S3 S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen AWS-Regionen in der AWS-Partition und stellt die Protokolldateien in dem Amazon-S3-Bucket bereit, den Sie angeben. Darüber hinaus können Sie andere konfigurierenAWS-Services zur weiteren Analyse und zur Reaktion der in erfassten Ereignisdaten CloudTrail protokolliert. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail-Benutzerhandbuch:

- Erstellen eines Trails für AWS-Konto
- AWS-Service-Integrationen mit CloudTrail Protokolle
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail

- Empfangen CloudTrail Protokolldateien aus mehreren RegionenundEmpfangen von CloudTrail-Protokolldateien von mehreren Konten

Alle Amazon FSxAPI-Aufrufewerden von CloudTrail protokolliert. Zum Beispiel werden durch AufrufeCreateFileSystemundTagResourceOperationen 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.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie im .CloudTrail-userIdentity-ElementimAWS CloudTrail-Benutzerhandbuch.

Grundlagen zu Amazon FSx -Protokolldateieinträgen

EINWanderwegist 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. Importieren in &S3;Veranstaltungstellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anforderungsparameter. CloudTrail -Protokolleinträge sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der dieTagResource-Operation, wenn ein Tag für das 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 Protokolleintrag, der die`UntagResource`-Aktion, wenn ein Tag für das Dateisystem von der Konsole aus 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"
}
```

Kontingente

Im Folgenden erfahren Sie mehr über die Kontingente bei der Arbeit mit Amazon FSx für NetApp ONTAP.

Themen

- Kontingente, die Sie erhöhen können
- Ressourcenkontingente für jedes Dateisystem

Kontingente, die Sie erhöhen können

Im Folgenden finden Sie die Kontingente für Amazon FSx für NetApp ONTAP für jede AWS-Konto, pro AWS-Region, die Sie erhöhen können.

Ressource	Standard	Beschreibung
ONTAP-Dateisysteme	100	Die maximale Anzahl der Dateisysteme von Amazon FSx für NetApp ONTAP, die Sie in diesem Konto erstellen können.
ONTAP-SSD-Speicher kapazität	524.288	Die maximale SSD-Speic herkapazität (in GiB) für alle Dateisysteme von Amazon FSx für NetApp ONTAP, die Sie in diesem Konto haben können.
ONTAP-Durchsatzkapazität	10,240	Die maximale Durchsatz kapazität (in MBps für alle Dateisysteme von Amazon FSx für NetApp ONTAP, die Sie in diesem Konto haben können.

Ressource	Standard	Beschreibung
ONTAP-SSD-IOPS	1 000 000	Die maximale Menge an SSD-IOPS für alle Dateisysteme von Amazon FSx für NetApp ONTAP, die Sie in diesem Konto haben können.
ONTAP-Backups pro Dateisystem	10.000	Die maximale Anzahl von vom Benutzer initiierten Volume-Backups für alle Dateisysteme von Amazon FSx für NetApp ONTAP, die Sie in diesem Konto haben können.

So fordern Sie eine Kontingenterhöhung an

1. Öffnen Sie die Seite AWS Support, melden Sie sich ggf. an und wählen Sie dann Create case (Fall erstellen) aus.
2. Wählen Sie für Fall erstellen die Option Konto- und Fakturierungsunterstützung aus.
3. Führen Sie im Bereich Falldetails die folgenden Einträge aus:
   - Wählen Sie für Typ die Option Konto aus.
   - Wählen Sie für Kategorie Andere Kontoprobleme aus.
   - Geben Sie für Betreff ein**`Amazon FSx for NetApp ONTAP service limit increase request`**.
   - Geben Sie eine detaillierte Beschreibung Ihrer Anfrage an, einschließlich:
     - Das FSx-Kontingent, das Sie erhöhen möchten, und der Wert, auf den es erhöht werden soll, falls bekannt.
     - Der Grund, warum Sie die Kontingenterhöhung beantragen.
     - Die Dateisystem-ID und die Region für jedes Dateisystem, für das Sie eine Erhöhung beantragen.
4. Geben Sie Ihre bevorzugten Kontaktoptionen an und wählen Sie Senden.

Ressourcenkontingente für jedes Dateisystem

In der folgenden Tabelle sind die Kontingente für Amazon FSx für NetApp ONTAP-Ressourcen für jedes Dateisystem in einem aufgeführt AWS-Region.

Ressource	Limit pro Dateisystem
Minimale SSD-Speicherkapazität	1 024 GiB pro Hochverfügbarkeits paar (HA)
Maximale SSD-Speicherkapazität	• Aufskalierung: 512 TiB pro HA-Paar, bis zu 1 PiB • Hochskalierung: 192 TiB
Maximale SSD-IOPS	Aufskalierung: • 200 000 pro HA-Paar (bis zu 12 Paare) Hochskalieren: • 160 000 in den Regionen USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Oregon) und Europa (Irland) • 80 000 in allen anderen , in AWS-Regionen denen FSx für ONTAP verfügbar ist
Minimale Durchsatzkapazität	• Aufskalierung: 3 072 MBps pro HA-Paar • Hochskalierung: 128 MBpss
Maximale Durchsatzkapazität	Aufskalierung: • 73 728 MBps [1] Hochskalieren:

Ressource	Limit pro Dateisystem
	• 4 096 MBpss [2] in den Regionen USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Oregon) und Europa (Irland) • 2 048 MBps in allen anderen , in AWS-Regionen denen FSx für ONTAP verfügbar ist
Maximale Anzahl von Volumes	• Aufskalierung: 1 000 • Hochskalierung: 500
Maximale Anzahl von Snapshots	1 023 pro Volume[3]
Maximale Anzahl von Backups	4 091 pro Volume[4]
Maximale Anzahl von SVMs	Aufskalierung: • 5 Hochskalieren: • 6 (Durchsatzkapazität von 128 MBpss) • 6 (256 MBpss Durchsatzkapazität) • 14 (512 MBpss Durchsatzkapazität) • 14 (1 024 MBpss Durchsatz kapazität) • 24 (2 048 MBpss Durchsatz kapazität) • 24 (Durchsatzkapazität von 4 096 MBpss)
Maximale Anzahl von Tags	50

Ressource	Limit pro Dateisystem
Maximale Aufbewahrungsdauer für automatisierte Backups	90 Tage
Maximale Aufbewahrungsdauer für vom Benutzer initiierte Backups	Kein Aufbewahrungslimit

Note

[1] Auf einem Scale-Out-Dateisystem mit 12 HA-Paaren (6.144 MBpss pro HA-Paar). Weitere Informationen finden Sie unter Paare mit hoher Verfügbarkeit (HA).

[2] Um 4 GBpss Durchsatzkapazität bereitzustellen, erfordert Ihr FSx-für-ONTAP-Skalierungsdateisystem eine Konfiguration der maximalen SSD-IOPS (160.000) und mindestens 5.120 GiB SSD-Speicherkapazität in einer unterstützten AWS-Region. Weitere Informationen darüber, welche 4 096 MBpss Durchsatzkapazität AWS-Regionen unterstützen, finden Sie unter Auswirkungen der Durchsatzkapazität auf die Leistung.

[3] Sie können jederzeit bis zu 1 023 Snapshots pro Volume speichern. Sobald Sie dieses Limit erreicht haben, müssen Sie einen vorhandenen Snapshot löschen, bevor ein neuer Snapshot Ihres Volumes erstellt werden kann.

[4] Sie können jederzeit bis zu 4 091 Backups pro Volume speichern. Sobald Sie dieses Limit erreicht haben, müssen Sie ein vorhandenes Backup löschen, bevor ein neues Backup Ihres Volumes erstellt werden kann.

Fehlerbehebung bei Amazon FSx für NetApp ONTAP

Verwenden Sie die folgenden Abschnitte, um Probleme zu beheben, die Sie mit FSx für ONTAP haben.

Themen

- Mein Multi-AZ-Dateisystem befindet sich in einem -MISCONFIGUREDZustand
- Sie können nicht auf Ihr Dateisystem zugreifen
- Sie können eine virtuelle Speichermaschine (SVM) nicht mit Active Directory verbinden
- Sie können eine virtuelle Speichermaschine oder ein virtuelles Volume nicht löschen
- Automatische tägliche Backups schlagen aufgrund unzureichender Volume-Kapazität fehl
- Sie verfügen über unzureichende Volume-Kapazität
- Fehlerbehebung bei Netzwerkproblemen

Mein Multi-AZ-Dateisystem befindet sich in einem -**MISCONFIGURED**Zustand

Es gibt eine Reihe potenzieller Ursachen dafür, dass sich ein Dateisystem wie folgt in einem -MISCONFIGUREDZustand befindet, der jeweils eine eigene Auflösung aufweist.

Themen

- Das VPC-Eigentümerkonto hat die Multi-AZ-VPC-Freigabe deaktiviert
- Sie können keine neue SVM auf einem Multi-AZ-Dateisystem erstellen

Das VPC-Eigentümerkonto hat die Multi-AZ-VPC-Freigabe deaktiviert

Multi-AZ-Dateisysteme, die von einem Teilnehmer AWS-Konto in einem gemeinsam genutzten VPC-Subnetz erstellt wurden, gehen aus einem der folgenden Gründe in einen -MISCONFIGUREDZustand über:

- Das Besitzerkonto, das das VPC-Subnetz freigegeben hat, hat die Multi-AZ-VPC-Freigabeunterstützung für FSx-für-ONTAP-Dateisysteme deaktiviert.
- Das Besitzerkonto hat die Freigabe des VPC-Subnetzes aufgehoben.

Wenn das Besitzerkonto die Freigabe des VPC-Subnetzes aufgehoben hat, wird in der Konsole für dieses Dateisystem die folgende Meldung angezeigt:

```
The vpc ID vpc-012345abcde does not exist
```

Sie müssen sich an das Besitzerkonto wenden, das das VPC-Subnetz für Sie freigegeben hat, um das Problem zu beheben. Weitere Informationen finden Sie unter FSx für ONTAP-Dateisysteme in gemeinsam genutzten Subnetzen erstellen .

Sie können keine neue SVM auf einem Multi-AZ-Dateisystem erstellen

Bei Multi-AZ-Dateisystemen, die von einem Teilnehmer AWS-Konto in einer freigegebenen VPC erstellt wurden, können Sie aus einem der folgenden Gründe keine neue SVM erstellen:

- Das Besitzerkonto, das das VPC-Subnetz freigegeben hat, hat die Multi-AZ-VPC-Freigabeunterstützung für FSx-für-ONTAP-Dateisysteme deaktiviert.
- Das Besitzerkonto hat die Freigabe des VPC-Subnetzes aufgehoben.

Sie müssen sich an das Besitzerkonto wenden, das das VPC-Subnetz für Sie freigegeben hat, um das Problem zu beheben. Weitere Informationen finden Sie unter FSx für ONTAP-Dateisysteme in gemeinsam genutzten Subnetzen erstellen .

Sie können nicht auf Ihr Dateisystem zugreifen

Es gibt eine Reihe potenzieller Ursachen dafür, dass Sie nicht auf Ihr Dateisystem zugreifen können, und zwar mit jeweils einer eigenen Auflösung, wie folgt.

Themen

- Die Elastic Network-Schnittstelle des Dateisystems wurde geändert oder gelöscht
- Die Elastic IP-Adresse, die an die Elastic Network-Schnittstelle des Dateisystems angefügt ist, wurde gelöscht
- Der VPC-Sicherheitsgruppe des Dateisystems fehlen die erforderlichen Regeln für eingehenden Datenverkehr
- Der VPC-Sicherheitsgruppe der Datenverarbeitungs-Instance fehlen die erforderlichen Regeln für ausgehenden Datenverkehr

- Das Subnetz der Datenverarbeitungs-Instance verwendet keine der Routing-Tabellen, die Ihrem Dateisystem zugeordnet sind
- Amazon FSx kann die Routing-Tabelle für Multi-AZ-Dateisysteme, die mit erstellt wurden, nicht aktualisieren AWS CloudFormation
- Kann nicht von einem Client in einer anderen VPC über iSCSI auf ein Dateisystem zugreifen
- Das besitzende Konto hat die Freigabe des VPC-Subnetzes aufgehoben
- Kann nicht über NFS, SMB, die ONTAP-CLI oder die ONTAP-REST-API von einem Client in einer anderen VPC oder On-Premises auf ein Dateisystem zugreifen

Die Elastic Network-Schnittstelle des Dateisystems wurde geändert oder gelöscht

Sie dürfen keine der Elastic Network-Schnittstellen des Dateisystems ändern oder löschen. Das Ändern oder Löschen einer Netzwerkschnittstelle kann zu einem dauerhaften Verbindungsverlust zwischen Ihrer Virtual Private Cloud (VPC) und Ihrem Dateisystem führen. Erstellen Sie ein neues Dateisystem und ändern oder löschen Sie die Amazon-FSx-Netzwerkschnittstelle nicht. Weitere Informationen finden Sie unter Dateisystem-Zugriffskontrolle mit Amazon VPC.

Die Elastic IP-Adresse, die an die Elastic Network-Schnittstelle des Dateisystems angefügt ist, wurde gelöscht

Amazon FSx unterstützt nicht den Zugriff auf Dateisysteme aus dem öffentlichen Internet. Amazon FSx trennt automatisch jede Elastic IP-Adresse, bei der es sich um eine öffentliche IP-Adresse handelt, die vom Internet erreichbar ist und an die Elastic Network-Schnittstelle eines Dateisystems angehängt wird. Weitere Informationen finden Sie unter Unterstützte Clients.

Der VPC-Sicherheitsgruppe des Dateisystems fehlen die erforderlichen Regeln für eingehenden Datenverkehr

Überprüfen Sie die in angegebenen Regeln für eingehenden Datenverkehr und stellen Sie sicherAmazon VPC-Sicherheitsgruppen, dass die mit Ihrem Dateisystem verknüpfte Sicherheitsgruppe über die entsprechenden Regeln für eingehenden Datenverkehr verfügt.

Der VPC-Sicherheitsgruppe der Datenverarbeitungs-Instance fehlen die erforderlichen Regeln für ausgehenden Datenverkehr

Überprüfen Sie die in angegebenen Regeln für ausgehenden Datenverkehr und stellen Sie sicher, dass die SicherheitsgruppeAmazon VPC-Sicherheitsgruppen, die Ihrer Rechen-Instance zugeordnet ist, über die entsprechenden Regeln für ausgehenden Datenverkehr verfügt.

Das Subnetz der Datenverarbeitungs-Instance verwendet keine der Routing-Tabellen, die Ihrem Dateisystem zugeordnet sind

FSx für ONTAP erstellt Endpunkte für den Zugriff auf Ihr Dateisystem in einer VPC-Routing-Tabelle. Wir empfehlen Ihnen, Ihr Dateisystem so zu konfigurieren, dass alle VPC-Routing-Tabellen verwendet werden, die den Subnetzen zugeordnet sind, in denen sich Ihre Clients befinden. Standardmäßig verwendet Amazon FSx die Haupt-Routing-Tabelle Ihrer VPC. Sie können optional eine oder mehrere Routing-Tabellen angeben, die Amazon FSx beim Erstellen Ihres Dateisystems verwenden soll.

Wenn Sie den Intercluster-Endpunkt Ihres Dateisystems, aber nicht den Verwaltungsendpunkt Ihres Dateisystems anpingen können (Ressourcen des Dateisystemsweitere Informationen finden Sie unter), befindet sich Ihr Client wahrscheinlich nicht in einem Subnetz, das einer der Routing-Tabellen Ihres Dateisystems zugeordnet ist. Um auf Ihr Dateisystem zuzugreifen, verknüpfen Sie eine der Routing-Tabellen Ihres Dateisystems mit dem Subnetz Ihres Clients. Informationen zum Aktualisieren der Amazon-VPC-Routing-Tabellen Ihres Dateisystems finden Sie unter Aktualisierung eines Dateisystems.

Amazon FSx kann die Routing-Tabelle für Multi-AZ-Dateisysteme, die mit erstellt wurden, nicht aktualisieren AWS CloudFormation

Amazon FSx verwaltet VPC-Routing-Tabellen für Multi-AZ-Dateisysteme mithilfe der Tag-basierten Authentifizierung. Diese Routing-Tabellen sind mit gekennzeichnet`Key: AmazonFSx; Value: ManagedByAmazonFSx`. Wenn Sie Multi-AZ-Dateisysteme von FSx für ONTAP mit erstellen oder aktualisieren, empfehlen AWS CloudFormation wir Ihnen, das `Key: AmazonFSx; Value: ManagedByAmazonFSx` Tag manuell hinzuzufügen.

Wenn Sie Ihr Multi-AZ-Dateisystem nicht erreichen können, überprüfen Sie, ob die mit dem Dateisystem verknüpften VPC-Routing-Tabellen mit gekennzeichnet sind`Key: AmazonFSx; Value: ManagedByAmazonFSx`. Wenn dies nicht der Fall ist, kann Amazon FSx diese Routing-

Tabellen nicht aktualisieren, um die schwebenden IP-Adressen der Verwaltungs- und Datenports an den aktiven Dateiserver weiterzuleiten, wenn ein Failover-Ereignis auftritt. Informationen zum Aktualisieren der Amazon-VPC-Routing-Tabellen Ihres Dateisystems finden Sie unter Aktualisierung eines Dateisystems.

Kann nicht von einem Client in einer anderen VPC über iSCSI auf ein Dateisystem zugreifen

Um von einem Client in einer anderen VPC über das Internet Small Computer Systems Interface (iSCSI)-Protokoll auf ein Dateisystem zuzugreifen, können Sie Amazon VPC Peering oder AWS Transit Gateway zwischen der VPC, die Ihrem Dateisystem zugeordnet ist, und der VPC konfigurieren, in der sich Ihr Client befindet. Weitere Informationen finden Sie unter Erstellen und Akzeptieren von VPC-Peering-Verbindungen im Amazon Virtual Private Cloud-Handbuch.

Das besitzende Konto hat die Freigabe des VPC-Subnetzes aufgehoben

Wenn Sie Ihr Dateisystem in einem VPC-Subnetz erstellt haben, das für Sie freigegeben wurde, hat das besitzende Konto möglicherweise die Freigabe des VPC-Subnetzes aufgehoben.

Wenn das Besitzerkonto die Freigabe des VPC-Subnetzes aufgehoben hat, wird in der Konsole für dieses Dateisystem die folgende Meldung angezeigt:

```
The vpc ID vpc-012345abcde does not exist
```

Sie müssen das besitzende Konto kontaktieren, damit es das Subnetz erneut für Sie freigeben kann.

Kann nicht über NFS, SMB, die ONTAP-CLI oder die ONTAP-REST-API von einem Client in einer anderen VPC oder On-Premises auf ein Dateisystem zugreifen

Um von einem Client in einer anderen VPC oder On-Premises auf ein Dateisystem über Network File System (NFS), Server Message Block (SMB) oder die NetApp ONTAP-CLI und REST-API zuzugreifen, müssen Sie das Routing mithilfe AWS Transit Gateway von zwischen der VPC, die Ihrem Dateisystem zugeordnet ist, und dem Netzwerk, in dem sich Ihr Client befindet, konfigurieren. Weitere Informationen finden Sie unter Zugriff auf -Daten.

Sie können eine virtuelle Speichermaschine (SVM) nicht mit Active Directory verbinden

Wenn Sie eine SVM nicht mit einem Active Directory (AD) verbinden können, überprüfen Sie zunächst Verbinden von SVMs mit einem Microsoft Active Directory. Häufige Probleme, die verhindern, dass eine SVM mit Ihrem Active Directory verbunden wird, sind in den folgenden Abschnitten aufgeführt, einschließlich der für jeden Umstand generierten Fehlermeldungen.

Themen

- Der SVM-NetBIOS-Name entspricht dem NetBIOS-Namen für die Heimatdomäne.
- Die SVM ist bereits mit einem anderen Active Directory verbunden
- Amazon FSx kann keine Verbindung zu Ihren Active-Directory-Domain-Controllern herstellen, da der NetBIOS-Name der SVM bereits verwendet wird
- Amazon FSx kann nicht mit Ihren Active-Directory-Domain-Controllern kommunizieren
- Amazon FSx kann aufgrund nicht erfüllter Portanforderungen oder Servicekontoberechtigungen keine Verbindung zu Ihrem Active Directory herstellen
- Amazon FSx kann keine Verbindung zu Ihren Active-Directory-Domain-Controllern herstellen, da die Anmeldeinformationen für das Servicekonto ungültig sind
- Amazon FSx kann aufgrund unzureichender Servicekonto-Anmeldeinformationen keine Verbindung zu Ihren Active-Directory-Domain-Controllern herstellen
- Amazon FSx kann nicht mit Ihren Active-Directory-DNS-Servern oder Domain-Controllern kommunizieren
- Amazon FSx kann aufgrund eines ungültigen Active-Directory-Domänennamens nicht mit Ihrem Active Directory kommunizieren.
- Das Servicekonto kann nicht auf die Administratorengruppe zugreifen, die in der SVM-Active-Directory-Konfiguration angegeben ist.
- Amazon FSx kann keine Verbindung zu den Active-Directory-Domain-Controllern herstellen, da die angegebene Organisationseinheit nicht vorhanden ist oder nicht zugänglich ist

Der SVM-NetBIOS-Name entspricht dem NetBIOS-Namen für die Heimatdomäne.

Das Verbinden einer SVM mit Ihrem selbstverwalteten Active Directory schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx kann keine Verbindung mit Ihrem Active Directory herstellen. Dies liegt daran, dass der von Ihnen angegebene Servername der NetBIOS-Name der Heimatdomäne ist. Um dieses Problem zu beheben, wählen Sie einen NetBIOS-Namen für Ihre SVM aus, der sich vom NetBIOS-Namen der Heimatdomäne unterscheidet. Versuchen Sie dann erneut, Ihre SVM mit Ihrem Active Directory zu verbinden.

Um dieses Problem zu beheben, befolgen Sie das unter beschriebene Verfahren, Verbinden einer SVM mit einem Active Directory mithilfe der AWS Management Console, AWS CLI und API um erneut zu versuchen, Ihre SVM mit Ihrem AD zu verbinden. Stellen Sie sicher, dass Sie einen NetBIOS-Namen für Ihre SVM verwenden, der sich vom NetBIOS-Namen der Home-Domain des Active Directory unterscheidet.

Die SVM ist bereits mit einem anderen Active Directory verbunden

Das Verbinden einer SVM mit einem Active Directory schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx kann keine Verbindung zu Ihrem Active Directory herstellen. Dies liegt daran, dass die SVM bereits mit einer Domain verbunden ist. Um diese SVM mit einer anderen Domain zu verbinden, können Sie die ONTAP-CLI oder REST-API verwenden, um die Verbindung dieser SVM zu Active Directory aufzuheben. Versuchen Sie dann erneut, Ihre SVM mit einem anderen Active Directory zu verbinden.

Gehen Sie wie folgt vor, um das Problem zu beheben:

1. Verwenden Sie die NetApp ONTAP-CLI, um die Verbindung der SVM mit ihrem aktuellen Active Directory aufzuheben. Weitere Informationen finden Sie unter Aufheben der Verbindung eines Active Directory mit Ihrer SVM mithilfe der NetApp ONTAP-CLI.
2. Befolgen Sie das unter beschriebene VerfahrenVerbinden einer SVM mit einem Active Directory mithilfe der AWS Management Console, AWS CLI und API, um erneut zu versuchen, Ihre SVM mit dem neuen AD zu verbinden.

Amazon FSx kann keine Verbindung zu Ihren Active-Directory-Domain-Controllern herstellen, da der NetBIOS-Name der SVM bereits verwendet wird

Das Erstellen einer SVM, die mit Ihrem selbstverwalteten AD verbunden ist, schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx kann keine Verbindung mit Ihrem Active Directory herstellen. Dies liegt daran, dass der von Ihnen angegebene NetBIOS-Name (Computer) bereits in Ihrem Active Directory verwendet wird. Um dieses Problem zu beheben, wählen Sie einen NetBIOS-Namen für Ihre SVM aus, der in Ihrem Active Directory nicht verwendet wird. Geben Sie ein NetBIOS (Computer) an und versuchen Sie dann erneut, Ihre SVM mit Ihrem Active Directory zu verbinden.

Um dieses Problem zu beheben, befolgen Sie das unter beschriebene Verfahren, Verbinden einer SVM mit einem Active Directory mithilfe der AWS Management Console, AWS CLI und API um erneut zu versuchen, Ihre SVM mit Ihrem AD zu verbinden. Stellen Sie sicher, dass Sie einen NetBIOS-Namen für Ihre SVM verwenden, der eindeutig ist und noch nicht in Ihrem Active Directory verwendet wird.

Amazon FSx kann nicht mit Ihren Active-Directory-Domain-Controllern kommunizieren

Das Verbinden einer SVM mit Ihrem selbstverwalteten AD schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx kann nicht mit Ihrem Active Directory kommunizieren. Um dieses Problem zu beheben, stellen Sie sicher, dass Netzwerkdatenverkehr zwischen Amazon FSx und Ihren Domain-Controllern zulässig ist. Versuchen Sie dann erneut, Ihre SVM mit Ihrem Active Directory zu verbinden.

Führen Sie folgende Schritte aus, um dieses Problem zu lösen:

1. Überprüfen Sie die unter beschriebenen Anforderungen und nehmen Sie die erforderlichen Änderungen vorAnforderungen an die Netzwerkkonfiguration, um die Netzwerkkommunikation zwischen Amazon FSx und Ihrem AD zu ermöglichen.
2. Sobald Amazon FSx in der Lage ist, mit Ihrem AD zu kommunizieren, befolgen Sie das unter beschriebene Verfahren Verbinden einer SVM mit einem Active Directory mithilfe der AWS Management Console, AWS CLI und API und versuchen Sie erneut, Ihre SVM mit Ihrem AD zu verbinden.

Amazon FSx kann aufgrund nicht erfüllter Portanforderungen oder Servicekontoberechtigungen keine Verbindung zu Ihrem Active Directory herstellen

Das Verbinden einer SVM mit Ihrem selbstverwalteten AD schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx kann keine Verbindung mit Ihrem Active Directory herstellen. Dies liegt entweder daran, dass die Portanforderungen für Ihr Active Directory nicht erfüllt werden, oder daran, dass das bereitgestellte Servicekonto nicht über Berechtigungen verfügt, um die virtuelle Speichermaschine mit der angegebenen Organisationseinheit mit der Domain zu verbinden. Um dieses Problem zu beheben, aktualisieren Sie die Active-Directory-Konfiguration Ihrer virtuellen Speichermaschine, nachdem Sie alle Berechtigungsprobleme mit Ports und Servicekonten behoben haben, wie im Amazon-FSx-Benutzerhandbuch empfohlen.

Führen Sie folgende Schritte aus, um dieses Problem zu lösen:

1. Überprüfen Sie die unter beschriebenen Anforderungen und nehmen Sie die erforderlichen Änderungen vorAnforderungen an die Netzwerkkonfiguration, um die Netzwerkanforderungen zu erfüllen, und stellen Sie sicher, dass die Kommunikation auf den erforderlichen Ports aktiviert ist
2. Überprüfen Sie die unter beschriebenen ServicekontoanforderungenAnforderungen an Active-Directory-Servicekonten. Stellen Sie sicher, dass das Servicekonto über die delegierten Berechtigungen verfügt, die erforderlich sind, um Ihre SVM mithilfe der angegebenen Organisationseinheit mit der AD-Domain zu verbinden.
3. Sobald Sie Änderungen an den Port-Berechtigungen oder dem Servicekonto vorgenommen haben, befolgen Sie das unter beschriebene Verfahren Verbinden einer SVM mit einem Active Directory mithilfe der AWS Management Console, AWS CLI und API und versuchen Sie erneut, Ihre SVM mit Ihrem AD zu verbinden.

Amazon FSx kann keine Verbindung zu Ihren Active-Directory-Domain-Controllern herstellen, da die Anmeldeinformationen für das Servicekonto ungültig sind

Das Verbinden einer SVM mit Ihrem selbstverwalteten Active Directory schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx kann keine Verbindung mit Ihrem/Ihren Active-Directory-Domain-Controller(n) herstellen, da die angegebenen Servicekonto-Anmeldeinformationen ungültig sind. Um dieses Problem zu beheben, aktualisieren Sie die Active-Directory-Konfiguration Ihrer virtuellen Speichermaschine mit einem gültigen Servicekonto.

Um dieses Problem zu beheben, verwenden Sie das unter beschriebene Verfahren, Aktualisieren einer vorhandenen SVM-Active-Directory-Konfiguration mithilfe der AWS Management ConsoleAWS CLI, und API um die Anmeldeinformationen des SVM-Servicekontos zu aktualisieren. Achten Sie bei der Eingabe des Servicekonto-Benutzernamens darauf, nur den Benutzernamen (z. B. `ServiceAcct`) und kein Domänenpräfix (z. B. `corp.com\ServiceAcct`) oder Domänensuffix (z. B.) anzugeben`ServiceAcct@corp.com`. Verwenden Sie nicht den Distinguished Name (DN), wenn Sie den Benutzernamen des Servicekontos eingeben (z. B. `CN=ServiceAcct,OU=example,DC=corp,DC=com`).

Amazon FSx kann aufgrund unzureichender Servicekonto-Anmeldeinformationen keine Verbindung zu Ihren Active-Directory-Domain-Controllern herstellen

Das Verbinden einer SVM mit Ihrem selbstverwalteten Active Directory schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx kann keine Verbindung mit Ihrem/Ihren Active-Directory-Domain-Controller(n) herstellen. Dies liegt entweder daran, dass die Portanforderungen für das Active Directory nicht erfüllt wurden oder dass das bereitgestellte Servicekonto nicht berechtigt ist, die virtuelle Speichermaschine mit der angegebenen Organisationseinheit mit der Domain zu verbinden.

Um dieses Problem zu beheben, stellen Sie sicher, dass Sie die erforderlichen Berechtigungen an das von Ihnen angegebene Servicekonto delegiert haben. Das Servicekonto muss in der Lage sein, Computerobjekte in der OU in der Domain zu erstellen und zu löschen, der Sie dem Dateisystem beitreten. Das Servicekonto muss außerdem mindestens über Berechtigungen für Folgendes verfügen:

- Zurücksetzen von Passwörtern
- Einschränken des Lesens und Schreibens von Daten durch Konten
- Überprüfte Fähigkeit zum Schreiben in den DNS-Hostnamen
- Überprüfte Fähigkeit zum Schreiben in den Prinzipalnamen des Service
- Möglichkeit zum Erstellen und Löschen von Computerobjekten

- Überprüfte Fähigkeit zum Lesen und Schreiben von Kontobeschränkungen

Weitere Informationen zum Erstellen eines Servicekontos mit korrekten Berechtigungen finden Sie unter Anforderungen an Active-Directory-Servicekonten und Delegieren von Berechtigungen an Ihr Amazon FSx-Servicekonto.

Amazon FSx kann nicht mit Ihren Active-Directory-DNS-Servern oder Domain-Controllern kommunizieren

Das Verbinden einer SVM mit Ihrem selbstverwalteten Active Directory schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx kann nicht mit Ihrem Active Directory kommunizieren. Dies liegt daran, dass Amazon FSx die bereitgestellten DNS-Server oder Domain-Controller für Ihre Domain nicht erreichen kann. Um dieses Problem zu beheben, aktualisieren Sie die Active-Directory-Konfiguration Ihrer virtuellen Speichermaschine mit gültigen DNS-Servern und einer Netzwerkkonfiguration, die den Datenverkehr von der virtuellen Speichermaschine zum Domain-Controller ermöglicht.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Wenn nur einige der Domain-Controller in Ihrem Active Directory erreichbar sind, z. B. aufgrund geografischer Einschränkungen oder Firewalls, können Sie bevorzugte Domain-Controller hinzufügen. Mit dieser Option versucht Amazon FSx, die bevorzugten Domain-Controller zu kontaktieren. Fügen Sie bevorzugte Domain-Controller mit dem `vserver cifs domain preferred-dc add` NetApp ONTAP-CLI-Befehl wie folgt hinzu:

   a. Um auf die NetApp ONTAP-CLI zuzugreifen, richten Sie eine SSH-Sitzung am Verwaltungsport des Dateisystems von Amazon FSx für NetApp ONTAP ein, indem Sie den folgenden Befehl ausführen. Ersetzen Sie durch *`management_endpoint_ip`* die IP-Adresse des Verwaltungsports des Dateisystems.

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

      Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

   b. Geben Sie den folgenden Befehl ein, wobei:

      - `-vserver vserver_name` gibt den Namen der virtuellen Speichermaschine (SVM) an.

- `-domain domain_name` gibt den vollqualifizierten Active-Directory-Namen (FQDN) der Domain an, zu der die angegebenen Domain-Controller gehören.
- `-preferred-dc IP_address,…` gibt eine oder mehrere IP-Adressen der bevorzugten Domain-Controller als durch Komma getrennte Liste in der bevorzugten Reihenfolge an.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_name -
domain domain_name -preferred-dc IP_address, …+
```

Der folgende Befehl fügt die Domain-Controller 172.17.102.25 und 172.17.102.24 zur Liste der bevorzugten Domain-Controller hinzu, die der SMB-Server auf SVM vs1 verwendet, um den externen Zugriff auf die Domain cifs.lab.example.com zu verwalten.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
 cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. Überprüfen Sie, ob Ihr Domain-Controller mit DNS aufgelöst werden kann. Verwenden Sie den `vserver services access-check dns forward-lookup` NetApp ONTAP-CLI-Befehl, um die IP-Adresse eines Hostnamens basierend auf der Suche auf dem angegebenen DNS-Server oder der DNS-Konfiguration des vservers zurückzugeben.

   a. Um auf die NetApp ONTAP-CLI zuzugreifen, richten Sie eine SSH-Sitzung am Verwaltungsport des Dateisystems von Amazon FSx für NetApp ONTAP ein, indem Sie den folgenden Befehl ausführen. Ersetzen Sie durch *`management_endpoint_ip`* die IP-Adresse des Verwaltungsports des Dateisystems.

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

   Weitere Informationen finden Sie unter Verwaltung von Dateisystemen mit der ONTAP CLI.

   b. Geben Sie den erweiterten ONTAP-CLI-Modus mit dem folgenden Befehl ein.

   ```
   FsxId123456789::> set adv
   ```

   c. Geben Sie den folgenden Befehl ein, wobei:

   - `-vserver vserver_name` gibt den Namen der virtuellen Speichermaschine (SVM) an.
   - `-hostname host_name` gibt den Hostnamen an, der auf dem DNS-Server nachgeschlagen werden soll.

- `-node node_name` gibt den Namen des Knotens an, auf dem der Befehl ausgeführt wird.
- `-lookup-type` gibt den Typ der IP-Adresse an, die auf dem DNS-Server gesucht werden soll. Der Standardwert ist `all`.

```
FsxId123456789::> vserver services access-check dns forward-lookup \
-vserver vserver_name -node node_name \
-domains domain_name -name-servers dns_server_ip_address \
-hostname host_name
```

3. Überprüfen Sie die Informationen, die Sie benötigen, wenn Sie eine SVM mit einem AD verbinden.
4. Überprüfen Sie die Netzwerkanforderungen, wenn Sie eine SVM mit einem AD verbinden.
5. Verwenden Sie das unter beschriebene VerfahrenAnforderungen an die Netzwerkkonfiguration, um die AD-Konfiguration Ihrer SVM mithilfe der richtigen IP-Adressen für Ihre AD-DNS-Server zu aktualisieren.

Amazon FSx kann aufgrund eines ungültigen Active-Directory-Domänennamens nicht mit Ihrem Active Directory kommunizieren.

Das Verbinden einer SVM mit Ihrem selbstverwalteten Active Directory schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx hat festgestellt, dass der bereitgestellte FQDN ungültig ist. Um dieses Problem zu beheben, aktualisieren Sie die Active-Directory-Konfiguration Ihrer virtuellen Speichermaschine mit einem FQDN, der den Konfigurationsanforderungen entspricht.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Überprüfen Sie die Anforderungen an den On-Premises-Active-Directory-Domainnamen, die unter Informationen, die beim Verbinden einer SVM mit einem Active Directory erforderlich sind Stellen Sie sicher, dass das AD, dem Sie beitreten möchten, diese Anforderung erfüllt.
2. Verwenden Sie das unter beschriebene Verfahren Verbinden einer SVM mit einem Active Directory mithilfe der AWS Management Console, AWS CLI und API und versuchen Sie erneut, Ihre SVM mit einem AD zu verbinden. Stellen Sie sicher, dass Sie das richtige Format für den FQDN der AD-Domain verwenden.

Das Servicekonto kann nicht auf die Administratorengruppe zugreifen, die in der SVM-Active-Directory-Konfiguration angegeben ist.

Das Verbinden einer SVM mit Ihrem selbstverwalteten Active Directory schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx kann Ihre Active-Directory-Konfiguration nicht anwenden. Dies liegt daran, dass die von Ihnen angegebene Administratorgruppe entweder nicht vorhanden ist oder für das von Ihnen angegebene Servicekonto nicht zugänglich ist. Um dieses Problem zu beheben, stellen Sie sicher, dass Ihre Netzwerkkonfiguration Datenverkehr von der SVM zum/zu den Domain-Controller(n) und DNS-Servern Ihres Active Directory zulässt. Aktualisieren Sie dann die Active-Directory-Konfiguration Ihrer SVM, stellen Sie die DNS-Server Ihres Active Directory bereit und geben Sie eine Administratorengruppe in der Domain an, auf die das bereitgestellte Servicekonto zugreifen kann.

Führen Sie folgende Schritte aus, um dieses Problem zu lösen:

1. Lesen Sie die Informationen zum Bereitstellen einer Domänengruppe, um administrative Aktionen für Ihre SVM auszuführen. Stellen Sie sicher, dass Sie den richtigen Namen der AD-Domain-Administratorgruppe verwenden.
2. Verwenden Sie das unter beschriebene Verfahren Verbinden einer SVM mit einem Active Directory mithilfe der AWS Management Console, AWS CLI und API und versuchen Sie erneut, Ihre SVM mit einem AD zu verbinden.

Amazon FSx kann keine Verbindung zu den Active-Directory-Domain-Controllern herstellen, da die angegebene Organisationseinheit nicht vorhanden ist oder nicht zugänglich ist

Das Verbinden einer SVM mit Ihrem selbstverwalteten Active Directory schlägt mit der folgenden Fehlermeldung fehl:

Amazon FSx kann keine Verbindung mit Ihrem Active Directory herstellen. Dies liegt daran, dass die von Ihnen angegebene Organisationseinheit entweder nicht vorhanden ist oder für das angegebene Servicekonto nicht zugänglich ist. Um dieses Problem zu beheben, aktualisieren Sie die Active-Directory-Konfiguration Ihrer virtuellen Speichermaschine und geben eine Organisationseinheit an, der das Servicekonto beitreten darf.

Führen Sie folgende Schritte aus, um dieses Problem zu lösen:

1. Überprüfen Sie die Voraussetzungen für die Verbindung einer SVM mit einem AD .
2. Überprüfen Sie die Informationen, die Sie benötigen, wenn Sie eine SVM mit einem AD verbinden.
3. Versuchen Sie erneut, die SVM mit diesem Verfahren mit der richtigen Organisationseinheit mit dem AD zu verbinden.

Sie können eine virtuelle Speichermaschine oder ein virtuelles Volume nicht löschen

Jedes FSx-für-ONTAP-Dateisystem kann eine oder mehrere virtuelle Speichermaschinen (SVMs) enthalten, und jede SVM kann ein oder mehrere Volumes enthalten. Wenn Sie eine Ressource löschen, müssen Sie zunächst sicherstellen, dass alle untergeordneten Elemente gelöscht wurden. Bevor Sie beispielsweise eine SVM löschen, müssen Sie zunächst alle Nicht-Root-Volumes in der SVM löschen.

> **Important**
>
> Sie können virtuelle Speichermaschinen nur über die Amazon-FSx-Konsole, API und CLI löschen. Sie können Volumes nur mit der Amazon-FSx-Konsole, API oder CLI löschen, wenn für das Volume Amazon-FSx-Backups aktiviert sind.

Um Ihre Daten und Konfiguration zu schützen, verhindert Amazon FSx unter bestimmten Umständen das Löschen von SVMs und Volumes. Wenn Sie versuchen, eine SVM oder ein Volume zu löschen, und Ihre Löschanforderung nicht erfolgreich ist, stellt Ihnen Amazon FSx Informationen in der AWS Konsole, AWS Command Line Interface (AWS CLI) und API zur Verfügung, warum die Ressource nicht gelöscht wurde. Nachdem Sie die Ursache des Löschfehlers behoben haben, können Sie die Löschanforderung erneut versuchen.

Themen

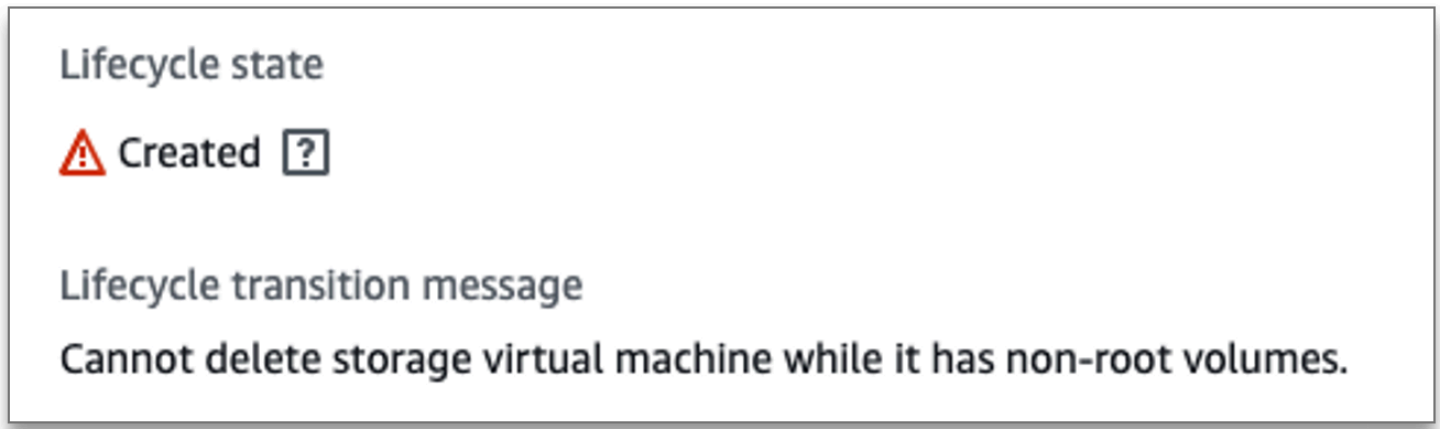
- Identifizieren fehlgeschlagener Löschungen
- SVM-Löschung: Auf Routing-Tabellen kann nicht zugegriffen werden
- SVM-Löschung: Peer-Beziehung
- SVM- oder Volume-Löschung: SnapMirror

- SVM-Löschung: Kerberos-fähiges LIF
- SVM-Löschung: Anderer Grund
- Volume-Löschung: FlexCache Beziehung

Identifizieren fehlgeschlagener Löschungen

Wenn Sie eine Amazon FSx SVM oder ein Volume löschen, sehen Sie in der Regel bis zu einige Minuten `DELETING` den `Lifecycle` Statusübergang der Ressource zu , bevor die Ressource aus der Amazon FSx-Konsole, der CLI und der API verschwindet.

Wenn Sie versuchen, eine Ressource zu löschen, und ihr `Lifecycle` Status von zu `DELETING` und dann zurück zu wechselt`CREATED`, weist dieses Verhalten darauf hin, dass die Ressource nicht erfolgreich gelöscht wurde. In diesem Fall meldet Amazon FSx ein Warnsymbol in der Konsole neben dem `CREATED` Lebenszyklusstatus. Wenn Sie das Warnsymbol auswählen, wird der Grund für das fehlgeschlagene Löschen angezeigt, wie im folgenden Beispiel gezeigt.



Die häufigsten Gründe, warum Amazon FSx das Löschen von SVM- und Volumes verhindert, finden Sie in den folgenden Abschnitten mit step-by-step Anweisungen zur Behebung dieser Probleme.

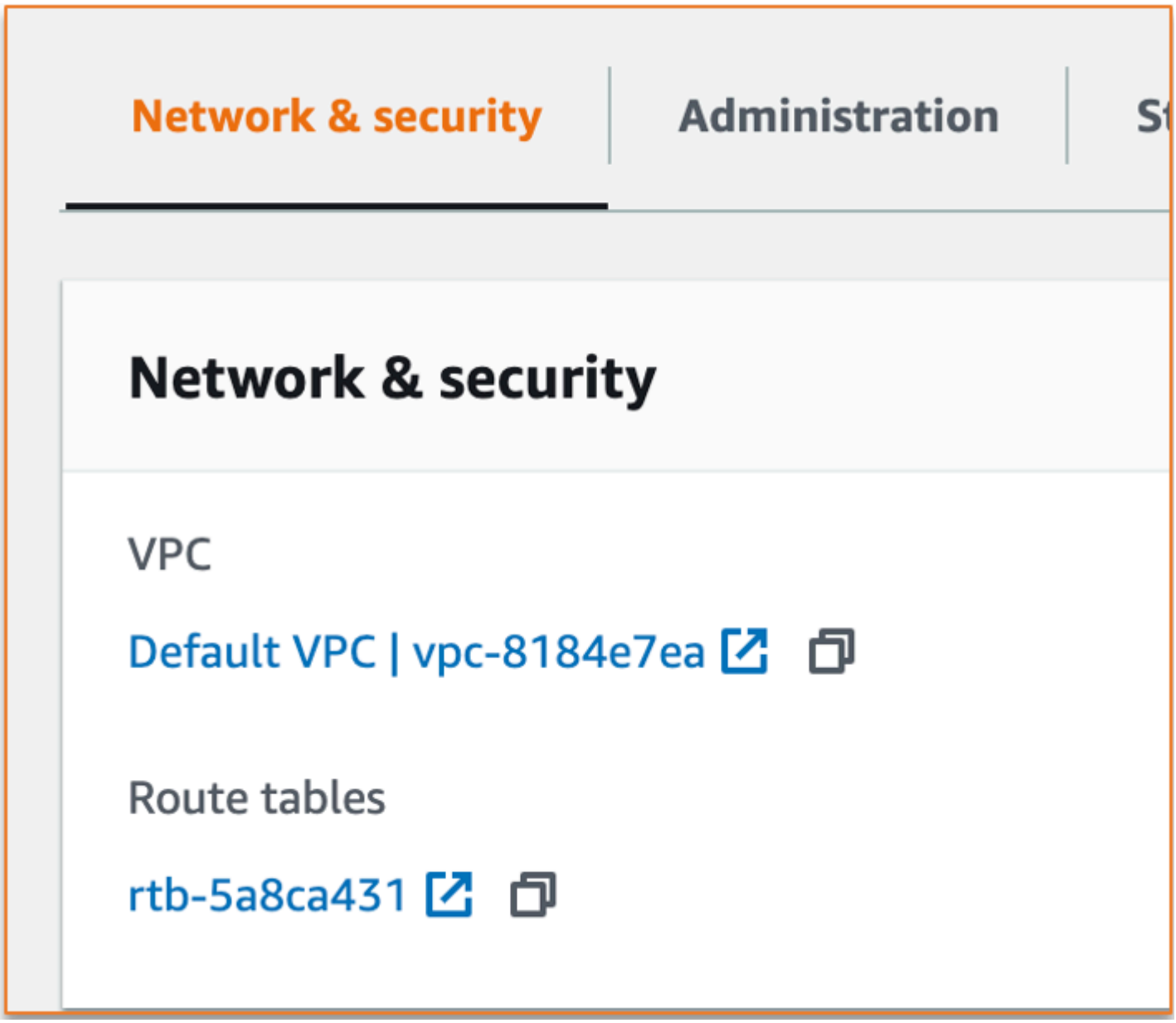
SVM-Löschung: Auf Routing-Tabellen kann nicht zugegriffen werden

Jedes FSx-für-ONTAP-Dateisystem erstellt einen oder mehrere Routing-Tabelleneinträge, um ein automatisches Failover und ein Failover über Availability Zones hinweg bereitzustellen. Standardmäßig werden diese Routing-Tabelleneinträge in der Standard-Routing-Tabelle Ihrer VPC erstellt. Sie können optional eine oder mehrere nicht standardmäßige Routing-Tabellen angeben, in denen FSx-für-ONTAP-Schnittstellen erstellt werden können. Amazon FSx markiert jede Routing-Tabelle, die mit einem Dateisystem verknüpft ist, mit einem -`AmazonFSx`Tag. Wenn dieses Tag

entfernt wird, kann dies verhindern, dass Amazon FSx Ressourcen löschen kann. Wenn diese Situation auftritt, sehen Sie Folgendes`LifecycleTransitionReason`:

```
Amazon FSx is unable to complete the requested storage virtual machine
operation because of an inability to access one or more of the route tables
associated with your file system. Please contact AWS Support.
```

Sie finden die Routing-Tabellen Ihres Dateisystems in der Amazon-FSx-Konsole, indem Sie zur Übersichtsseite des Dateisystems auf der Registerkarte Netzwerk und Sicherheit navigieren:



Wenn Sie den Link für Routing-Tabellen auswählen, gelangen Sie zu Ihren Routing-Tabellen. Stellen Sie als Nächstes sicher, dass jede der Routing-Tabellen, die Ihrem Dateisystem zugeordnet sind, mit diesem Schlüssel-Wert-Paar gekennzeichnet ist:

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

Wenn dieses Tag nicht vorhanden ist, erstellen Sie es neu und versuchen Sie dann erneut, die SVM zu löschen.

SVM-Löschung: Peer-Beziehung

Wenn Sie versuchen, eine SVM oder ein Volume zu löschen, das Teil einer Peer-Beziehung ist, müssen Sie zuerst die Peer-Beziehung löschen, bevor Sie die SVM oder das Volume löschen. Diese Anforderung verhindert, dass die per Peering verbundenen SVMs fehlerhaft werden. Wenn Ihre SVM aufgrund einer Peer-Beziehung nicht gelöscht werden kann, wird Folgendes angezeigt`LifecycleTransitionReason`:

Amazon FSx kann die virtuelle Speichermaschine nicht löschen, da sie Teil einer SVM-Peer- oder Übergangs-Peer-Beziehung ist. Bitte löschen Sie die Beziehung und versuchen Sie es erneut.

Sie können SVM-Peer-Beziehungen über die ONTAP-CLI löschen. Um auf die ONTAP-CLI zuzugreifen, führen Sie die Schritte unter aus[Verwaltung von Dateisystemen mit der ONTAP CLI](). Führen Sie mit der ONTAP-CLI die folgenden Schritte aus.

1. Verwenden Sie den folgenden Befehl, um nach SVM-Peer-Beziehungen zu suchen. Ersetzen Sie durch *svm_name* den Namen Ihrer SVM.

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

Wenn dieser Befehl erfolgreich ist, wird eine Ausgabe ähnlich der folgenden angezeigt:

```
            Peer        Peer                          Peering        Remote
Vserver     Vserver     State        Peer Cluster     Applications   Vserver
----------- ----------- ------------ ----------------- -------------- ---------
svm_name    test2       peered       FsxId02d81fef0d84734b6
                                                       snapmirror     fsxDest
svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                       snapmirror     fsxDest
2 entries were displayed.
```

2. Löschen Sie jede SVM-Peer-Beziehung mit dem folgenden Befehl. Ersetzen Sie *svm_name*, und *remote_svm_name* durch Ihre tatsächlichen Werte.

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

Wenn dieser Befehl erfolgreich ist, wird die folgende Ausgabe angezeigt:

```
Info: 'vserver peer delete' command is successful.
```

SVM- oder Volume-Löschung: SnapMirror

So wie Sie eine SVM mit einer Peer-Beziehung nicht löschen können, ohne zuerst die Peer-Beziehung zu löschen (siehe SVM-Löschung: Peer-Beziehung), können Sie eine SVM mit einer SnapMirror Beziehung nicht löschen, ohne zuerst die SnapMirror Beziehung zu löschen. Um die SnapMirror Beziehung zu löschen, verwenden Sie die ONTAP-CLI, um die folgenden Schritte auf dem Dateisystem auszuführen, das das Ziel der SnapMirror Beziehung ist. Um auf die ONTAP-CLI zuzugreifen, führen Sie die Schritte unter ausVerwaltung von Dateisystemen mit der ONTAP CLI.

> **Note**
>
> Amazon-FSx-Backups verwenden point-in-time, SnapMirror um inkrementelle Backups der Volumes Ihres Dateisystems zu erstellen. Sie können diese SnapMirror Beziehung für Ihre Backups in der ONTAP-CLI nicht löschen. Diese Beziehung wird jedoch automatisch gelöscht, wenn Sie ein Volume über die AWS CLI, API oder Konsole löschen.

1. Listen Sie Ihre SnapMirror Beziehungen im Zieldateisystem mit dem folgenden Befehl auf. Ersetzen Sie *svm_name* durch den Namen Ihrer SVM.

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

Wenn dieser Befehl erfolgreich ist, wird eine Ausgabe ähnlich der folgenden angezeigt:

```
Source            Destination    Mirror  Relationship   Total             Last
Path        Type  Path           State   Status         Progress  Healthy Updated
----------- ---- ------------    ------- -------------- --------- ------- --------
sourceSvm:sourceVol
            XDP  destSvm:destVol Snapmirrored
                                       Idle           -         true    -
```

2. Löschen Sie Ihre SnapMirror Beziehung, indem Sie den folgenden Befehl auf dem Zieldateisystem ausführen.

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

SVM-Löschung: Kerberos-fähiges LIF

Wenn Sie versuchen, eine SVM zu löschen, für die eine logische Schnittstelle (LIF) mit aktiviertem Kerberos aktiviert ist, müssen Sie zuerst Kerberos für diese LIF deaktivieren, bevor Sie die SVM löschen.

Sie können Kerberos auf einem LIF über die ONTAP-CLI deaktivieren. Um auf die ONTAP-CLI zuzugreifen, führen Sie die Schritte unter ausVerwaltung von Dateisystemen mit der ONTAP CLI.

1. Geben Sie den Diagnosemodus in der ONTAP-CLI ein, indem Sie den folgenden Befehl verwenden.

```
FsxId123456789abcdef::> set diag
```

Wenn Sie aufgefordert werden, fortzufahren, geben Sie ein**y**.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

2. Überprüfen Sie, für welche Schnittstellen Kerberos aktiviert ist. Ersetzen Sie durch *svm_name* den Namen Ihrer SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Wenn dieser Befehl erfolgreich ist, wird eine Ausgabe ähnlich der folgenden angezeigt:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    enabled
5 entries were displayed.
```

3. Deaktivieren Sie Kerberos LIF mit dem folgenden Befehl. Ersetzen Sie durch *svm_name* den Namen Ihrer SVM. Sie müssen den Active-Directory-Benutzernamen und das Passwort angeben, mit dem Sie diese SVM mit Ihrem Active Directory verbunden haben.

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

Wenn dieser Befehl erfolgreich ist, wird die folgende Ausgabe angezeigt. Geben Sie den Active-Directory-Benutzernamen und das Passwort an, mit dem Sie diese SVM mit Ihrem Active Directory verbunden haben. Wenn Sie aufgefordert werden, fortzufahren, geben Sie ein**y**.

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *************

Warning: This command deletes the service principal name from the machine account
 on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. Überprüfen Sie, ob Kerberos auf der SVM deaktiviert ist, indem Sie den folgenden Befehl verwenden. Ersetzen Sie durch *svm_name* den Namen Ihrer SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Wenn dieser Befehl erfolgreich ist, wird eine Ausgabe ähnlich der folgenden angezeigt:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    disabled
5 entries were displayed.
```

5. Wenn die Schnittstelle als angezeigt wird`disabled`, versuchen Sie erneut, die SVM über die AWS CLI, API oder Konsole zu löschen.

   Wenn Sie das LIF nicht mit den vorherigen Befehlen löschen konnten, können Sie das Kerberos-LIF mit dem folgenden Befehl erzwingen. Ersetzen Sie durch *svm_name* den Namen Ihrer SVM.

   > **Important**
   >
   > Der folgende Befehl kann das Computerobjekt Ihrer SVM in Ihrem Active Directory zusammenfassen.

   ```
   FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
    nfs_smb_management_1 -force true
   ```

   Wenn dieser Befehl erfolgreich ist, wird eine Ausgabe ähnlich der folgenden angezeigt. Wenn Sie aufgefordert werden, fortzufahren, geben Sie ein**y**.

   ```
   (vserver nfs kerberos interface disable)

   Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver
    "svm_name" will be deleted.
   The corresponding account on the KDC will not be deleted. Do you want to continue?
    {y|n}: y
   ```

SVM-Löschung: Anderer Grund

FSx für ONTAP SVMs erstellen ein Computerobjekt in Ihrem Active Directory, wenn sie Ihrem Active Directory beitreten. In einigen Fällen möchten Sie den Beitritt zu einer SVM zu Ihrem Active Directory mithilfe der ONTAP-CLI manuell aufheben. Um auf die ONTAP-CLI zuzugreifen, führen Sie die Schritte unter aus Verwaltung von Dateisystemen mit der ONTAP CLIund melden Sie sich bei der ONTAP-CLI auf Dateisystemebene mit `fsxadmin` Anmeldeinformationen an. Führen Sie mithilfe der ONTAP-CLI die folgenden Schritte aus, um den Beitritt zu einer SVM zu Ihrem Active Directory aufzuheben.

> **Important**
>
> Mit diesem Verfahren kann das Computerobjekt Ihrer SVM in Ihrem Active Directory entfernt werden.

1. Geben Sie den erweiterten Modus in der ONTAP-CLI ein, indem Sie den folgenden Befehl verwenden.

   ```
   FsxId123456789abcdef::> set adv
   ```

   Nachdem Sie diesen Befehl ausgeführt haben, wird diese Ausgabe angezeigt. Geben Sie ein**y**, um fortzufahren.

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

2. Löschen Sie das DNS für Ihr Active Directory mit dem folgenden Befehl. Ersetzen Sie durch *`svm_name`* den Namen Ihrer SVM.

   ```
   FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
    delete -vserver svm_name -lif nfs_smb_management_1
   ```

   > **Note**
   >
   > Wenn der DNS-Datensatz bereits gelöscht wurde oder der DNS-Server nicht erreichbar ist, schlägt dieser Befehl fehl. Fahren Sie in diesem Fall mit dem nächsten Schritt fort.

3. Deaktivieren Sie das DNS mit dem folgenden Befehl. Ersetzen Sie durch *svm_name* den Namen Ihrer SVM.

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
vserver svm_name -is-enabled false -use-secure false
```

Wenn dieser Befehl erfolgreich ist, wird die folgende Ausgabe angezeigt:

```
Warning: DNS updates for Vserver "svm_name" are now disabled.
     Any LIFs that are subsequently modified or deleted
     can result in a stale DNS entry on the DNS server,
     even when DNS updates are enabled again.
```

4. Melden Sie das Gerät von Active Directory an. Ersetzen Sie durch *svm_name* den Namen Ihrer SVM.

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

Nachdem Sie diesen Befehl ausgeführt haben, wird die folgende Ausgabe angezeigt, wobei durch den Namen Ihrer Domain ersetzt *CORP.EXAMPLE.COM* wird. Geben Sie bei Aufforderung Ihren Benutzernamen und Ihr Passwort ein. Wenn Sie gefragt werden, ob Sie den Server löschen möchten, geben Sie ein**y**.

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
     Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
 server.
     Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

Volume-Löschung: FlexCache Beziehung

Sie können Volumes, bei denen es sich um Ursprungs-Volumes für eine FlexCache Beziehung handelt, nur löschen, wenn Sie zuerst die Cache-Beziehung löschen. Um festzustellen, welche Volumes eine FlexCache Beziehung haben, können Sie die ONTAP-CLI verwenden. Um auf die

ONTAP-CLI zuzugreifen, führen Sie die Schritte unter ausVerwaltung von Dateisystemen mit der ONTAP CLI.

1. Verwenden Sie den folgenden Befehl, um nach FlexCache Beziehungen zu suchen.

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. Löschen Sie alle Cache-Beziehungen mit dem folgenden Befehl. Ersetzen Sie *dest_svm_name*, und *dest_vol_name* durch Ihre tatsächlichen Werte.

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. Nachdem Sie die Cache-Beziehung gelöscht haben, versuchen Sie erneut, Ihre SVM über die AWS CLI, API oder Konsole zu löschen.

Automatische tägliche Backups schlagen aufgrund unzureichender Volume-Kapazität fehl

Automatische tägliche Backups Ihres Volumes schlagen mit der folgenden Meldung fehl:

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

Automatische tägliche Backups schlagen fehl, da auf dem Volume nicht genügend freie Speicherkapazität vorhanden ist. Um diesen Zustand zu beheben, müssen Sie Speicherkapazität auf dem Volume freigeben. Sie können dies je nach Situation mit einer oder mehreren der folgenden Optionen erreichen:

- Erhöhen der Speicherkapazität des Volumes
- Erhöhen der Snapshot-Reservation des Volumes
- Deaktivieren der automatischen Snapshot-Löschung
- Löschen Sie den Backup-Snapshot nicht mit der ONTAP-CLI

Sie verfügen über unzureichende Volume-Kapazität

Wenn Ihnen der Speicherplatz auf Ihren Volumes ausgeht, können Sie die hier gezeigten Verfahren verwenden, um die Situation zu diagnostizieren und zu beheben.

Themen

- Bestimmen, wie Ihre Volume-Speicherkapazität verwendet wird
- Erhöhen der Speicherkapazität eines Volumes
- Verwenden der automatischen Volume-Größe
- Der primäre Speicher Ihres Dateisystems ist voll
- Löschen von Snapshots
- Erhöhen der maximalen Dateikapazität eines Volumes

Bestimmen, wie Ihre Volume-Speicherkapazität verwendet wird

Mit dem `volume show-space` NetApp ONTAP-CLI-Befehl können Sie sehen, wie die Speicherkapazität Ihres Volumes verbraucht wird. Diese Informationen können Ihnen helfen, Entscheidungen darüber zu treffen, wie Sie Volume-Speicherkapazität zurückgewinnen oder sparen können. Weitere Informationen finden Sie unter Um die Speicherkapazität eines Volumes zu überwachen (Konsole).

Erhöhen der Speicherkapazität eines Volumes

Sie können die Speicherkapazität eines Volumes mithilfe der Amazon-FSx-Konsole AWS CLI und der Amazon-FSx-API erhöhen. Weitere Informationen zum Aktualisieren eines Volumes mit einer erhöhten Kapazität finden Sie unter Ein Volume aktualisieren.

Alternativ können Sie die Speicherkapazität eines Volumes mit dem `volume modify` NetApp ONTAP-CLI-Befehl erhöhen. Weitere Informationen finden Sie unter Um die Speicherkapazität eines Volumes zu ändern (Konsole).

Verwenden der automatischen Volume-Größe

Sie können die automatische Volume-Größe verwenden, sodass ein Volume automatisch um eine bestimmte Menge oder auf eine bestimmte Größe wächst, wenn es einen Schwellenwert für den belegten Speicherplatz erreicht. Sie können dies für FlexVol Volume-Typen tun, bei denen es sich um den Standard-Volume-Typ für FSx für ONTAP handelt, indem Sie den `volume autosize`

NetApp ONTAP-CLI-Befehl verwenden. Weitere Informationen finden Sie unter Automatische Volumengrößenanpassung aktivieren.

Der primäre Speicher Ihres Dateisystems ist voll

Wenn der primäre Speicher Ihres FSx-für-ONTAP-Dateisystems voll ist, können Sie den Volumes in Ihrem Dateisystem keine Daten mehr hinzufügen, selbst wenn ein Volume zeigt, dass es über genügend verfügbare Speicherkapazität verfügt. Sie können die Menge der verfügbaren primären Speicherkapazität auf der Registerkarte Überwachung und Leistung auf der Seite mit den Dateisystemdetails in der Amazon-FSx-Konsole anzeigen. Weitere Informationen finden Sie unter Überwachung der SSD-Speichernutzung.

Um dieses Problem zu beheben, können Sie die Größe der primären Speicherebene Ihres Dateisystems erhöhen. Weitere Informationen finden Sie unter Aktualisierung des Dateisystems, des SSD-Speichers und der IOPS.

Löschen von Snapshots

Snapshots sind standardmäßig auf Ihren Volumes aktiviert, wobei die Standard-Snapshot-Richtlinie verwendet wird. Snapshots werden im `.snapshot` Verzeichnis im Stammverzeichnis eines Volumes gespeichert. Sie können die Volume-Speicherkapazität in Bezug auf Snapshots wie folgt verwalten:

- Manuelles Löschen von Snapshots – gewinnt Speicherkapazität zurück, indem Snapshots manuell gelöscht werden.
- Erstellen einer Richtlinie zum automatischen Löschen von Snapshots – Erstellen Sie eine Richtlinie, die Snapshots aggressiver löscht als die Standard-Snapshot-Richtlinie.
- Deaktivieren automatischer Snapshots – sparen Sie Speicherkapazität, indem Sie automatische Snapshots deaktivieren.

Weitere Informationen zum Löschen von Snapshots und zum Verwalten von Snapshot-Richtlinien zur Einsparung von Speicherkapazität finden Sie unter Löschen von Snapshots.

Erhöhen der maximalen Dateikapazität eines Volumes

Bei einem FSx-für-ONTAP-Volume kann die Dateikapazität ausgehen, wenn die Anzahl der verfügbaren Inodes oder Dateizeiger erschöpft ist. Standardmäßig beträgt die Anzahl der verfügbaren Knoten auf einem Volume 1 für jede Volume-Größe von 32KiB. Weitere Informationen finden Sie unter Kapazität der Volumendatei.

Die Anzahl der Inodes in einem Volume steigt entsprechend mit der Speicherkapazität des Volumes bis zu einem Schwellenwert von 648 GiB. Standardmäßig haben Volumes mit einer Speicherkapazität von 648 GiB oder mehr die gleiche Anzahl von Inodes, 21.251.126. Informationen zum Anzeigen der maximalen Dateikapazität eines Volumes finden Sie unter Die Dateikapazität eines Volumes anzeigen.

Wenn Sie ein Volume mit mehr als 648 GiB erstellen und mehr als 21.251.126 Knoten haben möchten, müssen Sie die maximale Anzahl von Dateien auf dem Volume manuell erhöhen. Wenn Ihrem Volume die Speicherkapazität ausgeht, können Sie die maximale Dateikapazität überprüfen. Wenn sie sich ihrer Dateikapazität nähert, können Sie sie manuell erhöhen. Weitere Informationen finden Sie unter So erhöhen Sie die maximale Anzahl von Dateien auf einem Volume (ONTAPCLI).

Fehlerbehebung bei Netzwerkproblemen

Wenn Sie Netzwerkprobleme haben, können Sie die hier gezeigten Verfahren verwenden, um das Problem zu diagnostizieren.

Sie möchten eine Paketverfolgung erfassen

Bei der Paketverfolgung wird der Pfad eines Pakets durch die Ebenen zu seinem Ziel überprüft. Sie steuern den Paketverfolgungsprozess mit den folgenden NetApp ONTAP-CLI-Befehlen:

- network tcpdump start – Startet die Paketverfolgung
- network tcpdump show – Zeigt aktuell ausgeführte Paketverfolgungen an
- network tcpdump stop – Stoppt eine laufende Paketverfolgung

Diese Befehle sind für Benutzer verfügbar, die die `-fsxadmin`Rolle auf Ihrem Dateisystem haben.

So erfassen Sie eine Paketverfolgung aus Ihrem Dateisystem

1. Um ein SSH in die NetApp ONTAP-CLI Ihres Dateisystems zu senden, führen Sie die im Verwenden der NetApp ONTAP-CLI Abschnitt des Benutzerhandbuchs zu Amazon FSx für NetApp ONTAP dokumentierten Schritte aus.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Geben Sie die Stufe der Diagnoseberechtigungen in der ONTAP-CLI ein, indem Sie den folgenden Befehl verwenden.

```
::> set diag
```

Wenn Sie aufgefordert werden, fortzufahren, geben Sie einy.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

3. Identifizieren Sie den Speicherort in Ihrem Dateisystem, an dem Sie Ihre Paketverfolgung speichern möchten. Das Volume muss online sein und im Namespace mit einem gültigen Verbindungspfad gemountet werden. Verwenden Sie den folgenden Befehl, um nach Volumes zu suchen, die diese Kriterien erfüllen:

```
::*> volume show -junction-path !- -fields junction-path
vserver volume    junction-path
------- --------- -------------
fsx     test_vol1 /test_vol1
fsx     test_vol2 /test_vol2
fsx     test_vol2 /test_vol3
```

4. Starten Sie die Ablaufverfolgung mit den mindestens erforderlichen Argumenten. Ersetzen Sie Folgendes:

   - Ersetzen Sie *node_name* durch den Namen des Knotens (z. B. `FsxId01234567890abcdef-01`).
   - Ersetzen Sie *svm_name* durch den Namen Ihrer virtuellen Speichermaschine (z. B. `fsx`).
   - Ersetzen Sie *microSD_Pfadname* durch den Namen des Volumes (z. B. `test-vol1`).

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
 e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
 packet traces are occurring. Use the
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
 disable Snapshots on the
tcpdump destination volume.
```

> **Important**
>
> Paket-Traces können nur auf der -e0eSchnittstelle und im `Default` IP-Bereich erfasst werden. In FSx für ONTAP verwendet der gesamte Netzwerkdatenverkehr die -e0eSchnittstelle.

Beachten Sie bei der Verwendung der Paketverfolgung Folgendes:

- Beim Starten einer Paketverfolgung müssen Sie den Pfad zu dem Speicherort der Trace-Dateien in diesem Format angeben: /clus/*svm_name* /*junction-path-name*
- Geben Sie optional den Dateinamen für die Paketverfolgung an. Wenn filter_name nicht angegeben ist, wird es automatisch in der Form generiert: *node-name* *_port-name* *_yyyymmdd_hhmmss* .trc
- Wenn fortlaufende Ablaufverfolgungen angegeben werden, wird der filter_name mit einer Zahl versehen, die die Position in der Rotationssequenz angibt.
- Die ONTAP-CLI akzeptiert auch die folgenden optionalen -pass-through Argumente:

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
<filter-expression>
```

- Weitere Informationen zu Filterausdrücken finden Sie auf der man-Seite pcap-filter(7).

5. Sehen Sie sich die Traces an, die gerade ausgeführt werden:

```
::*> debug network tcpdump show
Node                     IPspace  Port     Filename
-----------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. Stoppen Sie die Nachverfolgung:

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

7. Kehren Sie zur Ebene der Administratorberechtigungen zurück:

```
::*> set -priv admin
::>
```

8. Greifen Sie auf die Paketverfolgungen zu.

   Ihre Paket-Traces werden in dem Volume gespeichert, das Sie mit dem debug network tcpdump start Befehl angegeben haben, und können über den NFS-Export oder eine SMB-Freigabe aufgerufen werden, die diesem Volume entspricht.

Weitere Informationen zum Erfassen von Paketverfolgungen finden Sie unter So verwenden Sie debuggen network tcpdump in ONTAP 9.10+ in der NetApp Wissensdatenbank.

Dokumentverlauf für Amazon FSx für NetApp ONTAP

- API-Version: 2018-03-01
- Letzte Aktualisierung der Dokumentation: 6. Februar 2024

In der folgenden Tabelle werden wichtige Änderungen am Amazon-FSx NetApp -ONTAP-Benutzerhandbuch beschrieben. Um Benachrichtigungen über Dokumentationsaktualisierungen zu erhalten, können Sie den RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Unterstützung für 12 HA-Paare in Scale-Out-Dateisystemen hinzugefügt	Amazon FSx für NetApp ONTAP hat Unterstützung für 12 HA-Paare in Scale-Out -Dateisystemen hinzugefü gt. Dateisysteme mit 12 HA-Paaren können bis zu 72 GBpss Durchsatzkapazität und 2 400 000 SSD-IOPS über 12 Hochverfügbarkeitspaare (HA) bereitstellen. Weitere Informationen finden Sie unter Hochverfügbarkeitspaare (HA) und Leistung von Amazon FSx für NetApp ONTAP.	4. März 2024
Unterstützung für den Cloud-Schreibmodus hinzugefügt	Amazon FSx für NetApp ONTAP hat Unterstützung für den Cloud-Schreibmodus für -Volumes hinzugefügt. Weitere Informationen finden Sie unter Aktivieren des Cloud-Sch reibmodus auf einem Volume.	6. Februar 2024

Unterstützung für das Sichern von FlexGroup Volumes mit hinzugefügt AWS Backup	Sie können jetzt verwenden AWS Backup , um FlexGroup Volumes auf Ihren FSx-für-ONTAP-Dateisystemen zu sichern und wiederher zustellen. Weitere Informati onen finden Sie unter Verwenden von AWS Backup mit Amazon FSx.	11. Januar 2024
Amazon FSx hat die von verwalteten Richtlinien AmazonF SxFullAccess, AmazonFSxConsoleFu llAccess , AmazonFSx ReadOnlyAccess , AmazonFSxConsoleRe adOnlyAccess und AmazonFSxServiceRolePolicy AWS aktualisiert	Amazon FSx hat die Richtlinien AmazonFSx FullAccess , AmazonFSx ConsoleFullAccess , AmazonFSxReadOnlyA ccess , AmazonFSx ConsoleReadOnlyAccess und AmazonFSxServiceRo lePolicy aktualisiert, um die `ec2:GetSecurityGro upsForVpc` Berechtig ung hinzuzufügen. Weitere Informationen finden Sie unter Amazon-FSx-Updates für -AWS verwaltete Richtlinien.	9. Januar 2024

Amazon FSx hat die von AmazonFSxFullAccess und den von AmazonFSx ConsoleFullAccess 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
Unterstützung für Scale-Out-Metriken hinzugefügt	FSx für ONTAP bietet jetzt Amazon- CloudWatch Metriken für Dateisysteme mit mehreren HA-Paaren. Weitere Informationen finden Sie unter Aufskalieren von Dateisystemmetriken.	26. November 2023
Unterstützung für Scale-Out-Dateisysteme hinzugefügt	Amazon FSx for NetApp ONTAP hat Unterstützung für Scale-Out-Dateisysteme hinzugefügt, die bis zu 36 GBpss Durchsatzkapazität und 1 200 000 SSD-IOPS über sechs Hochverfügbarkeitspaare (HA) bereitstellen können. Weitere Informationen finden Sie unter Hochverfügbarkeitspaare (HA) und Leistung von Amazon FSx für NetApp ONTAP.	26. November 2023

Unterstützung für - FlexGroup Volumes hinzugefügt	Amazon FSx für NetApp ONTAP hat Unterstützung für - FlexGroup Volumes hinzugefügt. Weitere Informationen finden Sie unter Volume-Stile.	26. November 2023
Freigegebene VPC-Unterstützung für Multi-AZ-Dateisysteme hinzugefügt	Teilnehmerkonten können jetzt Multi-AZ-Dateisysteme in einer VPC erstellen, die für sie freigegeben wurde. Besitzerkonten können diese Funktion in der Amazon-FSx-Konsole, CLI und API verwalten. Weitere Informationen finden Sie unter Erstellen von FSx-für-ONTAP-Dateisystemen in gemeinsam genutzten Subnetzen.	26. November 2023
Amazon FSx hat die von AmazonFSxFullAccess und den von AmazonFSx ConsoleFullAccess 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 den von AmazonFSx ConsoleFullAccess 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 Erstellung zusätzlicher ONTAP-Rollen und -Benutzer hinzugefügt	Amazon FSx für NetApp ONTAP unterstützt jetzt das Erstellen zusätzlicher ONTAP-Rollen und -Benutzer, um Benutzerfunktionen und Berechtigungen bei Verwendung der ONTAP-CLI und REST-API zu definieren. Weitere Informationen finden Sie unter Rollen und Benutzer in Amazon FSx für NetApp ONTAP.	6. September 2023
Unterstützung für zusätzliche CloudWatch Metriken und ein erweitertes Überwachungs-Dashboard hinzugefügt	FSx für ONTAP bietet jetzt zusätzliche Leistungsmetriken und ein erweitertes Überwachungs-Dashboard für einen besseren Einblick in die Dateisystemaktivität. Weitere Informationen finden Sie unter Überwachung mit CloudWatch.	17. 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 Amazon-FSx-Updates für -AWS verwaltete Richtlinien.	24. Juli 2023
Unterstützung für die direkte Verwendung von NetApp System Manager hinzugefügt	Sie können Ihre FSx-für-ONTAP-Dateisysteme mit System Manager direkt von verwaltenNetApp BlueXP. Weitere Informationen finden Sie unter Verwenden von NetApp System Manager mit BlueXP.	13. Juli 2023
Unterstützung für die Überwachung von hinzugefügt	Sie können FSx für ONTAP-Dateisystemereignisse mit dem nativen NetAPP ONTAP überwachenEvents Management System (EMS). Sie können -Ereignisse mit der NetApp ONTAP-CLI anzeigen. Weitere Informationen finden Sie unter Überwachen von FSx-für-ONTAP--Ereignissen.	13. Juli 2023

Unterstützung für hinzugefügt SnapLock	FSx für ONTAP unterstützt jetzt -SnapLockVolumes. SnapLock ermöglicht es Ihnen, Ihre Dateien zu schützen, indem sie in einen Write Once Read Many (WORM)-Status übergehen, wodurch Änderungen oder Löschungen für einen bestimmten Aufbewahrungszeitraum verhindert werden. FSx für ONTAP unterstützt die Aufbewahrungsmodi Compliance und Enterprise mit SnapLock. Weitere Informationen finden Sie unter Arbeiten mit SnapLock.	13. Juli 2023
Unterstützung für die IPsec-Verschlüsselung von Daten während der Übertragung hinzugefügt	FSx für ONTAP unterstützt jetzt die Verwendung der IPsec-Verschlüsselung, um Daten während der Übertragung zwischen Dateisystemen und verbundenen Clients zu verschlüsseln. Weitere Informationen finden Sie unter Verschlüsseln von Daten während der Übertragung mit IPsec-Verschlüsselung.	13. Juli 2023

Die maximale Volume-Größe wurde erhöht	FSx für ONTAP hat die maximale Größe eines Volumes von 100 TB auf 300 TB aktualisiert. Weitere Informationen finden Sie unter Aktivieren der automatischen Volume-Größe.	13. 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 AmazonFSxConsoleFullAccess-Richtlinie.	13. Juli 2023
Unterstützung für das Verbinden vorhandener virtueller Speichermaschinen mit einem Active Directory hinzugefügt	Sie können vorhandene virtuelle Speichermaschinen mit einem Active Directory über die AWS Management Console AWS CLI und die API verbinden. Weitere Informationen finden Sie unter Verbinden einer SVM mit einem Active Directory.	13. Juni 2023

Unterstützung für NVMe-Lese-Cache für Single-AZ-Dateisysteme hinzugefügt	NVMe-Lese-Cache wird jetzt für Single-AZ-Dateisysteme unterstützt, die nach dem 28. November 2022 mit mindestens 2 GBps Durchsatzkapazität in den Regionen USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Oregon) und Europa (Irland) erstellt wurden. Weitere Informationen finden Sie unter Auswirkungen des Bereitstellungstyps auf die Leistung.	28. November 2022
Unterstützung für die Verwendung von In-VPC-IP-Adressbereichen zum Erstellen von Multi-AZ-Dateisystemen hinzugefügt	Sie können jetzt Multi-AZ-FSx-für-ONTAP-Dateisysteme erstellen, indem Sie Endpunkte angeben, die innerhalb des IP-Adressbereichs Ihrer VPC liegen. Weitere Informationen finden Sie unter Erstellen von FSx-für-ONTAP-Dateisystemen.	28. November 2022

Unterstützung für die Aktualisierung von VPC-Routing-Tabellen auf Multi-AZ-Dateisystemen hinzugefügt	Sie können jetzt eine neue VPC-Routing-Tabelle einem vorhandenen Multi-AZ-FSx-für-ONTAP-Dateisystem zuordnen (hinzufügen) oder eine vorhandene VPC-Routing-Tabelle von einem vorhandenen Multi-AZ-FSx-für-ONTAP-Dateisystem trennen (entfernen). Weitere Informationen finden Sie unter Aktualisieren eines Dateisystems.	28. November 2022
Unterstützung für die Verschlüsselung von Daten während der Übertragung mit AWS Nitro System hinzugefügt	Daten während der Übertragung werden automatisch verschlüsselt, wenn von unterstützten Amazon EC2-Instances in den Regionen USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Oregon) und Europa (Irland) aus darauf zugegriffen wird. Weitere Informationen finden Sie unter Verschlüsseln von Daten während der Übertragung mit AWS Nitro System .	28. November 2022

Unterstützung für das Erstellen von DP-Volumes hinzugefügt	Sie können jetzt DP-Volumes (Datenschutz) mithilfe der Amazon-FSx-Konsole AWS CLI oder der Amazon-FSx-API erstellen. Sie können DP-Volumes als Ziel einer - NetApp SnapMirror oder SnapVault -Beziehung verwenden, wenn Sie die Daten eines einzelnen Volumes migrieren oder schützen möchten. Weitere Informationen finden Sie unter Volume-Typen .	28. November 2022
Unterstützung für das Kopieren von Volume-Tags in Backups hinzugefügt	Sie können jetzt `CopyTagsToBackups` in der AWS CLI oder Amazon-FSx-API aktivieren, um Tags automatisch von Ihren Volumes in Backups zu kopieren. Weitere Informationen finden Sie unter Kopieren von Tags in Backups.	28. November 2022

Unterstützung für die Auswahl einer Snapshot-Richtlinie hinzugefügt	Sie können jetzt zwischen drei integrierten Snapshot-Richtlinien wählen AWS CLI, wenn Sie ein Volume mithilfe der Amazon-FSx-Konsole oder der Amazon-FSx-API erstellen oder aktualisieren. Sie können auch eine benutzerdefinierte Snapshot-Richtlinie auswählen, die Sie in der ONTAP-CLI oder REST-API erstellt haben. Weitere Informationen finden Sie unter Snapshot-Richtlinien.	28. November 2022
Unterstützung für zusätzliche Kapazitätsoption für den Dateisystemdurchsatz hinzugefügt	FSx für ONTAP unterstützt jetzt 4 096 MBpss Durchsatzkapazität für Dateisysteme, die nach dem 28. November 2022 in der Region USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Oregon) und Europa (Irland) erstellt wurden. Weitere Informationen finden Sie unter Auswirkungen der Durchsatzkapazität auf die Leistung.	28. November 2022

Unterstützung für zusätzliche SSD-IOPS hinzugefügt	FSx für ONTAP unterstützt jetzt 160.000 SSD-IOPS für Dateisysteme, die nach dem 28. November 2022 in der Region USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Oregon) und Europa (Irland) erstellt wurden. Weitere Informationen finden Sie unter Auswirkungen der Durchsatz kapazität auf die Leistung.	28. November 2022
Unterstützung für die Verwendung von FSx für ONTAP als externen Datenspeicher für VMware Cloud in hinzugefügt AWS	Sie können FSx für ONTAP als externen Datenspeicher für AWS Software-Defined Data Centers (SDDCs) von VMware Cloud in verwenden . Diese zusätzliche Unterstüt zung bietet Flexibilität bei der Skalierung des Speichers unabhängig von Rechenres sourcen für AWS Workloads von VMware Cloud in. Weitere Informationen finden Sie unter Verwenden von VMware Cloud mit FSx für ONTAP.	30. August 2022

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 die Menge der verwendeten SSD-Speic herkapazität einen von Ihnen angegebenen Schwellen wert überschreitet. Weitere Informationen finden Sie unter Dynamisches Erhöhen der SSD-Speicherkapazität.	3. Juni 2022
Amazon FSx ist jetzt in integriert AWS Backup	Sie können jetzt verwenden AWS Backup , um Ihre FSx-Dateisysteme zusätzlic h zur Verwendung der nativen Amazon-FSx-Backups zu sichern und wiederherzustellen. Weitere Informationen finden Sie unter Verwenden von AWS Backup mit Amazon FSx.	18. Mai 2022
Unterstützung für ONTAP-Dateisystembereitstellungen in einer einzelnen Availability Zone hinzugefügt	Sie können Single-AZ-FSx-für-ONTAP-Dateisysteme erstellen, die darauf ausgelegt sind, eine hohe Verfügbarkeit und Haltbarkeit innerhalb einer einzigen Availability Zone (AZ) zu gewährleisten. Weitere Informationen finden Sie unter Auswählen der Dateisyst embereitstellung.	13. April 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 die Änderung der Durchsatzkapazität für vorhandene ONTAP-Dateisysteme hinzugefügt	Sie können jetzt die Durchsatzkapazität ändern, die für Ihre vorhandenen ONTAP-Dateisysteme verfügbar ist. Weitere Informationen finden Sie unter Verwalten der Durchsatzkapazität.	30. März 2022
Unterstützung für SSD-Speicherkapazität und bereitgestellte IOPS-Skalierung hinzugefügt	Sie können jetzt die SSD-Speicherkapazität und die bereitgestellten IOPS für bestehende FSx-für-ONTAP-Dateisysteme erhöhen, wenn sich Ihre Speicher- und IOPS-Anforderungen weiterentwickeln. Weitere Informationen finden Sie unter Verwalten von Speicherkapazität und bereitgestellten IOPS.	25 Januar 2022

Unterstützung für Amazon-CloudWatch Metriken hinzugefügt	Sie können Ihr Dateisystem mit Amazon überwachen CloudWatch, das Rohdaten von FSx für ONTAP sammelt und in lesbare Metriken nahezu in Echtzeit verarbeitet. Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch.	19. Januar 2022
Unterstützung für zusätzliche Durchsatzoptionen für das Dateisystem hinzugefügt	FSx für ONTAP unterstützt jetzt Optionen von 128 MB/s und 256 MB/s für den Dateisystemdurchsatz. Weitere Informationen finden Sie unter Auswirkungen der Durchsatzkapazität auf die Leistung.	30. November 2021
Amazon FSx für NetApp ONTAP ist jetzt allgemein verfügbar	FSx für ONTAP ist ein vollständig verwalteter Service, der einen äußerst zuverlässigen, skalierbaren, leistungsfähigen und funktionsreichen Dateispeicher bietet, der auf NetAppdem ONTAP-Dateisystem von basiert. Es bietet die vertrauten Funktionen, Leistung, Funktionen und APIs von NetApp Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig verwalteten AWS Services.	2. September 2021

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.